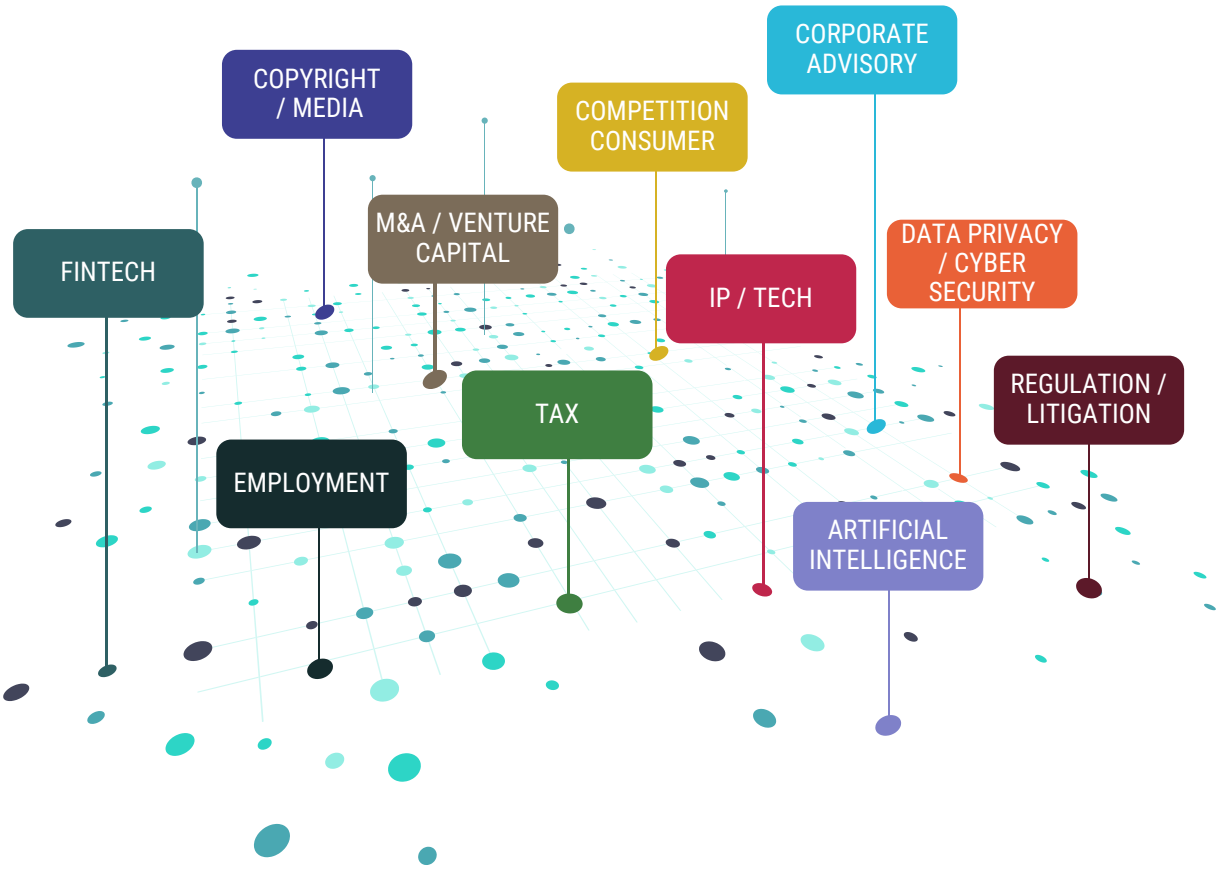
DE BRAUW
BLACKSTONE
WESTBROEK

DECODING EUROPE'S DIGITAL REGULATORY FRAMEWORK: OUR UPDATED DIGITAL GUIDE

JANUARY 2026

OUR DIGITAL EXPERTS



Written in collaboration with members of the Digital Working Group and relevant legal advisers. Special acknowledgments: Chehak Khajuria, Shubhanyu Singh Aujla, Wessel Geursen, Rebecca Aspetti, Kriszta Portik, Violeta Scekic, Julie Roelvink, Jolanda Streijl - van Neck. This guide reflects legal updates and developments up to December 2025. Any changes introduced after this date are not covered. Readers should verify whether subsequent updates may affect the content discussed herein.

CONTENTS


DSA
Competition law
GDPR
Product Liability Directive
Data Act
FSR
Tech & cyber security
DMA
FinTech
EUMR
19aGwB
OMNIBUS
Data Governance Act
Consumer Protection
ESG reporting
Financial markets regulation
UTCCD
Privacy & data
FDI
EU Chips Act
Cyber Resilience Act
Internal market
AI Act
NIS2 Directive
DORA
CRD
EHDS Regulation

1 — DIGITAL ENFORCEMENT IN FULL SWING

1 DIGITAL ENFORCEMENT IN FULL SWING

Over the past few years, the EU's digital strategy has delivered several tangible results, marking a pivotal phase in digital enforcement. Alongside the adoption of a plethora of new regulations and the resulting proliferation of rules, we are also seeing enforcement under ''traditional'' competition, consumer and data protection rules in digital markets. In parallel, initial efforts to comply with the **Digital Markets Act** (DMA) have unfolded by the delivery of the first specification proceedings, non-compliance decisions and fines, alongside the start of several investigations and the first non-compliance decision and fine under the **Digital Services Act** (DSA). "Gatekeepers" and other large digital platforms have expressed concerns that the vast emerging body of EU laws regulating the digital economy may hinder innovation. They point out delays in the rollout of new features and services compared to other regions, which they allege have relegated European consumers to a second-class digital experience.

The fragmentation of digital regulation and enforcement across the EU due to the sheer volume of regulations and newly appointed national enforcers presents a significant challenge. This challenge is compounded by the emerging potential of private enforcement in national courts which can undermine the European Commission's efforts to harmonise, and normalise forum shopping. Private enforcement is also likely to disrupt the "system of regulatory dialogue" envisaged by the DMA, as a gatekeeper could have to defend itself in a national court while discussions with the Commission about compliance are ongoing. Simultaneous investigations into similar breaches of competition, consumer and data protection rules, or of national rules resembling the DMA, further complicate compliance efforts. The risk of spillover and unintended effects in such cases, as well as from other overlapping enforcement areas previously kept separate, persists. Authorities, companies and consumers must therefore navigate a complex regulatory landscape for digital markets. Collaboration among these stakeholders is crucial for achieving predictable compliance, prioritising regulatory burdens, and fostering room for technological innovation.

Another pressing enforcement issue currently being addressed in the EU is the oversight of AI. Besides adopting the AI Act, this includes deliberations on how and to what extent the DMA's scope should be expanded to encompass AI-powered services. The integration of AI features into existing platforms raises the question of whether these improvements should be regarded as separate products or merely as upgrades. This integration may raise competition concerns about issues like tying practices, foreclosure by dominant platforms and algorithmic collusion. Competition authorities in the EU, including the Commission, have already started investigations into AI services offered by platforms. AI partnerships and acqui-hires between tech companies will also likely face increased merger scrutiny, as the Commission works to update its merger guidelines, considering factors such as data, privacy, interoperability and digital ecosystems.

At the same time, we are also seeing some broad global alignment with the EU's digital enforcement efforts, as many jurisdictions have adopted, or are in the process of adopting, similar digital regimes to regulate large online platforms. However, when divergences occur, the EU faces criticism that its fines on tech giants are punitive measures aimed specifically at successful US companies. Despite such challenges, the Commission remains dedicated to ensuring the fair and objective application of digital rules.

1.1 COMPLIANCE LANDSCAPE FOR IN-HOUSE COUNSEL

The DMA and the DSA, two of the EU's most high-profile digital regulations, have now been in effect for some time. Competition teams should be keeping resources set aside to understand the impact of these regulations on their businesses, engage in active regulatory dialogue and ensure ongoing compliance, including with EU and national competition rules.

For their part, consumer protection teams should prepare for the revised **Product Liability Directive**, adopted in November 2024 and set to apply from December 2026, and for the **AI Act**, which entered into force in August 2024 and has obligations that phase into applicability from 2025 to 2027. With the AI Act now in force and the new Product Liability Directive adopted, the EU continues to shape a comprehensive framework for AI governance and liability. On the other hand, as an example of the state of flux in the regulatory landscape, the proposed AI Liability Directive has been abandoned. While privacy compliance teams will have their hands full with the **Data Act** and the **Data Governance Act**, the Commission has finally withdrawn the **ePrivacy Regulation**, deadlocked since 2017. Meanwhile, information security and compliance teams will have to deal with the **Cyber Resilience Act**, the **NIS2 Directive** and the **Cyber Solidarity Act**.

Sector-specific rules must be factored in as well; for instance, financial institutions are subject to the **Digital Operational Resilience Act** (DORA), which has applied since January 2025, while companies in the health sector must consider the effects of the **European Health Data Space** (EHDS) Regulation.

Due to a remarkable overlap of themes across these laws, different teams within an organisation will face an urgent challenge to collaborate rather than focus on single regulatory domains as may have been useful in the past. Compliance based on traditional legal silos may prove less effective. In-house teams must deal with multiple frameworks, as business decisions can trigger obligations across digital, privacy, competition and consumer protection domains, with possible overlaps among competition rules, DMA, DSA, GDPR, AI Act, Data Act and Data Governance Act, to name some.

1.2 DIGITAL OMNIBUS PROPOSAL: A FIRST STEP TOWARDS A STREAMLINED EU DIGITAL RULEBOOK

Following the Draghi report, there has been a call within the EU to simplify legislation, reducing administrative burdens for businesses, public authorities and citizens, and enhancing competitiveness. The Commission proposes, among other things, to adjust and consolidate digital regulations and directives.

A key initiative in this regard is the Digital Omnibus **proposal**, published by the Commission in November 2025, which aims to rationalise the EU's complex digital legislative framework. The proposal seeks to consolidate, simplify and update substantial portions of the existing digital rules, as part of the Commission's broader 2025–2029 simplification agenda. The initiative responds to mounting concerns that the cumulative effect of EU digital rules has generated overlapping obligations, interpretative inconsistencies and disproportionate administrative burdens for organisations dealing with multiple regulatory regimes.

The Digital Omnibus prioritises measures that deliver tangible simplification without compromising the legislation's underlying policy objectives. Central to this approach is the consolidation of the Data Governance Act, the Open Data Directive and the Free Flow of Non-Personal Data Regulation into a single, expanded Data Act, which will serve as the principal legislative instrument governing Europe's data economy. By harmonising definitions, eliminating duplicative provisions and integrating parallel frameworks for public-sector data re-use, the Commission aims to establish more predictable and less costly compliance pathways for businesses and public authorities.

Additionally, the proposal includes targeted amendments to the GDPR and AI Act to reduce compliance friction while preserving the existing level of protection.

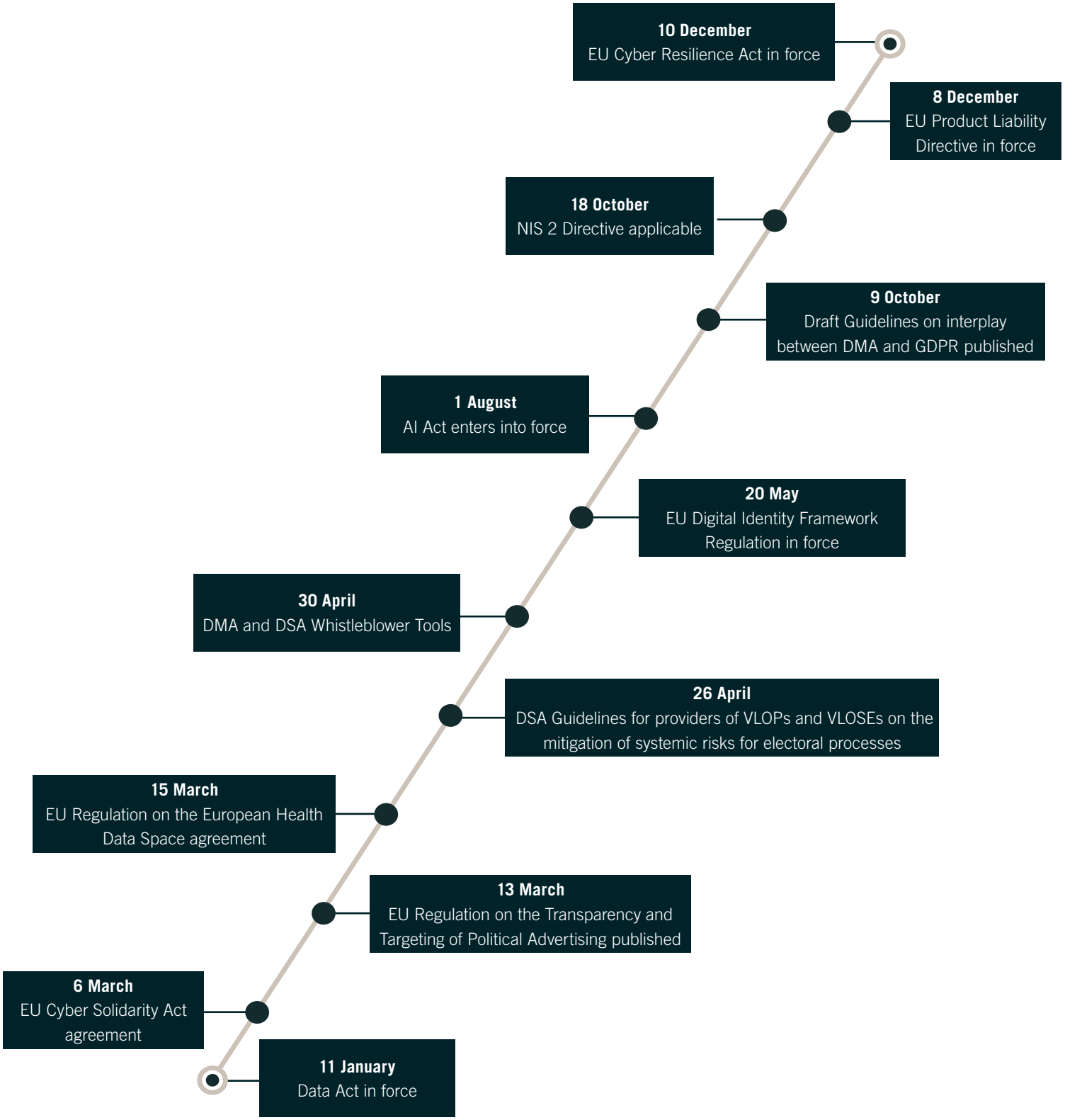
Another significant operational innovation is the introduction of a single EU-level entry point for incident and breach reporting, to be operated by European Union Agency for Cyber Security (ENISA), which will allow organisations to "report once" to satisfy obligations across GDPR, NIS2, DORA, Electronic Identification, Authentication and Trust Services (eIDAS) regulation and Critical Entities Resilience (CER) Directive, while maintaining the existing allocation of regulatory competences. The Commission anticipates that this mechanism will ease the reporting burden for entities operating across multiple sectors, reduce duplicative filings and address under-reporting in certain areas.

In parallel, the Digital Omnibus proposal aims to repeal rules – most notably the **Platform-to-Business (P2B) Regulation** – that have been effectively superseded by more recent legislation such as the DMA and DSA. The Commission intends to repeal the P2B Regulation, except for those provisions that contain definitions used in other EU legislation.

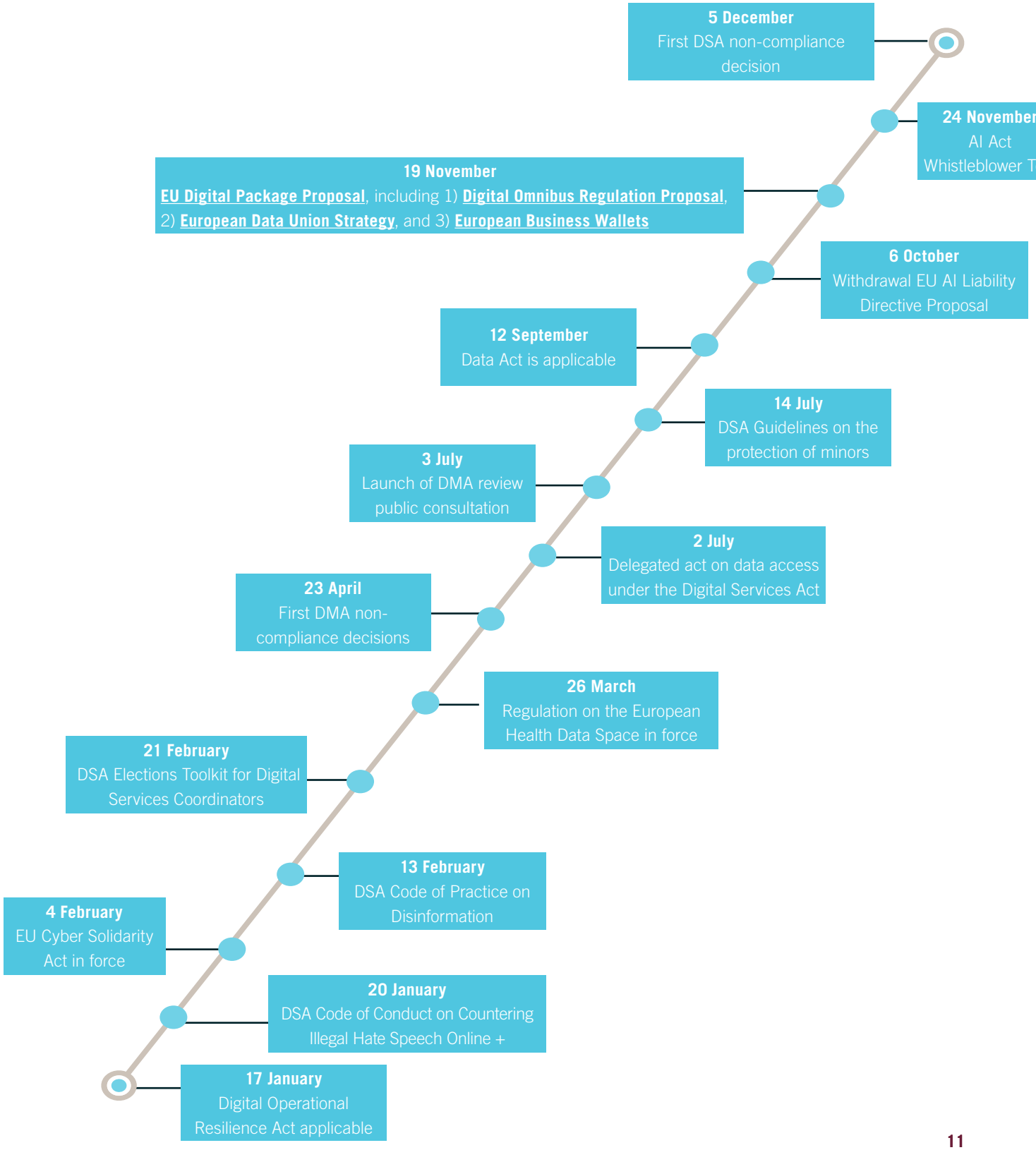
Taken together, these reforms constitute the first phase of the Commission's plan to "stress-test" the digital rules. A broader Digital Fitness Check will follow, focusing on the cumulative impact of the digital rulebook on competitiveness and on further opportunities for alignment across definitions, governance structures and supervisory frameworks. As part of the Digital Fitness Check, the European Commission is also expected to introduce a proposal for a Digital Fairness Regulation (DFR) by the end of this year. The DFR will be part of European Consumer law and will ban dark patterns, safeguard vulnerable users, regulate addictive design (such as rewards and gamification) and increase transparency about pricing.

Organisations should therefore anticipate continued legislative activity and prepare for a period in which simplification and consolidation become recurring features of EU digital regulation.

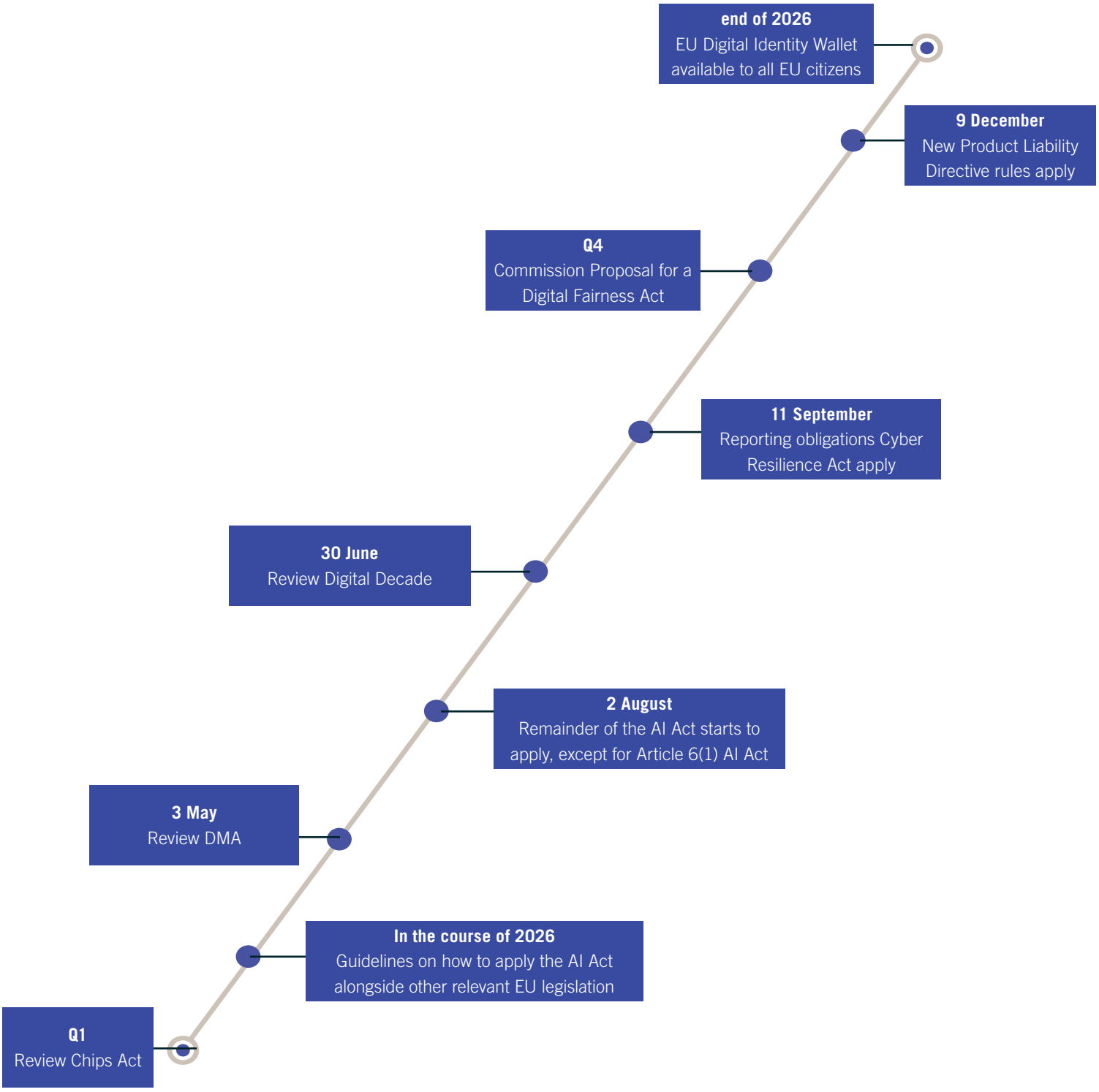
2024


10 December
EU Cyber Resilience Act in force
8 December
EU Product Liability Directive in force
18 October
NIS 2 Directive applicable
9 October
Draft Guidelines on interplay between DMA and GDPR published
1 August
AI Act enters into force
20 May
EU Digital Identity Framework Regulation in force
30 April
DMA and DSA Whistleblower Tools
26 April
DSA Guidelines for providers of VLOPs and VLOSEs on the mitigation of systemic risks for electoral processes
15 March
EU Regulation on the European Health Data Space agreement
13 March
EU Regulation on the Transparency and Targeting of Political Advertising published
6 March
EU Cyber Solidarity Act agreement
11 January
Data Act in force

2025


5 December
First DSA non-compliance decision
24 November
AI Act
Whistleblower Tool
19 November
EU Digital Package Proposal, including 1) Digital Omnibus Regulation Proposal, 2) European Data Union Strategy, and 3) European Business Wallets
6 October
Withdrawal EU AI Liability Directive Proposal
12 September
Data Act is applicable
14 July
DSA Guidelines on the protection of minors
3 July
Launch of DMA review public consultation
2 July
Delegated act on data access under the Digital Services Act
23 April
First DMA non-compliance decisions
26 March
Regulation on the European Health Data Space in force
21 February
DSA Elections Toolkit for Digital Services Coordinators
13 February
DSA Code of Practice on Disinformation
4 February
EU Cyber Solidarity Act in force
20 January
DSA Code of Conduct on Countering Illegal Hate Speech Online +
17 January
Digital Operational Resilience Act applicable

2026


end of 2026
EU Digital Identity Wallet available to all EU citizens
9 December
New Product Liability Directive rules apply
Q4
Commission Proposal for a Digital Fairness Act
11 September
Reporting obligations Cyber Resilience Act apply
30 June
Review Digital Decade
2 August
Remainder of the AI Act starts to apply, except for Article 6(1) AI Act
3 May
Review DMA
In the course of 2026
Guidelines on how to apply the AI Act alongside other relevant EU legislation
Q1
Review Chips Act

2 — FAIR AND CONTESTABLE DIGITAL MARKETS

2 FAIR AND CONTESTABLE DIGITAL MARKETS

2.1 DIGITAL MARKETS ACT

One of the more publicised initiatives in recent years (and potentially the most impactful in practice) is the Commission's Digital Services Package. The package consists of two landmark pieces of legislation: the DMA and the DSA. Together, these measures significantly reshape the regulatory framework for digital platforms operating in the EU.

The DMA **applies** to large online businesses that have a significant impact on the EU internal market, control a "core platform service" and hold an entrenched and durable market position. Typically, such businesses control important ecosystems in the digital economy. These businesses are aptly called "gatekeepers" (see our previous **article**). The Commission has also taken several steps to enforce the DMA against several gatekeepers. These efforts have gradually intensified. The Commission started by organising workshops in which the gatekeepers presented their plans for complying with the DMA obligations. It then also started regulatory dialogues called specification proceedings. Most recently, the Commission issued its first fines for non-compliance with the DMA and organised another round of workshops.

DIGITAL MARKETS ACT

Status	Final
In force	1 November 2022
Applicable	2 May 2023
Objective	- Make digital markets fair and contestable - Designate certain core platform service providers as gatekeeper platforms - Subject gatekeepers to new rules

To fall within the ambit of the DMA, the gatekeeper must provide a core platform service such as intermediation services, search, social networks, video-sharing, operating systems, or online advertising. In addition:

- the gatekeeper must have a significant impact on the internal market or, in quantitative terms, an annual EU-wide turnover of at least EUR 7.5 billion in the last three financial years or a market capitalisation of at least EUR 75 billion in the last financial year, and provide the same core platform service in at least three Member States;
- the core platform service must be an important gateway for businesses to reach end users (45 million monthly active end users and 10,000 annual active business users); and
- the gatekeeper must enjoy an entrenched and durable position in its operations (user thresholds met in each of the last three consecutive years before designation).

The DMA, which includes enforcement mechanisms reinforced with the possibility of imposing significant fines, introduces rules for gatekeepers, including prohibitions on:

- using wide or narrow parity clauses, as predicted by the *Commission's* revised rules on verticals (see our **previous article**)
- combining personal data from multiple services without GDPR-compliant consent, as foreshadowed in **proceedings** against Facebook and Google in Germany
- bundling services or prohibiting integration of third-party competing services, a requirement the Dutch competition authority **imposed** on Apple in relation to its prohibition on alternative payment systems for in-app purchases
- restricting advertiser and publisher access to detailed ad pricing information, a fallout from the Commission's abuse-of-dominance ad tech investigation into **Google**

- self-preferencing, as exemplified in the **Google Shopping decision**
- using non-public data provided by business users when competing with those same business users, as was the case in the Commission's now-settled **Amazon Marketplace** investigation.

In a nutshell, the DMA imposes two types of obligation on gatekeepers. Article 5 of the DMA contains obligations that are directly applicable or self-executing, and these are also referred to as "blacklist" obligations. Articles 6 and 7 contain obligations that may require further specification depending on the context, also referred to as "grey list" obligations. The DMA provides for non-compliance investigations and decisions that may result in fines for gatekeepers that fail to comply with its obligations. This is similar to infringement decisions under "regular" EU competition law. Additionally, the enforcement of grey-listed obligations is also subject to a new enforcement tool introduced by the DMA: the specification proceedings of Article 8(2) DMA. Finally, in response to concerns about killer acquisitions of nascent companies by entrenched players, gatekeepers are required to inform the Commission of any intended merger that involves a core platform service, or a service in the digital sector, or a service that enables data collection. This obligation notably extends to mergers that are not notifiable at the EU or Member State level or so-called ''below-threshold mergers''. By sharing information about such below-threshold mergers with the competition authorities of Member States, the Commission expected that those authorities would refer the mergers back under Article 22 EUMR. However, this is no longer possible following the CJEU's Illumina/GRAIL **judgement**, which clarified that a Member State's competition authority cannot refer a below-threshold merger to the Commission unless it has jurisdiction to review it under national law.

2.2 DESIGNATIONS UNDER THE DMA

The first decisions on designating gatekeepers under the DMA were adopted on 6 September 2023, leaving the designated gatekeepers a little over six months to develop and implement compliance programmes. As a result, Alphabet, Amazon, Apple, ByteDance, Meta and Microsoft have had to comply with the DMA's obligations in respect of their core platform services for which the Commission has designated them as gatekeepers. The Commission **added** Booking to the list of gatekeepers on 13 May 2024, giving it until 14 November 2024 to **comply** with the DMA. However, not all of these companies agree that their services should be counted among the 23 core platform services **identified** by the Commission. Apple, Meta and ByteDance have all taken issue with the Commission's findings, signalling an early hiccup in the Commission's efforts to regulate the digital landscape.

More recently, on 27 November 2025, the Commission received **notifications** from Apple indicating that its core platform services Apple Ads and Apple Maps meet the DMA thresholds, potentially triggering gatekeeper obligations in the near future.

2.3 APPEALS AND RULINGS ON DMA DESIGNATIONS

Meta was the first to **challenge** the Commission before the General Court, disputing that its Messenger and Marketplace services fall under the scope of the DMA. Meta argued that Messenger is simply a part of its social network service, Facebook, that allows Facebook platform users to chat with each other. Facebook is already designated as a core platform service – a designation Meta accepts. Regarding Marketplace, the Commission **revealed** on 23 April 2025 that it should no longer be designated under the DMA. After reviewing Meta's arguments and considering the company's additional enforcement and ongoing monitoring efforts to address the business-to-consumer use of Marketplace, the Commission determined that Marketplace had fewer than 10,000 business users in 2024. Consequently, Meta no longer meets the necessary criteria to presume that Marketplace serves as a significant gateway for business users to connect with end users. However, the Commission has **fined** Meta under competition law for tying Marketplace to Facebook.

Apple has **appealed** its designation as a gatekeeper by the Commission at the General Court in relation to its operating system iOS, the Commission's decision to designate the App Store as a single core platform service, and the Commission's decision to classify iMessage as a number-independent interpersonal communications service. In addition, Apple had **lodged** a separate appeal contesting the decision to open a market investigation into iMessage. Following Apple's rebuttal, the Commission ultimately **decided** that Apple should not be designated as a gatekeeper for iMessage.

Finally, ByteDance contests that its gatekeeper designation in connection with TikTok. It had **appealed** to the General Court, arguing the Commission applied the wrong legal standard in assessing its rebuttal of DMA presumptions regarding designations. On 17 July 2024, the General Court **issued** the first substantive DMA judgment, upholding ByteDance's designation as a gatekeeper. It found insufficient evidence to rebut the presumption of significant impact, confirmed TikTok's role as an important gateway for business users, and held that ByteDance has an entrenched, durable position. ByteDance has since **appealed** against this judgment.

2.4 MARKET INVESTIGATIONS UNDER THE DMA

Following an in-depth market investigation, the Commission **announced** on 16 October 2024 that X does not qualify as a gatekeeper in relation to its online social networking service. This decision is based on the finding that its online social networking service does not serve as a significant gateway for business users to connect with end users, even though X meets the quantitative thresholds set out in the DMA.

Following another market investigation, the Commission **designated** Apple as a gatekeeper with respect to its core platform service iPadOS. The Commission indicated that Apple demonstrates gatekeeper characteristics with respect to iPadOS. This assessment is based on the high number of business users and the lock-in effect experienced with iPadOS by both end users and business users.

More recently, the Commission has been collaborating with the Dutch Authority for Consumers and Markets (ACM) on three **market investigations** into cloud computing services under the DMA. Two of these will assess if Amazon and Microsoft should be designated as gatekeepers for their cloud computing services, evaluating whether these act as key gateways between businesses and consumers despite not meeting the DMA's thresholds. The third investigation will examine whether the DMA can effectively address practices that may limit competitiveness and fairness in the EU cloud computing sector.

2.5 FIRST NON-COMPLIANCE INVESTIGATIONS, PRELIMINARY ASSESSMENTS AND DECISIONS UNDER THE DMA

The Commission **opened** the first DMA non-compliance investigations in March 2024 targeting Alphabet, Apple and Meta. The Commission issued the first DMA non-compliance decisions in April 2025 against Apple and Meta and since the decisions, both companies have appealed.

Google

The Commission's non-compliance investigations into Google's parent, Alphabet, concerns anti-steering rules on Google Play and self-preferencing on Google Search. On 19 March 2025, the Commission **issued** two sets of preliminary findings against Alphabet regarding Google Search and Google Play. Regarding self-preferencing in Google Search, the Commission takes the view that Alphabet's self-preferencing of its own services above those of

third parties constitutes a DMA breach. In relation to the steering rules for Google Play, the Commission's preliminary findings suggest that Alphabet is failing to meet its steering obligations under the DMA. The Commission contends that Alphabet is imposing technical restrictions that impede certain steering practices, thereby breaching the DMA. On 13th November 2025, the Commission opened another **investigation** into Google's potential DMA breach involving the demotion of media publishers' content in search results. The Commission will assess whether these demotions restrict publishers' ability to do business, innovate or work with third-party content providers.

Apple

The Commission investigated Apple for anti-steering provisions in the AppStore and for the Safari choice screen. On 24 June 2024, the Commission **notified** Apple of its preliminary assessment that its AppStore rules violate the DMA. According to the Commission, these rules restrict app developers from freely steering consumers to alternative channels for offers and content. In April 2025, the Commission adopted a non-compliance decision against Apple. The Commission **found** that Apple violated its steering obligation as outlined in the DMA and this resulted in fine of EUR 500 million for Apple. The Commission determined that Apple's numerous restrictions prevent app developers from fully using the benefits of alternative distribution channels outside the App Store. Because of this, consumers are unable to take advantage of alternative, more affordable offers, as Apple blocks app developers from directly informing them about these options. The Commission has ordered Apple to eliminate the technical and commercial restrictions on steering and to cease any non-compliant behaviour moving forward.

Following constructive dialogue with Apple, the Commission **announced** on 23 April 2025 that it had closed its other investigation into Apple's user choice obligations. Consequently, Apple updated its browser choice screen and simplified the process for users to modify default settings for various functions, such as calling and messaging. Additionally, Apple enabled users to uninstall several preinstalled Apple apps, including Safari.

The Commission also initiated another non-compliance investigation into Apple's new contractual terms for developers, which are required to access certain new features enabled by the DMA. These features include the provision of alternative app stores and the ability to offer apps through alternative distribution channels. The Commission has **communicated** its preliminary views on Apple's contract terms. According to the DMA, Apple should permit the distribution of apps on its iOS operating system through methods other than the Apple App Store. However, developers interested in using alternative app distribution channels on iOS are discouraged from doing so because they must agree to business terms that include a new fee, Apple's Core Technology Fee.

Meta

The Commission investigated Meta's "pay or consent" model. On 1 July 2024, the Commission **sent** Meta its preliminary findings that its "pay or consent" model does not comply with the DMA. In its subsequent non-compliance decision under the DMA, the Commission **found** that Meta failed to comply with the DMA requirement to offer consumers the choice of an equivalent service that utilises less of their personal data. This has resulted in a fine of EUR 200 million for Meta. Regarding Meta's "pay or consent" model, the Commission stated that Meta was failing to provide users with the option to choose a service that uses less of their personal data while remaining comparable to the "personalised ads" service. This decision, however, considers only the period from March to November 2024. As of November 2024, Meta has launched an alternative version of its free personalised ads model, offering a new option that uses less personal data for displaying advertisements.

2.6 FIRST SPECIFICATION PROCEEDINGS UNDER THE DMA

Specification proceedings provide for formal regulatory dialogue between a designated gatekeeper and the Commission. During this dialogue, discussions take place on how the gatekeeper can comply with the DMA's grey-listed obligations and on the concrete steps needed to meet those obligations. The Commission must conclude these proceedings within six months. It does so by adopting a decision that imposes binding measures on the gatekeeper.

On 19 September 2024, the Commission **announced** that it had initiated two specification proceedings to help Apple fulfil its interoperability requirements. According to the DMA, Apple is required to offer free and efficient interoperability to third-party developers and businesses with hardware and software features managed by Apple's iOS and iPadOS operating systems, which are designated under the DMA.

The first proceedings concentrate on various iOS connectivity features and functions, primarily used for and by connected devices. The second proceedings examine the procedure Apple has established to handle interoperability requests from developers and third parties for iOS and iPadOS.

Subsequently, on 18 December 2024, the Commission **shared** its initial findings with Apple and posed measures, inviting third-party feedback.

On 19 March 2025, the Commission **issued** two decisions specifying the measures Apple must take to meet specific aspects of its interoperability requirements. The first set of measures targets nine iOS connectivity features mainly used by connected devices such as smartwatches, headphones and TVs. These measures will enhance access for device manufacturers and app developers to iPhone features, enabling better interaction, faster data transfer and simpler device setup. The second set of measures enhances the transparency and efficiency of Apple's process for developers seeking interoperability with iPhone and iPad features. It offers better access to technical documentation, timely updates and a clearer timeline for reviewing interoperability requests. On 2 June 2025, Apple requested the Commission to waive or modify the measures for some of the features included in the specification decision. In August 2025, the Commission **rejected** Apple's waiver requests for five iOS interoperability features, stating the company had failed to show exceptional circumstances under the DMA.

2.7 DMA ANNUAL REPORT

On 25 April 2025, the Commission **published** its second DMA annual report. The report outlines the actions taken from January to December 2024 to ensure the effective enforcement of the DMA. These actions include implementing additional designation decisions, engaging in regulatory dialogues with gatekeepers and third parties to enhance compliance strategies, and initiating specification proceedings and investigations into non-compliance by gatekeepers.

Furthermore, the report provides a summary of the information submitted by gatekeepers about their planned mergers and their audited accounts of consumer profiling methods. It also details the collaboration between the Commission and national authorities to ensure consistent, effective and complementary enforcement.

2.8 IMPACT ON BUSINESSES

The appeals against the Commission's designation and non-compliance decisions highlight the complexities of applying the DMA. For digital players, the first non-compliance decisions mark a turning point, signalling that non-compliance with the DMA carries considerable risks, not only in the form of potential fines but also through sustained regulatory scrutiny and operational uncertainty.

Many of the prohibitions introduced by the DMA are mere codifications of requirements established piecemeal by European and national enforcement actions. However, when designing the DMA, the Commission seems to have taken on board some but not all lessons from previous enforcement cases under competition law. To further complicate matters, the DMA's interaction with comparable national rules (such as **Section 19a** of the German Competition Act) may lead to tension and overlapping enforcement. Despite having similar objectives, parallel regulatory regimes may have distinct requirements which can cause a risk of fragmentation and lack of coherence in the EU. Moreover, the DMA risks creating an incoherent interpretation of consent by competition and data protection authorities and complicating the already intricate relationship between competition and data-protection enforcement. To overcome this issue, the Commission and national data protection authority's (DPAs), united in the European Data Protection Board (EDPB), have consulted draft **guidelines** on the interplay between DMA and GDPR.

The Commission also **introduced** a DMA whistleblower tool on 30 April 2024, similar to the one available for antitrust enforcement and the DSA. This tool allows individuals to confidentially and privately submit information on potential non-compliance by gatekeepers with their obligations under the DMA. For businesses, this tool can lead to increased accountability and pressure to adhere to fair practices, fostering a more competitive and equitable market environment.

On 3 July 2025, the Commission **launched** its first public consultation to review the DMA, seeking feedback on its impact, effectiveness and ability to respond to new challenges such as the emergence of AI-powered services. This was followed on 27 August by the publication of a **call for evidence** and an **AI questionnaire**. The Commission is soliciting feedback on whether AI-powered services can be addressed within the DMA's existing framework or require distinct regulatory treatment.

In recent DMA workshops organised by the Commission to reflect on the first year of DMA enforcement, gatekeepers expressed their concerns about the real-world consequences of the DMA. Gatekeepers claimed that the DMA inadvertently curbs innovation by deterring investment in novel features and services due to uncertainty in its application. The DMA was said to prevent the latest technological advancements from reaching European consumers. Tech giants called for predictability around what is required of gatekeepers, prioritisation of the most important matters covered by the DMA rules, and room to promote the courage to experiment and test ideas in the market. Gatekeepers have also advocated for the technology-neutral character of the DMA, which defines its scope by reference to specific services rather than the technology used. They suggested that AI solutions are integrated into the core platform services and they do not constitute separate services or products under the DMA.

2.9 PRIVATE ENFORCEMENT IN DIGITAL MARKETS

The opportunity and tendency to use private enforcement in the context of digital markets is growing, and with external funding options available, this trend will rise further. The DMA for one, paves the way for increased private enforcement. Both end users and business users can bring proceedings against gatekeepers that do not comply with their DMA obligations. Arguably, most, if not all, provisions of the DMA are sufficiently precise and unconditional to be relied on before national courts. Article 39 DMA establishes the role of national courts in

enforcing the regulation and sets out mechanisms for cooperation with the Commission. Claimants are expected to use private enforcement to primarily achieve two outcomes: behavioural change (by way of an injunction) and recovery of losses (damages). In addition, both standalone and follow-on claims are possible, as well as claims that fall somewhere in between.

Follow-on claims can rely on the primacy of the Commission's non-compliance decisions and their binding effect on national courts. Standalone cases are expected when the Commission does not target particular conduct, for various reasons, such as choosing not to prioritise certain cases due to resource constraints or delaying enforcement for geopolitical considerations (US tariff threats being a case in point). It is also conceivable that the Commission is engaging in regulatory dialogue with a gatekeeper to ensure compliance rather than pursuing an enforcement action, e.g., in the context of DMA specification proceedings. Third parties may bring claims if they feel the Commission did not properly consult them or that the gatekeepers are ignoring parts of the DMA requirements.

Standalone claims are also expected when the Commission, after its investigation, decides not to adopt a non-compliance decision and closes the proceedings by way of a DMA **closure decision**. The Commission can close an investigation when the information and evidence available do not support a finding of non-compliance, or when a constructive dialogue with the gatekeeper during the investigation results in the gatekeeper taking measures to become DMA-compliant (which are subject to the Commission's subsequent monitoring). However, a Commission closure decision does not mean the Commission has deemed the conduct to be DMA-compliant, and standalone claims are therefore still possible.

Standalone claims may even morph into follow-on actions, for instance when they prompt the Commission to launch investigations that result in findings of DMA non-compliance. Cross-fertilisation of claims is also possible. This would be the case if, for instance, standalone or follow-on claims based on the DMA are clubbed with those based on other laws (for example, DSA, competition law, data protection, and privacy and consumer protection).

When private enforcement eventually gains further momentum across the EU, there will also be accompanying risks. National courts will evaluate cases individually, which may lead to inconsistent rulings across Member States, while fragmentation could normalise forum shopping across the EU more generally. Different national rulings may include overlapping or conflicting remedies and measures as required by the various courts. The fragmentation of remedial outcomes could undermine the effectiveness of the entire system. In the context of the DMA, private enforcement is expected to disrupt the "system of regulatory dialogue" envisaged by the regulation. A gatekeeper would have to defend itself in a national court while speaking to the Commission about its compliance. There is also the possibility that the national court may go further than the measures "specified" by the Commission.

Germany has already amended its **Act against Restraints of Competition** to extend its national private enforcement apparatus for competition law to the DMA, and this has quickly been tested in practice. A German consumer association **challenged** Meta's plan to use Facebook and Instagram data for AI training under the DMA's data processing-related obligations. The Higher Regional Court of Cologne dismissed the request. More recently, Germany's Regional Court of Mainz ruled in **1&1 Mail & Media vs. Google** that Google must stop giving Gmail preferential treatment during Android account setup, finding that doing so breached the DMA's anti-tying rules. The court ordered Google to redesign the registration process to give users a real choice, relying on an injunction rather than damages. This case marks an early example of private enforcement under the DMA, demonstrating that national courts can act independently of the Commission and potentially influence platform practices across the EU.

The Netherlands, for its part, has established itself as a preferred jurisdiction in Europe for handling both follow-on and standalone damages claims. Different legal remedies are available in the Netherlands: injunctive relief, penalty payments as (additional) means of pressure, and damages claims. Claims, of course, can be both via individual & collective actions. The practical and efficient procedures adopted by Dutch courts, the relatively low costs associated with filing claims, and the availability of strong collective action systems such as the WCAM and WAMCA have all contributed to its claimant-friendly reputation. Dutch courts can therefore expect to see more private enforcement in the near future. On 2 October 2025, the Amsterdam District Court **issued** the first DSA private enforcement judgment, granting preliminary relief to Bits of Freedom against Meta concerning Facebook and Instagram recommender systems.

There has also been a significant CJEU **ruling** with ramifications for the whole of the EU, in a case referred by the Amsterdam District Court concerning jurisdictional issues about private enforcement and online platforms. The CJEU ruled that Dutch courts have jurisdiction to hear a representative action relating to Apple's alleged anticompetitive App Store conduct. The CJEU found that, as Apple designed the App Store NL for the Netherlands market, the alleged damage arising from app purchases made in that virtual space may be regarded as occurring in the Netherlands. As a result, Dutch courts have jurisdiction to hear claims relating to purchases made via the App Store NL.

3 — REGULATING DIGITAL SERVICES

3 REGULATING DIGITAL SERVICES

3.1 DIGITAL SERVICES ACT

Replacing parts of the 25-year-old **e-Commerce directive**, the DSA acts as the other half of the Commission's efforts to create a uniform set of rules to govern digital markets across Europe.

DIGITAL SERVICE ACT

Status	Final
In force	16 November 2022
Applicable	17 February 2024
Objective	- Establish rules for content moderation - Create transparent and safe user experiences on social media, app stores, digital marketplaces, online travel and accommodation platforms, etc

Like the DMA, the DSA targets online intermediaries and platforms, such as marketplaces, social networks, content-sharing platforms, app stores, and online travel and accommodation platforms. The DSA puts more emphasis on protecting consumers' fundamental rights, including the right to free speech and the right to privacy, as well as controlling the spread of disinformation, misinformation and abuse online. The DSA requires platforms to set up measures to counter the spread of illegal goods, services and content online, as well as mechanisms that allow users to flag such content. Acknowledging the role that platforms play in moderating online content, the DSA requires that all platforms offer: (i) choice about the content displayed in feeds; (ii) the data processed in order to display personalised feeds; (iii) transparency in terms of content moderation policies; and (iv) options for appealing decisions taken under such policies. In addition, advertising that targets children is prohibited, as is targeted advertisement relying on profiling that uses special categories of personal data, such as ethnicity, political views or sexual orientation. Beyond advertising, providers of online platforms accessible to minors must implement appropriate and proportional measures to ensure high level or privacy, safety and security for those minors on their services.

More stringent rules apply to very large platforms (VLOPs) and very large search engines (VLOSEs), defined as servicing over 45 million average monthly active recipients in the EU. Due to their access to large groups of the population, VLOPs and VLOSEs are required to implement measures to prevent systemic risks emerging from their services, in particular negative effects on the exercise of fundamental rights, electoral processes, public security, public health, or physical and mental well-being. The measures for mitigating such risks may include adapting content-moderation practices, adapting algorithmic and recommender systems, and implementing age verification and parental control tools

In terms of practical guidance, the Commission has published a range of guidelines over the last few years, including the '**Guidance on the requirement to publish user numbers**' (January 2023), '**Guidelines under the DSA for the mitigation of systemic risks online for elections**' (March 2024), '**Guidelines on protection of minors online under the Digital Services Act**' (July 2025), as well as plans to publish draft guidelines on trusted flaggers.

To foster collaboration among stakeholders, and to help put in place commitments contributing to the implementation of the DSA, the Commission welcomes the creation of voluntary codes of conduct. So far, two codes have been endorsed and integrated, namely the **Code of Conduct on Countering Illegal Hate Speech Online** (January 2025) and **Code of Conduct on Disinformation** (February 2025). The Commission has also encouraged the creation of **two other codes of conduct** on online advertising and accessibility.

Several other complementary mechanisms have been introduced, including the best-practice election **toolkit** on the DSA, which provides practical details on how the DSA Election Guidelines can be applied during electoral processes. In July 2025, the Commission also **published** a delegated act outlining rules granting access to data for qualified researchers under the DSA.

3.2 DESIGNATIONS UNDER THE DSA

The initial designation round in April 2023 identified 17 VLOPs, including: retail and services marketplaces Zalando, Alibaba AliExpress, Booking.com and Amazon; social media platforms Facebook, Instagram, LinkedIn, Pinterest, Snapchat, TikTok and Twitter; several Google services like Play, Maps, Shopping and YouTube; as well as the free online encyclopaedia Wikipedia. It also designated two VLOSEs: Microsoft's Bing and Google Search. In December 2023, additional VLOPs were designated: Pornhub and XVideos. In 2024, the Commission further designated Shein, Temu and XNXX as VLOPs. As of November 2025, the Commission has designated a total of 24 VLOPs and VLOSEs.

The designated VLOPs and VLOSEs were required to publish transparency reports and systemic risk assessment reports and undergo audits on their services soon after designation. VLOPs such as **Zalando** and **Amazon** immediately contested their designation, arguing that the methods used to calculate active users and evaluate systemic risk were incorrect. Both appeals were unsuccessful, with the General Court issuing the rulings in mid and late 2025. Zalando has since appealed against this ruling to the **CJEU** and is currently awaiting the outcome.

Meta and **TikTok** challenged the methodology used by the Commission to calculate supervisory fees imposed after their designation. They argued that the Commission had incorrectly calculated the number of active recipients and applied a faulty fee methodology. In September 2025, the challenges had a successful outcome, with the General Court annulling the Commission's decision and finding that the methodology should have been adopted via a delegated act rather than an implementing decision. Nonetheless, the methodology for calculating the average monthly active recipients was not in itself found to be in breach of the DSA. In November 2025, the Commission appealed the decisions in the cases against **TikTok** and **Meta**, so the annulment decision is not yet final.

3.3 REQUEST FOR INFORMATION AND FORMAL INVESTIGATIONS UNDER THE DSA

When it comes to enforcement under the DSA, the Commission and national Digital Services Coordinators have been actively overseeing compliance with the regulation, particularly for VLOPs and VLOSEs. Enforcement measures taken include issuing a number of Requests for Information (RFIs); initiating formal proceedings, issuing preliminary findings and retention orders; and ultimately adopting decisions accepting binding commitments.

More than half of the VLOPs have already received RFIs, including AliExpress, Amazon, Apple, Booking.com, LinkedIn, Meta (Facebook/Instagram), Microsoft, Pinterest, Pornhub, Shein, Snapchat, Temu, TikTok, X, XVideos, YouTube and Zalando. In making these requests, the Commission aims to assess whether these platforms are DSA-compliant.

In late 2023, the first non-compliance proceedings under the DSA started against **platform X**, focusing on the platform's compliance with the DSA's requirements to combat illegal content distribution and information manipulation. In July 2024, the Commission sent its **preliminary findings** to X alleging that it was breaching the DSA in areas linked to dark patterns, advertising transparency and data access for researchers. In December 2025, the Commission **fined** X EUR 120 million for breaching its transparency obligations under the DSA. The breaches are related to deceptive design of the "blue checkmark", lack of transparency of its advertising repository, and failure to provide access to public data for researchers, marking the first non-compliance fine under the DSA.

Other VLOPs have received similar notifications of potential DSA breaches, with an additional six preliminary findings since November 2025, including the most recent Meta and TikTok findings, published in October 2025, regarding researcher data access, notice and action mechanisms, and content moderation breaches.

Several other formal proceedings have been initiated on topics ranging from risk management, use of dark patterns, insufficient notice and action mechanisms, to content moderation and protection of minors.

In 2025, the Commission also issued retention orders to **X** requiring the platform to maintain records on changes to recommendation systems; and **TikTok** was ordered to retain internal material related to its algorithmic design, manipulation risks and monetisation of political content in the context of elections.

In June 2025, alongside AliExpress's preliminary findings of DSA breaches, the Commission accepted and **made binding** a series of commitments proposed by the platform. These commitments related to platforms verification; monitoring and detection systems aimed at mitigating certain risks related to hidden links; AliExpress's affiliate programme; and products potentially affecting health and minors, among other topics.

An analysis of the current DSA enforcement regime reveals that Article 25, which addresses Dark Patterns, has the highest conversion rate from RFIs to formal investigations, standing at 75%. This is closely followed by Article 16, concerning Notice and Action, and Articles 34/35, which focus on Protecting Minors, both with a conversion rate of 66%. In terms of scrutiny, Article 40, related to Researcher Data Access, is the most scrutinised, having received 19 RFIs. This is followed by Articles 28/34/35, which pertain to Minors Protection, with 13 RFIs. It is important to note that the DSA enforcement regime is still in its early stages, with most proceedings ongoing as of the date of this document.

The **first table** provides a comprehensive overview of the current enforcement mechanisms under the DSA, organised by specific obligations and articles; and the **second table** illustrates the timeline for the Commission's progression from an RFI to a formal investigation.

	Total RFIs*	Investigations Opened	Preliminary Findings	Binding Commitments**	RFI -> Investigation Rate	Active Cases
Art 16 (Notice and Action)	6	4	2	1	66%	4
Art 20 (Complaints)	7	3	2	1	43%	3
Art 25 (Dark Patterns)	4	3	3	0	75%	3
Art 26 (Profiling)	1	0	0	0	0%	0
Art 27/38 (Recommenders)	12	4	1	1	33%	4
Art 28/34/35 (Minors)	13	8	0	1	61%	8
Art 30 (Traceability)	6	1	0	1	16%	1
Art 31 (Compliance Design	4	0	0	0	0%	0
Art 32 (Consumer info)	2	0	0	0	0%	0
Art 34/35 (Illegal content)	14	3	1	1	21%	3
Art 34/35 (GenAI)	9	0	0	0	0%	0
Art 34/35 (Disinformation)	6	4	0	0	66%	4
Art 34/35 (Content Mod)	6	3	0	1	50%	3
Art 39 (Ad Repository)	11	3	2	1	27%	3
Art 40 (Researcher Access)	19	5	4	1	26%	5

**RFIs are not explicitly connected to DSA articles, so the number of RFIs is derived from general communications given by the Commission*

*** Binding commitments were offered by **AliExpress**, and those parts of the investigation that these relate to are closed*

Metric	Data*
Shortest Time	5 days (TikTok Lite - urgent matter)
Longest Time	~11 months, 14 days (Pornhub, Stripchat, XVideos - all minors protection cases)
Average Time (excluding TikTok Lite urgent case)	Approximately 5-7 months
Most Common Timeframe	4-6 months

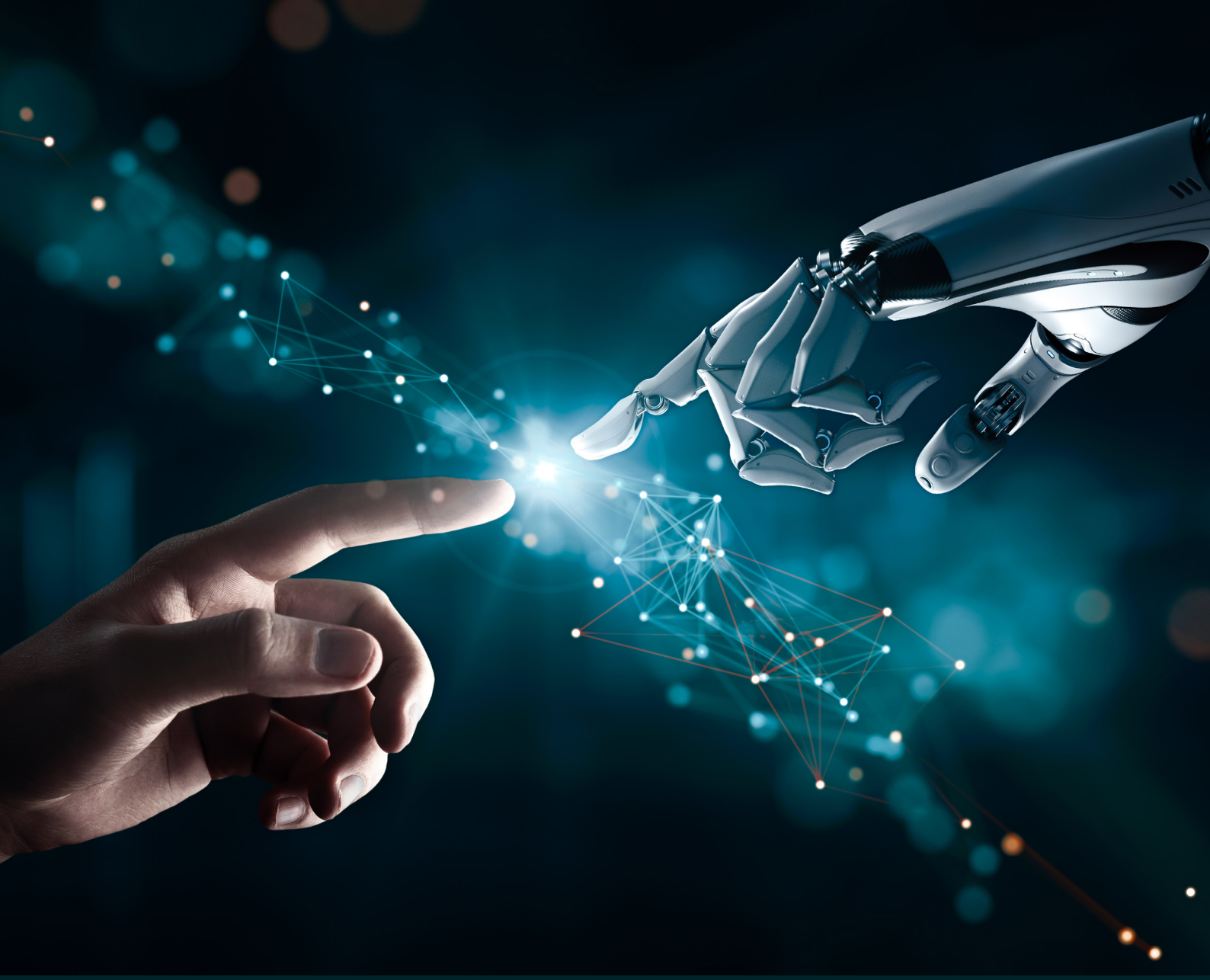
Commission has sent **over 100 RFIs (~70 have press releases and those are used for the table above, updated in November 2025)*

3.4 IMPACT ON BUSINESSES

Recent developments regarding designations, court challenges and enforcement activities under the DSA indicate that businesses operating online platforms are beginning to face a seemingly more structured compliance environment. While the DSA's core obligations are now in force, practical aspects such as calculating active recipients and defining researcher data access are still being clarified.

The supervisory approach is becoming more detailed, with the Commission and national authorities assessing both policy frameworks and operational practices of businesses. Requests for technical documentation and evidence of day-to-day implementation have become common. The high conversion rate of RFIs into formal investigations suggests that platforms should ensure their internal processes and governance structures are robust and that close cooperation with the Commission should be maintained.

Furthermore, the use of retention orders and binding commitments signals a shift towards more active oversight. Although these commitments are currently case-specific, they could shape future compliance standards for similar services. For businesses, this means increased operational demands, closer engagement with regulators and a need to remain aware of how ongoing investigations and upcoming guidance will impact compliance expectations.



4 — CONSUMER PROTECTION IN THE AGE OF AI

4 CONSUMER PROTECTION IN THE AGE OF AI

4.1 COMMISSION INITIATIVES

On the consumer law side of the competition, consumer and privacy law triad, three key Commission initiatives have shaped the agenda. The AI Act entered into force in 2024 and partially started to apply, creating a significant impact on businesses. The revised Product Liability Directive has also been adopted and will start applying at the end of 2026. By contrast, the proposed AI Liability Directive, aimed at harmonising liability rules for AI system providers and users, has been abandoned.

4.2 AI ACT

After several amendments and hasty trialogue negotiations, the **Artificial Intelligence Act** (AI Act) was published in the EU Official Journal in July 2024. The AI Act pursues ambitious goals: improving the internal market; promoting the use of human-centric and trustworthy AI; and ensuring a high level of protection concerning health, safety and fundamental rights while supporting innovation. These objectives reveal that the AI Act covers aspects of product safety and fundamental rights.

AI ACT

Status	Final
Published	12 July 2024
In force	1 August 2024
Objective	Promote trustworthy AI in the EU while ensuring high protection and supporting innovation

The AI Act applies primarily to providers and deployers of AI systems and general-purpose AI models. The regulation implements a risk-based approach, distinguishing between unacceptable risk, high risk and systemic risk. The AI Act introduces strict obligations based on the risks posed, transparency requirements, fines for non- compliance and specific rules for general-purpose AI models.

The AI Act bans the use of certain AI systems, such as biometric categorisation systems based on sensitive characteristics, emotion recognition in the workplace and in education, social scoring, predictive policing, and AI systems that manipulate individuals.

The AI Act imposes extensive regulatory requirements on high-risk systems. AI systems used in the following areas are classified as high risk: biometrics; education and vocational training, employment, workers management and access to self-employment; access to and enjoyment of essential private services and essential public services and benefits; law enforcement; migration, asylum and border control management; and administration of justice and democratic processes. Most obligations applicable to high-risk AI systems relate to the development phase and therefore primarily affect providers of these systems. Key requirements include data governance; human oversight; an "appropriate level" of accuracy, robustness and cybersecurity; quality management; technical documentation; and transparency obligations.

Under the AI Act, large language models are regulated as "general-purpose AI systems", namely systems based on a general-purpose AI (GPAI) model. Such models can serve a variety of purposes, both for direct use and for integration into other AI systems. GPAI models are trained on large-scale data using self-supervision, exhibiting significant generality in performing a wide range of tasks. Most of the obligations regarding GPAI models are

imposed on providers. Additional requirements apply to GPAI models with high-impact capabilities that are likely to pose systemic risks. For such systems, the Commission has approved a code of practice, offering providers an opportunity to demonstrate compliance with their obligations under the AI Act.

The following provisions of the AI Act have already started to apply: prohibitions (February 2025); codes of practice for GPAI models (May 2025); and general-purpose AI rules, including governance (August 2025). Obligations for high-risk systems were meant to become applicable in August 2027. However, in light of the absence of harmonised standards and regulatory guidance, the Commission is considering adjusting the timeline for high-risk systems. As part of the Digital Omnibus package, the Commission has proposed "targeted simplification measures", including a proposal to align the timeline for high-risk systems with the availability of standards, regulatory guidance and compliance tools. Regardless of the outcome of this process, providers of high-risk AI systems currently face considerable legal uncertainty. Whether the legislative procedure for these targeted amendments to the AI Act will be concluded before the requirements for high-risk systems become applicable, remains to be seen.

Comparable uncertainties exist regarding the enforcement of the AI Act. National competent authorities supervise the rules at the national level, while the AI Office established within the Commission oversees coordination at the European level. The AI Office is also responsible for enforcing the rules applicable to GPAI models and systems with systemic risks. Most EU Member States failed to meet the 1 August 2025 deadline for adopting domestic legislation concerning the supervision and enforcement of the AI Act at the national level. This has resulted in a fragmented enforcement landscape and creates legal uncertainty for those providers and deployers of AI systems that are subject to the AI Act.

4.3 PRODUCT LIABILITY DIRECTIVE

The revised EU Product Liability Directive 2024/2853 was published in the Official Journal on 18 November 2024, and came into force on 8 December 2024. The new rules apply to products placed on the market after 9 December 2026, which also marks the deadline for implementing the new directive into national law. The revisions aim to bring the EU's product liability regime in line with the digital age. For example, clarifying that that strict (no-fault) liability rules apply to product manufacturers and software providers and to providers of digital services that affect the functioning of the product. The directive also labels AI systems and AI-enabled goods as "products", which are subject to product-liability rules.

The amendments have implications for online platforms, too. When acting as manufacturers, importers or distributors of products (rather than intermediaries exempt from liability), such platforms are liable for defective products on the same terms as traditional businesses.

PRODUCT LIABILITY DIRECTIVE

Status	Final
In force	8 December 2024
Applicable	9 December 2026
Objective	Modernise existing rules on the strict liability of manufacturers for defective products

4.4 IMPACT ON BUSINESSES

The Product Liability Directive simplifies the process for individuals to bring claims under a strict product liability regime, while reducing legal certainty for businesses. It includes provisions that facilitate access to evidence and shift the burden of proof regarding causation between the defect and the harm. This directive is expected to have a profound impact on technology companies, whether they are engaged in manufacturing, distribution, import and use of AI systems, or in online platforms or digital services and software. Non-EU companies will also be affected, provided they place products on the EU market.

The new Product Liability Directive has the potential to facilitate pan-European mass claims litigation concerning liability for faulty AI systems and AI-enabled goods under the **Representative Actions Directive** – which all EU Member States were required to implement by 25 December 2022. For a discussion on this directive, see our latest **guide** on the new collective actions regime in the Netherlands.

5 — UNLOCKING THE POTENTIAL OF DATA IN EUROPE

5 UNLOCKING THE POTENTIAL OF DATA IN EUROPE

5.1 DATA GOVERNANCE ACT, DATA ACT AND REGULATION ON THE EUROPEAN HEALTH DATA SPACE

The past several years have seen significant progress on the implementation of the Commission's **European Strategy for Data**, with two pieces of legislation standing out: the Data Governance Act and the Data Act. Data is recognised as a highly valuable resource for economic growth, competitiveness and innovation, with the potential to deliver benefits across a variety of fields. The Strategy for Data intends to create a single market for data that enables the free movement of data between Member State businesses and citizens, while respecting privacy and data protection rules and ensuring that rules for access and use of data are fair, practical and clear.

Alongside the two acts, the EU is establishing data spaces: data infrastructures and governance frameworks that facilitate data availability for access and reuse through secure and trustworthy data-sharing environments. Common European Data Spaces are currently in different phases of development across 14 sectors including healthcare, environment, energy, agriculture, transportation, finance, manufacturing and public administration. Businesses in these sectors can expect a reduction in costs for acquiring, integrating and processing data, and lowered barriers for entering markets. They will also see a reduction in time-to-market for novel products and services. The EU is committed to expanding the rollout of data spaces, including through the introduction of a Common European Data Space on defence via the **Data Union Strategy**, adopted in November 2025.

5.2 DATA GOVERNANCE ACT

The **Data Governance Act** oversees the reuse of public or protected data across various sectors. It covers personal and non-personal data, with the GDPR applying where personal data is involved. The Data Governance Act seeks to increase trust in data sharing, strengthen mechanisms to increase data availability, and overcome technical obstacles to the reuse of data.

In order to generate more data available for reuse, the Data Governance Act creates a mechanism for:

- sharing and reusing certain private-sector data held by public authorities (for example, data submitted for licensing and approvals)
- enabling individuals and businesses to make their data available for the public good (data altruism)
- facilitating data sharing across sectors and borders
- regulating "data intermediaries" – organisations mediating between individuals, data-sharing organisations and third parties reusing that data – in order to enhance trust in data sharing.

DATA GOVERNANCE ACT

Status	Final
In force	23 June 2022
Applicable	24 September 2023
Objective	- Create a harmonised European framework for voluntary data sharing - Increase the amount of data available for re-use - Increase trust in data sharing

The Commission aims for the act to be a powerful innovation engine and lead to the creation of new jobs. However, implementation of the Data Governance Act has faltered and the Commission has **opened infringement procedures** against 18 Member States for failing to properly designate responsible authorities or empower them adequately. In addition, **Digital Omnibus package** proposed by the Commission on 19 November 2025 seeks to merge the Data Governance Act into the Data Act, placing the future of the Data Governance Act as a standalone legal instrument on uncertain footing. Under the proposal, the Data Governance Act would be repealed once the

Omnibus enters into force, with its key provisions on data intermediation services and data altruism consolidated and streamlined into the Data Act. The Data Governance Act's rules on the re-use of protected data would be integrated with the Open Data Directive, creating a single, harmonised framework governing the re-use of data held by public-sector bodies. Most notably, the mandatory notification regime for data intermediation service providers would be replaced by a voluntary, trust-enhancing system. In short, the proposal would fundamentally reshape the Data Governance Act's role within the EU data governance landscape if adopted in its current form.

5.3 DATA ACT

DATA ACT

Status	Final
In force	11 January 2024
Applicable	12 September 2025
Objective	- Stimulate a competitive data market - Open opportunities for data-driven innovation

This Data Act complements the Data Governance Act and provides legal clarity regarding the access to and use of data. It focuses on rights of access to the digital environment and will apply to public authorities and private businesses that manufacture or provide digital services or connected products (including IoT). The Data Act should enable users of those connected products and related services to access the data their devices generate, and to share this data with another entity or individual of choice – subject to limitations.

While users' ability to transfer data is recognised as critical to enabling switching, the Data Act has been criticised for being unnecessarily interventionist in its attempt to determine the scope of offerings to customers.

The act overlaps and potentially conflicts with competition law by imposing stringent requirements on businesses active in markets which show no actual signs of failure. It risks falling short of achieving its intended aim of boosting cloud adoption and could even prove significantly detrimental to effective competition in the medium to longer term.

The Digital Omnibus proposes significant amendments to the Data Act, including trade secret protections allowing data holders to refuse data sharing where substantial risks of unlawful disclosure to third countries exist, narrowing business-to-government data sharing triggers from "exceptional needs" to "public emergencies" only, and introducing compensation rights for microenterprises and small businesses.

5.4 REGULATION ON THE EUROPEAN HEALTH DATA SPACE

The Commission envisages the Common European data spaces as sectoral data-sharing ecosystems that will enable data to be reused and will be mediated by technologies and infrastructures conforming to certain standards.

The EHDS **regulation**, which entered into force on 26 March 2025, provides a legal framework regulating access to and exchange of electronic health data for the provision of health services (primary use), and for the re-use of that data for other permitted purposes (secondary use).

The regulation also introduces requirements for data quality and interoperability, and mandates the creation and maintenance of a technological infrastructure necessary for EU-wide access to and exchange of data for primary and secondary use.

In addition to health, the Commission plans to create other data spaces: Industrial, Green Deal, Mobility, Finance, Energy, Agriculture, Public Administration and Skills.

EHDS REGULATION

Status	Final
Published	5 March 2025
In force	26 March 2025
Objective	Create a health-data sharing ecosystem in Europe

5.5 DIGITAL OMNIBUS REGULATION PROPOSAL

The Commission aims to integrate and consolidate into the Data Act regulations and directives that promote the free movement of data and to thus repeal the Data Governance Act, the Free Flow of Data Regulation (FFDR), and the Open Data Directive. The FFDR's principle of free movement of non-personal data and its prohibition for Member States to unjustifiably require data to be stored in their Member State (localisation requirements) will be retained in the Data Act. The proposal streamlines data sharing by incorporating essential provisions from the Data Governance Act into the Data Act making obligations for data brokers clearer, "lighter" and voluntary. Rules for the reuse of public information from the Data Governance Act and Open Data Directive are combined into one Data Act chapter, aiming for simplification and maintaining openness, transparency and fair access. The Digital Omnibus regulation introduces an amendment to the Data Act allowing data holders to refuse the disclosure of trade secrets when there is a high risk of unlawful disclosure to entities under the jurisdiction of third countries with weaker protection of trade secrets than the EU. A new "lighter" regime is proposed for tailored data-processing services, while the right to switch providers of data-processing services remains unaffected. Currently, companies must report incidents under various EU legislative instruments, such as the second Network Information System (NIS2) Directive, GDPR and DORA. The proposal introduces a single entry point as a central hub for all reporting obligations.

Additionally, the proposal includes targeted amendments to the GDPR and AI Act. Finally, the Commission proposes repealing the P2B Regulation due to overlap with the DMA and DSA. The Commission intends to eliminate this overlap by repealing the P2B Regulation, except for those provisions that contain definitions used in other EU legislation. There is a lack of awareness among business users and providers of online intermediation services about their rights and obligations under the P2B Regulation. Due to insufficient compliance and implementation, the regulation's full potential is not being realised, according to the Commission.

5.6 IMPACT ON BUSINESSES

The Data Governance Act, the Data Act and the EHDS Regulation aim to unlock the economic and social potential of data (both personal and non-personal) in Europe. Taken together, these acts bring both new opportunities and new challenges for companies dealing with the increasingly intertwined European legal framework on data governance and data-related enforcement.

All three instruments also apply to both personal and non-personal data, which under EU law are subject to different legal regimes. This means that where personal data is involved, all data-sharing initiatives must also comply with the GDPR. They will then be subject to several different enforcement mechanisms (which will largely operate in silos) and to the supervisory authorities set up by each of the legislative instruments.

While the Data Act, Data Governance Act and the EHDS Regulation promise availability of more reusable data for research and innovation, it remains to be seen how well these mechanisms will operate in practice, considering that they also create certain barriers to non-personal data flows outside the EU. These barriers are similar but not identical to those already existing in the GDPR for transfers of personal data outside the EU. The Data Governance Act and the Data Act are likely to create tension with existing protection of intellectual property rights and trade secrets. Under the Data Act, businesses are expected to open, and provide access to, proprietary data for governments (B2G) and other businesses (B2B), and to enable customers to switch more easily (if that is not currently the case) between different cloud data-processing service providers, while small and medium-sized businesses remain exempt from many of its more stringent requirements. Transitional uncertainty, phased implementation, and variable national enforcement may affect how these obligations play out in practice.

6 — A SAFER DIGITAL SPACE

6 A SAFER DIGITAL SPACE

6.1 CYBER RESILIENCE ACT, CYBER SOLIDARITY ACT, NIS2 DIRECTIVE, AND DORA

Strengthening resilience to cybersecurity threats and supply chain disruptions remains a cornerstone of the European digital strategy. European legislators advanced this agenda in 2024 and 2025, with the entry into force of the Cyber Resilience Act in December 2024 and the Cyber Solidarity Act in February 2025. In January 2025, the EU also adopted a targeted amendment to the Cybersecurity Act, extending the cybersecurity certification framework to managed security services. Meanwhile, the transposition of the NIS2 Directive and the implementation of the DORA remain ongoing.

Taken together, the EU is pursuing a comprehensive approach covering products (Cyber Resilience Act), common incident response (Cyber Solidarity Act), financial sector resilience (DORA) and critical infrastructure (NIS2), supported by enhanced oversight mechanisms and investment in cybersecurity capacity.

In addition to the current framework, **the Digital Omnibus package** introduces a single EU-level entry point for cyber-incident reporting. Operated by ENISA, this mechanism would allow entities with reporting obligations under different legislation such as DORA, NIS2 and GDPR to submit notifications through a unified EU interface, streamlining the process. The proposal aims to reduce administrative burdens and improve timeliness. In short, the change would modify the operational landscape of EU cybersecurity legislation by centralising reporting processes.

6.2 CYBER RESILIENCE ACT

CYBER RESILIENCE ACT

Status	Final
Published	20 November 2024
In force	10 December 2024
Objective	Protect consumers and businesses by ensuring strong cybersecurity in products with digital elements

The Cyber Resilience Act entered into force on 10 December 2024. To give manufacturers sufficient time to adapt, application of the act has been postponed to three years after its entry into force, with the main obligations applying from 11 December 2027. Certain early obligations apply sooner: actively exploited vulnerabilities and severe incidents must be reported from 11 September 2026, and conformity assessment bodies must be notified from 11 June 2026.

The Cyber Resilience Act, which complements other legislation in this area (specifically the NIS2 Directive), aims to safeguard consumers and businesses that buy or use products or software with a digital component, by addressing two stated problems: the inadequate level of cybersecurity inherent in certain products, and the inability of consumers and businesses to determine which products are cybersecure or to set the products up in a way that ensures their cybersecurity is protected.

These problems are addressed by introducing mandatory cybersecurity requirements for products with digital elements throughout their entire life cycle. Targeted products include identity management systems software, password managers, biometric readers, smart home assistants and private security cameras. The Cyber Resilience Act applies to all products connected directly or indirectly to another device or network, with certain exceptions for open-source software or services already covered by existing rules, such as medical devices, aviation and cars.

The Cyber Resilience Act is expected to increase the compliance cost for manufacturers and developers of digital services, who will be tasked with ensuring conformity with the new rules if they want access to the EU market. The majority of manufacturers and service providers will continue to benefit from self-assessment provisions, but products classified as "important" (listed in Annex III) or "critical" (listed in Annex IV) may be subject to third-party conformity assessments. This includes important products such as operating systems, routers, modems, switches, password managers, firewalls, intrusion detection/prevention systems, and smart home assistants and security cameras. Maximum penalties for non-compliance can reach up to EUR 15 million or 2.5% of global annual turnover, whichever is higher.

6.3 CYBER SOLIDARITY ACT

The Cyber Solidarity Act entered into force on 4 February 2025. The regulation follows calls to set up an emergency response fund for cybersecurity. It aims to strengthen cybersecurity capacities by increasing preparedness for, and detection and awareness of, threats and incidents.

The Cyber Solidarity Act includes a European Cybersecurity Alert System and a Cybersecurity Emergency Mechanism to improve incident response capabilities using advanced technology like artificial intelligence. Additionally, a Cybersecurity Skills Academy will consolidate existing initiatives addressing the cybersecurity talent gap through online training and certifications, including certification schemes for managed security services. Implementation involves collaboration with entities like the European Union Agency for Cybersecurity and the European Cybersecurity Competence Centre.

CYBER SOLIDARITY ACT

Status	Final
In force	4 February 2025
Applicable	4 February 2025
Objective	Strengthen capacities in the EU to detect, prepare for and respond to cyber threats and incidents

6.4 NIS2 DIRECTIVE

The revised directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) entered into force in 2023 and updates EU cybersecurity rules introduced in 2016. It broadens the scope of companies' existing cybersecurity obligations, particularly in the area of resilience and incident response, and covers new sectors and entities.

All mid-size and large entities operating in those sectors, as well as certain "important" and "essential" entities irrespective of their size, will have to comply with the rules. NIS2 also introduces new oversight and accountability obligations and cyber risk-management measures and tightens incident-reporting requirements.

Social networking platforms, data centres, search engines, cloud computing services and online marketplaces will have to comply with the directive's security and notification requirements. While its predecessor gave Member States full discretion to determine administrative fines, NIS2 introduces fines of up to EUR 10 million or at least 2% of the total worldwide annual turnover (whichever is higher) of the infringing undertaking.

NIS2 DIRECTIVE

Status	Final
In force	16 January 2023
Applicable	18 October 2024
Objective	Further improve the resilience and incident response capacities of the public and private sector, and the EU as a whole

Implementation Status Across Member States

Member States were required to transpose the NIS2 Directive into national law by 17 October 2024, but implementation has been significantly delayed across the EU. In May 2025, the Commission **sent a reasoned opinion** to 19 Member States (Bulgaria, Czechia, Denmark, Germany, Estonia, Ireland, Spain, France, Cyprus, Latvia, Luxembourg, Hungary, the Netherlands, Austria, Poland, Portugal, Slovenia, Finland and Sweden) for failing to notify full transposition of the directive.

In the Netherlands, the ***Cyberbeveiligingswet***, a bill implementing the NIS2 Directive, is currently under discussion in the House of Representatives. The Dutch government aims for the bill to enter into force in the second quarter of 2026.

6.5 DIGITAL OPERATIONAL RESILIENCE ACT

DORA **entered** into force on 16 January 2023 and applies as of 17 January 2025. DORA aims to enhance digital operational resilience across the financial sector by harmonising laws on ICT-risk management, governance, incident management and reporting, digital operational resilience testing, and ICT third-party risks.

DORA

Status	Final
In force	16 January 2023
Applicable	17 January 2025
Objective	Decrease ICT risks faced by financial entities

DORA's scope is broad, applying to 20 categories of financial entities and to ICT third-party service providers. The definition of ICT services is intentionally broad and captures the full range of digital and technology-related services used by financial institutions.

DORA also introduces a new EU-level oversight regime for critical ICT third-party service providers (CTPPs). The European Supervisory Authorities (ESAs) have designated CTPPs based on information submitted through national supervisors. These CTPPs will fall under direct EU-level oversight. This marks a significant structural shift towards centralised monitoring of systemic ICT dependencies in the financial sector.

In parallel, DORA harmonises and strengthens the incident-reporting framework, consolidating previously fragmented sectoral requirements into a single EU-wide regime. Systemically important institutions are required to perform threat-led penetration testing at least every three years, contributing to a more consistent and risk-based testing approach across the EU.

DORA is also built on a principle of proportionality. Financial entities may take into account their size, overall risk profile, and the nature, scale and complexity of their activities when applying the framework. However, the regulation leaves the interpretation of proportionality to the competent authorities, which will assess whether a financial entity's ICT-risk management framework is effective and proportionate in practice.

DORA is accompanied by regulatory and implementing technical standards (RTS/ITS) developed by the European Supervisory Authorities (EBA, ESMA and EIOPA). These standards further specify the detailed requirements for ICT-risk management, incident reporting, testing, third-party risk management and governance. Some standards were adopted close to the date of application, and certain elements continue to be phased in as final RTS and ITS are published.

6.6 IMPACT ON BUSINESSES

The Cyber Resilience Act, Cyber Solidarity Act, NIS2 Directive, and DORA together establish a comprehensive regulatory framework that expands cybersecurity obligations for businesses operating in the Netherlands and across the EU. Organisations must navigate overlapping requirements spanning product security, incident reporting, operational resilience and critical infrastructure protection. The proposed Digital Omnibus package's centralised EU-level reporting mechanism, operated by ENISA, will require businesses to adapt their internal processes to submit notifications through a unified interface.

Manufacturers and developers of digital products face increased compliance costs under the Cyber Resilience Act, particularly those producing "important" or "critical" products subject to mandatory third-party conformity assessments. The majority of manufacturers will continue to benefit from self-assessment provisions, but products such as operating systems, routers, password managers, firewalls and smart home assistants may require third-party assessment. The delayed transposition of NIS2 in the Netherlands, with implementation expected in the second quarter of 2026, provides a limited window for affected mid-size and large entities to prepare.

The Cyber Resilience Act addresses the current inability of consumers and businesses to determine which products are cybersecure by introducing mandatory cybersecurity requirements for products with digital elements throughout their entire life cycle. The Cyber Solidarity Act's Cybersecurity Skills Academy will consolidate existing initiatives addressing the cybersecurity talent gap through online training and certifications, including certification schemes for managed security services. Organisations investing in compliance infrastructure may be better positioned to access EU markets.

7 — ENFORCEMENT DELUGE AT THE EU AND NATIONAL LEVEL

7 ENFORCEMENT DELUGE AT THE EU AND NATIONAL LEVEL

7.1 COMPETITION ENFORCEMENT

Alongside the adoption of new regulations and the resulting proliferation of rules, regular competition enforcement continues to be used in digital markets. In fact, competition enforcement against digital companies seems to be intensifying as authorities across the EU move beyond coordination towards more substantive cooperation. At the same time, the increasingly cross-border nature of digital markets has exposed challenges posed by the existing enforcement apparatus. These include the prospect of parallel investigations which lead to inefficiencies and divergent outcomes (and possibly new investigations) as well as the conclusion of existing proceedings with complex and potentially overlapping remedies. Below, we provide a snapshot of key competition law cases and investigations from recent years affecting the biggest tech players.

Google / Alphabet

Google remains at the centre of European competition enforcement, with recent developments spanning traditional dominance cases, platform interoperability and emerging AI-related concerns. EU courts have confirmed key aspects of earlier Commission decisions while continuing to refine the legal standards applicable to digital markets. The CJEU finally upheld the Commission's finding that Google's **self-preferencing** in comparison shopping infringed competition rules In another case, the General Court **upheld** most of the Commission's findings in the Google AdSense investigation, but it annulled the decision to impose a EUR 1.5 billion fine on the ground that the Commission had failed to consider all the relevant circumstances when assessing the duration of the contractual clauses that it deemed abusive. Google has since **appealed** this decision. In a separate case concerning tying practices relating to Google Android, Advocate General Kokott **recommended** that the CJEU dismiss Google's appeal.

Interoperability has also emerged as a recurring theme. Both EU and national courts have clarified that refusals to grant access to platform functionalities, such as **Android Auto**, may, in certain circumstances, amount to abuse, even where the platform is not strictly indispensable, particularly when access enhances the attractiveness of third-party services to consumers.

Google has faced further scrutiny in ad tech markets, culminating in a significant **fine** for preferentially treating its own online display advertising technology services to the detriment of competing providers, advertisers and online publishers.

More recently, enforcement attention has extended to the use of third-party content in the development of generative **AI services**, reflecting growing interest in how data access and training practices may affect competition in adjacent and emerging markets. In particular, the Commission is concerned that Google may have used the content of web publishers to provide generative AI-powered services and content uploaded on YouTube to train Google's generative AI models. The investigation will focus on whether Google is undermining competition by enforcing unfair terms on publishers and content creators, or by giving itself privileged access to their content in ways that could disadvantage developers of competing AI models.

Enforcement targeting Google at the national level continues as well. For example, in April 2025, Google **offered** the German competition authority commitments to end several restrictions on competition related to Google Automotive Services and the Google Maps Platform. This investigation stemmed from a complaint outlining concerns of abuse of dominance and harmful conduct by a digital gatekeeper, falling under the ex-ante digital rules of the German Competition Act (Section 19a GWB).

These public enforcement actions continue to generate follow-on litigation, including **damages claims** brought against multiple Google entities, underscoring the increasing interplay between public enforcement and private actions across the EU.

Apple

Apple has faced sustained enforcement attention focused on the governance of its ecosystem and the conditions imposed on third-party developers. At the EU level, this has included a significant fine relating to **anti-steering provisions** in the App Store, as well as **commitments** offered by Apple to address the competition concerns related to Apple's refusal to supply the Near-Field-Communication (NFC) or "tap and go" input on iOS to competing mobile wallet developers, reserving access to Apple Pay.

At the national level, authorities and courts have examined Apple's app distribution and payment rules, with particular attention to whether certain terms unduly restrict developers' freedom of choice. In the Netherlands, the Rotterdam District Court **upheld** the finding by the Dutch competition authority that Apple had abused its dominant position by imposing unfair terms on providers of dating apps in the App Store. The court reaffirmed that the Dutch competition authority was correct in determining that Apple's practices restricted the freedom of choice for these app providers. Specifically, dating app providers were required to use Apple's payment system, prohibited from directing users to alternative payment methods outside the App Store, and obliged to pay a substantial commission to Apple.

Apple's App Tracking Transparency Framework has also attracted scrutiny, with the **Polish** and **German** competition authorities assessing whether its differentiated application to Apple's own services compared to third-party apps could raise concerns of unequal treatment or self-preferencing. The **French** competition authority has already fined Apple for abusively applying this framework.

Looking ahead, recent **notifications** under the DMA indicate that additional Apple services may soon fall within the scope of the gatekeeper regime, potentially extending the regulatory framework that applies to Apple's platform activities.

Microsoft

Microsoft's recent enforcement experience has largely centred on product integration and ecosystem effects. At the EU level, the Commission's **investigation** into Microsoft's tying of Microsoft Teams to productivity suites concluded with **commitments** to address concerns around tying, interoperability, data portability and customer choice.

At the same time, in Germany, Microsoft has been designated as an **undertaking** of paramount significance for competition across markets, placing it under enhanced abuse control. This reflects a broader trend towards closer oversight of large digital ecosystems, even in the absence of a finding of infringement.

Beyond classic antitrust enforcement, Microsoft has also featured in merger control and AI-related assessments. The Commission has concluded that Microsoft's partnership with OpenAI did not constitute a **notifiable concentration** under EU merger rules, while signalling continued attention to potential ecosystem effects in AI and adjacent markets. In parallel, complaints relating to Microsoft's **search services** have been examined at the national level, with some proceedings dismissed at an early stage.

Meta (Facebook, Instagram, WhatsApp)

Meta's enforcement exposure illustrates the growing convergence between competition concerns and data and AI-driven business models. At the EU level, the company has been fined for tying practices involving Facebook Marketplace, while more recent investigations have focused on access to WhatsApp for AI providers, both by the **European Commission** and the **Italian** competition authority which even imposed interim measures suspending the terms excluding competing AI Chatbots from WhatsApp.

Alongside these developments, Meta has also resolved proceedings in Germany relating to combining user data from different sources. After Meta implemented the required measures, the German authority **closed** its proceedings against the company in October 2024, reflecting the continued role of negotiated outcomes in complex digital cases.

Amazon

Amazon continues to attract scrutiny both as a marketplace operator and for its consumer-facing practices. Authorities have examined the company's influence over seller pricing and visibility, particularly the use of internal pricing mechanisms that could affect third-party offers. In Germany, the Bundeskartellamt issued a preliminary **legal assessment** regarding Amazon's influence on seller pricing on the Amazon Marketplace and its Fair Pricing Policy. Additionally, the German Federal Court has **dismissed** Amazon's appeal against its designation as an undertaking of paramount significance for competition across markets. As of now, Meta, Amazon, Alphabet, Apple and Microsoft hold this designation.

Consumer-oriented practices have also been addressed. In Italy, Amazon group companies were **fined** for pre-selecting the recurring purchase option for a wide range of products, considered an unfair commercial practice. These proceedings illustrate the breadth of enforcement tools applied to large digital platforms, spanning both competition and consumer law.

Booking / Booking.com

The CJEU has **clarified** that price-parity clauses may fall within the scope of Article 101(1) TFEU. The CJEU's ruling indicates that, while the ancillary restraints doctrine may not apply, the Vertical Restraints Block Exception Regulation (VBER) is available to exempt price parity clauses. The ruling also highlights the importance of considering the two-sided nature of OTA platforms in defining the relevant market when applying the VBER / article 101 TFEU. See our **article** on this case here.

In the Netherlands, the Amsterdam District Court has **declared** inadmissible a claim by the German Hotel Association (IHA) against Booking.com over its Genius loyalty programme. IHA argued that the programme breaches the prohibition on abuse of dominance, but the court held that under Dutch procedural law, IHA lacked a material interest, as the relevant legal relationship exists only between Booking.com and participating accommodation providers.

In Italy, the competition authority accepted **commitments** offered by Booking.com to address concerns around promotional programmes, and closed its investigation. This outcome highlights the use of commitments and dialogue in resolving competition questions, balancing regulatory expectations with operational continuity.

7.2 PRIVACY AND DATA-PROTECTION ENFORCEMENT

Increased EU-level coordination and big-ticket fines for violations of the GDPR by, predominantly, big tech companies reflect the increased enforcement of European data protection rules. The European Data Protection Board (EDPB), an independent European body composed of the heads of the national data protection authorities and the European Data Protection Supervisor (EDPS), plays a vital role in ensuring that the GDPR is consistently applied and enforced. The EDPB's **binding decisions** tend to broaden the scope of GDPR obligations and can mandate multibillion-euro fines for GDPR violations. These decisions must be followed by data protection authorities throughout the EU. No binding decisions have been issued in 2025.

In April 2024, the EDPB adopted **Strategy 2024-2027**, which revolves around four pillars. It aims first to strengthen harmonisation across the EU and promote consistent compliance with data protection rules. The second pillar focuses on deepening cooperation and fostering a shared enforcement culture among supervisory authorities to ensure effective oversight. The third addresses emerging digital and cross-sector challenges, ensuring that data protection keeps pace with technological and legislative developments. Finally, the strategy underscores the EU's commitment to shaping and engaging in the global conversation on data protection, promoting high standards and international collaboration. The **2024-2025 work programme** underscores these priorities, while the EDPB's coordinated enforcement action (CEF) for 2025 focused on the right to erasure (Article 17 GDPR).

Despite all these coordinated efforts, public enforcement cooperation suffers from legal and organisational weaknesses that make it slow and inefficient; for example, there remains a persistent problem of data protection authorities' lack of financial and human resources, diverging enforcement priorities across the EU, and incoherent administrative rules and procedures which ultimately burden small and medium enterprises. To address the latter, the Commission proposed a **regulation harmonising procedural rules relating to GDPR enforcement**. In November 2025, the Council **adopted** the proposal as the final legislative step. The regulation will enter into force in 2027.

7.3 KALEIDOSCOPIC ENFORCEMENT AT THE CROSSROADS OF COMPETITION, CONSUMER AND PRIVACY LAWS

Competition and consumer authorities already routinely investigate data-related issues overlapping with the GDPR. And, with the progressive enforcement of the DMA, the DSA, the Data Act and various other data-related legislation, the problem of the "**kaleidoscopic enforcement**" of digital, competition, data protection and consumer laws (a concept coined to refer to overlapping or conflicting enforcement against the same data-related violation by different authorities in different Member States) is likely to grow.

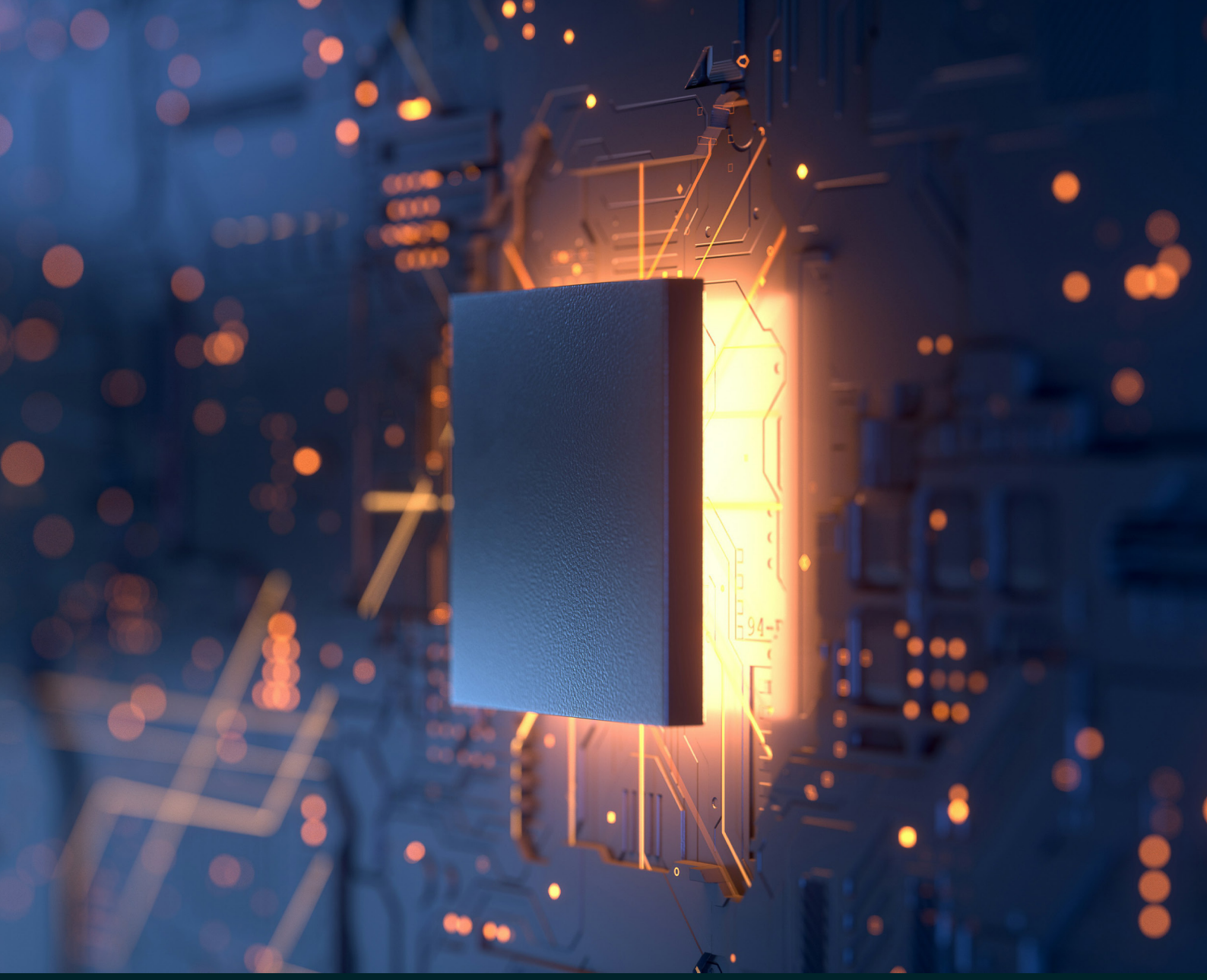
A compliance concern arising from such kaleidoscopic enforcement is the incorporation of the GDPR concept of "consent" into the DMA. To illustrate, in March 2024, the Commission **initiated** DMA non-compliance investigations against several gatekeepers, including into Meta's "pay or consent model". The Commission found the model in **breach** of the DMA obligation to give users the required choice to opt for a service that uses less of their personal data but is otherwise equivalent to the "personalised ads" service. The Commission also looked into whether users can freely exercise their right to consent to the combination of their personal data. Notably, the Commission's non-compliance **decision** against Meta followed an EDPB **opinion** on "consent or pay" models. According to the EDPB, "consent or pay" models in most cases will not comply with the requirements for valid consent under the GDPR if users are presented only with a binary choice between consenting to the processing of personal data for behavioural advertising purposes or paying a fee. This case demonstrates that applying the GDPR simultaneously with other data-related acts, including the DMA, exacerbates compliance challenges, particularly given the notable absence of a pan-European interdisciplinary coordination mechanism.

However, in response to these challenges, in October 2025, the Commission and the EDPB opened a public consultation on draft **joint guidelines** on the interplay between the DMA and the GDPR. The draft Guidelines aim to ensure that the DMA and GDPR are interpreted and applied in a compatible manner, focusing on provisions with significant overlaps that merit clarification and a common interpretation among the competent authorities. This approach seeks to avoid risks that gatekeepers instrumentalise their compliance with one framework to make their compliance with the other less effective, while ensuring cooperation and coordination between the Commission, as the sole DMA enforcer, and data protection supervisory authorities, as GDPR enforcers.

In addition to the overlap between the DMA and GDPR, provisions of the DSA on algorithmic transparency and accountability also overlap with similar provisions of the GDPR and of the AI Act. The Commission has focused DSA enforcement efforts on very large online platforms and search engines since March 2024. These efforts have consisted of several formal **RFIs** regarding the mitigation measures these actors have in place to address risks linked to generative AI. In May 2024, the Commission compelled **Microsoft** to provide information under the DSA regarding specific risks stemming from Bing's generative AI features. The Commission has also sent RFIs to YouTube, Snapchat, TikTok and X on the design and functioning of their recommender systems under the DSA. Recommender systems are a key part of the formal non-compliance proceedings opened against TikTok, AliExpress, Facebook, Instagram, Temu and X. Moreover, the Commission has initiated multiple formal proceedings against designated platforms, including investigations into duties related to the protection of minors, the integrity of electoral processes, the dissemination of illegal content, dark patterns, advertising transparency and data access.

Last, similar to the overlap between the DMA and GDPR or between the DSA, GDPR and AI Act, GDPR enforcement has also overlapped with a fundamental concept of EU competition law. In the recent ***ILVA* judgment**, the CJEU ruled that the notion of "undertaking" in competition law must be applied not only when calculating the maximum possible fine for a GDPR breach, but also when determining the actual fine to be imposed. Consequently, when determining the actual fine, not only should the individual turnover of the legal entity controlling or processing the personal data in breach of the GDPR be considered as one of the factors, but also the combined total worldwide turnover of the group or economic entity to which the company belongs. Furthermore, it can be **argued** that unlike the EDPB's position, the maximum possible fine is only one of the factors in determining the actual fine and is not necessarily the starting point.

In addition, the CJEU's **Lindenapotheke** judgment sheds further light on the intersection between competition law and data protection law, specifically on whether a competitor can assert a violation of data protection law (in this case, the GDPR) as a violation of national unfair competition law. The CJEU has ruled that the GDPR does not preclude national law from allowing competitors to bring proceedings for GDPR infringement under unfair competition law.



8 — OTHER NOTABLE DEVELOPMENTS

8 OTHER NOTABLE DEVELOPMENTS

8.1 LESS RED TAPE FOR COMPANIES

On 30 January 2025, **Digitalisation Directive II** - further expanding and upgrading the use of digital tools and processes in company law - entered into force. The directive aims to enhance cross-border operations, improve transparency and reduce administrative burden. Member States have until 31 July 2027 to adopt laws necessary to comply with the directive. The directive includes measures such as: applying the "once-only principle" to avoid the redundant submission of information when companies set up a branch or company in another Member State; introducing an EU Company Certificate containing a basic set of information about companies, which will be available free of charge in all EU languages; and streamlining formalities by introducing a multilingual standard model for a digital power of attorney authorising a person to represent a company in another Member State and by removing the need for an apostille or certified translations for company documents.

It also seeks to increase transparency by making essential company information publicly available through the Business Registers Interconnection System (BRIS) and facilitating searches through interconnected EU systems. The directive aims to enhance the digitalisation of EU company law and promote "digital by default" solutions while contributing to the EU's Digital Decade objectives.

8.2 STATUS OF EU PATENT RULES

In 2023, the Commission proposed several new regulations to support companies, particularly small and medium-size enterprises, in maximising the potential of their inventions, leveraging new technologies and enhancing the EU's competitiveness and technological sovereignty. The regulations, referred to collectively as the patent initiatives, focus on: standard essential patents (SEPs); the compulsory licensing of patents in crisis situations; and supplementary protection certificates (SPCs).

In October 2025, the Commission **withdrew** the proposal on SEPs – which aimed to introduce a new, detailed system for the registration of all standard essential patents in force in one or more Member States - stating that there was no foreseeable agreement between the European Parliament and the Council. In November 2025 the European Parliament voted in favour of a decision to ask the CJEU to annul the Commission's decision to withdraw the proposal.

The European Parliament has **adopted** the proposed regulation on compulsory licensing for crisis management and the regulation is currently awaiting publication in the official journal.

The **proposals** aiming to reform the EU system for granting SPCs are currently under review by the European Parliament and Council.

Together, these initiatives seek to eliminate fragmentation across Europe, reduce red tape and enhance efficiency in patent protection. The patent proposals complement the Unitary Patent system, operational as of 1 June 2023 and covering 18 Member States. This system addresses shortcomings in national patent regimes by offering a one-stop shop for patent registration and enforcement. Patent applicants must first file a European Patent application, and then they may request unitary effect for participating Member States. As such, the system streamlines procedures, lowers costs and ensures the uniform protection of patents

Additionally, the EU SME Fund will continue to offer voucher services to support innovation in patent registration and new plant varieties.

Together, the Unitary Patent system, the new Unified Patent Court and the patent proposals are expected to encourage innovation, economic growth and foreign investment into the EU.

The recent Anne Frank Fonds **case** highlights the growing complexity of digital content distribution, particularly in relation to territorial control of works online. In Anne Frank Fonds, now before the CJEU following a November 2024 referral from the Dutch Supreme Court, the central question concerns whether geo blocking can effectively prevent a "communication to the public" in a blocked country when users may still access the content through VPN services. The CJEU will also need to assess whether publishers remain liable despite the intervening role of VPN providers. The outcome will have significant implications for rightholders' ability to manage territorial exploitation in an online environment where technical restrictions are easily circumvented. For more information, read the Advocate General's **opinion**, issued on 15 January 2026.

8.3 COMBATTING ONLINE PIRACY OF SPORTS AND LIVE EVENTS

In 2023, the Commission issued a **recommendation** to combat the large-scale online piracy of sports and other live events, urging Member States, rights holders and intermediary service providers to take effective measures while respecting fundamental rights and personal data protection rules. The aim is to protect the viability of the EU sports and creative industries. The recommendation focuses on prompt treatment of notices related to live events, dynamic injunctions and improving commercial offers and awareness among consumers. It emphasises enhanced cooperation between national authorities, rights holders and intermediaries, along with establishing a monitoring system with clear key performance indicators to assess its impact. In November 2025, the Commission reviewed the recommendation's effects and noted that it had had positive effects, but that these were limited given the recommendation's non-binding nature. The Commission will consider further the contribution of different online intermediaries and explore whether new measures are needed.

8.4 EU DIGITAL IDENTITY WALLET AND EUROPEAN BUSINESS WALLET

In May 2024, the **European Digital Identity Framework** entered into force, featuring a personal digital wallet accessible via a secure mobile app. The innovation aims to grant EU citizens, residents and businesses trustworthy access to public and private online services across Europe, offering control over personal data while ensuring convenience.

The EU Digital Identity Wallet is undergoing large-scale pilots funded by the Digital Europe Programme to refine its technical specifications, covering various everyday-use cases.

The Commission is collaborating with Member States on technical aspects and has published a toolbox to build the prototype European Digital Identity Wallet app, with mandatory requirements. Member States must offer at least one EU Digital Identity Wallet to all citizens and residents by 2026. The framework builds on the existing eIDAS Regulation, enhancing secure digital identity across borders and extending benefits to the private sector and mobile users.

The Commission's new digital package also includes a **proposal** on European Business Wallets that will offer companies a single digital identity to simplify paperwork and make it much easier to do business. These wallets will let companies securely identify themselves, sign and exchange verified documents, and communicate across the EU. This will reduce paperwork and administrative burdens with potential savings of over EUR 160 billion a year. Once the proposal has been adopted, public administrations will have two years to roll it out while technical standards are finalised through ongoing EU digital identity work and pilot projects.

8.5 CONNECTIVITY ACROSS EUROPE

On 23 February 2023, the Commission presented a plan to ensure Gigabit connectivity throughout the EU by 2030, in line with its Digital Decade objectives. A key element, the **Gigabit Infrastructure Act (GIA)**, entered into force in May 2024 and became fully applicable by 12 November 2025, replacing the 2014 Broadband Cost Reduction Directive. The GIA streamlines the deployment of high-speed networks, including fibre and 5G, and aims to reduce costs, simplify procedures and ensure faster, more reliable connectivity across Europe.

At the same time, the Commission finalised the **Gigabit Recommendation** in February 2024. This guidance complements the GIA by advising national regulatory authorities (NRAs) on setting access obligations for operators with significant market power to foster competition. It provides clarity on when access to civil-engineering infrastructure is needed to address competitive bottlenecks and sets out expectations for NRAs to manage the transition from copper networks to fibre efficiently. These efforts reflect a growing demand for more bandwidth at faster speeds to support the development and use of technologies such as cloud, artificial intelligence, data spaces, virtual reality and the metaverse. While aiming to meet increasing connectivity demands, drive technological progress and ensure fair access to high-speed internet across the EU, the Commission is also drawing the borders of new rights for EU citizens: digital rights.

8.6 WEB 4.0 AND VIRTUAL WORLDS STRATEGY

On 11 July 2023, the Commission **adopted** a strategy on Web 4.0 and virtual worlds to guide the next technological transition and ensure an open, secure, trustworthy, fair and inclusive digital environment for EU citizens, businesses and public administrative bodies. The strategy aims to reflect EU values and principles in Web 4.0 and virtual worlds, empowering people, reinforcing skills, supporting businesses, enhancing government services and shaping global standards. A few of its key pillars include: empowering people through awareness and skills development; supporting a European Web 4.0 industrial ecosystem; enhancing virtual public services; and shaping global standards for open and interoperable virtual worlds and Web 4.0.

This strategy aligns with the Digital Decade policy programme's objectives and addresses various aspects of digitalisation to harness the opportunities and mitigate the risks associated with the ever-evolving internet landscape. More recently, the Commission launched the **European Partnership for Virtual Worlds**, bringing together industry, academia, research organisations and users to support research and innovation. The partnership aims to position the EU as a global leader in virtual worlds technologies. Signed with the Virtual Worlds Association and its 18 funding members, it comes as the global virtual worlds market is projected to grow from EUR 27 billion in 2022 to over EUR 800 billion by 2030.

debrauw.com

Burgerweeshuispad 201
1076 GR Amsterdam
The Netherlands

DE BRAUW
BLACKSTONE
WESTBROEK