Council of the European Union

Brussels, 1 December 2025
(OR. en)

16212/25

TELECOM 450
CYBER 360

NOTE

From:	Commission services
To:	Delegations
Subject:	2025 Annual Progress Report on Simplification, Implementation and Enforcement – Tech Sovereignty, Security and Democracy

Delegations will find in the Annex the above-mentioned report.

ANNEX

European Commission

2025
ANNUAL PROGRESS REPORT

Simplification, Implementation & Enforcement

Henna VIRKKUNEN

Executive Vice-President of
the European Commission for Tech Sovereignty,
Security and Democracy

SEPTEMBER 2025

DRAFT REPORT

1. Introduction

As Commission Executive Vice-President for Tech Sovereignty, Security and Democracy, I am directly responsible for the Digital and Frontier Technologies portfolio. My responsibilities entail leading Europe's efforts in shaping a competitive, resilient and inclusive digital future and maintaining or attaining leadership in strategic digital technologies, such as artificial intelligence, quantum, semi-conductors and other frontier technologies. My priorities include: overseeing the path towards reaching Europe's 2030 Digital Decade targets; boosting Artificial Intelligence application and innovation; improving access to secure, fast, and reliable connectivity; ensuring the timely and predictable implementation of the European Digital Rulebook, notably by ensuring effective enforcement action under the Digital Services Act and the Digital Markets Act; deploying digital public infrastructure e.g. the EU wallets; designing a European Data Union Strategy; preserving the unique place of media in Union democracies and culture, and making online more secure.

This report presents highlights of the main achievements on simplification and implementation across my portfolio over the period from 1 January to 31 July 2025, in line with my Mission Letter[1].

2. Executive Summary

This progress report highlights the main achievements and ongoing efforts under my leadership to simplify and enhance the efficiency of Europe's digital rulebook, ensure its implementation and maintain its enforcement effectively.

The Commission is conducting a comprehensive stress-test of EU digital rules, to ensure that they remain effective and efficient, and that their application is optimised in the real world. With this in mind, the Commission will put forward a Digital Simplification Package to be adopted in the autumn, including a Digital Omnibus to simplify and optimise rules on data, cyber and artificial intelligence, but also an EU Business Wallets to support the regulatory compliance and interactions between businesses and administrations. The Package will also launch a comprehensive digital fitness check.

At the same time, Europe's digital rulebook remains robust, and its effective implementation is a priority for the Commission. Substantial progress has been achieved on this front, through dedicated implementation and enforcement action. For instance, the Commission took enforcement action to protect minors and safeguard the integrity of elections under the Digital Services Act. DG CONNECT has also been engaging with Member States and businesses on several fronts, not least to ensure they prioritise the timely implementation of the Artificial Intelligence Act. Nevertheless, when Member States were too late in making EU rules effective at national level, the Commission has not shied away from infringement cases, for instance regarding cybersecurity regulation.

3. Delivering Results: Key Measures

A. Simplification and stress tests

Europe has a robust digital rulebook and its effective implementation is a priority for the Commission. At the same time, digital regulation must keep up with the societal, technological and market developments in our changing world. And it must enable innovation and technological advancements. It has to strengthen the competitiveness for

[1] See also Communication 'A Simpler and Faster Europe'.

Europe to build a strong economic future around its well-established values of democracy, equality, the rule of law and human rights.

The Commission's ambition is to stress-test how effective and efficient the rules are and to optimise their application in the real world, in line with this Commission's Political Guidelines. The digital rulebook will be subject to a comprehensive stress-test along the entire mandate, starting already in 2025 with immediate simplification measures.

With these objectives in mind, the Commission will first present[2] **a Digital Simplification Package** in Q4 this year. Since the beginning of the year, my services have focused on the preparatory steps for the proposal. The Package will have three major components.

First, the Commission will present to the co-legislators a **Digital Omnibus regulatory proposal**, focusing on three areas of the digital acquis with immediate measures that will optimise the effectiveness of our rules with significant cost reductions for businesses. The targeted amendments will restructure the data acquis to overcome practical obstacles for innovation and data availability – in full respect of privacy and trade secrets –, streamline the sectorial and fragmented cybersecurity incident reporting obligations, and make targeted adjustments to ensure the optimal application of the Artificial Intelligence Act from the offset.

The Commission will propose these adjustments with a clear objective to deliver fully on the societal objectives of the rules. The three main areas of intervention were selected based on a first screening of the digital regulation, for example when it comes to reporting obligations. The proposals will be thoroughly informed by **a series of consultation steps taken in 2025** and their results will be communicated in detail to the co-legislator together with the legal proposals:

- **Calls for evidence and public consultations** on the overall scoping and approach to the Digital Omnibus (in September 2025), as well as on the simplification needs in three specific areas of the intervention: on the Data Union Strategy and its regulatory simplification plans, on the review of the Cybersecurity Act and further simplification of incident reporting obligations, and on the Apply AI strategy and ways to support a competitive AI industry in the EU, including by ensuring the proper application of the Artificial Intelligence Act.
- **Implementation dialogues** on the data acquis and on the cybersecurity acquis.
- **'Reality checks'** series of focus groups with businesses subject to the digital rules on cybersecurity reporting, on data, Artificial Intelligence and EU Digital Identity. The reality checks explored how businesses experience the application of the digital rules in their daily operations and tested ways to streamline the processes they are subject to and cut cost in a meaningful way while delivering on the core objectives of the obligations.

With the separate proposal of a **Digital Networks Act** and the revision of the **Cybersecurity Act** also planned for this year, this will round-up the series of immediate regulatory simplification measures that the Commission will bring to the co-legislator in 2025. The Digital Networks Act will propose a far-reaching **simplification** of the regulatory framework, not only reducing and simplifying existing rules, but also coordinating their application, including in the area of spectrum. The Cybersecurity Act revision will among others aim to facilitate compliance with existing cybersecurity risk management measures.

Second, the Digital Simplification Package will show how digital solutions can themselves simplify the regulatory compliance processes for businesses and administrations with the proposal of **EU Business Wallets**, a key enabler for simple and effective compliance processes. Just like the EU Digital Identity Wallets which should be available to individuals as of the end of 2026, the Business Wallets will bring a secure interface for businesses and other legal entities like public administrations to interact with each other, for example as they submit they comply with their reporting obligations or make proof of certifications they have acquired for offering their rule-compliant services.

Third, the Package will show the Commission's full commitment both to apply thoroughly individual rules, and to look consistently and comprehensively at their cumulative effect. For this, the Package will include a report on the interactions of the Digital Services Act (DSA) with other pieces of legislation for example related to consumer protection and product safety based on Article 91 DSA. It will also mark the start of a comprehensive **digital fitness check**, as announced earlier this year, with a public consultation.

[2] Commission work programme 2025 - European Commission

Further, the Commission will continue to assess how specific pieces of law deliver on their objectives, with a series of evaluations and assessments. In 2026, notably, the Audiovisual Media Services Directive, the Copyright in the Digital Single Market Directive and the Digital Markets Act will go through an assessment, as well as the Digital Decade Programme. In all these efforts, the Commission will keep as a high priority an assessment as to whether further simplification steps are possible, and where further clarity and coherence is needed.

Moreover, since January 2025, my services have been assessing the digital dimension of policy initiatives, in line with the Interoperable Europe Act. By embedding the Digital-Ready Policymaking Principles across all stages of policy design, the Commission promotes the use of more precise legal requirements that include digital implementation by default and encourages the reuse of existing data and digital solutions to minimise duplication. This results in rules that are easier to understand, implement, and comply with thus enhancing legal clarity and reducing administrative burden.

B. Implementation

Implementing the digital rulebook is my top priority. My services have been working on supporting Member States and businesses to implement and apply the rules; engaging with businesses and authorities alike, building a mutual understanding of the blockages and levers for the optimal application of the rules; and taking direct enforcement measures at EU level, notably in the case of the Digital Services Act and the Digital Markets Act.

The implementation of the Digital Services Act

The **Digital Services Act (DSA)** safeguards consumers and business users by protecting their fundamental rights online.

Over the reporting period, the Commission has given priority to the application of the DSA's provisions that seek to ensure privacy, safety and security of minors online. In order to help providers and to ensure consistent application throughout the Union, the Commission adopted Guidelines on protection of minors under the DSA, in consultation with the European Board for Digital Services. One of the measures considered is to further restrict access to services or parts of the service which constitutes a high risk to minors, such as adult content services. The Commission has released a user-friendly and privacy-oriented comprehensive age verification blueprint setting a 'gold standard' in age assurance online[4].

The DSA also requires providers of online platforms offering services to users in the Union to assess and mitigate risks linked to illegal products and goods that may affect public health and well-being, improve traceability of traders and enhance transparency in online advertising content in their recommender systems, therefore effectively protecting users and businesses in the digital environment.

In February 2025, the voluntary Code of Conduct on Disinformation was integrated into the framework of the DSA, which includes the Rapid Response System for elections, which allows swift reporting of time-sensitive content, accounts or trends viewed as threats to the integrity of elections. This system was notably used for the 2024 European elections, the German elections in February 2025, and the 2025 Polish elections (see in Annex).

Digital Services Coordinators (DSCs), together with other national Competent Authorities, where applicable, are responsible for enforcing the DSA towards providers established within their territories. DSCs play a vital role in coordinating and ensuring compliance with the DSA across the EU. Over the reporting period, the DSCs have stepped up their capacity and supported the Commission's own proceedings with relevant information, in particular in the four openings of proceedings related to adult content platforms. As explained below, those Member States which have not designated or fully empowered a Digital Services Coordinator have faced infringement proceedings. I am committed to advancing quickly in these proceedings in order to put pressure on Member States to allow citizens and business to benefit fully from the DSA.

The European Board for Digital Services (EBDS) was established to facilitate the collaboration among the DSCs and the Commission. For this purpose the Board has created Working Groups, including one on protection of minors and one on consumer protection and online marketplaces (see in Annex). The Board's work plan indicates its key priorities, such as enhancing effective cooperation on complaint handling.[3] The Board also provided its views on the Commission's preliminary findings regarding specific investigations.

[3] The Commission chaired seven meetings of the Board between January 2025 and July 2025.

The Artificial Intelligence Act

The **Artificial Intelligence Act** **(AI Act)** sets out risk-based rules to ensure that AI in the EU is safe and trustworthy. On 2 February 2025, its general provisions (including AI literacy obligations) and prohibitions entered into application. To facilitate compliance and practical application of these rules, the Commission has adopted Guidelines on the AI system definition, as well as a living repository of AI literacy practices and a Q&A on how to comply with the AI Act's AI literacy obligations.

On 2 August 2025, the AI Act's rules for general-purpose AI models (GPAI) entered into application. To help providers of such models meet their transparency, copyright and systemic-risk obligations under the AI Act, the General-Purpose AI Code of Practice (Code), a voluntary tool, was developed in a unique co-regulatory, multistakeholder process and was published in July 2025, signed by a large number of model developers. In addition, the Commission has published Guidelines on the obligations for providers of general-purpose AI models and a Template to summarize the data used to train a model. By 2 August 2025, Member States also had to establish or designate national competent authorities and lay down rules to empower those authorities to impose penalties. This is an important step towards legal certainty for the market. Since the adoption of the AI Act in 2024, DG CONNECT is engaging with all Member States, to ensure they prioritise the timely implementation and guide them towards a pragmatic approach. The main channel is the AI Board and its sub-groups, where there is high engagement from Member States. In addition to AI Board implementation Roundtables (in March and June 2025), my services also provided guidance to Member States on the content of national laws on penalties and on notifications (in June 2025)[4]. Despite these efforts, many Member States are delayed in the national implementation, which is a serious concern. In parallel, the Commission has also put in place the EU-level governance bodies and coordination mechanisms to ensure a coherent application across Member States[5].

To ensure the smooth implementation of the AI Act and address inquiries on its roll-out, the Commission has also decided in early 2025 to set up a dedicated AI Act Service Desk to be operational in October 2025. It will be an information hub with simple, straightforward information on the application of the AI Act and the possibility to receive targeted answers to questions.

The Data Acquis

I held my first **Implementation Dialogue** on **Data Policy** in July 2025. This political exchange gathered feedback from selected stakeholders on the implementation of EU data rules, with a view to identifying solutions to streamline and simplify the existing regulatory framework. An important takeaway is that, while the EU has strong foundational data regulations, fragmented enforcement across the EU and overlapping digital legislation create complexity. Industry representatives also reported issues of interoperability and quality of data. They stressed the importance of transparency, clearly defined access rights e.g., for internet-of-things data, the need for incentives to use existing data intermediation mechanisms, and for having better access to public sector data. Further, regulatory support and sandboxes could allow businesses, in particular smaller companies, to better navigate different regulatory regimes. I emphasised the commitment of my services to supporting companies - especially SMEs - in complying with data legislation in a practical and proportionate manner, and to providing clear guidance in close cooperation with national authorities. Building on this exchange and on the contributions to the public consultation on the Data Union Strategy, my services are working to improve and simplify the current legal framework and unlock the full potential of the European data economy, including through concrete regulatory adjustments in the forthcoming Digital Omnibus (see also Section A. Simplification, above).

The **Data Act** started applying from 12 September 2025 and aims to unlock the value of data generated by connected objects, a key innovation area in Europe. During the reporting period, the Commission services continued to help stakeholders adapt to the new rules through sector-specific dedicated workshops, bilateral meetings with companies to discuss specific issues in-depth, updates of the Frequently Asked Questions document on the Data Act provisions. Furthermore, the Commission steered the work of the **Expert Group on B2B data sharing and cloud computing contracts**, which is assisting the Commission in the development of model contractual terms for data

[4] The Commission also provided a template for the mandatory reports on the resources of the national competent authorities in July 2025.
[5] The Commission has adopted the Rules to establish a Scientific Panel and launched a Call for Expression of interest to select experts. Moreover, my services have also launched a Call for expression of interest to join the AI Act Advisory Forum.

sharing and standard contractual clauses for cloud computing contracts which must help companies implement the Data Act provisions. This expert workstream also served to further engage with stakeholders on the Data Act through six public webinars.

On the occasion of the entry into application of the Data Act on 12 September 2025, the Commission also pledged to set up a dedicated Data Act Legal Helpdesk to give companies direct assistance with questions on how to implement the new measures, as well as to provide guidance on the use of data when it comes to protecting trade secrets.

Further, the Commission continued to facilitate Member States' implementation of the Data Act through the **European Data Innovation Board (EDIB).** Through the EDIB, the Commission supports the work of national competent authorities implementing the Data Governance Act and the Data Act, ensuring a harmonised approach to specific issues such as penalties for infringements. The Commission services also sought EDIB's opinion on the draft guidelines due to be adopted on reasonable compensation of data holders for making data available under the Data Act (Article 42).

Media freedom and pluralism

The **European Media Freedom Act (EMFA)** implementation and enforcement, together with the ongoing evaluation of the **Audiovisual Media Services Directive**, forms an integral part of integrated efforts to ensure a European approach to media that recognizes their unique place in our democracies and cultures, while fostering their commercial development.

Together with Commissioner Mcgrath, we have engaged and assisted Member States to facilitate implementation of the EMFA, which entered into application in August 2025.

EMFA contains important provisions aimed at fostering the sustainability and resilience of the media sector such as those aimed to ensure access to audiences to their media content on user interfaces and transparency in audience measurement. It includes mechanisms to improve the cross border enforcement of the media content rules under the Audiovisual Media Services Directive (currently under evaluation), crucial to ensure a coordinated approach to protecting audiences, in particular minors, from harmful content across the EU, complementing the DSA enforcement it contains safeguards against unwarranted removal or restriction of legitimate media content by very large online platforms, the implementation of which may feed into DSA enforcement and will be important to foster media plurality and freedom of expression in the digital environment.

.Electronic Identity

As regards the **EU Digital Identity Regulation**, the Commission is advancing in a structured and coherent manner with the legal and technical steps needed for the timely implementation of the framework, not least for the making available of EU Digital Identity Wallets (EUDI wallets) to all EU citizens and residents by the end of 2026. The Commission has adopted 25 implementing acts harmonising standards, requirements and technical specifications governing the EUDI Wallets and trust services at national level. Of these, 16 implementing acts have been published in the Official Journal of the EU, while the remaining ones are expected to be published in the autumn. Additional implementing acts mostly focusing on trust services remain to be adopted in 2025 and 2026 to finalise this work[6].

Over the reporting period, the Commission has also worked with Member States in the European Digital Identity Cooperation Group to develop the Architecture and Reference Framework needed to ensure the technical implementation of the EUDI Wallets. The Cooperation Group is an advisory group that notably supports the implementation of the EU Digital Identity Wallets, notified electronic identification means, and trust services.

Cybersecurity

I held my second **Implementation Dialogue on Cybersecurity Policy** on 15 September 2025. A broad range of stakeholders shared feedback on implementation and simplification of cybersecurity rules. A lesson is the importance of simplifying regulatory compliance, reducing the documentation burden, while promoting innovation and maintaining robust security standards. Representatives from all sectors, including SMEs, also emphasised the need

[6] Note that the European Data Protection Supervisor has given its opinion on the implementing acts to ensure data protection under the GDPR Regulation (EU) 2016/679, which is applicable to data processing activities under the EUID Regulation.

for clear, harmonised legislation and consistent implementation. In particular, industry representatives underlined the importance of simplifying incident reporting processes and aligning timelines to achieve greater synergies between cybersecurity rules. The need for more investment in cybersecurity capabilities and cyber skills in Europe, as well as the need for more strategic information sharing were also highlighted. I emphasised my commitment to simplifying the cybersecurity rules, particularly for SMEs, and to improving cyber skills. I also highlighted that it is essential to maintain a balance between security and innovation. The participants' feedback will inform the simplification initiatives planned for later this year, in particular the Digital Omnibus and the revision of the Cybersecurity Act (see also Section A. Simplification, above).

Member States had to transpose the **Directive on measures for a high common level of cybersecurity across the Union (NIS2)** by 17 October 2024, which aims to increase the EU common level of cybersecurity across 18 critical sectors, sets clearer rules for cybersecurity risk-management and incident reporting, and stronger supervision tools. Building on Commission initial implementation work[7] and to further facilitate the implementation of NIS2, the European Union Agency for Cybersecurity ENISA published additional Technical Implementation Guidance in June 2025, developed together with Member States and in consultation with stakeholders. Moreover, my services have been supporting Member States in their transposition efforts, through the NIS Cooperation Group or on a bilateral basis. They also discussed NIS2 implementation with industry in conferences and workshops or bilaterally[8]. These discussions have also provided useful feedback for the ongoing simplification exercise. The Commission has been also exchanging with the Member States that had transposed NIS2 by way of questionnaires and country visits to understand better the implementation and effects of the newly adopted national laws on the ground[9].

The Cyber Resilience Act (CRA) is the first horizontal legislation for the cybersecurity of products globally. It aims to increase the level of cybersecurity of software and hardware products circulating on the internal market by introducing horizontal cybersecurity requirements. While its main obligations will start to apply in 2027, the Commission has already been engaging widely with Member States, industry and other stakeholders to prepare its implementation and provide legal certainty to economic operators. In February 2025, the Commission has asked European standardisation organisations to develop harmonised standards that will facilitate compliance by businesses. The Commission also set up an Expert Group on Cybersecurity of Products with Digital Elements, involving private sector and Member States experts, to assist and advise on the implementation of the CRA, including the preparation of guidance documents, implementing and delegated acts. The Commission is also cooperating with ENISA for the setup of the single reporting platform for vulnerabilities provided for in the CRA.

The **Cybersecurity Act (CSA)** contributes to enhancing supply chain security by establishing a European cybersecurity certification framework. European cybersecurity certification schemes provide an important tool for businesses to meet their obligations under the CSA. The first European cybersecurity certification scheme based on the widely used international standards of Common Criteria (EUCC) adopted in 2024 has been available to manufacturers since February 2025. First conformity assessment bodies have been accredited and certificates issued. The Commission is working in close cooperation with ENISA and Member States to facilitate the implementation of the scheme and ensure its maintenance, including by updating the implementing regulation to ensure that it reflects state-of-the art requirements, and by adopting implementing acts specifying the governance of the certification framework, such as the notification of conformity assessment bodies. The Commission has asked ENISA to work on other certification schemes[10].

The EU has supported the implementation of EU cybersecurity legislation (such as NIS2, CRA) with funding for public administrations and SMEs under the Digital Europe Programme and its Cybersecurity Work Programme 2023-2024. Overall, EUR 80 million have been made available through Calls for Proposals managed by the European

[7] See Implementing Regulation (EU) 2024/2690.

[8] This, besides earlier Commission Guidelines adopted as Commission Communications (Communication from the Commission – Commission Guidelines on the application of Article 4 (1) and (2) of Directive (EU) 2022/2555 (NIS 2 Directive) and Communication from the Commission – Commission Guidelines on the application of Article 3(4) of Directive (EU) 2022/2555 (NIS 2 Directive)).

[9] Note that the strengthening and streamlining of cybersecurity of the Union entities entered in the practical phase associated to the implementation of the Regulation on laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union.

[10] Including a candidate scheme for ID Wallets, as well as a candidate scheme for Managed Security Services to support the implementation of the EU Cybersecurity Reserve under the Cyber Solidarity Act.

Cybersecurity Competence Centre. As an illustration, a EUR 22 million project was funded to bring capacities of European SMEs in line with CRA requirements and obligations[11].

Digitalisation and the Interoperable Europe Act[12]

Digital-ready policymaking considers digital aspects from the start of the policy cycle to ensure that it is future-proof, interoperable. It also contributes to more effective implementation by ensuring legislation can be readily supported by interoperable digital means. The Commission adopted a number of proposals for EU legislation building on the digital-ready policymaking principles over the reporting period[13].

In order to ensure a harmonised approach and to support the implementation of interoperability regulatory sandboxes under the **Interoperable Europe Act**, the Commission adopted an Implementing Act on 17 July 2025, laying down rules for the establishment and the operation of the interoperability regulatory sandboxes. This contribution focused on reducing administrative burden and clarifying entry criteria, making the sandbox process more accessible and efficient for innovators. Article 9 of the Interoperable Europe Act mandates the Commission to establish an interoperability regulatory sandbox to reinforce policy implementation support projects, if requested by the Board. My services have started to define the processes to set up projects to support public sector bodies in the digital implementation of Union policies ensuring the cross-border interoperability of trans-European digital public services (policy implementation support project), thus contributing to a smooth and transparent implementation process.

The Cyber Solidarity Act (CySol), which entered into force in February 2025, aims to improve preparedness, detection and response to significant and large-scale cybersecurity incidents across the Union. Implementation of its Cybersecurity Emergency Mechanism has started: the first services for the EU Cybersecurity Reserve have been procured[14], and a first call for proposals for the coordinated preparedness testing action is planned for autumn 2025. Moreover, the first Cross Border Cyber Hubs, which form part of CySol's European Cybersecurity Alert System, are being established.

C. Enforcement

Most important infringement procedures

Over the reporting period the Commission did not shy away from enforcement action whenever appropriate[15]. In May 2025 the Commission decided to refer five Member States (Czechia, Spain, Cyprus, Poland and Portugal) to Court due to missing appointment and empowerment of Digital Services Coordinators, which are essential to enable the supervision and enforcement of the Digital Services Act. Such enforcement puts pressure on Member States to put in place a coherent and efficient regulatory system enabling citizens and business to reap full benefits of the DSA. As Belgium, Luxembourg, the Netherlands and Sweden have nominated and empowered Digital Services Coordinators the Commission has closed the respective infringement cases.

In May 2025 the Commission decided to send reasoned opinions to 19 Member States as they had failed to notify on time the full transposition of the NIS2 Directive. The objective is that Member States enhance the EU's overall cybersecurity resilience and to strengthen the management and supervisory measures for a broader range of critical sectors and digital providers.

Rulings of the Court of Justice and sanctions paid by Member States for failing to comply with EU law

[11] Other projects focused on activities such as: implementation, validation, piloting and deployment of technologies; collaboration, communication, awareness-raising activities, knowledge exchange and training; ensuring coherent cybersecurity frameworks, facilitating compliance for hardware and software producers; support to Cybersecurity certification.

[12] Regulation (EU) 2024/903 of the European Parliament and of the Council of 13 March 2024 laying down measures for a high level of public sector interoperability across the Union.

[13] Cf. the February 2025 Commission Proposal for a Regulation amending Regulation (EU) 2023/956 as regards simplifying and strengthening the carbon border adjustment mechanism, or the April 2025 Proposal for a Directive of the European Parliament and of the Council on the conservation and sustainable use of marine biological diversity of areas beyond national jurisdiction.

[14] Under the Digital Europe Programme (DEP) Work Programme 2025-2027 adopted in March 2025.

[15] For more information, a Public Register illustrates the Commission's enforcement activities and Member States' compliance with EU law in general through interactive maps and customisable graphs.

In May 2025 the Court of Justice handed down judgements in eight cases where Member States had failed to transpose the directives on time concerning the Directive on Copyright in the Digital Single Market (in Bulgaria, Denmark and Portugal), the SatCab II Directive (in Bulgaria) and the Open Data Directive (in Belgium, Bulgaria, Latvia and Netherlands). The Court of Justice found the Member States failed to notify the complete transposition of the abovementioned directives and imposed financial sanctions, as requested by the Commission, in an aggregate amount of EUR 19 350 000.

By a 2024 judgment of the Court on 29 February 2024 in case C-679/22, Ireland had been condemned to pay financial penalties due to its failure to transpose and communicate transposition measures for the amended Audiovisual Media Services Directive. Ireland notified the remaining transposing measures and paid the last penalty payment on 30 January 2025. In this light, the case was closed on 7 May 2025.

Follow-up to complaints

On 26 June 2025 the Commission closed 153 complaints concerning the French decree and underlying law imposing a minimum delivery fee to be charged on the online sale of books being delivered in France[16]. This follows the preliminary ruling request submitted by the French Conseil d'État (case C-366/24). The judgement of the Court of Justice is expected to provide the necessary legal certainty on the compatibility of the said decree with EU law.

Enforcement of the DSA and DMA

The **Digital Services Act (DSA) and the Digital Markets Act (DMA) conferred upon the Commission new powers**: to take action when platforms and market participants do not respect the law.

In relation to the DSA, the Commission's enforcement actions this year have already had a positive impact for consumers and businesses alike, for example, ensuring the protection of minors online, creating a safe level playing field for online traders on online marketplaces, and safeguarding the integrity of elections.

On 27 May, the Commission opened investigations against four platforms offering pornographic content, concerning their DSA obligations on the protection of minors, including the issue of age verification mechanisms.

The DSA also requires providers of online platforms offering services to users in the Union to assess and mitigate risks linked to illegal products and goods, improve traceability of traders and enhance transparency in online advertising content in their recommender systems.

On 18 June, the Commission accepted a series of binding commitments by AliExpress concerning, among other things, their moderation and monitoring systems, their advertising and recommender system transparency, and the traceability of their traders. At the same time, the Commission also preliminarily found AliExpress in breach of their DSA obligations to devote sufficient resources to their moderation systems and its enforcement against malicious traders.

Similarly, on 28 July, the Commission also found Temu in breach of the DSA in relation to the requirement to properly assess the risks of illegal product dissemination on their marketplace. The Commission's investigation of Temu is a good example of coordinated investigations in cooperation with Digital Services Coordinators, customs authorities, market surveillance authorities, which proceeded in parallel to a separate investigation by the Consumer Protection Cooperation Network. The Commission has also cooperated with the Consumer Protection Cooperation Network in its enforcement actions against Shein. This coordinated approach followed the February 2025 **E-commerce Communication**, in which the Commission outlined its goal to create a safer market for consumers, using all tools in its regulatory toolbox to address the hazards and harms stemming from the exponential increase of low-value imports sold directly to EU consumers from third-country markets, in particular, when those goods are non-compliant with EU requirements. The Communication presented a cohesive and coordinated enforcement strategy across customs rules, market surveillance and consumer protection rules, as well as digital rules, in particular the DSA[17].

The Digital Markets Act (DMA), one of the first comprehensive regulations targeting the power of major digital companies, including large digital platforms offering core services like search engines, app stores, and messenger services, is designed to protect contestability and fairness in digital markets and thereby enable innovation and choice. The Commission's enforcement actions under the DMA has already led to positive results for users' choice, for example by enabling data portability, interoperability, as well as enabling uninstalling of software applications

[16] The Commission had issued a formal reaction to the notification of the draft decree under Directive (EU) 2015/1535 and had formally intervened to the proceedings before the CJEU.
[17] A report on the results of the strategy is planned for 2026.

and changing default settings. As an illustration, in April 2025, the Commission found Apple and Meta in breach of the DMA concerning the Apple App Store anti-steering measures (practices used by platform owners or intermediaries to prevent their business users from directing their customers to cheaper or alternative offers, outside of the platform's control) and Meta's 'consent or pay' model respectively and fined them EUR 500 million and EUR 200 million respectively.

4. Way forward

The proposal for a Digital Omnibus will be an important first step to cut red tape for businesses and to support a competitive single market. Simplification will remain a key priority. The Commission will continue the engaged open dialogue with the European Parliament and the Council as we progress in stress-testing over the next years how our rules support Europe's competitiveness and security priorities, but also how they open opportunities for the well-being of our society. Already at the end of 2025, the Commission's services will start conducting a Digital Fitness Check for the digital acquis, consulting broadly and expecting to conclude mid-term with potentially further simplification measures. In 2026, notably, the Digital Decade Policy Programme will go through an assessment and the evaluations will be done for example for the Audiovisual Media Services Directive and the Copyright in the Digital Single Market Directive. Based on all these activities, the Commission will consider which further simplification measures are necessary.

The Commission is also scaling up its capacity to give direct assistance in the application of the digital rules. To further help with the implementation of the AI Act, the Commission plans to launch the AI Act Service Desk in October 2025, a central information hub on the AI Act allowing stakeholders to ask for help and receive tailor-made answers. This initiative will provide straightforward and free access to information and guidance on the applicable regulatory framework, which will particularly serve the needs of smaller AI solution providers and deployers. The answers will consist of practical advice that will help understand and comply with the AI Act. The AI Act Service Desk will be provided by a dedicated team in DG CONNECT's AI Office, supported by a contractor to handle incoming requests. It will offer an interactive platform where businesses and other stakeholders, including public authorities, will be able to ask questions, get answers and have access to technical tools to help them apply the AI Act, e.g. decision trees and other self-assessment tools.

Annex: examples

1. General-Purpose AI Code of Practice

The general-purpose AI Code of Practice (Code) is a voluntary tool for helping providers of general-purpose AI (GPAI) models meet their transparency, copyright and systemic-risk obligations under the AI Act. Published on 10 July 2025, the Code offers a voluntary compliance pathway that is assessed as an adequate means of demonstrating compliance with the AI Act by the Commission and Member States.

The Code was developed in a unique co-regulatory process, drafted by independent experts in a multi-stakeholder process that was steered and facilitated by the Commission:

- **Open call and large-scale engagement.** In July 2024, the AI Office (DG CONNECT) opened a call for participation. A kick-off in September 2024 brought together almost 1 000 representatives from GPAI model providers, downstream AI users, industry bodies, civil-society groups, rights-holders, academia and independent experts. Including stakeholders across all fields helped ensure that decisions that were taken in this process are socially grounded and legitimate.
- **Independent technical experts to develop the Code.** The Commission appointed 13 independent Chairs and Vice-Chairs and organised four thematic working groups that developed the Code based on stakeholder input. Chairs worked across four iterative drafting rounds (first draft November 2024; fourth and final draft July 2025), with the Commission publishing the draft at each stage.
- **Continuous stakeholder input.** Working group meetings for all stakeholders in a plenary and dedicated workshops for GPAI providers followed each draft. Specific workshops for civil society organisations and downstream providers were added after the third draft. Written comments were accepted for at least two weeks after every working-group meeting, ensuring continuous stakeholder input.
- **Member-State and parliamentary oversight.** The AI Board (made up of Member State representatives) and the European Parliament were briefed throughout. Observers from international agencies attended plenaries, bolstering legitimacy and coherence with global AI-safety initiatives.

The AI Office coordinated agendas, published minutes, hosted online collaboration tools and maintained a public webpage archiving drafts, meeting slides and Q&As, facilitating scrutiny by stakeholders and media, which ensured the overall transparency of the overall process.

2. Collaboration among national authorities and the Commission in the Working Groups of the European Board for Digital Services

The European Board for Digital Services, composed of the Member States' Digital Services Coordinators (DSCs) and chaired by the European Commission, is a cornerstone for the consistent application of the Digital Services Act. It has set up eight Working Groups, each dedicated to a specific aspect of the Digital Services Act (DSA), to facilitate the collaboration among DSCs and with the Commission.

As an illustration, the Board's Working group 5 (Consumer Protection and Online Marketplaces) ("WG 5") serves as a forum for discussions, sharing of expertise and information both from the Commission's side and the DSCs on various topics: e.g. presentation of best practices of cooperation between various authorities at the Member State level – national e-commerce task forces, delimitation between the DSA and the consumer protection acquis, interplay between General Product Safety Regulation (GPSR) and DSA. Members from the Consumer Protection Cooperation Network regularly participate in WG 5 meetings.

WG5 has established two workstreams composed of experts: the first one focuses on developing a common approach for Member States to map and outline the responsibilities of each relevant national authority in the field of e-commerce. Such mapping should be the first step in establishing cross-sectoral cooperation through e-commerce task forces at national level. Except for Digital Services Coordinators it should include consumer protection, market surveillance and custom authorities. The members of the workstream have already started to draft guidelines/handbook reflecting a shared understanding and a consistent approach, and the result of this mapping exercise in Member States is foreseen before the end of the year 2025. The second WG5 workstream on

online financial scams specifically focuses on identifying scam patterns, sharing Member State's enforcement approaches, strengthening responses across platforms and assess ways of deepening the EU-wide coordination in this topic.

Another example is the working group on protection of minors. Following the publication of the draft Guidelines of the Commission on protection of minors online, the Board launched a coordinated action to protect minors as regards pornographic platforms and assigned this task to Working Group 6 (Protection of minors). This coordinated action seeks to ensure that minors are protected from pornographic content also beyond very large online platforms.

3. 'DSA officers' in Member States

In the context of the implementation and enforcement of the Digital Services Act vis-à-vis very large online platforms and very large online marketplaces, the Commission has placed 'DSA officers' in all Commission Representations in the Member States' capitals. This is to ensure that enforcement is consistent, close to the citizen and well-coordinated with different sector-specific authorities. For instance, as announced in its E-commerce Communication of February 2025, the Commission, via those DSA officers, has supported the creation by Member States of e-commerce task forces including DSCs, the consumer protection, market surveillance and customs authorities.

4. Implementing and promoting interoperability under the Interoperable Europe Act

With the help of the Commission, the Interoperable Europe Board adopted comprehensive **Guidelines** on interoperability assessments, in line with the Interoperable Europe Act (IEA). These guidelines explain when an interoperability assessment is mandatory under the IEA, indicate key elements to consider, and outline various ways to perform these. The Guidelines also provide information on how stakeholders can contribute to the further development of these guidelines.

To promote the sharing and reuse of interoperability solutions across Union entities and public sector bodies, the Commission has published a **catalogue of open source software solutions** of public administrations on the Interoperable Europe Portal. This valuable resource for developers, organisations, and individuals encourages the adoption of open-source software, which can lead to cost-effective, efficient, and collaborative solutions.

In keeping with the IEA, the Commission launched the **Interoperable Europe Community** in May 2025, which provides a common space for public and private stakeholders, to co-create, exchange knowledge, and contribute to the practical implementation of interoperability across the EU, driven by real-world experience and collective expertise. In line with the IEA, the Community also supports the Interoperable Europe Board by providing input to guide its strategic decisions on cross-border digital public services.

5. Code of Conduct on disinformation under the DSA

In 2018, the Code of Practice on Disinformation was announced – marking the first time worldwide that industry agreed, on a voluntary basis, to self-regulatory standards to fight disinformation[18]. The Code was further strengthened in 2022. In February 2025, the Commission and the European Board for Digital Services endorsed the official integration of the voluntary Code of Conduct on Disinformation into the framework of the Digital Services Act (DSA) from 1 July 2025 onwards. A substantial number of signatories – 42 to date – have signed the Code, including major online platforms (e.g. Google, Meta, Microsoft and TikTok).

The Code of Conduct contains a broad range of commitments made by major online platforms and other players to fight **disinformation** with measures such as demonetising the dissemination of disinformation, addressing manipulative behaviours, empowering users and fact-checking.

A hallmark of the Code is the implementation by signatories of the Rapid Response System for elections, which allows non-platform signatories to swiftly report time-sensitive content, accounts or trends that they view as threats to the integrity of elections. This system was used for example for the 2024 European elections, the German elections in February 2025, the 2025 Polish elections. It was finalised in 2025 and will be activated by default for all national elections in EU Member States.

[18] https://digital-strategy.ec.europa.eu/en/library/code-conduct-disinformation

The Code of Conduct is expected to play an important role in the wider system of enforcement under the DSA, contributing to its practical application, and particularly serving as a relevant benchmark for DSA implementation when it comes to risks related to disinformation.

From 1 July 2025 onwards, the commitments made by the signatories designated as VLOPs and VLOSEs must be assessed at least once a year via independent audits.

12