



2026 **ANNUAL PROGRESS REPORT**

Simplification, Implementation & Enforcement

Henna Virkkunen

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



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 strengthening competitiveness, resilience and strategic autonomy in a fast-changing digital world. My priorities include: overseeing the path towards reaching Europe's 2030 Digital Decade targets; boosting Artificial Intelligence application and innovation, high performance computing and quantum; supporting innovation, strategic industry segments and equipment manufacturing for semiconductors; 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 cybersecurity rules; deploying digital public infrastructure, e.g. the EU wallets; advancing Europe's digital sovereignty and interoperability through secure, interoperable digital public services; 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, implementation and enforcement across my portfolio over the period from 1 August 2025 to 31 July 2026, in line with my Mission Letter¹.

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, as well as to ensure its implementation and maintain its enforcement effectively.

To guarantee the most optimal effect of our rules, we are continuously stress-testing them and evaluating their functioning in practice. With this objective in mind the Commission has put forward a Digital Simplification Package, including two legislative (omnibus) proposals, which provide a clear path for developing responsible AI in Europe, as well as measures to simplify compliance and interactions between businesses and administrations (European Business Wallets). The Commission also proposed legislation to set up a single market for connectivity (Digital Networks Act), and to enable a genuine European cloud ecosystem (Cloud and AI Development Act).

In the meantime, significant efforts have been put into effective implementation and enforcement of Europe's digital rulebook, a priority for the Commission. For instance, we have been very active with Member States to ensure their alignment with the European Media Freedom Act; we have set up the AI Act Service Desk and the Data Act Legal Helpdesk to help public authorities and other stakeholders understand and comply with the applicable requirements. We have also provided guidance in several areas to facilitate implementation. Further, the Commission took enforcement action against specific online platforms, including non-compliance decisions under the Digital Services Act and the Digital Markets Act, inter alia to ensure the protection of minors online, the safety or fairness of online market places. When Member States were too late in making EU rules effective at national level, the Commission took enforcement action where appropriate, as in the case of cybersecurity legislation.

3. Delivering Results: Key Measures

A. Simplification and costs savings

The **European Union's digital rulebook pursues a double objective**. We have set the rules of the game for fair markets and put in place measures to encourage innovative home-grown companies. Importantly, we have also made our online spaces safer for citizens and created trust in our products. To ensure their most optimal effect, it is also important to continuously stress-test rules, and assess their functioning in practice. The **'regulatory deep cleaning'** of the digital rules, announced in the [Communication on Better Regulation and Enforcement](#), is a cornerstone priority for the Commission towards that simplification objective.

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

On 19 November 2025, and following extensive consultations², the Commission put forward two legislative proposals as part of the [Digital Simplification Package](#): an [AI Omnibus](#), and a [Digital Omnibus](#). The Commission estimates that €1.2 billion administrative cost savings could be made each year with the proposed measures³, on top of additional one-off savings. This would amount to at least €5 billion in overall cost savings by 2029, provided the measures are adopted as proposed and not diminished in their ambition during negotiations. The proposals deliver on fundamental pillars of our digital competitiveness: artificial intelligence, data and cyber security. In doing so, they also put particular emphasis on supporting small and medium-sized enterprises (SMEs) and small mid-caps (SMCs), which too often face a disproportionate share of regulatory burden.

The **AI Omnibus** entered into force on 27 July 2026. It introduces targeted amendments to support a clearer, more effective and innovation-friendly implementation of the AI Act, while preserving its core objectives of protecting health, safety, and fundamental rights. It streamlines procedures, clarifying the interplay of AI rules with sectoral legislation and postponing the application of high-risk rules on AI to 2 December 2027 for stand-alone high-risk AI systems, and 2 August 2028 for high-risk AI systems embedded in products in order to better align with the delivery of harmonised standards. It also strengthens support for SMEs and SMCs, and improves access to regulatory sandboxes and real-world testing. Finally, it bolsters protections where it is needed the most. The agreement also includes a targeted prohibition of AI systems generating non-consensual intimate content and child sexual abuse material. This is an important response to harmful uses of AI.

My objective is clear: set a path for the development of responsible AI in Europe, in line with our values and protection of fundamental rights. To do so, we cannot be dependent on third countries. This is why the AI Omnibus is intrinsically linked to the Digital Omnibus. By simplifying our data rules, we support the innovation capacity of our European industry and provide for ourselves the means to spearhead AI development in the EU. This simplification drive, in complement to the [Tech Sovereignty Package](#) adopted by the Commission in June 2026, is one of the keys towards achieving digital sovereignty.

The **Digital Omnibus** makes significant progress in building a resilient AI and digital economy in the EU. First, the Commission proposed to consolidate four legal instruments⁴ into one (the Data Act) – to streamline the application of our rules, in particular for our start-ups and scale-ups, and unlock the full potential of data sharing. Second, the Commission proposed targeted amendments to the General Data Protection Regulation (GDPR), to increase legal certainty for our European businesses to be able to train AI. As technologies – notably artificial intelligence – have evolved, it is crucial to ensure a more harmonised framework for the application of data protection rules across the EU. The changes reduce burden for smaller operators, and provide for more legal certainty on important notions such as the use of pseudonymised data. These are fundamental elements to reach an agreement upon.

Data shared in Europe means AI made in Europe. This will unleash Europe's potential for AI innovation, by facilitating data use for AI training.

In addition to these necessary changes to our data rulebook, **the Digital Omnibus also proposes to simplify compliance in other areas of our acquis:** significantly streamlining incident reporting obligations under five EU legal acts (NIS2, DORA, CER, GDPR and eIDAS) by channelling the reports through a Single-Entry Point, simplifying cookie rules for European consumers, as well as repealing the Platform-to-Business Regulation in two steps, in view of streamlining our platforms legislation.

In line with the '**One Europe One Market Roadmap**'⁵ of the European Parliament, the Council and the Commission, it is crucial to maintain a clear course for ambitious digital simplification. We must collectively deliver on these important changes for our rulebook. In keeping with stakeholder feedback received after the adoption of the Commission's [proposal](#), I am resolute in making the necessary efforts to make our continent more competitive – and face the challenges ahead of us.

² Several calls for evidence and public consultations were conducted across 2025 on the different parts of the proposal. In addition, five reality checks were organised with stakeholders in September 2025, as well as a specific consultation with European SMEs.

³ See [here](#)

⁴ The Free-Flow of Non-Personal Data Regulation (Regulation (EU) 2018/1807), the Open Data Directive (Directive (EU) 2019/1024), the Data Governance Act (Regulation (EU) 2022/868), and the Data Act (Regulation (EU) 2023/2854).

⁵ Available [here](#)

Simplification does not only translate through Omnibus proposals. The Commission is committed to delivering on a **“simple-by-design” approach**, across all new legislation.

The **European Business Wallets** legislative [proposal](#), adopted on 19 November 2025, is a reflection of this. Building on the EU Digital Identity Framework, the initiative provides for a new digital solution that will allow businesses to prove their identity, hold documents and exchange verified business data quickly and securely throughout the single market without having to navigate a maze of varying systems and repeated paperwork. Much like the EU Digital Identity Wallets provide citizens with a single, trusted way to manage their personal identity online, the Business Wallets will do the same for economic operators: a single digital tool with the same legal effect everywhere in the EU, simplifying significantly reporting, Know-Your-Customer obligations, supply chain management and public procurement to mention some. The Business Wallets could also provide the foundation for companies to fully automatise interactions with public authorities through the use of AI. The Commission estimates that the Business Wallet could unlock at least €160 billion in savings for businesses each year. This is a considerable and tangible dividend for European competitiveness, in particular SMEs. The file has, since its adoption by the Commission, moved through the legislative process at pace – with the Council notably agreeing on its general approach on 9 June 2026, and discussions advancing at speed in the European Parliament. This is an important development and a clear illustration of how simplification, digitisation and competitiveness can reinforce one another in practice.

“Simple-by-design” also includes ensuring the effective implementation of the **Interoperable Europe Act**⁶, which is essential to improve cross-border digital public services, support seamless data exchange between public administrations, and reduce fragmentation in the Digital Single Market. In this regard, the Interoperable Europe Act provides an important foundation, as its implementation supports the cross-border interoperability of public sector systems that is necessary for solutions such as the European Business Wallets to function effectively across the Union.

Building on this approach, the Commission has also made simplification proposals in three important areas of our digital rulebook, particularly relevant for technological sovereignty: telecoms, cybersecurity and cloud. On telecoms, the Commission adopted in January 2026 the [Digital Networks Act](#) proposal. As part of an ambitious simplification drive aimed at streamlining existing reporting duties and administrative burden, the proposal merges four legal acts into one directly applicable Regulation, replacing the [European Electronic Communications Code \(EECC\)](#), the [BEREC Regulation](#), the [Radio Spectrum Policy Programme](#) as well as core parts of the [Open Internet Regulation](#). The objective is to foster the Single Market by making digital connectivity rules more consistent across EU countries, reduce fragmentation by harmonising spectrum management, access rules and investment conditions, and ultimately create a more integrated EU market for electronic communications networks and services. On cybersecurity, the Commission adopted in January 2026 its proposal for the [revision of the Cybersecurity Act](#) – with important simplification of our European cybersecurity certification framework, and eased compliance for SMEs and SMCs. The Commission estimates that the proposed measures through this revision would save more than €514 million in administrative costs. Negotiations are progressing on both files; I encourage the co-legislators to reach a political agreement as soon as possible – to deliver clear change, and reinforce our Single Market.

In the context of the recently adopted Tech Sovereignty package – that identifies simplification as one of the key horizontal enablers for technological sovereignty, the proposal for a **Cloud and AI Development Act (CADA)** is designed as an enabling legislation for Europe’s cloud and AI ecosystem. CADA simplifies and harmonises investment conditions for data centres by streamlining procedures to develop sustainable projects and improving access to key resources. This gives operators greater predictability to deploy capacity where it is most needed, while remaining aligned with Europe’s climate commitments. The proposal also establishes a Union-wide sovereignty framework to make it easier for public buyers to understand, compare and procure sovereign cloud and AI computing services. As negotiations begin, preserving this enabling role will be essential to strengthen Europe’s resilience and strategic autonomy.

Reinforcing our Single Market also means looking ahead. The Commission is preparing a **Digital Fitness Check, stress-testing the complementarity**, efficiency and effectiveness of our digital rules. Its aim is to ensure that the overall system remains fit for the future, looking more specifically into coherence across specific legal notions and definitions, the cumulative impact of rules, governance systems, and potential tools or experimental

⁶ [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 (Interoperable Europe Act).

practices that could further relieve administrative burdens from compliance processes. Following a call for evidence which closed on 11 March 2026, the Commission intends to carry out further consultations and reality checks ahead of finalising the Digital Fitness Check and reporting to Parliament and Council in early 2027. This comprehensive project is complemented by a **series of reviews and evaluations**: the Audiovisual Media Services Directive, the Copyright in the Digital Single Market Directive, the Digital Markets Act, and the Digital Decade Policy Programme.

Finally, I have taken particular effort this year in also assessing the EU's tertiary legislation. It is crucial to address all layers – and even more so the technical ones, where additional burden layers may sometimes materialise. While my services in DG CONNECT initially had 57 delegated and implementing acts planned for 2026, we were able to deprioritise 30 of them. The careful planning of delegated and implementing acts, with due regard to their necessity, impacts and appropriate timing will remain a priority for the Commission, while ensuring that no significant implementation burden is added in the process.

B. Implementation

Media

The European approach to media recognises their unique place in our democracies and cultures, while fostering their independence, resilience, and free movement of services. Implementation and enforcement of the [European Media Freedom Act](#) (EMFA), together with the ongoing review of the [Audiovisual Media Services Directive](#) (AVMSD), constitute integrated efforts towards such an approach. EMFA contains important provisions aimed at fostering the sustainability and resilience of the media sector.

Following the entry into application of most of the EMFA provisions on 8 August 2025⁷, together with Commissioner McGrath, we have continued to closely monitor the alignment of national laws and have engaged with Member States in the process of implementing it within their national frameworks, tailoring the level of engagement to their level of preparedness. This included exchanges in the framework of the Audiovisual and Media Working Party of the Council. Further, in December 2025, the Commission services sent 23 administrative letters to Member States that were not yet aligned with the EMFA.

Moreover, as announced in the European Democracy Shield, we maintained an active dialogue, through bilateral engagements and the European Board for Media Services, with relevant industry players and civil society organisations to ensure that the safeguards and mechanisms provided by the EMFA are effectively applied across the EU.

In addition, the Commission facilitated the application of EMFA, including through the adoption of [Guidelines](#) to facilitate the implementation by very large online platforms (VLOPs) of self-declaration functionality for media service providers.

In May 2026, I held an [Implementation dialogue](#) on the AVMSD with a selected group of 21 representatives from the sector to discuss the achievements and effectiveness of the AVMSD implementation, as well as to discuss suggestions for its review foreseen in the Commission Work Programme 2026. The stakeholders widely agreed on the importance of simplifying and modernising the AVMSD to ensure that it remains effective in today's rapidly evolving media landscape. They notably called for a more level playing field between broadcasters and video-sharing platforms, in particular by modernising advertising rules, signalling that the practices of adding restrictions at national level for broadcasters (e.g. gold-plating) has exacerbated the existing asymmetry. They also called for clearer and more effective rules to ensure the prominence of services of general interest, legal clarity on how the AVMSD applies to influencers and ensuring coherence between the AVMSD and the DSA. The feedback collected aimed to inform the ongoing AVMSD evaluation and review process, planned for the third quarter of 2026, and complemented the public consultation that closed in May 2026.

Artificial Intelligence

On AI Act implementation, [the AI Act Service Desk](#) and [Single Information Platform](#) were launched by the Commission to provide a central point of access for up-to-date information, compliance support and various practical tools to help public authorities and other stakeholders understand and comply with the applicable requirements. In

⁷ In July 2025, in view of the impending date of entry into application of the EMFA on 8 August 2025, together with Commissioner McGrath we sent a package of letters addressed to national ministers responsible for the EMFA implementation in all Member States.

parallel, the Commission continuously supports cooperation between national authorities through the AI Board, to exchange expertise, address implementation questions and promote a coherent approach across the Union. The Commission has also developed [various guidelines](#) on key provisions of the AI Act, among else, on the classification of high-risk AI systems.

Data

To facilitate Data Act compliance and help businesses unlock its full value, the Commission has established practical support mechanisms, including [Guidance on Vehicle Data](#) accompanying the Data Act, and the [Data Act Legal Helpdesk](#), which provides guidance on the application of the Data Act to stakeholders, including businesses. Updated [FAQs](#) about the Data Act, together with [model contractual terms for data sharing and cloud computing](#), are already helping stakeholders make effective use of the new opportunities created by the Data Act, while further guidance on key definitions and reasonable compensation is under preparation. The European Data Innovation Board, chaired by the Commission, continued to support cooperation among competent authorities to promote a harmonised and effective enforcement framework. In parallel, the first pilot projects on automated and trusted data sharing for regulatory reporting were launched, which is paving the way for a more structural reduction of compliance burdens.

Digital Services

The Digital Services Act (DSA) requires designated very large online platforms (VLOPs) and search engines (VLOSEs) to identify, analyse and assess any systemic risks stemming from the design or functioning of their service, including to the exercise of fundamental rights, and to take effective measures to mitigate these risks. It increases transparency in the EU's online environment and empowers users to challenge platforms' content moderation decisions. In just two years, 165 million content moderation decisions have been appealed, and almost 50 million of these were reversed⁸⁹.

The Commission has given particular priority to the protection of minors online. This has been further supported by the Commission's Guidelines on the protection of minors under the DSA and its preliminary findings on age verification. In this context, the Commission published the 2025 [blueprint](#) for a secure and privacy-preserving EU age verification solution, with the feature-complete solution [becoming available](#) for rollout to citizens in April 2026. That same month, the Commission [adopted a recommendation](#) inviting Member States to use the blueprint and prepare implementation plans to enable the deployment of national age verification solutions by 31 December 2026. In February 2026, the Commission organised a [roundtable with civil society organisations](#) to exchange updates on the implementation of the Digital Services Act (DSA).

The Commission has continued its work on developing relevant guidelines under the DSA. In particular, it launched a [targeted consultation on draft guidelines on trusted flaggers](#) in May 2026.

The European Board for Digital Services (EBDS)¹⁰, in cooperation with the Commission, published in November 2025 and July 2026 the first and second reports on the most prominent and recurrent systemic risks and mitigation measures. These reports provide a comprehensive overview of the risk landscape under the DSA, with a specific focus on the protection of minors.

On 17 November 2025, the Commission published a [report](#) underscoring the DSA's interaction with 54 other EU legal acts and assessing the DSA's designation threshold for very large online platforms and search engines. This report showed that, while there are overlaps in the European regulatory landscape, overall, the DSA is highly complementary to other Union legal act²s in ways that are mutually reinforcing.

The Commission's [Delegated Act on Data Access for authorised researchers under the DSA](#) officially entered into force on October 29, 2025. Together with the [Data Access Portal](#), this initiative aims to ensure consistent and predictable standards for vetted researchers across the EU. The aim is to enable unprecedented access to the internal data of VLOPs and VLOSEs to research the systemic risks and the mitigation measures in the European Union, as part of the DSA's all-of-society approach to holding platforms accountable.

⁸ See [here](#)

⁹ Since September 2023, the DSA Transparency Database has made 39,5 billion content moderation decisions visible, <https://transparency.dsa.ec.europa.eu>

¹⁰ In total, the Commission chaired six meetings of the EBDS and 65 working group meetings, during the reporting period.

Digital Markets

During the reporting period, the Commission continued its active programme of implementation of the Digital Markets Act (DMA) across the seven designated gatekeepers.

The [first review of the DMA](#), completed on 27 April 2026, confirmed that the Regulation remains fit for purpose and is already producing positive effects in digital markets. The Commission concluded that no legislative revision is required at this stage, with the focus remaining on effective implementation, simplification efforts, compliance and enforcement.

During its [fifth meeting](#) in December 2025, the [High-Level Group on the Digital Markets Act](#) notably endorsed a joint paper mapping out the regulatory interplay between the DMA and applicable artificial intelligence rules, and proposing enhanced cooperation between competent authorities as regards AI systems developed and deployed by gatekeepers. The Group's thematic sub-groups on data-related obligations, interoperability, and artificial intelligence continued their work throughout the period.

To support the coherent application of the DMA alongside the GDPR, the Commission and the European Data Protection Board launched a targeted consultation on [draft guidelines on the interplay between the DMA and the GDPR](#) in October 2025, which attracted over 100 [contributions](#) from businesses, civil society, and academics. The final guidelines are expected to be adopted in the second half of 2026.

In May 2026, the Commission published its [third annual report on the implementation of the DMA](#), covering activities undertaken in 2025. The Commission also published a [factsheet documenting concrete interoperability and data portability outcomes](#) for smartphone users, illustrating how DMA obligations are translating into practical benefits. In July 2026, the Commission organised [thematic roundtables](#) as part of its ongoing market investigation into the application of the DMA to the cloud sector, bringing together stakeholders who were actively engaged in the investigation, and other experts. The Commission also engaged with the designated gatekeepers on this topic.

The Commission has also continued its close engagement with gatekeepers and stakeholders through regulatory dialogues, and compliance workshops. The Commission was also monitoring how the measures resulting from the two specification decisions concerning Apple are applied in practice, also checking that the deadlines are respected and that the interoperability solutions are effective. These efforts contribute to legal certainty and facilitate effective compliance, while preserving the DMA's ability to address rapidly evolving digital markets.

Cybersecurity

In September 2025, I held an [Implementation Dialogue on Cybersecurity Policy](#). A broad range of stakeholders (23 representatives took part) shared with me feedback on implementation and simplification of cybersecurity rules. They were notably calling for simplifying incident reporting processes to follow the “report once-share with many” principle and achieving greater synergies between the different reporting rules.

The Commission followed up with the [Digital Omnibus Regulation Proposal in November 2025](#), which proposes a single-entry point which would allow incident reporting under five Union acts via one channel. The Commission also proposed the [revision of the Cybersecurity Act](#) and the [accompanying amendments to the NIS2 Directive](#) in January 2026. The package notably aims to simplify and streamline certification processes, critical sectors' demonstration of compliance with the NIS2 Directive cybersecurity risk-management measures, as well as to clarify the scope of the Directive to simplify its implementation.

In the meantime, my services continued to regularly address Member States' questions on the transposition and discuss the practical implementation of the [NIS2 Directive](#) through the NIS Cooperation Group, bilateral meetings, as well as country dialogues and visits with national authorities and relevant entities. Further, Member States' efforts in transposing the NIS2 Directive efficiently and coherently are supported and informed by studies, reports and guidance issued by the European Union Agency for Cybersecurity ([ENISA](#)). My services also support extensively public authorities and industry in implementing the [Cyber Resilience Act \(CRA\)](#), whose main obligations will apply as of December 2027, while reporting obligations apply from September 2026. The Commission also adopted an extensive [package of guidance](#) on the CRA in July 2026 to provide clear and actionable support and make implementation work in practice. My services also continue to engage in a number of fora such as the CRA Expert Group (with Member States and industry), the CRA Administrative cooperation group (with the national market surveillance authorities) and the CRA notifying authorities group (with the national authorities in charge of notifying conformity assessment bodies), as well as through country visits and bilateral engagements.

Chips

During the March 2026 [Implementation Dialogue on the Chips Act](#), I exchanged with 19 stakeholders on the effective implementation of the Chips Act, as well as their recommendations for its revision. On that occasion, high-level representatives shared with me a [report](#) titled '[Industry Blueprint for Semiconductor Sovereignty, Competitiveness and Resilience](#)', authored by the Industry Advisory Group, a working group of the [Industrial Alliance on Processors and Semiconductor Technologies](#). The report argued for a more comprehensive approach to Europe's semiconductor industrial policy, taking into consideration the entire value chain, as well as a more concerted effort between supply-side and demand-side measures, in order for Europe to secure its position in an increasingly strategic and competitive global semiconductor landscape. The dialogue helped inform the preparation of the [Chips Act 2.0 proposal](#) adopted by the Commission in June 2026. As part of the Chips Act 2.0 proposal, the Commission published the evaluation and impact assessment as a [Staff Working Document](#), taking into account the feedback on and experience of implementation of the Chips Act. The proposal for Chips Act 2.0 contains multiple simplification measures, such as the removal of provisions relating to the European Chips Infrastructure Consortium and Design Centres of Excellence and the merger of the Integrated Production Facility ('IPF') and Open EU Foundry ('OEF') status into one status, namely 'European Semiconductor Technology Initiatives'. The clarification of the 'first-of-a-kind' scope further simplifies first-of-a-kind procedures for both Member States and companies.

Interoperable Europe Act

During the reporting period, support continued to be provided to Member States at national, regional and local level focused on facilitating the application of the Interoperable Europe Act and promoting a common interoperability approach across public administrations at European level.

Key measures included the establishment and operationalisation of the [Interoperable Europe governance framework](#), notably the [Interoperable Europe Board](#) and the [Interoperable Europe Community](#), providing a structured forum for cooperation, exchange of experience and coordination among Member States and Union institutions. Support was provided through guidance and practical tools to facilitate the implementation of the Regulation, including preparatory work on [interoperability assessments](#), the promotion of the [European Interoperability Framework \(EIF\)](#), and activities supporting the [identification, sharing and reuse of interoperable solutions](#) through the Interoperable Europe Portal.

The Commission also supported capacity-building by organising awareness-raising activities, workshops, peer learning, expert exchanges and community-building initiatives such as the [Seasonal School](#) aimed at strengthening interoperability knowledge and capabilities across public administrations and focused on the development of common approaches and the promotion of solution reuse awarding the [first Interoperable Europe labels to solutions](#).

In addition, Union funding instruments, including the Digital Europe Programme, supported the set-up of a European Digital Infrastructure Consortium by Member States ([IMPACTS-EDIC](#)), [GovTech initiatives](#), and the development of reusable digital solutions, contributing to the practical implementation of the Interoperable Europe Act and the wider digital transformation of public administrations.

Digital identity

In the reporting period, important progress continued to be made to support Member States' efforts to introduce EU Digital Identity Wallets (EUDIW) for all by the end of 2026, as required by the [European Digital Identity Regulation](#). During the reporting period, the Commission adopted 25 [Implementing Acts](#), establishing a harmonised framework for the development and operation of Wallets, defining common technical specifications, standards, and requirements needed to ensure interoperability, security, and trust across all Wallet solutions in the EU.

The Commission also provided several components to facilitate technical implementation, including an Architecture and Reference Framework developed jointly with Member States' experts; wallet software components and libraries to facilitate national wallet development; and a set of common testing specifications for the functional certification of national wallets.

Implementation progress among Member States remains uneven, reflecting both significant variances in maturity and readiness. Since December 2025, six Member States have shared their draft national certification schemes to the European Digital Identity Cooperation Group (EDICG) to the Commission for comments.

In December 2025, the Commission hosted the first [‘Launchpad’ event](#) bringing together wallet providers, service providers, and Member State administrations for a multi-day testing event. Such testing enables cross-border interoperable use cases. The Commission also supported testing use cases through the two new Large-Scale Pilots funded from the Digital Europe Programme.¹¹

Electronic communications

During the reporting year, the Body of European Regulators for Electronic Communications (BEREC) continued to assist the Commission and the national regulatory authorities (NRAs) in implementing electronic communications rules and other parts of the digital rulebook. Among others, BEREC issued [Guidelines on geographical surveys](#), on [access to in-building infrastructure](#) and on the [co-ordination of civil works](#), which help implement the [Gigabit Infrastructure Act](#). Also, under the Electronic Communications Code, BEREC adopted Guidelines on [retail](#) and [wholesale roaming](#), under the Electronic Communications Code, as well as Guidelines on [Very High Capacity Networks](#).

C. Enforcement

Most important infringement procedures against Member States

Over the reporting period the Commission consistently took enforcement action where appropriate¹². While in some Member States infringements regarding full implementation and enforcement of [the Digital Services Act \(DSA\)](#) have been resolved, leading to [closure](#) of seven out of a total of 13 infringement procedures, the Commission took further steps to ensure that the competent authorities are nominated and fully empowered in all Member States, protecting [user rights](#) granted under the DSA. In particular, following the May 2025 Commission decision to refer five Member States (Cyprus, Czechia, Poland, Portugal and Spain) to the Court of Justice of the European Union (CJEU), Cyprus has since adopted legislation remedying the infringement, which led to [closure](#) of the proceedings in November 2025. For the remaining Member States, [Court cases](#) have been initiated between December 2025 and March 2026 and are ongoing before the CJEU (Spain, ref. C-841/25, Portugal, ref. C-58/26, Poland, ref. C-59/26 and Czechia, ref. C-168/26). Additionally, in April 2026, the Commission opened infringement regarding [Croatia](#), which has not adequately empowered its competent authority with the sanctioning powers set out in the DSA.

The state of play concerning the transposition of Directive (EU) 2022/2555 (**NIS2 Directive**) evolved significantly during the reporting period. By 30 June 2026, 21 Member States who initially had received Letters of formal notice had communicated full transposition. Two Member States communicated partial transposition (Germany and Finland) and four Member States (Ireland, Spain, France and the Netherlands) had still not communicated any transposition measures to the Commission. Therefore, on 8 July 2026 the Commission [decided](#) to refer those four Member States to the CJEU. Eventually, the Netherlands communicated full transposition on 10 July 2026 and on 19 July, France notified partial transposition of the NIS2 Directive.

In December 2025, the Commission opened infringement proceedings against [Hungary](#) for failing to comply with several provisions under the **European Media Freedom Act (EMFA)** and certain requirements under **the Audiovisual Media Services Directive (AVMSD)**, in particular those concerning interference in the work of journalists and media outlets in Hungary, the protection of journalistic sources and confidential communications, as well as requirements relating to public service media, the transparency of media ownership, the assessment of media market concentrations, and the allocation of state advertising. Moreover, the letter referred to certain requirements concerning the independence of national media regulatory authorities under the AVMSD. Discussions are ongoing with the new government on the next steps. Moreover, my service continued to monitor and assess whether Member States are taking all the necessary measures to bring their laws into compliance with the EMFA. Depending on progress, the Commission may decide to step up enforcement actions towards other Member States.

¹¹ Use cases concern e.g. digital travel credentials; smart ticketing and check-in; mobile vehicle registration; banking and payments. The two new Large-Scale Pilots are funded from the Digital Europe Programme for € 23,6m (total funding €47,3m). More than 550 public authorities and private organisations, across 26 Member States, together with Norway, Iceland and Ukraine, are contributing to this effort.

¹² 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 November 2025, the Commission opened infringement proceedings against [Italy](#) as it considered that it had not fulfilled its obligations under the [European Electronic Communications Code](#) and the Framework Directive. In particular, despite longstanding exchanges within the framework of the [Radio Spectrum Policy Group](#), Italy had not yet taken sufficient administrative action to eliminate harmful interference caused by Italian radio broadcasters in the FM (frequency modulation) frequency band (87.5-108 MHz) into France, Croatia, Malta and Slovenia, which prevents the latter's respective broadcasters from using radio spectrum in the FM band for their own FM radio programmes.

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

The CJEU decided on two Hungarian cases important for the digital sector and beyond. In a [judgment](#) of 26 February 2026, the CJEU found that Hungary had failed to fulfil its obligations under EU law, highlighting issues with proportionality, good administration, and freedom of expression in the handling of spectrum assignment to Klubrádió, an analogue FM radio station which had broadcast in Budapest.

In a [judgement](#) of 21 April 2026 in case C-769/22 (Commission v Hungary) the CJEU rejected Hungary's argument that its national identity justified the adoption of laws undermining the Article 2 values of equality and non-discrimination. This landmark judgement regarding the EU's fundamental values such as human dignity, equality, and the rule of law provided for in Article 2 TEU, since the Court recognised that Article 2 TEU, independently of any other specific EU legislation, empowers the Commission and the Court to directly confront systemic, horizontal backsliding on democracy and human rights.

The Commission is proactively monitoring Hungary's compliance with the two judgements.

In the reporting period, Belgium, Bulgaria, Latvia and the Netherlands paid a total amount of EUR 13.250.000, following 2025 judgements of the CJEU imposing financial sanctions in non-communication cases concerning the Open data Directive (EU) 2019/1024 (respectively [C-215/23](#), [C-237/23](#), [C-238/23](#) and [C-213/23](#)). In the same period Bulgaria (cases [C-186/23](#) and [C-198/23](#)) and (Poland (cases [C-212/23](#) and [C-201/23](#)) paid financial sanctions imposed by the Court in two judgements concerning two copyright directives for a total amount of EUR 18.502.187,48.

DSA and DMA enforcement

The **Digital Services Act (DSA)** and the **Digital Markets Act (DMA)** equipped the Commission with new powers to take action when online platforms and online search engines fail to ensure that their services are safe and secure and/or undermine the contestability of digital markets. During the reporting period, the Commission further intensified the supervision and enforcement of the **DSA**, giving particular priority to the protection of minors and the safety of online marketplaces, in addition to other priority areas, such as ensuring election integrity and tackling financial scams and fraud¹³.

During the reporting period, four online platforms have been designated as very large online platforms (VLOPs) and search engines (VLOSEs)¹⁴.

In October 2025, the Commission preliminarily found both TikTok and Meta in breach of their obligations under the DSA to grant researchers adequate access to public data. In December 2025, the Commission adopted the first non-compliance decision under the DSA against [X](#). In this decision, the Commission found that X breached its transparency obligations under the DSA and imposed a fine of €120 million. That same month, the Commission secured [TikTok's commitment](#) to ensure full transparency around advertising on its services.

The protection of minors online is a key enforcement priority under the DSA, including addictive design and its impacts on minors¹⁵. In February 2026, the Commission opened proceedings against [Shein](#) concerning addictive

¹³ In total, since the entry into application of the DSA in 2024, the Commission has formally taken 17 decisions initiating proceedings into the compliance by providers of 12 very large online platforms (VLOPs) and search engines (VLOSEs) with the DSA obligations, adopted preliminary findings in 14 cases, adopted 3 decisions making commitments binding upon the providers concerned and adopted two non-compliance decisions imposing fines. More information is available [here](#).

¹⁴ Note the [designations](#) of ChatGPT, as VLOSE, and of Reddit and Roblox, as VLOPs, in late August 2026.

¹⁵ Addictive design refers to platform features that encourage prolonged use, such as infinite scroll, autoplay, push notification and highly personalised recommender systems.

design, alongside the lack of transparency of recommender systems and the sale of illegal products, including child sexual abuse material. On the basis of its [Guidelines](#) on the Protection of Minors under the DSA, the Commission also issued preliminary findings against [TikTok](#) in February 2026 and [Meta](#) in July 2026 respectively, identifying potential breaches of the DSA linked to addictive design and risks to minors on TikTok, Instagram, and Facebook. Also in July, the Commission sent [TikTok](#) preliminary findings indicating that the account settings available to minors do not ensure the high level of privacy, safety and security required under the DSA.

In March 2026, the Commission preliminary found [Pornhub, Stripchat, XNXX and XVideos](#) in breach of the DSA for failing to institute effective age verification measures, and therefore exposing minors to age-restricted content on their services. Also in March, the Commission launched an investigation into [Snapchat](#)'s compliance with child protection rules under the DSA. In April 2026, the Commission preliminarily found [Meta](#) in breach of the DSA for not doing enough to keep under-13-year-olds off Instagram and Facebook, despite this being a standard the company has committed to in its own terms and conditions. All of these providers can now examine the available evidence and exercise their right to defence.

The Commission also took action to improve the safety of online marketplaces. In May 2026, the Commission issued a fine of €200 million to [Temu](#) after finding that the company failed to diligently identify, analyse, and assess the systemic risks of illegal products being offered on its platform and the resulting harm to consumers in the European Union. In February 2026, the Commission has also opened proceedings against [Shein](#) for its addictive design, the lack of transparency of recommender systems, as well as the sale of illegal products, including child sexual abuse material. In July 2026, the Commission fined [AliExpress](#) €550 million for breaching its obligations under the DSA to diligently assess and mitigate systemic risks linked to the sale of illegal, unsafe or counterfeit products on its platform.

Beyond the protection of minors and marketplace safety, the Commission also addressed other risks. In January 2026, the Commission launched a new investigation into [X](#) regarding its risk management linked to the deployment of Grok's functionalities into X in the EU. The concerns include the spread of illegal content, such as manipulated sexually explicit images.

In January 2026, the Commission designated [WhatsApp](#) as a VLOP under the DSA after its Channels feature exceed the threshold of 45 million average monthly users in the EU.

The [Digital Markets Act \(DMA\)](#) continued to deliver on its objective of ensuring fair and contestable digital markets while providing a clear and harmonised regulatory framework across the Union. It further delivered tangible benefits, including greater user choice, additional innovation opportunities, reduced lock-in, improved interoperability, enhanced data portability and new business opportunities for companies that depend on core platform services to reach customers. Next to implementation efforts, the Commission continued to take targeted enforcement action to ensure that the obligations applicable to designated gatekeepers translate into practical benefits for end users and business users.¹⁶

In 2025, four proceedings under the DMA reached a final stage, comprising two specification decisions and two non-compliance decisions accompanied by fines. In 2026, four additional proceedings under the DMA were completed, comprising two specification decisions and two non-compliance decisions accompanied by fines. There are currently five ongoing [proceedings](#), spanning non-compliance investigations, and market investigations. The Commission also continued the investigation concerning Apple's new business terms during 2025 and 2026 and started market investigations in topical fields such as cloud and AI.

In November 2025, the Commission opened non-compliance [proceedings](#) concerning Google Search's 'Site Reputation Abuse Policy' ('SRAP') for demoting publishers' subdomains when they host third-party commercial content, whereby not allowing fair, reasonable and non-discriminatory (FRAND) access to Google Search.

In the context of the ever-growing relevance of cloud-related services (including for AI), in November 2025, the Commission opened three [market investigations](#) into cloud computing services. Two of the investigations assess whether Amazon and Microsoft should be designated as gatekeepers for their cloud computing services. In relation to these two investigations, on 25 June 2026, the Commission preliminarily [found](#) that Amazon and Microsoft should be designated as gatekeepers for their cloud computing services. The other investigation assesses whether the

¹⁶ More information on the DMA, including cases, is available [here](#).

current obligations under the DMA are effective in addressing practices that limit competitiveness or are unfair in the cloud sector.

In January 2026, the Commission opened two sets of specification proceedings to assist Google in complying with its obligations on Android interoperability for third-party AI service providers and online search data sharing with rival search engines on FRAND terms; preliminary measures on the latter were published in April 2026. In July 2026, the Commission adopted the final decisions in the two sets of specifications. They comprise the measures that Google must implement to ensure effective [interoperability for alternative AI assistants](#) and [the sharing of Google Search data](#) with eligible beneficiaries, including AI chatbots offering search functionalities.

In February 2026, the Commission [found](#) that Apple's online advertising service **Apple Ads** and Apple's online intermediation service **Apple Maps** should not be designated under the Digital Markets Act ('DMA'). The decisions followed Apple's notification of these services on [27 November 2025](#). The Commission continued to monitor market developments regarding these services, should any substantial changes arise.

In July 2026, the Commission adopted [two decisions finding non-compliance](#) by Google for self-preferencing its own services on Google Search, and for putting in place restrictions on businesses to direct consumers to alternative, often cheaper, purchase channels on Google Play (steering). The Commission issued Google a fine of €460 million for the self-preferencing case, and a fine of €430 million for the steering case.

4. Way forward

Over the reporting period, the Commission has proposed major legislative texts to cut red tape for businesses and to support a more competitive, resilient and autonomous single market.

Looking forward, and besides continued enforcement of our digital rulebook, I intend to pursue the thorough regulatory deep cleaning of our horizontal and sectoral digital legislation. The Commission is working on a Digital Fitness Check¹⁷, stress-testing the complementarity, efficiency and effectiveness of our digital rules, with the aim to future-proof the overall digital regulatory system. This comprehensive analysis will build on consultation steps and reality checks, complemented by a series of completed or ongoing evaluations and reviews: the Audiovisual Media Services Directive¹⁸, the Copyright in the Digital Single Market Directive¹⁹, the Digital Markets Act⁴, and the Digital Decade Policy Programme²⁰. It also builds upon existing simplification efforts under the Digital Omnibus, on which it is important to reach a fast and ambitious agreement between the co-legislators. I plan to finalise the Digital Fitness Check and report on this to Parliament and Council in early 2027.

I will be happy to continue to engage with the European Parliament and the Council as we progress on our major regulatory reforms and on our further stress-testing efforts over the next years.

¹⁷ [Digital fitness check – testing the cumulative impact of the EU's digital rules](#)

¹⁸ [Audiovisual Media Services Directive – AVMSD | Shaping Europe's digital future](#)

¹⁹ [Directive - 2019/790 - EN - dsm - EUR-Lex](#)

²⁰ [Digital Decade - Policy programme | Shaping Europe's digital future](#)

Annex: examples

Increasing legal certainty on data use for AI innovation

In the constantly evolving technological environment where AI is and will be used by most people, it is important to clarify in which situations processing of personal data for the development and operation of AI models and systems could be carried out in a lawful manner, in accordance with the requirements of the GDPR.

The [Digital Omnibus](#) proposes therefore to clarify that the processing of personal data for the development and operation of AI models and systems may be carried out for purposes of a legitimate interest, within the meaning of Article 6(1)(f) GDPR. Considering that the development of certain AI systems and AI models may involve the collection of large amounts of data, including personal data and special categories of personal data, the proposal introduces also a narrow exception from the prohibition on processing special categories of personal data for the development and operation of AI. By increasing legal certainty for innovative businesses, the proposed amendments aim to directly contribute to the objective to develop responsible European AI that is trustworthy and non-discriminatory. At the same time, they seek to preserve the European gold-standard of data protection, through clear safeguards.

The Digital Omnibus proposal further clarifies that pseudonymised data would not be personal data for a third party receiving it, if that recipient does not have the means to identify the individual. The proposal also lays out that an entity for which the information is not personal data, in principle, does not fall within the scope of application of the GDPR, for the processing of that data. In practical terms, this would increase legal certainty for operators in situations where pseudonymisation techniques are used and is also likely to encourage a broader uptake of techniques which protect the confidentiality of personal data and reduce the amount of personal data processed.

Simplifying user privacy choices for access to connected devices

The [Digital Omnibus](#) proposes to amend the rules on the access to connected devices ('terminal equipment') in the ePrivacy Directive. The current rules, requiring users' consent as a rule with some exceptions have led to consent fatigue, caused by repetitive, often hard to understand cookie banners. These banners are ineffective for users and businesses alike. Users find it hard to make a choice and understand what their data is being used for. For businesses, the banners cause compliance cost and, due to the limited exceptions to the consent requirement, require to collect users' consent even for low-risk situations – such as ensuring the security of the device or the service used or for creating aggregated information to measure the audience of a service.

The targeted updates thereby serve three simplification elements – delivering key change for both citizens and businesses.

First, the Digital Omnibus amendments make clear that users need to be able to say “no” with a single click instead of having to either manually having to select the choice for each purpose or by clicking through multiple layers. In addition, a rule that prohibits to ask again during six months will help protect users against repetitive requests and will make their choice be respected. The proposal further strengthens users' possibility to set their preferences centrally via machine readable consent signals and for websites and mobile applications to have to respect such signals.

Second, businesses will not have to ask for consent for a limited list of purposes that do not represent high risks. For example, a company placing cookies to create statistics about the use of their website would no longer need to collect consent – thus making the use of a banner redundant. This would especially take away burdens from SMEs that often use such cookies.²¹ These targeted adjustments lead to estimated cost savings of more than €800 million per year.²²

²¹ See [Commission Staff Working Document accompanying the Digital Omnibus Proposal](#) Brussels, 19.11.2025 SWD(2025) 836 final, p. 50.

²² Idem, p. 44-55.

Thirdly, the enforcement of the rules on cookies where personal data are concerned will be subject to the GDPR's rules on enforcement. This will harmonise the interpretation and applicable fines throughout the Union and consistently make the independent national Data Protection authorities competent for enforcing the rules.

Internet of Things data sharing with better protections of trade secrets

The [Data Act](#) mandates sharing of Internet of Things (IoT) data, in view of creating a fairer and more competitive digital economy. Users of connected products have a right to receive data they generate through the use of these products, even if such data represent trade secrets.

The current rules of the Data Act allow data holders to refuse data sharing where they can demonstrate that it is highly likely to suffer serious economic damage from the disclosure of trade secrets. The [Trade Secrets Directive](#) provides additional protection of such know-how. However, there are significant concerns about the potential leakage of trade secrets to entities in third countries, where the Trade Secrets Directive does not apply and where trade secrets may not be subject to an equivalent level of protection.

The [Digital Omnibus](#) addresses the risk of disclosure of trade secrets to third country entities with weaker protections for trade secrets by extending the possibility to refuse data sharing for cases where data holders estimate there is a high risk of unlawful disclosure to entities that are subject to third country jurisdictions with weaker or non-equivalent protection compared to that of the EU. This aims to help prevent trade secrets leakage to third countries which can undermine the competitiveness of, and may cause irreparable harm to, European companies.

By strengthening the protection of trade secrets, the proposal fosters trust in the EU data economy and reinforces legal predictability. The EU's framework serves as a benchmark for data sovereignty, minimising confidentiality breaches and mitigating the risk of data exploitation by third country free riders or the largest global tech companies. These entities may capitalise on weaker legal regimes abroad to improperly access trade secrets, possibly without adequate oversight or repercussions, and thus disadvantage other market players. Thus the amendment is an important element in protecting EU companies' trade secrets and their competitiveness. At the same time, the amendment in the Digital Omnibus maintains the principal policy objective of enabling data sharing and preventing abuse of the trade secrets handbrake. Importantly, EU users and data recipients remain safeguarded under the proposed rule, as the existing mechanism, including the need for data holders to substantiate refusals and notify competent authorities, remains intact. This ensures the Data Act's balance is maintained and its policy objectives can be fully achieved.

Compliance automation

We support the development of Compliance Automation solutions by funding research and innovation projects that help organisations comply with EU data and digital legislation more efficiently by exploring technologies such as machine-readable legal requirements, and automated compliance checking with the objective of reducing compliance costs while improving legal certainty and facilitating innovation.

In this context, two Compliance Automation projects were successfully launched under the [Digital Europe Programme](#) in the first half of 2026.

The [AIConform project](#) aims to deliver a modular, interoperable framework that automates the extraction, exchange, verification, and auditing of regulatory obligations across sectors. The system operationalises EU rules (AI Act, NIS2, eIDAS 2.0) via machine-readable templates, a legal knowledge graph, and agentic workflows that turn legislative updates into executable checks. AIConform will be validated in three real operational environments — public administration, manufacturing, and energy.

The [OIVA project](#) addresses inefficiencies in regulatory compliance processes that slow down investments, weaken oversight, increase business costs, and add administrative burden for authorities across Europe. These challenges are particularly evident in three highly regulated sectors: vehicle recycling, built environment, and financial reporting. The project builds shared digital infrastructures and compliance tools — all designed to scale across sectors and member states.

Single-Entry Point for incident reporting

The Commission proposed in the [Digital Omnibus package](#) to establish a Single-Entry Point for reporting incidents and data breaches. It is intended to substantially simplify the Union's incident reporting framework. By providing a single reporting channel for entities subject to multiple reporting obligations under Union law, the proposal aims to reduce administrative burden, avoid the duplication of information and enhance the consistency and efficiency of incident reporting. The Commission estimates that a Single-Entry Point would reduce costs for reporting entities by 50%, saving at least €41.5 million per year²³.

This simplification concerns the reporting process only and does not affect the substantive cybersecurity or incident-reporting obligations applicable under Union law. On the contrary, by reducing unnecessary administrative complexity, it enables notifying entities and competent authorities to focus their resources on the timely detection, assessment and management of significant incidents, thereby supporting a high level of cybersecurity across the Union. The European Union Agency for Cybersecurity (ENISA) would play a supporting and coordinating role, without gaining access to the data shared or stored. Trusted relationships between national authorities and entities would remain unaffected.

In addition, in view of further simplification the Commission is striving to harmonise the notification templates within the legal frameworks, as well as, where possible across these, to also reduce the data fields that entities need to complete.

²³ Idem, p. 63.