Council of the European Union

Brussels, 20 November 2025
(OR. en)

15698/25
ADD 2

Interinstitutional Files:
2025/0359 (COD)
2025/0360 (COD)

SIMPL 186
ANTICI 185
DATAPROTECT 307
CYBER 337
TELECOM 417
PROCIV 155
CODEC 1872

PROPOSAL

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	20 November 2025
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	SWD(2025) 836 final
Subject:	COMMISSION STAFF WORKING DOCUMENT Accompanying the documents Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL Amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus) Amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI)

Delegations will find attached document SWD(2025) 836 final.

Encl.: SWD(2025) 836 final

EUROPEAN
COMMISSION

Brussels, 19.11.2025
SWD(2025) 836 final

COMMISSION STAFF WORKING DOCUMENT
Accompanying the documents

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

Amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus)

Amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI)

{COM(2025) 837 final} - {COM(2025) 836 final}

Table of Contents

Introduction 4
1.1. Context 4
1.2. The Commission's digital simplification agenda 5
1.2.1. The Digital Omnibus: a first step, with targeted amendments 5
1.2.1. The European Business Wallet 6
1.2.2. The Digital Fitness Check: a second step to 'stress test' the digital legislation 6
1.2.3. Guidelines and supporting actions 7
1.3. Outline and supporting consultations 8
1. The Data Acquis 10
1.1. One Data Act 10
1.1.1. Analysis of problems and opportunities 10
1.1.2. Simplification measures and impacts 16
1.1.2.1. Free Flow of Non-Personal Data Regulation 16
1.1.2.2. Creating a single legal instrument for re-use of public sector documents 17
1.1.2.3. Clarifications and streamlining of rules on data intermediation services 19
1.1.2.4. Preventing trade secrets leakage to third countries 22
1.1.2.5. Narrowing down the scope of B2G only to public emergencies 24
1.1.2.6. Switching between data processing services 26
1.1.2.7. Removing essential requirements regarding smart contracts for executing data sharing agreements 29
1.1.2.8. Extending SME exceptions to small midcaps for access to public sector data under the Data Governance Act and the Open Data Directive 30
1.1.3. Preserving the objectives of the rules and other impacts 33
1.2. Adjustments to the data protection rulebook 35
1.2.1. Analysis of the problems and opportunities 35
1.2.2. Simplification measures and impacts 40
1.2.2.1. The definition of personal data 40
1.2.2.2. Mechanism to give greater legal clarity on anonymisation and pseudonymisation techniques 40
1.2.2.3. The processing of personal data for scientific research purposes 41
1.2.2.4. The processing of personal data for the development and operation of AI 42
1.2.2.5. The exercise of the individual's right of access 43

1.2.2.6. Controller's information requirements 43
1.2.2.7. Requirements for automated individual decision-making 43
1.2.2.8. Data breach notification to supervisory authorities 44
1.2.2.9. Notion of high risk and the lists of processing activities requiring and not requiring data protection impact assessment 45
1.2.3. Estimated impacts 45
1.3. Modernising the cookies policy: addressing consent fatigue and better alignment with data protection rules 47
1.3.1. Analysis of the problems and opportunities 47
1.3.2. Simplification measures and impacts 51
1.3.2.1. Consent fatigue and cumbersome cookie banners 51
1.3.2.2. Express choices with one click 51
1.3.2.3. Standards for machine-readable preferences 52
1.3.2.4. Browsers signals 52
1.3.3. Estimated impacts 52
1.3.4. Preserving the objectives of the rules and other impacts 58
2. Incident reporting 60
2.1. Analysis of the problems and opportunities 60
2.2. Simplification measures and impacts 63
2.3. Estimated impacts 65
2.4. Preserving the objectives of the rules and other impacts 70
3. Targeted amendments to the Artificial Intelligence Act 72
3.1. Analysis of the problems and opportunities 72
3.2. Simplification measures and impacts 77
3.3. Estimated impacts 80
3.4. Preserving the objectives of the rules and other impacts 85
4. Repeal of the Platform-to-Business Regulation 87
4.1. Analysis of the problems and opportunities 87
4.2. Simplification measures and impacts 89
4.3. Estimated impacts 90
Conclusion 92
ANNEXES 93
Annex I - Stakeholder consultations 93
Annex II – Summary of cost savings estimates 136

Annex III - Competitiveness Check 138
Annex IV - SME Check 141
Annex V - Detailed list of reporting obligations in the digital acquis 146

INTRODUCTION

1.1. Context

In its Communication on implementation and simplification ("A simpler and faster Europe"[1]), the Commission presented its approach to adapting the Union's regulatory framework to a more volatile world: a new drive to simplify, clarify and improve our common acquis.

This vision reflects the broader plan for Europe's competitiveness laid out by Commission President von der Leyen in her political guidelines for the 2024-2029 term[2]. As also highlighted in the Draghi[3] and Letta[4] reports, the accumulation of rules has sometimes had an adverse effect on competitiveness. Fast and visible improvements are needed for people and businesses, through a more cost-effective and innovation-friendly implementation of our rules – all the while maintaining high standards and agreed objectives.

The European Council Conclusions of 20 March 2025 further called for the Commission to "keep reviewing and stress-testing the EU acquis, to identify ways to further simplify and consolidate legislation"[5]. It also stressed the need to follow up with new sets of simplification initiatives. In its Conclusions of 26 June, the European Council underlined the importance of "simplicity by design" legislation, "without undermining predictability, policy goals, and high standards"[6]. The European Council Conclusions of 23 October 2025 reaffirmed "the urgent need to advance an ambitious and horizontally-driven simplification and better regulation agenda at all levels – EU, national and regional – and in all areas to ensure Europe's competitiveness", and called on the Commission to "swiftly bring forward further ambitious simplification packages among others […] on digital"[7].

In its resolution on "the implementation and streamlining of EU internal market rules to strengthen the single market", voted on 11 September in plenary[8], the European Parliament

[1] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A simpler and faster Europe: Communication on implementation and simplification, COM(2025)47 final, 11 February 2025
[2] Von der Leyen, U. (2024) *Europe's Choice: Political Guidelines for the Next European Commission 2024-2029*. Available at: e6cd4328-673c-4e7a-8683-f63ffb2cf648_en
[3] Draghi, M. (2024) *The future of European competitiveness*. Available at: The Draghi report on EU competitiveness
[4] Letta, E. (2024) *Much more than a market*. Available at: Enrico Letta - Much more than a market (April 2024)
[5] European Council, Conclusions, EUCO 1/25, Brussels, 20 March 2025, paragraph. 13.
[6] European Council, Conclusions, EUCO 12/25, Brussels, 26 June 2025, paragraph 30.
[7] European Council, Conclusions, EUCO 18/25, Brussels, 23 October 2025, paragraphs 33 and 35.
[8] European Parliament, Resolution on the implementation and streamlining of EU internal market rules to strengthen the single market, 11 September 2025 (2025/2009/INI).

emphasised the need for simplification to facilitate business compliance without compromising the EU's core policy objectives.

1.2. The Commission's digital simplification agenda

With a value added of €791 billion across the European Union in 2022[9], and permeations that extend to most strands of the economy, the ICT sector holds an increasing part in this simplification effort. Stakeholders of different nature have been calling for targeted amendments of certain rules, to both streamline compliance costs and clarify interplays in their sector.

The Commission is committed to a comprehensive 'stress-test' of the digital rulebook throughout the legislative mandate. The aim is very clear: to ensure that the rules continue to be fit for supporting innovation and growth, they deliver on their objectives and are a driver for competitiveness. Throughout this process, the Commission will seek to provide compelling solutions to simplify, clarify and solidify the effectiveness of the rules and their enforcement through all available instruments, be it regulatory adjustments, enhanced cooperation across authorities, promoting digital solutions that simplify 'by design' regulatory compliance, or other accompanying measures.

1.2.1. The Digital Omnibus: a first step, with targeted amendments

The Digital Omnibus proposal is a first step to optimise the application of the digital rulebook. It includes a set of technical amendments to a large corpus of digital legislation, selected to bring immediate relief to businesses, public administrations, and citizens alike, to stimulate competitiveness. The immediate objective is to ensure that compliance with the rules comes at a lower cost, delivers on the same objectives, and brings in itself a competitive advantage to responsible businesses. The amendments were prioritised building on the consultations with stakeholders and first implementation dialogues conducted by Executive Vice-President Henna Virkkunen and Commissioner Michael McGrath.

For these reasons, the amendments focus on unlocking opportunities in the use of data, as a fundamental resource in the EU economy, not least in view of supporting the development and use of trustworthy artificial intelligence solutions in the EU market. Targeted amendments to the data protection and privacy rules support this objective and provide immediate simplification measures for businesses and individuals, strengthening their ability to exercise their rights.

In addition, the amendments to the Regulation (EU) 2024/1689 (the Artificial Intelligence Act), presented in a separate legal proposal part of the Digital Omnibus, seek to facilitate the smooth and effective application of the rules for safe and trustworthy development and use of AI.

The Digital Omnibus also proposes a very clear solution for streamlining cybersecurity incident reporting, bringing under the umbrella of a single reporting mechanism all related reporting obligations.

[9] Eurostat (2025) *Statistics explained : ICT sector – value added, employment and R&D*. Available at: ICT sector - value added, employment and R&D - Statistics Explained - Eurostat

Finally, the proposal repeals outdated rules in the area of platform regulation, superseded by more recent regulations.

The amendments seek to streamline the rules, reducing the number or laws and harmonising provisions. They cut administrative costs by simplifying provisions and procedures. They relieve small mid-caps from certain obligations across the data acquis and Regulation (EU) 2024/1689 (the Artificial Intelligence Act), in addition to small and micro-enterprises already covered by a special regime. They also stimulate opportunities for a vibrant business environment, creating more legal certainty and opportunities, in particular in sharing and re-using data, in processing personal data or training Artificial Intelligence systems and models.

At the same time, the proposed amendments remain technical in their nature, seeking to adjust the regulatory framework but not to amend its underlying objectives. The measures are calibrated to preserve the same standard for protections of fundamental rights.

1.2.1. The European Business Wallet

Together with the Digital Omnibus, the Commission is also tabling its proposal for a European Business Wallets Regulation, as a cornerstone initiative to simplify regulatory compliance and reduce administrative burdens for businesses.

The Business Wallets will be designed as secure digital tools for businesses, acting as a single platform to simplify their interactions across the EU. By implementing a unique and persistent identifier, businesses will be empowered to digitally verify identities, sign documents, timestamp, and exchange verified digital information seamlessly across borders through the use of a single solution. By adopting European Business Wallets, companies, especially SMEs, will be able to navigate compliance with ease, freeing up vital resources that can be redirected toward growth and innovation.

1.2.2. The Digital Fitness Check: a second step to 'stress test' the digital legislation

As a second step in the commitment to 'stress-test' the digital rulebook, the Commission is also conducting a Digital Fitness Check. Whereas the Digital Omnibus proposals are immediate and targeted, the analysis the Commission will undertake in the Digital Fitness Check will focus on cumulative impact of the digital rules, seeking to test how they support the EU's competitiveness and where further adjustments will need to be proposed in the second half of the legislative mandate.

The Digital Fitness Check is launched at the same time as the Omnibus proposal, with a wide public consultation. The Commission seeks to engage with all stakeholders and consult broadly. The objective is to follow up with an overview and a wide mapping of how the digital rulebook covers strategic sectors of the EU's industry, and address the how the cumulative effect of the rules impacts their competitiveness. On this basis, the analysis will go deeper in a second step on the synergies and areas that could be further aligned, ranging from definitions and legal concepts, to the effectiveness and interplay of the governance systems and other supporting measures.

The 'stress-test' of the digital acquis will also continue through implementation dialogues, as well as with evaluations of all of the main legal instruments. In the current planning, among

other initiative, the Commission is expecting to publish in 2026 a review of the Digital Markets Act, of the Digital Decade Policy Programme, the Chips Act, the Audiovisual Media Services Directive, and an evaluation of the Copyright Directive. For 2027, the acts expected to be evaluated include, among others, the Cyber Solidarity Act, the Open Internet Regulation, NIS2 and the Digital Services Act. In 2028, the Commission should evaluate the European Media Freedom Act and the Data Act, for example, followed by evaluation of the AI Act in 2029 and an evaluation of the sunset clause of the Regulation establishing the European Cybersecurity Competence Centre and Network.

1.2.3. Guidelines and supporting actions

Stakeholders have stressed repeatedly that, in many instances, the simplification effort is less about modifying the rules, and more about providing clarity on their application. The Commission is prioritising a series of guidelines aimed at supporting the uniform application of the rules, without prejudice to the interpretations of the Court of Justice.

As regards the data acquis, the Commission announced its prioritisation in the Data Union Strategy, notably focusing on guidelines on reasonable compensation to clarify what can be charged for data sharing, providing legal certainty to both data holders and data recipients. In addition new guidance is envisaged regarding clarifications of selected definitions in the Data Act.

To support the application of the Artificial Intelligence Act, the Commission continues to prioritise issuing further guidance, focusing on offering clear and practical instructions to apply the AI Act in parallel with other EU legislation. This includes:

- Guidelines on the practical application of the high-risk classification
- Guidelines on the practical application of the transparency requirements under Article 50 AI Act
- Guidance on the reporting of serious incidents by providers of high-risk AI systems
- Guidelines on the practical application of the high-risk requirements
- Guidelines on the practical application of the obligations for providers and deployers of high-risk AI systems
- Guidelines with a template for the fundamental rights impact assessment
- Guidelines on the practical application of rules for responsibilities along the AI value chain
- Guidelines on the practical application of the provisions related to substantial modification
- Guidelines on the post-market monitoring of high-risk AI systems
- Gudelines on the elements of the quality management system which SMEs and SMCs may comply with in a simplified manner
- Guidelines on the AI Act's interplay with other Union legislation, for example joint guidelines of the Commission and European Data Protection Board on the interplay of the AI Act and EU data protection law, guidelines on the interplay between the AI Act and the Cyber Resilience Act, and guidelines on the interplay between the AI Act and the Machinery Regulation
- Guidelines on the competences and designation procedure for conformity assessment bodies to be designated under the AI Act

In particular, stakeholder consultations reveal the need to offer guidance on the practical application of the AI Act's research exemptions under Article 2(6) and (8), including how they apply in sectoral contexts like in the pre-clinical research and product development in the field of medicinal products or medical devices, which the Commission will work on with priority.

1.3. Outline and supporting consultations

This Staff Working Document (SWD) presents the supporting analysis for each of the Digital Omnibus' proposed simplification measures. It is structured in four sections: the Data acquis (including the data protection and ePrivacy frameworks), Artificial Intelligence, Cybersecurity, and Platform rules. For each section, it describes the issues observed and related stakeholder views, presents the solutions put forth in the Digital Omnibus and illustrates the benefits and costs, as well as stakeholder views on the solutions.

It provides estimated cost savings, where feasible and proportionate. Provided the proposal enters into force by early 2027, **the Digital Omnibus could amount to at least EUR 5 billion in administrative cost savings for businesses by the end of the Commission mandate in 2029, as well as a further EUR 1 billion for public authorities.** This estimate does not include measures that were not immediately quantifiable on the basis of available data, but are expected to deliver important added value for all types of stakeholders, nonetheless.

Several consultations were carried out in the preparation of the proposal. Each were conceived as complementary to one another, addressing either different topical aspects or different stakeholder groups. Three public consultations and calls for evidence were published on initiatives related to the key pillars of the proposal in the spring of 2025. A consultation ran on the Apply AI Strategy from 9 April to 4 June[10], another on the revision of the Cybersecurity Act from 11 April to 20 June[11], and finally another on the European Data Union Strategy from 23 May to 20 July[12]. Each questionnaire had a dedicated section (or at times multiple) on implementation and simplification concerns, directly related to the reflexions on the Digital Omnibus. Taken together, 718 unique responses were obtained as part of this first consultation stream.

A Call for Evidence on the Digital Omnibus was further published from 16 September to 14 October 2025[13]. Its aim was to give the opportunity to stakeholders to comment on a consolidated proposal for the scope of the Digital Omnibus. 512 responses were received, submitted by diverse stakeholder groups, not least businesses and business associations, civil society, academics, authorities as well as individual contributions from citizens.

[10] European Commission (2025) *Call for evidence and public consultation on the Apply AI Strategy*. Available at: Apply AI Strategy – strengthening the AI continent

[11] European Commission (2025) *Call for evidence and public consultation on the revision of the Cybersecurity Act.* Available at: The EU Cybersecurity Act

[12] European Commission (2025) *Call for evidence and public consultation on the European Data Union Strategy*. Available at: European Data Union Strategy

[13] European Commission (2025) *Call for evidence on the digital package and omnibus*. Available at: Simplification – digital package and omnibus

Executive Vice-President Henna Virkkunen hosted two implementation dialogues on the key topics addressed in the Digital Omnibus: the first on data policy[14] (1 July 2025), and the second on cybersecurity policy[15] (15 September). Commissioner McGrath hosted an implementation dialogue on the application of the General Data Protection Regulation[16] (16 July 2025).

The Commission's services also conducted several 'reality checks' - deep-dive focus groups with businesses and representatives of civil society organised between 15 September and 6 October 2025 to discuss the practical implementation challenges experienced on a day-to-day basis and estimate compliance costs.

With a view of consulting specifically small and medium-sized enterprises (SMEs), and collecting their feedback, a dedicated SME Panel was run via the Enterprise Europe Network (EEN)[17] between 4 September to 16 October 2025.

Finally, the Commission's services received numerous position papers and hosted bilateral meetings with a variety of stakeholders. The Commission's services also engaged with Member States in roundtables or in the context of various Council Working Parties.

A detailed overview of these stakeholder consultations is included in Annex I. Annex II presents a summary of the cost savings estimates for the proposals. Additionally, an SME Check (Annex III) and Competitiveness Check (Annex IV) underline more specific impacts on small and medium-sized enterprises and European competitiveness altogether. Last, Annex V presents a detailed list of reporting obligations identified in the entirety of the digital acquis, used as starting point for the scoping of the simplification measures.

[14] European Commission (2025) *Implementation dialogue – data policy*. Available at : Implementation dialogue – data policy - European Commission

[15] European Commission (2025) *Implementation dialogue on cybersecurity policy with Executive Vice-President Henna Virkkunen*. Available at: Implementation dialogue on cybersecurity policy with Executive Vice-President Henna Virkkunen - European Commission

[16] European Commission (2025) *Implementation dialogue on the application of the general data protection regulation with Commissioner Michael McGrath*. Available at: Implementation dialogue on the application of the general data protection regulation with Commissioner Michael McGrath - European Commission

[17] EEN is the world's largest support network for small and medium-sized enterprises, and is implemented by the European Commission's European Innovation Council and SMEs Executive Agency (EISMEA).

1. THE DATA ACQUIS

Data is a key enabler of competitiveness in the digital economy. Data availability and access are decisive for innovation, developing new technologies, analysing trends as well as identifying gaps and shortcomings to enhance efficiency across industries and in all sectors. The recent technological advancements including in the area of AI have shown that Europe must have in place solid, consolidated data governance structures and rules to achieve this goal. The applicable rules must be tailored to enhance competitiveness and innovation. They need to be clear, applied in a coherent and consistent manner, and their interplay needs to leave no room for ambiguity.

Yet, the data acquis is fragmented across multiple laws. The Digital Omnibus seeks to pull into one coherent law the rules supporting a competitive single market for data sharing and use.

The General Data Protection Regulation is the cornerstone for the protection of personal data. It can be a powerful tool for supporting data-driven innovation while ensuring the highest level of data protection. The Digital Omnibus includes a series of amendments to give further legal clarity in this regard and to modernise the rules, where needed. It also brings practical solutions to the long-overdue issue of consent fatigue and costly cookie banners.

1.1. One Data Act

Diverse stakeholders across sectors such as civil society, health, energy, manufacturing and mobility[18] have underlined that in recent years, the EU has created many legislative acts related to data sharing which has led to uncertainties about how the acts interact with each other. This feedback echoes the findings from an assessment of the implementation of the rules, to an extent that a consolidation of at least some of them appears warranted. In the Digital Omnibus, the single market rules on data are consolidated in one legal act – the Data Act. Further simplification measures are also proposed, including for giving legal certainty and stimulating data-driven innovation.

1.1.1. Analysis of problems and opportunities

Free Flow of Non-Personal Data Regulation (FFDR)

The rules. The FFDR aims to ensure the free flow of data other than personal data within the Union by laying down rules relating to data localisation requirements, the availability of data to competent authorities and the porting of data for professional users. The Regulation inter alia prohibits unjustified data localisation requirements and encourages switching as well as data portability between data-processing services through self-regulatory codes of conduct. In addition, each Member State designates a Single Information Point and a Point of Contact for cross-border cooperation.

[18] The European Commission organised six stakeholder workshops in Spring and Summer 2025 inviting European level associations and individual stakeholders to roundtable discussion to address aspects such as simplification and investigate on the current state of play in the realm of data. These stakeholder workshops were organised with representatives from civil society, health sector, mobility sector, technology providers, business associations, energy and manufacturers sector.

The main issues. The FFDR has applied since 28 May 2019, with limited uptake and modest stakeholder interest. While it sought, among other things, to facilitate cloud switching through self-regulatory codes, these mechanisms have been superseded by the binding framework in the Data Act.

Although the FFDR envisages Single Points of Contacts and Single Information Points as an information/coordination backbone, awareness of the FFDR and such tools is uneven. About half of the respondents to the public consultation for the Data Union Strategy report only some, little or no familiarity, and uncertainty dominates assessments[19]. Moreover, 62 % of respondents to the public consultation (comprising companies, including SMEs, non-governmental organisations and national public authorities) stated that they did not know whether the rules of the FFDR needed to be modified in order to reduce data localisation requirements. Public authorities showed particularly strong uncertainty relative to the other stakeholder groups. This general uncertainty is mirrored by the fact that fewer than 4 in 10 respondents to the public consultation see any FFDR objective already fully met; the weakest scores concern trust in/security of (cross-border) data storage/processing and practical switching/porting.

Respondents have reported low visibility of monitoring and enforcement, calling for communication channels with more visibility. More than two-thirds (ca. 68 %) however could not judge whether enforcement was sufficient. Only about one in five explicitly considered the set-up adequate, echoing the limited visibility reality check. In an SME Panel consultation led by Commission services in September-October 2025, responding SMEs expressed similar lack of awareness with the FFDR[20].

Additionally, stakeholders have experienced several practical issues with the FFDR. First, the implementing public authorities claim low user demand for the application of the FFDR. No publicly reported cases appear under Article 5(2) FFDR's cooperation mechanism nor under Article 5(4) FFDR's penalty mechanism. Secondly, Chapter VI of the Data Act has introduced a modern horizontal legal framework addressing switching between data processing services. It has rendered Article 6 FFDR practically obsolete.

The objectives. Cutting all outdated rules to reduce legal uncertainties and supporting, through core principles for the single market for data, the growth of innovative companies and their competitiveness.

Data Governance Act (DGA)

The rules. The Data Governance Act seeks to increase trust in data sharing, strengthen mechanisms to increase data availability by setting out common rules for data intermediation and altruistic data sharing. Additionally, the Data Governance Act establishes safeguards for international access and transfer of data.

Rules for data intermediation services focus on neutrality and transparency, ensuring individuals and companies control how their data is shared. Providers must operate through a

[19] See Annex I, Chapter II, for a more detailed overview of the types of respondents that can be referred to throughout the section.
[20] See Annex I, Chapter III.

separate legal entity, complete a notification procedure, and may use an official label once approved.

For data altruism - voluntary data sharing for public-interest purposes - organisations can register and use a trust label if they are non-profit, transparent, and provide safeguards for data providers. They are supposed also respect a forthcoming rulebook and comply with national arrangements supporting data altruism.

The Data Governance Act further established the European Data Innovation Board (EDIB) as an expert body to provide guidance and expert opinions on data sharing and to foster exchanges between Member States to share best practices. The EDIB is equally tasked under the Data Act to assist in developing consistent enforcement for B2C, B2B and Business to government data sharing.

The main issues. While common rules for data intermediaries are important for stimulating the re-use and sharing of data in trusted environments, current requirements and obligations have not led to the market stimulation that was initially expected. According to the Impact Assessment and support study accompanying the Proposal for a Regulation on Data Governance, the European market was expected to include 100–150 data intermediation service providers; however, only 27 have registered to date[21].

While the delayed set up of competent authorities in a range of Member States[22] can partially explain the low level of uptake, feedback from the implementation of the rules shows that certain rules need targeted amendments to increase their effectiveness and facilitate scaling up of data intermediaries. For instance, stakeholders express the need to clarify (e.g. the commercial element in the definition of data intermediation service, the interplay between the definition in Article 2(11) and Article 10, the exemption of 'closed groups') and streamline definitions, including with regard to the Data Act. Furthermore, as highlighted in an evaluation conducted on behalf of the European Commission covering the DGA, ODD and FFDR, which is expected to be published by the end of the year, the DISP (data intermediation service provider) market remains immature and awareness of this type of service is limited. Surveyed DISPs for the forthcoming study indicate that some provisions are burdensome and weigh on business-model sustainability. While neutrality and user trust are acknowledged as essential, prohibitions on data enrichment and cross-sector analytics, notably under Article 12(c) and (e), are reported to constrain innovation and commercial viability[23].

When it comes to data sharing mechanisms under the Data Governance Act, the rules on data intermediation services were thus especially singled out for being able to benefit from greater alignment, simplification and clarity to increase their uptake.

---

[21] European Commission (2025) *EU register of data intermediation services*. Available at: https://digital-strategy.ec.europa.eu/en/policies/data-intermediary-services

[22] On 23 May 2024, the Commission launched infringement proceedings against 18 Member States for failure to notify competent authorities. As of November 2025, 6 Member States have not notified competent authorities. Available at: https://digital-strategy.ec.europa.eu/en/news/commission-calls-18-member-states-comply-eu-data-governance-act .

[23] Study supporting the evaluation of the Free Flow of Non-Personal Data Regulation, Open Data Directive and Data Governance Act, Interim report, 19 September 2025 (forthcoming), p. 168.

In the context of an EDIB meeting to discuss these matters, 50% of respondents reported that the requirement of providing data intermediation services through a separate legal person was especially burdensome, triggering costs and a hindrance to finding a viable business model. Moreover, according to respondents to the public consultation on the Data Union Strategy, the biggest obstacle to altruistic data sharing is administrative or legal complexity followed by low trust and financial sustainability. This highlights that the current conditions can be amended to further facilitate the uptake of those provisions.

Regarding the EDIB, the current rules are considered very rigid, not providing enough strategic flexibility to reap the full potential of the expert body. This was notably put forward by a number of public authorities in response to the Call for Evidence for the Digital Omnibus.

The objectives. The proposed amendments are expected to overcome identified issues in the current implementation of the Data Governance Act. They should help reaching the policy objectives fully by stimulating the emerging market of data intermediation and, implicitly, value creation through the reuse of data. In addition, the governance system for the rules should be leaner and more effective, allowing for strategic discussions and quicker responses to emerging issues within the EDIB.

Re-use of public sector data under the DGA and the Open Data Directive (ODD)

The rules. The rules for the access to and re-use of information held by the public sector across the Union are currently fragmented as they are regulated by two different horizontal instruments:

- The **Open Data Directive** sets out rules for public sector bodies to share information for re-use. However, information that is subject to intellectual property rights of third parties, that is protected due to statistical confidentiality or that cannot be shared because of data protection concerns ("protected data") is out of scope.
- **The DGA** (Chapter II) aims at increasing the availability of such data by setting out a common set of rules when a public sector body decides to share such protected data. Thus, two instruments, containing the same principles to a certain extent, currently govern the re-use of public sector information.

The main issues. Both regimes set out rules for the re-use of information held by public sector bodies. Their scope and the corresponding rules differ however, with the interplay between those rules sometimes not clear. For example, it is not clear which rules apply to data that is anonymised under the rules for protected data, after anonymisation. Furthermore, the Open Data Directive applies to documents, including data, whereas the Data Governance Act applies to protected data only, without including non-digital information.

This regime leads to confusion, creates unnecessary complexity resulting in increased compliance costs for public sector bodies when making such information available as they will first need to assess what legal regime is applicable to the request. The majority of Member States and representatives from competent bodies called for an alignment of the rules of the two instruments. At the same time, businesses and research organisations across industries and irrespective of size also need to navigate within this dual and in some cases overlapping regime.

The results of the public consultation on the Data Union Strategy have shown that more than half of the respondents wished that the public sector makes "more efforts to allow processing of confidential data". This shows that the rules of the Data Governance Act should be maintained and enforced. According to an assessment of the Data Governance Act conducted in Q2-3 of 2025 in the context of an EDIB meeting, (designated) competent public sector bodies in Member States perceive the current regime of having two legal instruments regulating the re-use of information held by public sector bodies as burdensome and creating unnecessary complexity. Roughly 70% of the answers received by participants explicitly advocated for creating a single regulatory regime to clarify for data holding public sector bodies what requirements apply to them. This indicates that the current framework is perceived as complex and burdensome. The assessment revealed that national public sector bodies perceive that without alignment between the two instruments, the data landscape will remain fragmented with inconsistent conditions for re-use.

Start-ups, small enterprises, enterprises that qualify as medium-sized enterprises and enterprises from sectors with less-developed digital capabilities struggle to re-use data and documents. At the same time a few very large players have emerged with considerable economic power in the digital economy, including through the accumulation and aggregation of vast volumes of data and the technological infrastructure for monetising them. Recent data from a Commission study indicates that larger enterprises are more strongly driven by open data and use those data more frequently, despite them being available to everyone. For example, whereas only 5% of Small Enterprises with 10 to 49 employees performed data analytics on government authorities' open data, 11% of Medium-sized Enterprises with 50 to 259 employees did so and even 22% in the case of Large Enterprises with more than 250 employees.[24] The costs and burdens relating to re-use of data and documents held by public sector bodies (lodging and pursuing requests for data, setting up APIs, paying fees, data cleaning etc.) are mainly the same for all re-users regardless of their size, however. for all re-users, however.

Furthermore, given the rules for the re-use of public sector data are currently largely governed in a Directive, the national transposition rules differ across Member States. Stakeholders, including representatives of public sector bodies, ministries and competent bodies as well as companies wanting to re-use data and documents have identified the lack of harmonisation as a factor that makes re-use more complicated and burdensome, even more so in cross-border scenarios. Namely, charging practices differ across Member States, as well as their transposition of what data cannot be made openly available due to personal data protection concerns. This was underlined for example by participants to the reality check on the re-use of public sector data organised by the Commission's services[25].

The objectives. The objective is to harmonise and bring under a single instrument the rules on the re-use of data and documents held by public sector bodies, currently regulated under the Open Data Directive and Chapter II of the Data Governance Ac for protected data. Public sector bodies and re-users should be provided with more clarity with streamlined definitions.

[24] Study supporting the evaluation of the Free Flow of Non-Personal Data Regulation, Open Data Directive and Data Governance Act, Interim report, 19 September 2025 (forthcoming), p. 127-128.
[25] See Annex I, Chapter IV.

Moreover, to prevent a reinforcement of existing market imbalances, public sector bodies shall receive the possibility to introduce specific conditions for the re-use of information by very large entities.

The Data Act

The rules. The Data Act entered into application on 12 September 2025. The Data Act introduces mandatory data sharing obligations to boost greater and fairer data availability, while preserving the rights and interests of those who invest in data generation technologies. Given the Act's recent applicability, evidence of its effects is not yet available.

The main issues. Stakeholders generally express broad support for the objectives and mechanisms of the Data Act. Due to the recent entry into application of the Data Act, extensive evidence on its practical effects is not yet available. However, ex ante evidence sources and early stakeholder perceptions (in particular from data holders) signal some areas that could warrant targeted adjustment for an optimal implementation. Strong concerns have notably been voiced on four core aspects:

- Chapter II of the Data Act mandates data holders to provide access to data, including trade secrets with appropriate confidentiality measures, to users and third parties within the EU. However, there are significant concerns about the potential leakage of trade secrets to entities in third countries. Participants in sectoral workshops frequently expressed fears of unlawful access and misuse by third-country entities, and many were specifically worried about trade secret exposure. A key issue involves the lack of clarity on foreign legal environments, compelling many stakeholders to have to assess these frameworks to determine how to protect confidential data. This concern was echoed by 42% of the respondents in the Data Union Strategy public consultation. Additionally, 86% of the respondents emphasized the importance of maintaining EU-level protection and 84% called for the EU to prioritize safeguards against unauthorized access from third countries.
- Chapter V of the Data Act requires data holders to make data available to public sector bodies, the Commission, the European Central Bank, or Union bodies when an 'exceptional need' arises. However, data holders argue that the scope of 'exceptional need' is overly broad, leading to a lack of clear and proportionate pathway for public sector access to business data. Rather, the focus should lay on public emergencies. This was particularly reflected in contributions from large companies and business associations in the Call for Evidence to the Digital Omnibus.
- Chapter VI of the Data Act empowers users of data processing services to switch between providers of data processing services. The absence of vendor lock-in, including contractual barriers to switching, allows users to freely choose the services that best meet their needs and permits providers to compete for a larger pool of potential customers. However, small providers and providers of tailored solutions highlight that the potential benefits of switching accruing to the users are outweighed by the administrative burden accruing on these stakeholders of having to review existing contracts in a way that ensures compliance with the Data Act.

- Chapter VIII of the Data Act aims to ensure, under Article 36, that smart contracts used to automate data-sharing agreements were interoperable, secure and trustworthy. It established essential requirements for vendors who create or integrate smart contracts for others, while remaining technologically neutral and allowing a presumption of conformity when harmonised standards were followed. However, industry stakeholders criticise these provisions as unclear in scope, potentially capturing a wide range of software and running the risk of constraining innovation opportunities.

The objectives. The proposed amendments are designed to address key concerns raised in the early implementation of the Data Act by providing clarity and precision to definitions and rules, while keeping the core policy objectives of unlocking data and boost innovation in data sharing tools for a flourishing digital single market. This concerns the rules on trade secret protection, business to government data sharing, cloud switching, and smart contracts for executing data sharing agreements. This will help harness the Data Act's full potential.

1.1.2. Simplification measures and impacts

1.1.2.1. Free Flow of Non-Personal Data Regulation

To address the described practical issues, the Omnibus proposes to repeal the FFDR, while upholding the principle of free flow of non-personal data within the Union enshrined in the FFDR. The principle remains paramount for a digital single market and the data economy in the Union. It should thus be maintained and included in the Data Act as a horizontal regulation that covers rules on non-personal data.

Cost savings. This measure preserves the main cost-saving channel for businesses, i.e. the ability to place non-personal data in the most efficient EU location. This reduces parallel legal analysis and thus lowers costs even though it is to be noted that the instrument has not been effectively used. However, public authorities would be relieved from burdensome monitoring activities that do not meet any demand (Single Information Point and Single Point of Contact). Using an EU-wide central cost assumption of EUR 62,712 per FTE (derived from Eurostat's 2024 hourly labour cost[26] and an assumption of 1,872 annual productive hours[27]), this leads – assuming a saving of 0.5 FTE from the monitoring relief, based on Commission estimates – to savings for public authorities of EUR 31,356 per Member State annually and EUR 846,612 annually across the EU. Table 1 outlines the anticipated cost savings and underlying assumptions for the calculations.

[26] Eurostat (2025) *EU hourly labour costs ranged from €11 to €55 in 2024*. Available at: EU hourly labour costs ranged from €11 to €55 in 2024 - News articles - Eurostat

[27] Eurostat (2025) *People in the EU worked on average 36 hours per week*. Available at: People in the EU worked on average 36 hours per week - News articles - Eurostat

Table 1: Estimated cost savings for changes to the Free Flow of Non-Personal Data Regulation

Item	Unit	Assumptions	Formula	Estimated administrative cost savings	
				Public authorities	
Reduction of administrative costs by avoiding information gathering by public authorities	EUR	Annual productive hours in the EU: 36h p.w x 52 = 1,872 Average annual cost per FTE in the EU; 1,872 annual hours x 33.5€ (average hourly labour cost) = 62,712 Saving per MS: 0.5 x 62,712= 31,356	31,356 x 27	**One-off**	**Recurrent**
				N/A	≈ **EUR 846,612** per year

Moreover, the simplification of switching rules strengthens the freedom to conduct a business and the free movement of services that build on non-personal data.

Stakeholder views
In the various consultations organised, no clear support could be noted, across stakeholder categories, for preserving the Regulation as a whole. Member States in particular have flagged, including through a workshop organised by the Commission's services and a wider consultation that they support the data localisation ban regulated by the FFDR, as a core principle of the digital single market. They expressed serious scepticism as to the relevance of the other provisions. In view also of the efficiencies described above, the chosen simplification, i.e. retaining only the FFDR's prohibition of unjustified data localisation requirements under the Data Act, is the most targeted way to cut red tape while preserving the core internal-market safeguard. The measures will allow a stronger focus and communication on the most pertinent issue of data localisation requirements, contribute to a better understanding of the adopted rules and enable further regulatory implementation. Keeping the FFDR alongside the Data Act (or expanding the FFDR to cover broader switching) would maintain duplication and confusion. Similarly, sector-by-sector localisation bans (e.g. in mobility or energy) would risk renewed fragmentation and inconsistent enforcement.

1.1.2.2. Creating a single legal instrument for re-use of public sector documents

The proposal brings all rules on the re-use of information held by public sector bodies under the same instrument by integrating Chapter II of the Data Governance Act and the Open Data Directive into a new coherent chapter for the re-use of public sector information in the Data Act. Changes include aligning definitions between the two acts, such as 'data' and 'documents' and creating common provisions. The principles of the two instruments will remain unchanged to guarantee that Europe does not experience a set-back when it comes to the achievements made for open data. For example, principles inherent to both instruments, such as non-

discrimination, prohibition of exclusive agreements or information on means of redress can be streamlined and included as general principles for the re-use of public sector information. General principles relating to charging can be established, extending the possibility to pay charges online through widely available cross-border services for re-use of documents covered under the Open Data Directive to modernise the law. The scope of the current Chapter II DGA of "data" will be enlarged to "documents", thus bringing in scope non-digital information.

The current rules on the conditions of re-use under the DGA can be further aligned, clarified and streamlined to be more user friendly. This includes reducing redundancies, aligning definitions and clarifying the applicable regime in case of anonymisation of personal data. In addition, the current rules on transfers of non-personal data to third countries international transfers should be moved into a new dedicated Article.

In the spirit of fostering innovation and maintaining fair competition within the Union's digital market, it is imperative to ensure that access to and reuse of public sector data benefit a wide range of market participants and do not inadvertently reinforce existing dominant positions. In particular very large enterprises, hold significant power and influence over the internal market. To prevent such entities from leveraging their substantial market power to the detriment of fair competition and innovation, public sector bodies shall be able to set out special conditions to the re-use of data and documents by such entities. For example, they should be able to demand higher charges and fees, based on objective criteria, and taking into consideration an entity's economic power, ability to acquire data or the designation as a gatekeeper under Regulation (EU) 2022/1925.

This way, opportunities for smaller businesses and new market entrants to innovate and compete in the digital economy are safeguarded. The online public consultation on the Data Union Strategy also inquired whether it is advisable to exclude some undertakings, designated as gatekeepers, as defined under Article 3 of Regulation (EU) 2022/1925, from benefiting from certain conditions for the reuse of public sector data, as set out in the Open Data Directive. The objective would be to prevent such entities from leveraging their substantial market power to the detriment of fair competition and innovation.

Finally, the transformation of the rules of the Open Data Directive into a directly applicable Regulation means creating a legal framework uniformly applicable across all EU Member States, eliminating the need for national transposition. It is important to note that a significant part of public sector data is already today subject to the directly applicable Implementing Regulation on high-value datasets. This solution presents numerous benefits for public administrations holding public sector data as well as for re-users, as they can streamline processes and reduce the administrative burden associated with interpreting and implementing diverse national laws. This shift could lead to improved data quality and standardisation, enabling better data management and enhancing interoperability for efficient cross-border data sharing. A reduced legal fragmentation could stimulate EU-wide data-driven markets by making it easier for businesses to develop and offer cross-border services and products. Enforcement of directly applicable rules will likely become more consistent. Stakeholders

participating in the reality check on re-use of public sector data[28] also highlighted that a transformation into a Regulation would improve awareness about the opportunity to re-use such data. The proposal does not change national access regimes and aims at providing enough flexibility for national solutions – an important factor underlined by Member States.

Overall, this proposal expected to reduce search and compliance costs for re-users by providing a single, clearer, directly enforceable procedural framework; shorten time to access through more predictable and harmonised conditions; improved data management and quality across borders.

Stakeholder views
More than 60% of respondents to the public consultation on the Data Union Strategy supported consolidation across the data acquis. According to a survey conducted in the framework of the EDIB, roughly 70% of respondents, including public sector bodies and competent bodies supported a single instrument for the re-use of public sector information. Stakeholders also highlighted that pertaining the definition of "documents" as encompassing digital and non-digital information was important and no concerns were voiced when extending the notion of data currently in scope of Chapter II Data Governance Act to "documents" as under the definition of the ODD. Some representatives from Member States reported that this would reflect nationally established practices. Moreover, the proposed amendments to the current conditions for re-use under the DGA will facilitate compliance with those rules as they will be easier to understand and implement and should thus help to boost the making available and re-use of protected data, representing a key driver for Europe's competitiveness.
On the special regime for very large enterprises and in particular gatekeepers' access to public sector data, 42% of respondents - mainly businesses and public authorities – were in favour, while 33% - many of which representing non-EU companies and business associations – were against.
Finally, on the occasion of its alignment with the Data Governance Act it is proposed to transform the Open Data Directive into a directly applicable Regulation. In the online public consultation on the Data Union Strategy 57% of respondents were in favour of such an option, while 15% were against this change.

1.1.2.3. Clarifications and streamlining of rules on data intermediation services

The proposed amendments will turn the mandatory regime applicable today into a voluntary, streamlined scheme that should enhance trust, while cutting costs and stimulating the business model. The amendments will further clarify the notion of 'data intermediation service provider' (DISP). The notification and use of the label will be made voluntary. The requirement to provide the service via a separate legal entity will be removed.

Certain provisions that have proven to be ineffective, such as the obligation for Member States to establish national arrangements for data altruism, or that are potentially overly burdensome, such as the mandate to develop a rulebook for data altruism organisations, will be repealed. Alongside potential savings, the measure could lead to reduced regulatory oversight, lower market transparency and diminished user trust. However, these effects are likely limited in scope at this stage due to the market's small scale and early level of development.

Cost savings. The proposed amendments consist of several factors that can lead to savings: First, data intermediation services can choose not to register their services which will save them administrative fees with the competent authority.

[28] See Annex I, Chapter IV.

Secondly, the deletion of the requirement for data intermediation service providers to offer services through a separate legal entity is expected to create the biggest impact. This can be broken into one-off costs and recurrent overhead costs.

In terms of one-off costs, the current average formation cost alone (without taking into account the often-required original share capital) across the EU varies between EUR 250- EUR 4,000.[29] An average of EUR 2,125 across the EU can thereby be assumed.

Annual overhead costs result from separate corporate overhead structures (board, HR, IT, accounting) and the resulting labour costs as well as other fixed costs (office space, IT equipment). These can also be avoided. The impact can only be approximated as it will depend on a wide range of factors, not least the size of the company and labour costs. Taking into account conservative estimates for the above factors, the annual overhead costs for setting up a company with 50 employees, which is believed to be the typical size of a data intermediation service provider, can be estimated to amount up to EUR 40,000.[30]

Assuming a potential total maximum of 150 data intermediaries in the EU according to the Impact Assessment accompanying the Data Governance Act, this could result in savings up to EUR 318,750 of one-off costs and in terms of recurrent costs up to EUR 6,000,000. Table 2 presents the cost savings and underlying assumptions.

Moreover, the proposed amendment could incentivize new players to provide data intermediation services by reducing market-entry barriers, thereby accelerating the development of this ecosystem of providers. Estimating that the average fixed cost of operating a data intermediation service amounts to around EUR 250,000 per year[31], removing the requirement to provide such services through a separate legal entity would therefore lower fixed operating costs by roughly 17% (40,000 in annual overhead costs + 2,125 in one-off formation cost)/250,000 = 0.1685). To approximate the potential market impact, a range of entry-cost elasticities could be applied, reflecting how the number of market entrants typically reacts to changes in fixed costs. In digital and professional-service markets, where barriers are mostly related to administration rather than infrastructure, companies tend to be more receptive. On

[29] Legal Bison (2025) *Company Formation in Europe*. Available at: Company Formation in Europe - LegalBison

[30] Indicative EU-average overhead for a stand-alone entity of around 50 employees, excluding statutory audit and one-off incorporation costs. Basket and mid-case assumptions: payroll administration approximately EUR 15 000 [EUR 25 per payslip × 50 × 12]; bookkeeping and annual accounts approximately EUR 3 500; routine tax/VAT filings approximately EUR 1 200; data-protection/compliance support approximately EUR 3 000; insurance (professional indemnity and cyber) approximately EUR 8 000; corporate secretarial/registered office approximately EUR 500; banking and membership fees approximately EUR 900; routine legal advice approximately EUR 4 000; incidental translations or notarials approximately EUR 500; plus a modest variance buffer across Member States. Central estimate: approximately EUR 40 000 per year. Figures are stylised and may vary by Member States.

[31] This is an indicative EU-average stylised composition of fixed operating costs. Fixed operating costs are baseline, volume-independent expenditures. Basket and mid-case assumptions: (i) Core management and support staff: approximately EUR 150 000 (two administrative/operations FTEs at EUR 60 000 each and 0.5 FTE compliance at EUR 30 000); (ii) Base infrastructure and security tooling: approximately EUR 40 000; (iii) Facilities and connectivity: approximately EUR 15 000 (office space, utilities and business-grade internet); (iv) Software maintenance and support contracts: approximately EUR 15 000; (v) Depreciation or amortisation of set-up assets: approximately EUR 20 000; (vi) Other fixed items: approximately EUR 10 000 (training, limited travel and equipment refresh). Total: approximately EUR 250 000 per year. These figures are indicative and may vary by Member State, labour market conditions, architectural choices, and security requirements.

this basis, a cost elasticity range of -0.8 to -1.4 is assumed, meaning that a 10% cost decrease could raise entry by about 8-14 %. Applied to a 17% cost reduction, this implies an increase in entrants of around 13-22 % bringing the total from the DGA baseline of 150 to roughly 171–186 DISPs, or an additional 21 to 36 new providers EU-wide.

Table 2: Estimated cost savings for changes to the Data Governance Act

Item	**Unit**	**Assumptions**	**Formula (stylised)**	**Estimated administrative cost savings**	
				Businesses	
EU-wide annual saving from deleting requirement of separate legal person	EUR	Median formation cost across EU: EUR 2,125 150 providers Recurrent annual overhead costs for a separate legal entity per company of 50 staff: EUR 40,000 per year	EUR 2,125 x 150 providers EUR 40,000 x 150 providers	**One-off** ≈ **EUR 318,750**	**Recurring** ≈ **EUR 6 million** per year
Other estimated effects					
Additional Data Intermediation Service Providers (DISPs)	Number of DISPs	Baseline number of DISPs: 150 DISPs Average fixed cost per DISP = EUR 250,000 Separate-entity cost = EUR 40,000/year + EUR 2,125 one-off Entry-cost elasticity range = -0.8 to -1.4	Cost reduction share = 42,125/250,000 = 17 % % increase in entrants = 0.17 × [0.8–1.4] = 14–24 % New total = 150 × (1 + 0.14-0.24) = 171-186 Δ DISPs: 171-186	Between +21 to +36 DISPs EU-wide	

In addition, the proposed amendments would also help to clarify and streamline definitions, thus resulting in a more harmonised acquis and facilitating the user friendliness of the instruments. This should support affected entities to understand the rules faster and reduce burden.

For altruistic data sharing, further clarifying the definition would help organisations find a viable business model and foster the uptake of such mechanisms. In addition, the deletion of

the specific rulebook for data altruism organisations will save the latter from additional compliance burden and thus make data sharing more attractive. In addition, the Article on national arrangements for data altruism (Article 16 DGA) requiring Member States to report national policies to facilitate data altruism should be deleted as it has proven ineffective and puts further reporting obligations on Member States. By deleting this provision, costs related to reporting will be saved while it will still be possible for Member States to develop national policies on data altruism.

Stakeholder views
The Commission has consulted concerned stakeholders and competent authorities, namely in a workshop in spring 2025 as well as in a dedicated sub-group of the European Data Innovation Board consisting of enforcement authorities. Competent authorities, in particular the French authority, flagged the loophole of the notion of 'closed group' which appears to have been used as an argument to be exempted from obligations. More generally, stakeholders have almost consistently voiced the difficulty of finding a sound financial model without being able to offer added-value services. One mid-sized company argued that splitting off their data intermediation business would trigger overhead costs of more than EUR 1 million in their specific case. During the implementation dialogue on data held by EVP Virkkunen, representatives of data intermediations services providers highlighted the importance of a European framework for B2B data sharing for the EU's competitiveness. In the Call for Evidence to the Digital Omnibus, SME associations asked for less burdensome requirements for data altruism organisations and data intermediation service providers.

1.1.2.4. Preventing trade secrets leakage to third countries

The Digital Omnibus will introduce an amendment in the Data Act to create a rule that data holders can refuse disclosure of trade secrets when they 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. The intention is to prevent situations where (a) an EU entity leaks trade secrets to non-EU entities and (b) non-EU entities established in the EU, who are directly or indirectly controlled by a foreign entity and may be subject to extraterritorial rules or otherwise, leak trade secrets outside of the EU. This rule does not affect the position of EU stakeholders as potential recipients, and especially SMEs, established in the EU, and is therefore aligned with the Data Act's objective to support European and smaller market players.

The proposed rule provides a robust framework for data holders to safeguard against significant losses from unlawful trade secret disclosure to third country entities. 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, minimizing confidentiality breaches and mitigating the risk of data exploitation by third country free riders or the largest global tech companies. These entities may capitalize on weaker legal regimes abroad to improperly access trade secrets, possibly without adequate oversight or repercussions, and thus disadvantage other market actors.

Cost savings. While calculating the cost of trade secret leakage under the Data Act is challenging due to several factors, such as the specifics of the trade secret being compromised, the identity of the recipient, and how the information is subsequently utilized, the proposed rule

is designed to effectively prevent abuse of trade secrets that could severely impact data holders. Moreover, it is expected to yield cost and time savings for companies. For instance, according to a study[32], large firms spend around EUR 1 million annually on data management agreements and relevant administrative and legal overhead. Additionally, the cost of setting up application programming interfaces (APIs)[33], which varies between EUR 30,000 and 2.5 million depending on their scope and complexity, is averaged at around EUR 50,000[34]. Legal risks related to being entangled in a litigation over the co-generated IoT data and non-agreement between the parties, could reach about EUR 1 million annually, as per interviewed stakeholders[35]. These risks escalate, or rights/claims could even become unenforceable, in cross-border litigation. By allowing data holders to refuse trade secret disclosure to third-country entities with weak protections, this rule alleviates burdens associated with data and trade secret preparation, sharing and protection.

Data holders might incur increased legal and compliance expenses as they need to assess the trade secret protection frameworks of foreign jurisdictions and demonstrate the risk of unlawful exposure. In its 2025 report on the protection and enforcement of intellectual property rights in third countries, the Commission found that "insufficient protection of trade secrets and the challenges in enforcing them in a number of countries, notably in China and India, also causes irreparable harm to European businesses[36]. When the Data Act entered into application (12 September 2025), the Commission announced that it would develop guidance on trade secret protection under the Data Act. This was reiterated in the Data Union Strategy. Such guidance may assist data holders in the assessment needed to apply the proposed rule.

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.

[32] Study to support an impact assessment on enhancing the use of data in Europe, European Commission, 2022, p. 271.

[33] API: A system access point or library function that has a well-defined syntax and is accessible from application programs or user code to provide well-defined functionality. Source: NIST Computer Security Resource Center (CSRC), "Application Programming Interface (API) — Glossary." Available at: https://csrc.nist.gov/glossary/term/application_programming_interface (accessed 8 November 2025)

[34] Ibid, p. 254.

[35] Ibid, p. 265.

[36] SWD(2025) 131 final, p. 5.

Stakeholder views
Stakeholders generally recognise that the trade secrets regime under the Data Act provides an important safeguard to protect confidential business information. However, many industry associations, particularly those representing data holders, are concerned with leakage of trade secrets to third countries. They fear that third country entities may exploit the Data Act's provisions to transfer trade secrets abroad, where legal protections are weaker, facilitating accelerated reverse engineering that compromises their competitive advantage. For industries that rely on proprietary technologies or that are at the forefront of data-driven innovation, trade secrets are seen as central to their strategic development. Misuse of trade secrets not only represents a breach of confidentiality but also poses a tangible risk to their innovation appetite and economic stability. Accordingly, these organisations call for stronger safeguards to prevent trade secret leaks.
From the perspective of data recipients, particularly SMEs, there are strong concerns that trade secret protections under the Data Act could be misused by data holders to hinder legitimate data access. This was particularly put forward by several SME associations in the Call for Evidence to the Digital Omnibus. While they acknowledge that protecting trade secrets can be a legitimate ground to limit disclosure, they warn that excessive or unjustified reliance on this safeguard could undermine the Data Act's objective of fostering a fair and competitive data economy. Data recipients fear that broad or discretionary activation of trade secret claims may disproportionately benefit larger companies with established data advantages, discouraging smaller or independent players from participating and fairly competing in data-driven innovation. They therefore argue against granting unilateral discretion to data holders, and stress the importance of maintaining the agreed upon balance in the Data Act, with proportionate safeguards, transparency, and procedures.

1.1.2.5. Narrowing down the scope of B2G only to public emergencies

The Digital Omnibus proposes to narrow the scope of Chapter V of the Data Act from "exceptional need" to "public emergency". The intention is to reduce the burden on businesses, addressing private sector concerns regarding the unclarity of the Chapter V's business-to-government (B2G) data sharing regime. The proposal streamlines the B2G framework by concentrating exclusively on public emergencies. This focus reduces ambiguity concerning the interaction of various EU and national laws and strengthens stakeholders' understanding of the B2G rules.

Cost savings. The revised B2G data sharing framework significantly reduces administrative and legal burdens on companies. While one-off costs, such as infrastructure setup, for instance an application programming interface (API) for public sector bodies to access data in an anonymised way (initially estimated at EUR 552,5 million EU-wide[37]), and recurring costs, such as personnel and data management (estimated at EUR 98,5 million annually[38]), remain relevant for addressing B2G requests for public emergencies, the new framework is designed to lessen these costs.

The exclusive focus on public emergencies minimises complexities such as the need to customise data infrastructure and extensive contract negotiations for a wider scope of situations, potentially affecting the estimates for one-off costs[39]. The same goes for the need for detailed

[37] Study to support an impact assessment on enhancing the use of data in Europe, European Commission, 2022, page 227.
[38] Ibid., p. 227.
[39] Ibid., p 223.

data processing activities, such as cataloguing, metadata reporting, and quality assessments, which were more intensive under the broader B2G system. The shift to a more centralised and standardised approach streamlines these tasks, and companies need to put less effort in assessing and normalising data for public interest purposes, potentially reducing the anticipated costs of EUR 78,06 million for these activities[40]. In addition, under the previous broad nature of "exceptional need", data holders were estimated to have to establish teams of 1 to 5 FTEs with technical and legal knowledge to deal with B2G requests, representing an annual cost at the EU level of EUR 20,5 million[41]. By restricting data requests to public emergencies, the framework alleviates the burden, particularly in verifying conditions such as market availability of data or whether the absence of other viable measures to obtain the data exist, thus reducing operational resources and time required for this verification. This translates into further cost savings and enhances legal certainty. All calculations and assumptions for the above are presented in Table 3.

Finally, this approach also leads to cost reductions for competent authorities. For instance, it simplifies the management of data sharing mandates across Member States, easing coordination, especially in complex cross-border scenarios that would otherwise require extensive communication between competent authorities to ensure compliance with diverse legal requirements.

Table 3: Estimated cost savings for changes to Chapter V of the Data Act

Item	**Unit**	**Assumptions**	**Formula (stylised)**	**Estimated administrative cost savings**	
				Businesses	
Narrow the scope of Chapter V Data Act from "exceptional need" to "public emergencies"	EUR	*One-off infrastructure costs* (e.g. set up API): EUR 552,5 million at EU level. Assuming a 5% reduction due to less need for customization of the data infrastructure[42]. *Recurrent annual expenses* (e.g. personnel, data management agreements, clean data): 98,5 million EUR, estimated at 9 FTEs. Assuming a 20% reduction due to streamlined processes[43].	0.05×552,500,000= 27,625,000 0.2×98,500,000=19 ,700,000	**One-off** ≈ **EUR 27,625 million**	**Recurring** ≈ **EUR 19,7 million** per year

[40] Ibid., p 227.
[41] Ibid., p. 227.
[42] Commission estimate.
[43] Ibid.

Stakeholder views
Businesses have criticized the broad and unclear scope of 'exceptional need' in Chapter V of the Data Act, fearing it could impose undue burdens and ambiguity. This was particularly reflected in the Call for Evidence to the Digital Omnibus, particularly by large companies and business associations. They call for a more precise framework to ensure that data requests are legitimate, necessary and justified. Member States echo the need for clarity and seek to reduce bureaucratic burden and legal uncertainty. The statistical community will be able to rely on the revised Statistics Regulation, rather than the Data Act for accessing privately held data, as it offers a fair, clear and predictable approach more in line with their long-term objectives and operational requirements. Nevertheless, in public emergencies, statistical bodies can still invoke the Data Act. This aligns with the principle of Chapter V being activated as a mechanism to specifically address public emergencies.

1.1.2.6. Switching between data processing services

The Digital Omnibus proposes to introduce a specific lighter regime for data processing services which are custom-made, i.e. where the majority of features and functionalities of the service has been adapted by the provider to the specific needs of the customer[44]. As opposed to off-the-shelf solutions, contracts on the provision of these custom-made services are usually the outcome of dedicated negotiations[45]. This is particularly relevant in the Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) segment. Where such contracts were concluded before the entry into application of the Data Act, costly re-negotiations may be required to bring them into compliance with the provisions on cloud switching.

While the right to switch providers of data processing services introduced in the Data Act remains untouched, this new specific lighter regime for custom-made data processing services takes account of the additional costs and administrative burden connected to the need to reopen and renegotiate contracts for the provision of custom-made services. This includes removing pre-commercial, commercial, technical, contractual and organisational obstacles, which, *inter alia* inhibit customers from terminating their contract after the notice period. This new specific lighter regime for custom-made data processing services would save providers the additional costs and administrative burden connected to the need to reopen and renegotiate contracts concluded before the entry into force of the Data Act. The Omnibus therefore proposes to exempt from the switching provisions custom-made services other than Infrastructure-as-a-Service (IaaS) if these are provided to a customer based on a contract concluded before 12 September 2025. For reasons of financial planning and certainty for investors, some providers of data processing services, especially SMEs and SMCs, may prefer to use fixed-term contracts. The customer's right to switch, including when a service is provided based on a fixed-term contract could create the risk that a portion of such contracts are terminated prematurely. This could put the business model of SaaS providers, especially SMEs and SMCs, under significant

[44] This is distinct from the existing specific regime for custom-built services under Article 31(1) of the Data Act, which applies to data processing services of which the majority of main features has been custom-built to accommodate the specific needs of an individual customer or where all components have been developed for the purposes of an individual customer, and where those data processing services are not offered at broad commercial scale via the service catalogue of the provider of data processing services.

[45] United Nations Commission on International Trade Law (2019) *Notes on the Main Issues of Cloud Computing Contracts*. Available at: 19-09103_eng.pdf.

financial strain and uncertainty. Therefore, the Digital Omnibus proposes to clarify that data processing services provided on the basis of fixed-term contract may include provisions for proportionate early-termination penalties as a way of recouping upfront investments in the case of early termination.

In addition, the Digital Omnibus proposes to create a specific lighter regime for data processing services, except IaaS, provided by SMEs and SMCs. Similarly, the need to renegotiate contracts to bring them into compliance with the provision on cloud switching creates a disproportionately high administrative burden for SMEs and SMCs compared to larger providers. The Omnibus thus proposes to exempt from the switching provisions PaaS and SaaS provided by SMEs and SMCs if these are based on a contract concluded before 12 September 2025. Moreover, the Omnibus explicitly exempts those providers from a possible need to renegotiate or amend those contracts before their expiry.

Finally, the Digital Omnibus clarifies that the obligation in Article 29 of the Data Act to first reduce and then remove switching charges, including egress charges, is excluded from those two specific lighter regimes. This preserves one of the key achievements that the Data Act brings for cloud customers. To avoid contract re-negotiations, the proposal clarifies that contractual provisions contrary to Article 29 would be considered null and void.

Cost savings. Based on stakeholder input, the proposed specific lighter regime for custom-made PaaS and SaaS can be expected to cover at least 100,000 contracts in the EU. If assuming an average cost of approximately EUR 10,000 for the re-negotiation of an individual contract, this would imply savings in the magnitude of EUR 1 billion due to non-incurred costs.

Regarding the specific lighter regime for SMEs and SMCs, the number of affected providers can be approximated by looking at the number of SaaS startups. In France alone, there are approximately 2600 SaaS startups. Enlarging this to SMEs and SMCs, a conservative estimation leads to at least 5,000 SMEs and SMCs EU-wide, which are active in the SaaS and PaaS segment. Assuming an average number of 50 contracts per provider in this bracket would lead to a total of 250,000 contracts for the provision of SaaS or PaaS by SMEs or SMCs. The calculations laid down in Table 4 below (also presenting the assumptions for the above estimated cost savings for custom-made data processing services) would thus lead to cost savings of around EUR 500 million if these contracts would not have to be re-opened.

Table 4: Estimated cost savings for changes creating a specific lighter regime for data processing services under the Data Act

Item	**Unit**	**Assumptions**	**Formula (stylised)**	**Estimated administrative cost savings**	
				Businesses	
	EUR			**One-off**	**Recurring**

Specific lighter regime for data processing services which are custom-made		Number of professionals (lawyer) required per contract: 1,25 Number of technicians (IT expert) required per contract: 1,25 Number of clerks (secretary) required per contract: 0,2 EU average labour cost of professionals: EUR 40,50/h EU average labour cost of technicians: EUR 32,70/h EU average labour cost of clerks: EUR 26,30/h Number of hours for contract re-negotiation: 105 hours Number of contracts concluded before 12 Sept 2025: 100,000	Cost to re-negotiate one contract: (1,25 x 40,50 x 105) + (1,25 x 32,70 x 105) + (0,2 x 26,30 x 105) = EUR 10.159,80/contract Cost to re-negotiate contracts concluded before 12 September 2025: = 100,000 contracts x 10.159,80 EUR/contract = € 1,015,980,000	≈ **EUR 1,015,980,000**	N/A
Specific lighter regime for data processing services provided by SMEs and SMCs	EUR	Number of professionals (lawyer) required per contract: 1 Number of technicians (IT expert) required per contract: 1 Number of clerks (secretary) required per contract: 0,2 EU average labour cost of professionals: EUR 40,50/h EU average labour cost of technicians: EUR 32,70/h EU average labour cost of clerks: EUR 26,30/h Number of hours for contract re-negotiation: 30 hours Number of SaaS/PaaS SMEs/SMCs in EU: 5,000 Number of SaaS/PaaS contracts by SME/SMC: 50 Number of contracts concluded before 12 Sept 2025: 250,000	Cost to re-negotiate one contract: (1 x 40,50 x 30) + (1 x 32,70 x 30) + (0,2 x 26,30 x 30) = EUR 2.353,80/contract Cost to re-negotiate contracts concluded before 12 September 2025: = 250,000 contracts x EUR 2.353,80/contract = EUR 588,450,000	*SME/SMCs* **One-off** ≈ **EUR 588,450,000**	**Recurring** N/A

Stakeholder views
Businesses have criticised the obligation of removing contractual obstacles to switching in contracts concluded before 12 September 2025 as a significant burden, particularly where the initial contract is the outcome of dedicated negotiations, which is typically the case for services that do not function without prior configuration to an individual customer. Smaller providers, in particular start-ups and scale-ups but also SMEs and SMCs, have voiced the clear need for predictable revenues over a fixed period of time. In cases where a customer has committed to a fixed-term contract but then makes use of their right to switch, these providers have expressed a need to recoup upfront investment and retain financial certainty.

1.1.2.7. Removing essential requirements regarding smart contracts for executing data sharing agreements

The Digital Omnibus proposes to delete Article 36 of the Data Act, which introduced specific requirements for smart contracts used in the context of data sharing. Article 36 was intended to ensure that automated data sharing execution mechanisms were interoperable, reliable, included proper access controls, and could safely be stopped or adjusted when needed. The objective was to provide legal certainty for emerging blockchain-based solutions that could facilitate data access and use.

Since the adoption of the Data Act, however, the development and use of smart contracts in data-sharing scenarios has remained at an early and experimental stage – also reflecting the relative recentness of the legislation. Market actors are testing different technical and governance models, and no common standards or practices have emerged. Industry stakeholders have raised concerns that the scope of Article 36 is unclear and may unintentionally capture a much broader set of distributed-ledger-technology (DLT)-based smart contracts, as well as ordinary built-in software features that merely automate data access, that were not meant to fall within the Data Act's scope. Another strong criticism relates to the core characteristics of public blockchains. These systems rely on key features like immutability, decentralised control, and cryptographic transparency to ensure trust and security. If rules required these systems to include built-in options to stop their operation or give special access to a specific actor, those features would be weakened. This could make open, permissionless blockchains harder to build and discourage innovation in this area.

In this context, prescribing detailed regulatory requirements at Union level would risk locking in specific technological choices or stifling innovation in an area that continues to mature. Market actors are currently better placed to test, validate, and refine solutions adapted to their specific business models and technical environments.

Smart contracts remain a highly promising tool to foster secure, transparent and efficient data sharing, and there is strong support to develop them further and deploy them in the context of the Data Act. Removing Article 36 thus prevents regulatory complexity, reduces uncertainty, and maintains the flexibility needed to foster innovation in decentralised and automated data-sharing solutions, while preserving the overall coherence of the Data Act.

Cost savings. There are no reliable estimates of the costs or savings linked to Article 36, but its removal reduces administrative and technical burdens. Developers would no longer need to

redesign smart contracts to meet specific requirements such as interruption or archiving functions, nor carry out conformity assessments and prepare related documentation.

The deletion of Article 36 also eases pressure on authorities, which would no longer have to oversee compliance for a still emerging market and technology. It also creates a more flexible environment for innovation, allowing market actors to experiment freely and develop new smart contract solutions, which in turn can stimulate further economic activity and technological progress. Overall, deleting Article 36 lowers costs for both businesses and regulators, while keeping the Data Act's broader safeguards in place.

Stakeholder views

Stakeholder engagement on Article 36 has been modest, reflecting both its limited practical relevance and lack of widespread awareness. As smart contracts for data sharing are still in an early stage of development, few organisations have direct or practical experience with such tools. Many stakeholders acknowledge the intention but consider the rule premature, given the lack of mature use cases and common standards.

Blockchain developers are the most vocal critics, arguing that Article 36 adds legal and technical uncertainty without clear benefits, particularly for decentralized technologies. The main concern is focused on the Article 36 requirement for safe termination or interruption ("kill switch"), seen as one of the most technically challenging and conceptually incompatible rules for public blockchains.

Member States have also expressed concerns about the lack of practical and administrative expertise and administrative experience needed to oversee compliance and enforce Article 36 and call for a more flexible approach to allow for greater development and deployment of smart contracts.

1.1.2.8. Extending SME exceptions to small midcaps for access to public sector data under the Data Governance Act and the Open Data Directive

Currently, the Data Governance Act and the Open Data Directive foresee special rules to support small and medium enterprises (SMEs) – approximately 26.1 million active entities in the EU[46]. These rules take into account the specific circumstances that these entities face – such as limited resources – and create a favourable environment to help them grow and be competitive at home and abroad. The Data Governance Act currently supports SMEs by exempting them from charges for the re-use of data made available under Chapter II. The Open Data Directive facilitates the re-use of public sector documents by recommending that public bodies apply a fee equivalent to the "marginal cost," particularly when the requester is an SME and free of charge re-use is not possible.

However, when SMEs grow beyond 249 employees, they become "large enterprises" and become subject to greater compliance obligations. In this regard, the Draghi report calls for extending some mitigation measures, benefiting SMEs, to small mid-caps (SMCs) while the Letta report also advocates for distinguishing mid-caps from large corporations in EU

[46] Schulze Brock, P., Katsinis, A., Lagüera Gonzalez J., Di Bella, L., Odenthal L., Hell M., Lozar B., Secades Casino B. (2025) *Annual Report on European SMEs 2024/2025, SME performance review*. Publications Office of the European Union, Luxembourg. Available at: https://publications.jrc.ec.europa.eu/repository/handle/JRC142263

regulations. According to a 2022 study[47], one of the main difficulties for SMCs concerns complying with regulations and administrative requirements.

As many reports have highlighted, this transition in business size disproportionately affects SMCs across every sector, as they lose access to the exemptions available to SMEs, despite not yet having the resources of the largest companies. Consequently, compliance costs rise sharply as SMEs face the same obligations and enforcement standards as multinational corporations.

To address this "cliff-edge", the Commission has introduced in the Omnibus IV simplification Package[48] a new category of companies (approx. 38,000 in the EU) – small mid-caps (250-749 employees, with an annual turnover not exceeding EUR 150 million or an annual balance sheet total not exceeding EUR 129 million) which should also benefit from the favorable environment created for SMEs. Accordingly, the Digital Omnibus will propose to extend some provisions currently applicable to SMEs to SMCs in the data acquis.

Extending mitigating measures to a new, larger set of companies could create new incentives for SMEs to grow, as the current threshold regime may discourage companies from scaling up by delaying hiring or restructuring to avoid crossing the SME threshold. Reducing compliance costs would allow resources (legal and administrative) to be reallocated to core business activities such as R&D, product development and market expansion. Together, these factors would put EU SMEs in a more competitive position than SMEs in jurisdictions without such requirements.

The following measures are proposed to be extended to SMC privileges:

- The possibilities under the Data Governance Act for Member States to provide cheaper access to re-use of data from protected databases for SMEs and to establish separate, simplified information channels at the level of national single information points for SMEs should be extended to SMCs;
- For the Open Data Directive, the provision that documents should be made available for re-use to start-ups and SMEs free of charge and, where charges are necessary, they should be in principle limited to the marginal costs (Recital 36) should be extended to SMCs;
- Furthermore, the special focus on SMEs when identifying high-value datasets (Article 14 (2)(b)) and when evaluating the scope and social and economic impact of the Directive (Article 18 (2)(a)) should be extended to SMCs.

[47] European Commission (2022) *Study to map, measure and portray the EU mid-cap landscape – Final report*, Publications Office of the European Union. Available at: **https://data.europa.eu/doi/10.2873/546623**

[48] Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2016/1036, (EU) 2016/1037, (EU) 2017/1129, (EU) 2023/1542 and (EU) 2024/573 as regards the extension of certain mitigating measures available for small and medium sized enterprises to small mid-cap enterprises and further simplification measures.

Cost savings. According to the Commission's impact assessment (SWD(2025) 501 final)[49], based on a 2022 study[50], around 38,000 companies would be SMCs defined as 250-749 employees.

The Impact Assessment for the Data Governance Act[51] assumed an average fee of around EUR 500 per application to re-use public sector data, with public sector bodies able to make the data available free of charge or at a discounted price. This fee could be waived for SMCs, depending on Member States' implementation.

Assuming, on average, between 0.25 and 1 application per firm per year, this corresponds to potential savings of between EUR 125 and EUR 500 per company. Extending reduced-cost access to protected public sector databases from SMEs to all SMCs could therefore generate aggregate savings of between EUR 5 million and EUR 19 million per year across the EU, assuming approximately 38,000 SMCs. Data and assumptions are presented below in Table 5.

The assumption range follows a simplified approach derived from the methodology used in the Impact Assessment accompanying the Data Governance Act. These figures are indicative lower and upper-bound estimates, intended to reflect varying degrees of data-re-use activity across sectors and Member States.

By making SMCs eligible for reduced-cost access under the DGA, Member States could achieve annual savings within this range while broadening the number of organisations able to re-use protected public sector data and strengthening the overall uptake of data-sharing mechanisms.

[49] European Commission, Commission Staff Working Document – Impact Assessment Accompanying the Proposal for a Directive amending Directives 2014/65/EU and (EU) 2022/2557 and the Proposal for a Regulation amending Regulations (EU) 2016/679, (EU) 2016/1036, (EU) 2016/1037, (EU) 2017/1129, (EU) 2023/1542 and (EU) 2024/573 as regards the extension of certain mitigating measures available for small and medium-sized enterprises to small mid-cap enterprises and further simplification measures, SWD(2025) 501 final, Brussels, 21 May 2025.

[50] European Commission (2022) *Study to map, measure and portray the EU mid-cap landscape – Final report*, Publications Office of the European Union. Available at: https://data.europa.eu/doi/10.2873/546623

[51] European Commission, Commission Staff Working Document: Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act), SWD(2020) 295 final, Brussels, 25 November 2020.

Table 5: Estimated cost savings for SMCs under changes to the Data Governance Act

Item	Unit	Assumptions	Formula (stylised)	Estimated administrative cost savings	
				SMCs	
Extend to small mid caps the possibility benefit from cheaper access to data from protected public databases.	EUR	Fee per application to re-use public data = EUR 500 Average number of applications per firm per year: 0.25-1 38,000 companies fall under the definition of small mid-caps	Recurring cost (per year): EUR 500 × (0.25-1) × 38,000	**One-off**	**Recurring**
				N/A	≈ **EUR 4,750,000 - 19,000,000** per year

In addition, extending the existing Open Data Directive provisions to small mid-caps (SMC) companies is expected to further enhance data re-use and stimulate innovation, by making public sector information more accessible to a broader range of economic actors. This measure should therefore have a positive overall effect on data sharing and value creation across the EU data economy.

1.1.3. Preserving the objectives of the rules and other impacts

The planned measures under this section will preserve the original objectives of the Open Data Directive, the Data Governance Act and the Data Act: more easily accessible and re-usable data. The main objective of the Digital Omnibus Regulation is to streamline the number of data-related regulations into one coordinated Regulation, the Data Act, and to simplify the regimes. Therefore, most of the expected original impacts remain valid, and will in some cases even be strengthened. For example, merging the rules of the Open Data Directive with the rules of Chapter II Data Governance Act and including them into the Data Act will turn rules of the current Open Data Directive into a Regulation, contributing to greater harmonisation.

With the targeted amendments to the regime on data intermediation services providers and data altruism organisation, it should become more attractive to offer intermediation services or support data altruism. More voluntary data-sharing is expected, with more companies finding services that support them in this endeavour (e.g. offering match-making, contractual support, technical support with anonymisation or secure processing environments). Where such data-sharing is altruistic, in particular, it can lead to advancements in research on topics of general interest or societal goals (research on less common diseases, environmental protection, biodiversity) that cannot benefit from a strong commercial investment in research. However, the deletion of the requirement to register for data intermediation service providers may lead to

reduced transparency and accountability of the market. Without registration, competent authorities would likely have more limited visibility over operators' activities. User trust could also potentially be impacted. Nonetheless, these risks are considered limited, due to the intrinsic low risk associated to these types of activities. The overall stimulating impact on the data intermediation market, and positive externalities described above, are deemed on the whole beneficial to society.

Sharpening the trade secrets protection will make the Data Acts regime on sharing of data from connected devices more robust. This will strengthen know-how protection as an emanation of the fundamental freedom to conduct business (Article 16 of the Charter) and the right to protection of intellectual property (Article 17 para. 2 of the Charter).

The proposed reduction of scope of the Chapter V Data Act (business-to-government data sharing) by deleting the possibility for public sector bodies to demand access to privately held data where they have exhausted all other means (namely the purchase of non-personal data on the market, by relying on existing obligations to make data available or the adoption of new legislative measures), can theoretically reduce the social value created by the Data Act. That social value, however, comes at a high cost for a high amount of businesses who struggle to plan data sharing mechanisms on that basis as described above.

Last, while the changes to Chapter VI of the Data Act on contracts may have a light competition impact (due to the distinction made between contracts concluded before the entry into application of the Data Act, and after thereof), the latter are assessed as moderate since only covering a small segment of the market. The overall impact on the Data Act's objectives is limited since the change would only apply to custom-made services. Customers will remain bound by the contract signed until its expiry, unless the contracts included a possibility for early termination.

For all of the above changes, the monitoring frameworks laid out in the initial respective Impact Assessments will continue to serve as the reference for the continuous assessment of their implementation.

1.2. Adjustments to the data protection rulebook

The GDPR is the cornerstone of EU digital legislation. Its risk-based, technology neutral approach means that businesses' data protection obligations are tailored to the specific risks posed by their operations involving the processing of personal data. Stakeholders broadly share the view that the GDPR represents a balanced and sound legal framework on the protection of personal data. At the same time, businesses consider that further measures, including targeted legislative measures, could improve the application of the GDPR.

In this regard, stakeholders have raised in particular the need to provide more clarity to certain key GDPR concepts and to simplify certain obligations for data controllers, insisting on the respect of the GDPR risk-based principle, notably as regards AI and other new technologies. However, all stakeholders, including businesses, warn against the broad reopening of the GDPR, noting that they have invested in compliance and that fundamental changes to its framework would create unnecessary costs and legal uncertainty, contrary to the aim of simplification. All stakeholders also underline the need for more practical guidance and increased stakeholder engagement from the enforcers of the GDPR, the data protection authorities (DPAs) which, at EU level, come together within the European Data Protection Board (the EDPB). In addition, they call for more tailor-made support, such as templates and checklists, especially for SMEs.

While some of those concerns can be best tackled through non-legislative measures, as they do not concern the letter of the GDPR, and the work on them is already on-going[52], others are more efficiently addressed by means of legislative adjustments in the GDPR. The targeted amendments proposed in the Digital Omnibus are based on specific feedback from stakeholders and aim to address the compliance challenges they have raised without undermining the GDPR policy objectives, including the high level of data protection. Where relevant, the amendments of the GDPR proposed in the Digital Omnibus are reflected in Regulation (EU) 2018/1725 on the protection of natural persons with regard to the processing of personal data by the EU institutions, bodies, offices and agencies in order to maintain a strong and coherent data protection framework in the Union and ensure a consistent interpretation.

1.2.1. Analysis of the problems and opportunities

The rules. The GDPR protects individuals when their personal data is processed. It is at the centre of the legal framework that guarantees the fundamental right to data protection, as enshrined in the Charter of Fundamental Rights of the European Union and in the Treaties. The GDPR has the dual function of protecting an individual's right to data protection and ensuring the free movement of personal data within the Union, and it applies to organisations in both the public and the private sector.

[52] European Data Protection Board (2025) *The Helsinki Statement on enhanced clarity, support and engagement*. Available at: The Helsinki Statement on enhanced clarity, support and engagement | European Data Protection Board

Personal data means any information relating to an identified or identifiable individual. The GDPR gives individuals control over their personal data. The GDPR creates obligations for controllers and processors, the entities responsible for the processing of personal data. The GDPR includes also an obligation to maintain records of personal data processing with an exception for certain processing activities by small and medium-sized companies and organisations with less than 250 employees. The Commission has proposed to simplify this obligation for those entities as well as for small mid-cap companies and organisations with the same number of employees, as a part of its Omnibus IV proposal[53], which is currently being discussed by the co-legislators.

The GDPR establishes key principles that apply to the processing of personal data, namely lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality. Certain types of personal data, known as special categories of personal data, are afforded special protection under the GDPR.

Under the GDPR, the monitoring and enforcement of the application is a responsibility of national authorities, in particular data protection authorities and courts. The GDPR equips the independent data protection authorities with harmonised enforcement powers and establishes a cooperation and consistency mechanism for cases that concern cross-border processing. The EDPB, an EU body which is composed of the heads of the DPA of each Member State and the European Data Protection Supervisor, is responsible for ensuring the consistent application of the GDPR. To this end, it issues guidelines and opinions and also exercises a dispute resolution function between DPAs. In 2025, the co-legislators reached a political agreement on the Commission's proposal for a GDPR procedural rules Regulation which will ensure better and faster cooperation between DPAs when enforcing the GDPR. The decisions and lack of action by national DPAs can be challenged in competent national courts.

The main issues. Complying with the GDPR involves both costs and benefits for businesses. In addition to initial implementation costs, companies encounter operational compliance costs, such as those related to monitoring, reporting[54] and training. The overall impact depends on the nature of the business model in question.[55] According to some reports[56], the overall spending on data privacy around the world has remained relatively constant or even slightly increased over the past four years (2021-2024) for companies with more than 250 employees, while for companies with less than 250 employees it has generally decreased. In this context, it is

[53] Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2016/1036, (EU) 2016/1037, (EU) 2017/1129, (EU) 2023/1542 and (EU) 2024/573 as regards the extension of certain mitigating measures available for small and medium sized enterprises to small mid-cap enterprises and further simplification measures.

[54] The GDPR does not as such place any reporting obligations on businesses. However, the GDPR obliges them, for instance, to maintain records of processing, carry out data protection impact assessments for high-risk processing activities and to notify data breaches to supervisory authorities.

[55] Commission Nationale de l'Informatique et des Libertés (2024) *The economic impact of GDPR, 5 years on*. Available at: The economic impact of GDPR, 5 years on | CNIL

[56] Cisco (2025) *2025 Data Privacy Benchmark Study*. Available at: Cisco Data Privacy Benchmark Study - Cisco. This report draws upon data gathered in autumn 2024 from an anonymous survey of security and privacy professionals. The survey included 2600+ respondents in 12 countries (5 Europe, 4 Asia, and 3 Americas), including EU Member States France, Germany, Italy, and Spain.

noteworthy that 96% of respondents from the organisations surveyed have assessed that, overall, the benefits from privacy investment outweigh the costs. This has been explained by the fact that compliance with privacy laws is usually considered as a business advantage as it enhances the organisation's reputation and customer trust.[57] However, it is in general difficult to quantify the benefits of the GDPR as they are not directly visible in the market.[58] Compliance with the GDPR may also have "residual" positive effects. It has for instance been assessed that the GDPR has helped avoid between EUR 585 million and 1.4 billion in losses due to the fact that compliance with data protection rules contributes to combatting underinvestment in cybersecurity. These gains have been assessed to represent only a small portion of the total benefits of the GDPR in the field of cybersecurity.[59]

The overall satisfaction with the effects of data protection laws is echoed in the feedback received from European stakeholders on the application of the GDPR. The participants of the Implementation Dialogue on the application of the GDPR, organised on 16 July 2025, were asked about challenges they have encountered in the application of the GDPR and suggestions for its improvement. The participants comprised of EU-level umbrella organisations representing different sectors of the industry and civil society, including members of the GDPR multi-stakeholder Expert Group ensuring a balanced representation of business and civil society[60]. The vast majority of stakeholders were of the opinion that the GDPR provides a balanced legal framework, which is, in principle, fit for purpose.

However, challenges were identified in particular in relation to the consistent interpretation and enforcement of the GDPR by supervisory authorities and stakeholders emphasised the need to reinforce legal certainty by introducing measures to reduce legal fragmentation and improve the consistent application of the GDPR. The need for greater consistency in the application and enforcement of the GDPR has been recognised also by data protection authorities and the European Data Protection Board.[61] In practice, the need for more harmonised and consistent interpretation of the GDPR is evidenced, for example, by the lack of fully harmonised lists established by DPAs at national level which stipulate when a Data Protection Impact Assessment is required and the low number of lists indicating when Data Protection Impact Assessment is not required (whitelists)[62].

---

[57] For instance, 95% of respondents consider that privacy remains core to customer service and that customers will not buy from a company if their data is not properly protected and 90% is of the respondents are of the view that strong privacy laws make customers more comfortable sharing their data in AI applications.

[58] Commission Nationale de l'Informatique et des Libertés (2024) *The economic impact of GDPR, 5 years on*. Available at : The economic impact of GDPR, 5 years on | CNIL

[59] Commission Nationale de l'Informatique et des Libertés (2025) *Cybersecurity economics and the benefits of GDPR*. Available at: Cybersecurity economics and the benefits of GDPR

[60] The GDPR Multi-stakeholder Expert Group is an advisory body established by the Commission. It provides feedback and expertise from a wide range of stakeholders on the GDPR's application, including challenges they face in relation to its application.

[61] EDPB, The Helsinki Statement on enhanced clarity, support and engagement, 3 July 2025.

[62] See the EDPB Opinion's on the different draft lists of Member States requirements for when a DPIA is required and is not required (whitelists). Opinions | European Data Protection Board.

Stakeholders also called for more clarity to certain key aspects central to the interpretation of the GDPR, such as the definition of personal data[63] in light of the recent case law of the European Court of Justice, in order to ensure a common and harmonised understanding of this core concept throughout the EU.

In addition, many stakeholders considered that certain obligations placed on organisations are burdensome and unnecessary given the low risk the processing causes to data subjects. For example, the obligation to inform data subjects about the processing of their personal data, when the data subject has in practice already received relevant information, is not seen as necessary to data subjects concerned. Also, the obligation to notify the data protection authorities of a low-risk data breach was considered burdensome. Some GDPR obligations, in particular those mentioned above, were considered particularly challenging to fulfil for small and medium-sized enterprises and organisations due to their limited internal structures and expertise in data protection and overall resources. According to some surveys, the average number of data breach notifications to DPAs was 363 notifications per day from January 2024 to January 2025.[64] The number of notifications is particularly high in some Member States.[65] These numbers can be partly explained by the current relatively low threshold for notifications and they imply that the current obligation can create considerable resources implications also to GDPR enforcers.

Some of the concerns raised by stakeholders can be addressed through targeted legislative amendments to the GDPR. While it is not possible to calculate the exact cost savings to organisations of such amendments[66], it can be generally assessed that enhancing legal certainty by clarifying certain GDPR key notions and further harmonising its application will bring direct benefits to organisations, for instance, due to reduced need for legal advice and consultancy and decreased non-compliance costs. Furthermore, it is possible to produce some direct cost savings for organisations by cutting administrative burdens through reduced ”reporting” obligations, when possible without undermining the high level of data protection under the GDPR, and by providing a centralised channel for ”reporting”. Finally, some legislative amendments could provide untapped opportunities to organisations by enhancing innovation and enabling a wider

[63] CJEU, Case C-413/23 P *EDPS v SRB,* 4 September 2025.

[64] DLA Piper GDPR fines and data breach survey, January 2025, available at dla-piper-fines-and-data-breach-survey-2025.pdf.

[65] E.g. the total number of data breach notifications between 25 May 2018 and 27 January 2025 in the Netherlands was 171,140, in Germany 167,454, in Poland 70,204, in Denmark 53,802, in Ireland 42,334, in Sweden 35,827, in Finland 34,355, in France 24,329, in Spain 11,711 and in Italy 11,096. *Ibid.*

[66] This is partly due to the fact that companies of different sizes and from different sectors experience varying levels of compliance costs, the costs incurred may include both direct and indirect costs (due to non-compliance) and compliance may involve not only costs caused by initial compliance efforts but also long-term costs (which may be outbalanced to some degree by ’compliance savings’), which are extremely difficult to calculate. In addition, given the constantly evolving digital environment, the economic impacts of the GDPR are intertwined with broader technological developments and regulatory changes, making it challenging to attribute specific effects solely to the GDPR.

and more effective uptake of new technologies in their operations, while ensuring that individuals' fundamental right to data protection is appropriately safeguarded.

The objectives. The proposed amendments aim to harmonise, clarify and simplify GDPR provisions, without affecting the core principles and requirements of the GDPR or undermining the high level of data protection. They would increase legal certainty and facilitate operators' compliance, taking into account the need to support operators' responsible use of personal data to boost economic growth and innovation and to maintain individual's trust in and willingness to engage with digital technologies.

Stakeholder views

Based on the Commission 2024 report on the application of the GDPR and subsequent stakeholder consultations, including the Implementation Dialogue on the application of the GDPR, stakeholders generally consider that the GDPR is a legislative framework which takes different interests into account in a balanced way, and continues to deliver. However, business stakeholders have suggested some measures, including targeted amendments to the GDPR, to clarify certain key concepts and to reduce controllers' certain obligations that are deemed unnecessary . Member States, in their submissions to the Council of the European Union's Working Party on Data Protection also generally note that they are not in favour of a general reopening of the GDPR. Most Member States were cautious about amending the GDPR and only supported targeted amendments to reduce certain obligations on controllers and to bring more harmonisation to certain concepts in the GDPR itself. Civil society stakeholders have underlined in this context the need to preserve the current high level of data protection. There is a general call to ensure a more harmonised and consistent interpretation and enforcement of the GDPR, but there also is a consensus that there should not be a general reopening of the GDPR.

All stakeholders underlined the need for more practical guidance and increased stakeholder engagement from the national data protection authorities and the European Data Protection Board. They also called for more tailor-made support, such as templates and checklists, especially for SMEs.

The importance of clear articulation of different pieces of EU legislation was raised by all stakeholders. Many considered that this could be achieved through guidance and enhanced cooperation of different regulatory authorities. Others stated that this would require streamlining certain key concepts and reporting requirements but should not be used as a pretext to lower the level of data protection.

Stakeholders identified in particular the following challenges:

- The lack of clarity on certain notions in the GDPR, including what constitutes "personal data", in particular when an individual is "identifiable";
- The burden of preparing "privacy notices" in particular for small operators carrying out low-risk processing;
- The burden of handling abusive requests for access to personal data;
- The lack of clarity on the notion of "high-risk" processing, which triggers the obligation to undertake a data protection impact assessment under the GDPR;
- The broad application of the notion of special categories of personal data in the GDPR;
- The lack of clarity on the possibility to process personal data and in certain instances special categories of personal data for the development and operation of artificial intelligence;
- The notification of low-risk data breaches to the supervisory authorities, including the relationship with reporting requirements under other EU digital legislation;
- The lack of clarity on the conditions for carrying out automated individual decision-making.

1.2.2. Simplification measures and impacts

1.2.2.1. The definition of personal data

The GDPR provides that personal data is any information relating to an "identified or identifiable" natural person (Article 4), having regard to the means reasonably likely to be used to identify the person. A person is considered to be identifiable where she or he can be identified directly or indirectly, having regard to the means reasonably likely to be used to identify the person. Stakeholders have indicated that there is a lack of clarity on when an individual is "indirectly identifiable", and therefore whether the GDPR applies to certain data. This includes the situation where "pseudonymous" data are transmitted to a recipient. Taking into account the recent case-law of the Court of Justice of the European Union, the proposal clarifies that information is not to be considered personal data for a given entity where that entity does not have the means reasonably likely to be used to identify the natural person to whom the information relates. The proposal further clarifies that an entity for which the information is not personal data, in principle, does not fall within the scope of application of Regulation (EU) 2016/679, for the processing of that data. The proposed amendment would bring clarity to this GDPR key notion, also reflecting the recent case-law of the CJEU. It 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.

1.2.2.2. Mechanism to give greater legal clarity on anonymisation and pseudonymisation techniques

Uncertainty about GDPR-compliant anonymisation has been among the most pressing problems signalled by industry over the years. Companies would like to have more certainty about specific pseudonymisation techniques and criteria to be used for assessing risks of re-identification.[67]

To further support entities in their efforts to use pseudonymisation, the proposal puts forward a mechanism to further clarify the means and criteria to determine whether data resulting from pseudonymisation can be considered non-personal for certain entities. This will significantly increase legal clarity and certainty and reduce compliance burden, as companies will be able to use and rely on the implementation of such means and criteria as an element to demonstrate that data no longer constitutes personal data for them. This is especially true for innovative start-ups and SMEs that often do not have the resources to solicit expert legal advice. Using the means and criteria outlined in those implementing acts will, however, not release controllers from the ultimate responsibility to verify that data shared with other parties are non-personal or, where this is not the case, that the requirements under the GDPR are met. Considering that such assessments always come with a certain risk of an authority declaring the used technique non-compliant, the proposed amendment will seriously facilitate operations for businesses.

1.2.2.3. The processing of personal data for scientific research purposes

The research community has complained about the lack of clarity about conditions for GDPR-compliant scientific research despite the fact the GDPR affords specific status for such research by providing, for example, the possibility to rely on a broad consent and the presumption of compatibility for further processing.

Scientific advancement, strengthening the European technological basis, and encouraging the EU to become more competitive, including in its industry, are objectives laid down in the EU's Founding Treaties, in particular under Article 179(1) TFEU on achieving a European Research Area, in which researchers, scientific knowledge and technology circulate freely, while promoting all the research activities deemed necessary by virtue of other Chapters of the Treaties. Furthermore, Article 13 of the Charter of Fundamental Rights of the European Union provides that scientific research shall be free of constraint, and academic freedom shall be respected.

The proposed amendments would address the lack of clarity about the conditions for scientific research by providing a definition of scientific research (Article 4 GDPR), further clarifying that further processing for scientific purposes is compatible with the initial purpose of processing (Article 5(1)(b) GDPR), and by clarifying that scientific research constitutes a legitimate interest within the meaning of Article 6(1)(f) GDPR. It is also proposed to extend the exceptions from the information obligation for processing (Article 13), by stipulating that when the provision of information proves impossible or would involve a disproportionate effort or renders impossible or seriously impairs the achievement of the objectives of that processing, the controller does not need to provide the information. These changes would facilitate research and innovation in the Union.

1.2.2.4. The processing of personal data for the development and operation of AI

The proposal clarifies 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 of Regulation (EU) 2016/679, except where other Union or national laws explicitly require consent, such as requirements on gatekeepers designated under the Digital Markets Acts – notably Article 5(2) of Regulation (EU) 2022/1925. The proposed amendment would clarify when the controller may rely on Article 6(1)(f) GDPR to pursue a legitimate interest in the context of development and use of AI systems and models.

It also takes into account 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. Special categories of personal data may exist in the training, testing or validation data sets or be retained in the AI system or the AI model. In order not to disproportionately hinder the development and operation of AI and taking into account the capabilities of the controller to identify and remove special categories of data, the proposal introduces an exception from the prohibition on processing special categories of personal data for the

development and operation of AI (Article 9 GDPR). The derogation should only apply where the controller does not aim to process special categories of personal data, but such data are nevertheless residually processed. The controller is still required to implement appropriate technical and organisational measures to avoid processing of special categories of personal data and is required to take such measures during the entire lifecycle of an AI system or AI model. It is required to remove such data once it is identified and to protect such data from being used to infer outputs, being disclosed or otherwise made available to third parties. The proposed amendment would clarify situations where it has previously been unclear whether such processing could be carried out in a lawful manner, in accordance with the requirements of Article 9(2) GDPR. It would therefore directly contribute to the objective to support innovation and develop European AI that is trustworthy and non-discriminatory, while maintaining a high level of data protection.

1.2.2.5. The exercise of the individual's right of access

The GDPR provides individuals with the right to access their personal data (Article 15 GDPR). The right of access should allow the data subjects to be aware of, and to verify, the lawfulness of the processing and enable them to exercise their rights under the GDPR. In some cases, the right of access is used by data subjects in an abusive manner for purposes other than the protection of their personal data. This has frequently been raised as an issue for controllers who are required to dedicate significant resources to responding to abusive access requests. The abuse of the right would arise, for instance, where the data subject intends to cause the controller to refuse an access request in order to subsequently demand compensation, potentially under the threat of bringing a claim for damages. The proposal provides that, in such cases, the controller may refuse to comply with the request or may charge a reasonable fee. Moreover, controllers should bear a lower burden of proof to demonstrate that an access request was excessive. The proposed amendment would provide legal clarity to controllers on lawful options to handle situations where access requests are clearly abusive. This would allow controllers to allocate their resources more effectively and focus in a timely manner on genuine access requests and other requests contributing to the exercise of data subjects' rights.

1.2.2.6. Controller's information requirements

The GDPR requires data controllers to provide the data subject with information on the processing of his or her personal data (Article 13). This information is typically provided in so-called privacy notices. Currently, the obligation to provide the required information does not apply where and insofar as the data subject already has the information. The proposal extends the derogation to situations where the processing is not likely to result in a high risk to the data subject, and where there are reasonable grounds to expect that the data subject already has the information. This would especially be the case when the relationship between the controller and the data subject is very clear and limited and the controller's activity is not particularly data-intensive or high risk. Examples of this include the relationship between craftspersons and their clients, as well as the processing of personal data by associations and sport clubs to manage their membership, communicate with their members or to organise various activities. The

proposed amendment would ease the information obligation in situations meeting this obligation would bring no genuine added value to data subjects and could therefore be considered unnecessary. The change would benefit in particular small operators, such as craftspersons and sport clubs, that carry out low-risk data processing to whom information obligations may cause disproportionate burden given that the processing of personal data is not their core activity.

1.2.2.7. Requirements for automated individual decision-making

The GDPR provides for rules governing the processing of personal data when the data controller makes decisions which have legal effects or similarly significant effects on the data subject, based solely on automated processing (Article 22). The provision clarifies the circumstances as to when decisions based solely on automated processing are permitted. In particular, it clarifies that when assessing whether a decision is necessary for entering into, or performance of, a contract between the data subject and a data controller, the assessment of "necessity" should not require that the decision could be taken only by solely automated processing. This means that the fact that the decision could also be taken by a human does not prevent the controller from taking the decision by solely automated processing. Some controllers have reported that this is a reason which has prevented them from applying Article 22. The proposed amendments would clarify this scenario and provide greater legal certainty to controllers regarding when they can lawfully make use of automated individual decision-making and what are the conditions for it. The grounds for using automated decision-making , as well as the current requirements on suitable measures to safeguard the data subject's rights, including the right to obtain a human review, as well as on processing of special categories of personal data by automated means would remain unchanged.

1.2.2.8. Data breach notification to supervisory authorities

The GDPR requires data controllers to notify a personal data breach to the competent supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons (Article 33). It is proposed that this threshold is aligned with that for communicating a personal data breach to the data subject (Article 34), so that one uniform threshold, namely that of 'high risk', applies. In the case of a data breach that is not likely to result in a high risk to the rights and freedoms of natural persons, the controller is not required to notify the competent supervisory authority. It is also proposed that controllers use a single-entry point, to be established by amending Directive (EU) 2022/2555, when they notify data breaches to the supervisory authority[68]. In addition, it is proposed that the European Data Protection Board prepare a common template for notifying data breaches to the competent supervisory authority and a common list of circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person. The proposed amendments would make it easier for controllers to notify a breach through a single channel,

[68] See also Chapter 2 of this Staff Working Document.

including in cases where a data breach is only one of the elements of a broader incident to be reported. They could also significantly reduce controllers' administrative burden by not requiring them to notify data breaches which are likely to cause only a low risk to data subjects. Furthermore, they could alleviate the workload of data protection authorities, allowing them to concentrate their resources especially on high-risk data breaches. The changes would also harmonise at EU level the notion of "high risk" in the context of data breach notifications and thereby bring more clarity to controllers.

1.2.2.9. Notion of high risk and the lists of processing activities requiring and not requiring data protection impact assessment

The GDPR requires controllers to conduct a data protection impact assessment where the processing of personal data is likely to result in a high risk to the rights and freedoms of a natural person (Article 35). Each supervisory authority is obliged to establish and make public a list of processing operations which require such impact assessment. In addition, the GDPR provides that supervisory authorities may establish and make public a list of the processing operations which do not require a data protection impact assessment. It is proposed that instead of national lists, a single list of processing operations be provided at EU level, introducing a common list throughout the EU and indirectly ensuring a common understanding of what constitutes "high-risk" processing throughout the EU. In addition, the publication of an EU-level list of the type of processing operations for which no data protection impact assessment is required would become mandatory. The lists of processing operations would be prepared by the Board and adopted by the Commission as an implementing act. It is also proposed that the Board is given the task to prepare a common template and a common methodology for conducting data protection impact assessments, to be adopted by the Commission as an implementing act. The proposed amendments would provide legal certainty to controllers by reducing fragmentation in the requirements of conducting a data protection impact assessment and clarifying the notion of "high risk".

1.2.3. Estimated impacts

The proposed amendments would **strengthen European competitiveness** and support the uptake of new technologies. The changes would benefit operators that process personal data by simplifying GDPR rules and further harmonising their interpretation and application. This can be expected to bring operators **direct regulatory gains** through improved operational efficiency and risk mitigation as well as an improved environment for innovation and development. These gains would result in **cost -savings,** including through needing less time and resources to ensure GDPR-compliant data processing. While it is not possible to support these claims with precise figures, as explained above in section 1.2.1, the expected advantages can be described in qualitative terms, as done in section 1.2.2.

SMEs and other small operators **would benefit from most or all of the proposed changes**. For instance, greater clarity would be provided to SMEs as to when a data protection impact assessment is required and when it is not. The simplification of information requirements would

greatly assist SMEs that are not engaging in data-intensive or high-risk processing activities, such as craftspersons, hairdressers or bakers, as they would be relieved of the requirement to prepare privacy notices. SMEs would also benefit from the change that low-risk data breaches do not need to be notified to the supervisory authority, reducing considerably their administrative burden. The proposed clarifications to the right of access would also reduce SMEs' burden in situations where that right is used for purposes other than data protection. Previously, if this right was abused, a controller had little legal recourse to refuse to act on a request, even when replying to it required significant resources.

The proposed amendments to the GDPR **would not negatively impact individuals' fundamental rights,** including their right to data protection. Instead, they would simplify requirements for low-risk processing, harmonise certain standards and clarify certain key GDPR concepts, which would allow controllers to better understand the requirements for the processing of personal data and could therefore lead to improved data protection. They would also allow controllers to implement more effective data protection policies and concentrate their resources towards more data-intensive or otherwise higher-risk activities for which the measures to protect personal data are most critical. Finally, by increasing legal certainty, the proposed changes would ensure a more harmonised application and enforcement of the GDPR, which would benefit also individuals.

Concerning the proposed amendments to the GDPR provisions directly concerning individuals' data protection rights (Article 12 and 13), those changes would not affect the level of data protection provided, putting the individuals concerned at a disadvantage. The reduction of information requirements (Article 13) would only concern situations where the individual already has the information necessary to exercise his or her rights under the GDPR, based on the close relationship with the controller, and where the controller's activity typically requires only limited processing of personal data with low risks – such as the processing of customer data by a craftsperson. In addition, individuals would be entitled to obtain additional information on the processing of their personal data through an access request based on Article 15 GDPR. Similarly, the proposed amendments to the conditions concerning the exercise of the right of access (Article 12) would not lower the level of data protection. Those clarifications are specifically designed to prevent the abuse of that right and they would not prevent individuals from exercising it for the purpose of protecting their personal data. In addition, in situations where an alleged abuse arises, it would be for the controller to prove that this is the case.

The proposed targeted amendments respond to specific concerns raised by stakeholders and Member States in the context of consultations referred to in the above sections.

1.3. Modernising the cookies policy: addressing consent fatigue and better alignment with data protection rules

Addressing the issue of cookie consent fatigue, caused by repetitive and often non-transparent cookie banners is long overdue. The Digital Omnibus proposes targeted amendments to address this and simplify users' experience online, reducing the number of cookie banners that users are flooded with online. The proposal makes a targeted adjustment in the ePrivacy Directive, to allow for a more developed regulatory framework set under the GDPR to appropriately address the issue.

The withdrawal of the proposal for an ePrivacy Regulation leaves the current rules dating from 2009 on storing of and access to information stored on a device ("terminal equipment"), including by means of cookies or similar technologies in place. These rules require users' or subscribers' consent, except for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or when strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.[69] These rules do not only cause a substantial burden for businesses, but have also caused "cookie consent fatigue" amongst users who are solicited with numerous cookie banners in their daily interactions online. The design of those banners, the presentation of the information and the frequency in which the banners are displayed often make it hard if not impossible for individuals to understand what will happen to their data. This hampers their ability to make a real choice over the use of their personal data. To address this, the proposal aims to closer align the rules for accessing personal data by placing cookies or similar technologies on terminal equipment with those of the GDPR, while maintaining the consent requirement as a rule. The package brings forward measures to ensure that individuals stay in control over their data including by centrally setting their preferences, for example via a browser. This is done via a targeted amendment, relying on the strong protection standard of the GDPR.

1.3.1. Analysis of the problems and opportunities

The rules. The ePrivacy Directive (Directive 2002/58/EC) sets out a framework for privacy in the digital age, and more specifically for the confidentiality of communications and the protection of access to terminal equipment to protect the right to privacy of users. In this context, Article 5(3) ePrivacy Directive establishes rules on storing of information and the gaining of access to information already stored in the terminal equipment, including by use of cookies and similar technologies. The aim of the provision is to protect users' devices ("terminal equipment") and to protect any information (personal or non-personal data) stored on or

[69] See Article 5(3) Directive 2002/58/EC (ePrivacy Directive).

accessed from the user's device. As a general rule, Article 5(3) requires (i) clear and comprehensive information on and (ii) consent for storing information on or accessing stored information on the user's devices. While exemptions to this general consent requirement exist (e.g. no consent is needed for cookies that are strictly necessary to provide the service requested by the user or that are technically necessary for the provision of the service), consent of the user is necessary in most cases. These rules date from the early 2000s, were amended in 2009, and are a *lex specialis* to the GDPR when personal data is being processed. Article 5(3) only regulates access to the information (based on consent in most cases) on the user's device ('terminal equipment'), while processing of personal data obtained are governed by the GDPR (in line with Article 6 GDPR).

The main issues. Today, the rules on cookies laid out by the ePrivacy Directive are outdated and inadequate for contemporary privacy and data needs. To obtain the user's consent, many entities currently use cookie banners to comply with the consent requirement. The design of these banners and their wide-spread use cause nuisance known as 'consent fatigue' among users.

From a privacy and data protection point of view, the design and presentation of the information on the banners is complex. Users are often overwhelmed with information and asked to give consent for a multitude of processing purposes, often lacking transparency and real control over what will be done with their data. According to industry studies, this leads to users feeling overwhelmed or bothered ("consent fatigue") often randomly either accepting (54%) or rejecting (26%[70]) all cookies, in order to access the content they would like to see, without making an informed decision, mindlessly accepting without proper consideration, thereby undermining the intended protection. Consumers generally do not feel fully in control of the online content they are shown and the decisions they make online.[71] In addition, the controllers often continue relying on consent for the subsequent processing of information collected via cookies even if that is not the most appropriate legal basis for processing under the GDPR.

Moreover, the effectiveness of the current regime is questionable. In a 2022 evaluation of the Directive, only 3 out of 30 competent authorities indicated that Art 5(3) functions "well", most (13/30) assessed it as "fair", and 3/30 as "poor".[72] In addition, enforcement of Article 5(3) ePrivacy Directive and the applicable GDPR provisions may be subject to different national authorities depending on the transposition by Member States. This leads to uncertainty and diverging practices across Member States but also between the different authorities within a Member State. Also on the business side, 62% stated that Article 5(3) ePrivacy Directive was a problem.[73] The consent requirement for placing or accessing information on terminal devices is seen as overly rigid, covering even non-intrusive practices such as creating statistics about

[70] IAB Europe (2025) *Optimisation over reform: understanding EU consumers' perception and knowledge of the ad-funded internet and related privacy rights issues*. Available at: IAB-Europe-Ad-Funding-Online-Services-Report-2025-FINAL.pdf.

[71] BEUC (2023) *Connected, but unfairly treated: consumer survey results on the fairness of the online environment.* Available at: BEUC-X-2023-113_Fairness_of_the_digital_environment_survey_results.pdf. Less than half (43%) of respondents to the study reported that they feel in full control.

[72] European Commission, Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector, 2022.

[73] Ibid.

the use of websites and mobile applications, audience measurement, preserving the security of the device or the offered service.

Most respondents to the Data Union Strategy consultation view the ePrivacy Directive as outdated and in urgent need of reform: around 45% of 101 respondents do not think that the current ePrivacy rules provide a good balance and reflect well the technical situation as regards processing of data on IoT devices in professional/industrial use, as opposed to only 11% who said this is the case; one respondent noted that in their sector, 60% of data is lost due to rules designed for a very different technological context.

In a dedicated 'reality check' focus group with stakeholders on the cookie framework of Art. 5(3) ePrivacy Directive[74], several of the participating stakeholders held that requiring consent in all cases as currently mandated was too rigid. Stakeholders also report that the current regime does not give incentives to use privacy-enhancing technologies as mitigation measures, for instance apply pseudonymisation or use secure processing environments. Since consent is always required this creates an incentive to collect consent also for intrusive processing purposes (e.g. location data not necessary for the service provided) as such data may be further monetized.

Finally, different interpretations and fragmentation of the enforcement of these rules across Member States which result from the current status as a Directive pose challenges to harmonised enforcement and accountability of non-compliant actors, ultimately hampering the strong protection of citizens. This includes the fact that in some Member States, data protection authorities are competent to enforce the rules, while in other Member States other supervisory authorities have been designated to enforce the rules of the ePrivacy Directive, often leading to diverging interpretations. A majority of businesses consulted reiterate these concerns about fragmented enforcement, and call for greater harmonisation to increase legal certainty.

While civil society organisations and consumer protection organisations underline that the current regime is necessary to protect users, they also see problems with how businesses ask users for consent. According to the representatives, cookie pop-up banners are complex by design, making it difficult for users to understand what will happen to their data. They claim that a majority of users do not want to be tracked.

Costs for businesses. Implementation and compliance with the current rule can be costly. The cost for businesses to set up cookie banners vary depending on the solutions the entity opts for. In 2014, at the time of evaluation and impact assessment to review the Directive, average compliance costs were estimated around EUR 900 per website (including the costs associated with legal advice, updates to privacy policies, and technical updates to websites).[75] Considering an average inflation rate of 2% per year from 2014-2025, we can estimate an average cost of

[74] See Annex I, Chapter IV.

[75] European Commission, Commission Staff Working Document Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) {COM(2017) 10 final}, part 1/3, p. 37.

EUR 1,200 per website over the lifespan of three years[76], resulting in yearly costs of EUR 400. During the 'reality check' focus group on Art. 5(3) ePrivacy Directive, one business association reported that the average yearly cost of maintaining a cookie banner for a middle-sized publisher amounts to EUR 100,000–500,000. Another stakeholder from the e-commerce industry estimated that it incurred yearly personnel costs of around EUR 2.0 million to comply with ePrivacy rules (not only focusing on Article 5(3)). The estimates of costs reported by SMEs in a dedicated SME panel conducted by the Commission[77] indicated yearly costs between EUR 100 to EUR 2,000 per year.

Taken together, this data would lead to confirm the EUR 400 as an average annual cost estimate. Assuming a total of 10 million active websites in the Union and estimating that about 41% display a cookie banner[78], the estimate cost over a year amounts to EUR 1.64 billion - and 4.92 billion over a period of 3 years.

An indication of scale: productivity estimates. Out of the total EU population of 450.4 million[79], roughly 75% use the internet to find information about goods and services[80] and thus visit websites. Assuming that an average user visits 100 websites a month[81] of which 85% use cookie banners[82], spending an average of 3,5 seconds[83] per banner, this would result in approximately 334 million hours spent on cookie banners per year. Considering the average hourly wage across the EU[84], this equates to costs of roughly EUR 11.2 billion per year. This value of lost productivity time would apply if internet users would browse websites predominantly for professional reasons and during working hours. However, as people visit websites mostly during their free time, such loss of productivity needs to adjust the value to the monetary value that individuals can award to leisure time. Calculating that value is not impossible and done notably when calculating the value of investments in transport systems, e.g. to calculate what the monetary value cutting commuters' travel time would have. Depending on a range of factors (reason for travel, mode of transport), transport planning

[76] The three years are an assumption of the average lifespan of a website, according to Deloitte, Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector, cited in European Commission, Commission Staff Working Document Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) {COM(2017) 10 final}, part 1/3, p. 37.

[77] See Annex I, Chapter III.

[78] Deloitte, Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector, cited in European Commission, Commission Staff Working Document Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) {COM(2017) 10 final}, Annexes to the report, p.14.

[79] Eurostat (2025) *Population change – Demographic balance and crude rates at national level*. Available at : [demo_gind] Population change - Demographic balance and crude rates at national level

[80] Eurostat (2025) *Individuals – internet activities.* Available at: [isoc_ci_ac_i] Individuals - internet activities

[81] Legiscope (2024) *Europeans Spend 575 Million Hours Clicking Cookie Banners Every Year*. Available at: Europeans Spend 575 Million Hours Clicking Cookie Banners Every Year.

[82] Ibid.

[83] Estimates start as low as two seconds. Legiscope (2024) assumes 5 seconds.

[84] Eurostat (2025) *Labour cost levels by NACE Rev. 2 activity.* Available at: [lc_lci_lev] Labour cost levels by NACE Rev. 2 activity

departments allocate between 30% and 70% of after-tax wage as the monetary value of leisure time[85]. That suggests that the gained value is in the order of EUR 3.36 billion to EUR 5.6 billion.

The objectives. Addressing the challenges identified for citizens and businesses alike, the framework governing the accessing and storing of personal data on a user's device should be placed under the strong protection framework of the GDPR. This reform shall ensure one single protection framework, for situations where personal data are being processed. This will not only lower costs for businesses via the reduction of cookie banners. It will also significantly simplify and enhance the experience of citizens online while continuing to offer the highest levels of protection for their personal data. In particular, users' rights to exercise their data protection rights and expressing their choices online are strengthened.

1.3.2. Simplification measures and impacts

1.3.2.1. Consent fatigue and cumbersome cookie banners

To address the growing problem of consent fatigue and ineffective cookie banners, and as a first step to modernizing the current ePrivacy framework, the Commission proposes to update the rules on storing information or on gaining access to information stored on devices ("terminal equipment"). The latter is designed to regulate amongst others the use of cookies and other similar technologies, therefore often referred to as the 'cookie Article'.

The proposal seeks to reduce the number of cookie consent banners by reducing the cases where consent will need to be obtained. The reform proposal moves the protection under the General Data Protection Regulation ('GDPR') and maintains the consent requirement as a rule when accessing a natural person's device.

In addition, the proposal will clarify that accessing the device and processing of personal data from connected devices which is necessary for certain specific low-risk purposes is considered lawful: carrying out the transmission of an electronic communication over an electronic communications network, provision of service, audience measurement when carried out by a media service provider under data protection safeguards, creating website and application usage statistics, and maintaining or restoring the security of the provided service.

1.3.2.2. Express choices with one click

In order to enhance user control over their data and device, and to avoid the usage of "dark patterns", i.e. artificially driving up consent rates by using manipulative or misleading cookie banner designs, a requirement is introduced that it must be possible for the user to give or refuse consent to processing via a single-click button whenever consent is used as a legal basis.

[85] See different studies referenced in this US Department of Transportation memo: Revised Departmental Guidance on Valuation of Travel Time in Economic Analysis, https://www.transportation.gov/sites/dot.gov/files/docs/Value%20of%20Travel%20Time%20Memorandum.pdf

Moreover, when the user has made a choice to give or refuse consent, the proposal requires the controller to respect this choice and, in case of refusal, prohibits asking the user again for a period of 6 months.

The Impact Assessment for the ePrivacy Regulation proposal already found that citizens do not have time to read long and complex privacy statements and find it difficult to understand what their consent implies.[86] Ideas to allow internet users to set their cookie consent preferences go back to the 2009 amendment to the ePrivacy Directive (cf. Recital 66 of Directive 2009/136/EC), are reflected in Article 21(5) of the GDPR as well as in the 2017 proposal of the Commission on a Regulation on Privacy and Electronic Communications (COM(2017)10). The proposal creates an obligation on controllers to respect the machine-readable expression of consent preferences via their online interfaces.

1.3.2.3. Standards for machine-readable preferences

Controllers would be obliged to respect the preferences of data subject set in an automated and machine-readable manner communicated via their online interfaces, i.e. web browsers or a mobile application[87]. The legal obligation should be accompanied by the development of standards, to ensure that the obligation can be easily met, and that the rigor of the GDPR requirements is carefully included by design in the technological solutions that will be developed. This is necessary to ensure that both website or app providers and the providers of the service used to set the preference signal can rely on a 'common vocabulary' of processing purposes and use the same technical specifications.

The obligation for controllers to accept centrally set machine-readable preferences does not apply to the providers of media services. This exemption is justified by the important role of media services providers in guaranteeing a plurality of opinions and safeguarding freedom of speech, both being central pillars of any liberal, democratic society. They need to maintain the possibility to individually ask each user of their services for consent to process their personal data, ensuring that users of media services are fully informed of the use of data in the advertising practices that are necessary for the provision of the media services.

1.3.2.4. Browsers signals

Given the pivotal role of web browsers in the users' navigation online, they can play an important role in supporting data subjects to set cookie consent preferences in accordance with the standards to be developed and to communicate, in a machine-readable manner, to websites the machine-readable expression of cookie consent preferences, colloquially also known as the 'browser signal'.

[86] Impact Assessment accompanying the ePrivacy Regulation Proposal part 1, p. 5.
[87] Cf. definition in Article 3 lit. (m) Regulation (EU) 2022/2065 ('Digital Services Act').

1.3.3. Estimated impacts

While the proposed amendments will not lead to the complete disappearance of cookie banners, it is expected that they will significantly reduce and simplify their use.

Since the proposal will lay down that processing of personal data from the device will be lawful for certain specific low-risk purposes, there will be less instances in which providers of websites and mobile applications will have to rely on consent. For an estimated 60% of used cookies[88], consent will not be required any longer. For providers of websites that do not use cookies based on consent, the cost of EUR 1,200 per website will be saved over the three-year life span of the website, thus resulting in significant reduction of burden.

As an example, for savings generated through such a measure for public sector websites, an approximate of EUR 320.2 million could be saved through the proposed amendments[89].

Assuming that the new measures will result in 50% of European private sector websites and 80% of public sector websites[90] no longer relying on consent and using cookie banners, and taking the estimates presented in the previous section, this would result in overall savings of EUR 2.4 billion[91] across the EU for a three year life span of websites, and more than EUR 800 million per year. The assumptions for the calculations are laid out in Table 6 below.

The proposed whitelist for purposes that will be considered to lawful will significantly reduce burden, especially for SMEs. The SME Panel consultation carried out by Commission services in September-October 2025 showed that 40% of responding SMEs primarily rely on cookies to create website statistics[92]. Companies relying on the whitelist will benefit from additional clarity and reduced burden, since they can rely on those grounds directly. The whitelisted grounds are very restricted and represent purposes of low-risk to the rights and freedoms of individuals' purposes.

Where cookies requiring consent are used, cookie banners can be designed in a less complex way. This not only helps users better understand the implications of their consent and can result in less cognitive burden for users to understand the information provided. It also contributes to cost reduction for businesses, including maintenance cost when adding new functions requiring cookies.

As concerns European productivity cost, judging from a conservative point of view, the cost will be decreased since i) less cookie banners will be used on the market, ii) cookie banners

[88] Deloitte (2020) *Cookie Benchmark Study*. Available at: Cookie Benchmark Study: April 2020 | PDF | Http Cookie | Privacy. The study assumes that roughly 30% of cookies on a website are used for tracking for advertising purposes. Conservatively, we have calculated with 40% in which consent would still be necessary.

[89] Eurostat (2025) *E-government activities of individuals via websites*. Available at: [isoc_ciegi_ac] E-government activities of individuals via websites. 70% of citizens interacted with public authorities online in one year, leading to 315 million users across these websites. Since these users would not be confronted with cookie banners anymore, assuming that they visit the site only once a year, it would lead to savings of productivity cost of EUR 10.2 million (315 million x 3,5 seconds x EUR 33.5 average wage).

[90] The assumption is higher for public sector websites, since those websites are assumed to particularly rely on cookies for purposes that will be included in the whitelist.

[91] 50% of current cost in EU (4,9 billion).

[92] See Annex I, Chapter III.

will be more transparent and less complex demanding less time from users to understand and make their choices; iii) users' choices will need to be respected for a certain time, prohibiting the repeated request for consent, and iv) users will be able to set cookie preferences centrally.

In a 2016 survey, 60% of EU citizens said that they have changed their privacy settings of their internet browser[93]. We assume that those users would also make use of centralised browser settings to set cookie preferences, amounting to approximately 200 million users. Given that these would not need to read and interact with cookie banners anymore, it would lead to reducing time spend interacting with cookie banners by 198 million hours per year, thus saving – when adjusting with leisure value of 30% - the equivalent of EUR 500 million per year.[94]

[93] Commission Staff Working Document Impact Assessment Accompanying the document Proposal for Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) {COM(2017) 10 final} part 3, p. 15.

[94] 200 million users x (85 websites a month with cookie banners x 3,5 seconds per banner x 12 months) x average hourly wage of EUR 33,5.

Table 6: Estimated cost savings from the changes made to the cookies regime

Item	Unit	Assumptions	Formula (stylised)	Estimated administrative cost savings
				Recurring
Cost savings for companies	EUR	Half of websites will no longer need to provide a cookie banner 10 million active European websites, of which 41% display a cookie banner	0,5 x (0,41 x 10 million websites x EUR 400)	**EUR 820 million** per year
Cost savings for public sector	EUR	1m public sector websites all of which provide cookie banners today. [95] In the future, at least 80% of the cookies placed in the public sector context (assuming substantial use for statistical purposes) will no longer need consent.	0,8 x (1.000.000 x EUR 400)	**EUR 320 million** per year
Productivity cost savings per year	EUR	The average user visits 100 websites a month, of which 85% use cookie banners, spending an average of 3.5 seconds per banner. This would result in approximately 334 million hours spent on cookie banners per year. With an average wage of EUR 33.5, and 30-70% of after tax wage as the monetary value of leisure time	Yearly cost per user [(85 x 3,5sec x 12months)/3600seconds] x EUR 33,5 = EUR 33.2 Yearly cost in total for the EU 33.2 x (450,000,000 x 0.75) = 33.2 x 337,500,000 = 11.2bn 11.2bn x 0,3=3.36bn 11.2bn x 0,7= 5.6 bn Median: (3.36+5.6)/2= 4.48	EUR 3.36bn to EUR 5.6bn, median; **EUR 4.48 billion** per year
Cost savings for users using cookie consent	EUR	50 million users to use browser settings, 3,5 seconds per banner, 100 websites a month 85% of which use cookie	50 million x (3,5 seconds x 85 websites x 12 months) x EUR 10,05 leisure value per hour	~ **EUR 500 million** per year

[95] Based on: Commission staff working document, Executive summary of the impact assessment for the proposal of a Directive on accessibility of public sector websites, SWD(2012) 402 final of 3.12.2012, which estimated the number of 'government websites' at 380.500 and 'public sector websites' at 761.000.

preferences per year		banners, EUR average wage 33,5, adjusted to 30% leisure value		

Stakeholder views

Stakeholders across sectors indicated that privacy and data protection concerns were the major obstacles or concerns to data sharing.[96] More than 60% of respondents to the public consultation on the Data Union Strategy indicated that consolidation of the ePrivacy framework was necessary. The majority of respondents to the public consultation on the Data Union Strategy calling for a reform of the ePrivacy framework call for better alignment with the GDPR and to rely on broader grounds for processing personal data than consent. This was further widely reflected in the Call for Evidence to the Digital Omnibus. For many stakeholders across industries, the ability to rely on legitimate interest was considered particularly valuable. Business representatives, especially from the e-commerce and publishing sectors, stressed that the underlying risk-based approach allows them to process personal data while considering the specific context of each processing operation. Highly sensitive processing operations that are particularly intrusive to the individual would not be able to be based on legitimate interest and should still require consent.

In the responses to the Data Union Strategy Public Consultation, civil society and consumer protection organisations generally opposed the loosening of the consent requirement in Article 5(3) of the ePrivacy Directive as they feared a reduction in the protection of the right to privacy. However, the proposal does not aim to allow the access to the terminal equipment for unlawful purposes but only for low-privacy-impact purposes and aims at tackling the identified issues. The possibility to accept or refuse the placing of cookies and by including a basis for central setting of cookie preferences users' rights will be safeguarded and strengthened. According to a Eurobarometer Survey on ePrivacy conducted in 2016[97], 69% think that default settings of your browser should stop your information from being shared. This option was not retained as it would go against the aim of making sufficient data available. To provide strong safeguards and a true choice, rather the option of providing for a mechanism to set cookie preferences centrally has been chosen. The proposal responds to challenges identified by civil society organisations in a stakeholder workshop of promoting rights-compliant innovation and of improving consent management. However, not all civil society organisations are opposed to introducing a more flexible, risk-based approach as long as the dangers of very intrusive tracking technologies would be taken into account and still necessitate consent. Furthermore, they generally support centralised consent setting as such a solution would empower the user to exercise a better control over their data and counterbalance the claimed practice of businesses to design their cookie banners and policies in a complex manner by design.

During the aforementioned 'reality check' on the cookie policy framework under Article 5(3) of the ePrivacy Directive, several stakeholders favoured a risk-based approach with more consent-exemptions for low-risk activities such as fraud prevention, web analytics, security purposes, contextual advertising, improving the customer journey, and purposes not involving personal data. Moreover, they stressed that personalised advertisement could not be considered low-risk and should therefore remain subject to consent. Among the stakeholders, there was a divide whether audience measurement, which could include processing for offering personalised content, should be white-listed as well. While one business association argued this served the public interest (e.g. supporting enforcement of online child protection

[96] The European Commission organised six stakeholder workshops in Spring and Summer 2025 inviting European level associations and individual stakeholders to roundtable discussion to address aspects such as simplification and investigate on the current state of play in the realm of data. These stakeholder workshops were organised with representatives from civil society, health sector, mobility sector, technology providers, business associations, energy and manufacturers sector.

[97] European Commission (2016) *Eurobarometer on ePrivacy*. Available at : Eurobarometer on ePrivacy | Shaping Europe's digital future

rules, allocation of press subsidies), a civil society representative underlined its privacy-intrusiveness, especially in publishing.
Furthermore, stakeholders were divided on whether to regulate centralised consent setting. Some businesses raised competition law concerns about the dominance of a few browser providers and the importance of understanding website use. Others, particularly from civil society, supported this as a user-centric and simplifying choice. They argued competition risks could be addressed through instruments like the DMA, supported by open standards. On the necessary scope of privacy protection related to terminal equipment, civil society repeatedly insisted that focussing on personal/non-personal data would be misguided as the right to privacy (which the current ePrivacy Directive protects) was a different fundamental right (Art. 7 Charter) from data protection (Art. 8), protecting notably the confidentiality of communications and not only personal data.
Accordingly, even without personal data-relevance, terminal equipment should be protected against unauthorized access. On the topic of privacy-enhancing technologies (PET), in the same reality check there was a large agreement on the importance of incentivizing the use of PETs. While not being perfect, PETs could significantly reduce privacy-related risks of tracking and other technologies. Several stakeholders pointed out that under the current approach, investing in PETs was unattractive, as Art. 5(3) requires consent even if using a PET. Civil society cautioned against an overly reliance on PETs due to "privacy washing"-risk, as the effectiveness of PETs heavily depended on their design.
Notably, and on a more general level, stakeholders from the publishing business are in favour of introducing a risk-based approach and of moving away from a strict consent requirement. They believe that processing of personal data for all purposes, including and especially for personalised advertisement, should be possible based on the grounds provided for in the GDPR, particularly legitimate interest. Moreover, publishers are very critical of centralised consent settings if this would mean that they cannot ask every website user for consent anymore. They argue that they are already at a considerable competitive disadvantage vis-à-vis big tech companies that can rely on vast amount of user data for which they do not need to place cookies because the consent is usually given when creating a user account for the service. Accordingly, big tech companies receive an increasingly large share of advertisement spend while advertisement revenues for publishers decrease. Moreover, they believe that centralised consent settings would strengthen big tech companies by creating new gatekeepers at browser level.

1.3.4. Preserving the objectives of the rules and other impacts

The proposed reform represents a targeted amendment to the current framework and will place the conditions of accessing devices that lead to the processing of personal data under the strong protection framework of the GDPR. It maintains the protection of devices ("terminal equipment"), only allowing access with the consent of the user in principle and the added whitelisted purposes to ensure legal certainty. This approach ensures that the legal framework continues to offer the highest levels of protection for personal data, while simplifying the experiences of data subjects in exerting their rights and expressing their choices online.

The proposal also foresees measures to strengthen users' privacy and control. The *status quo* in the application of the rules is ineffective: the complex design and confusing layers of decision implemented make it hard for data subjects to take full control over their choices in accepting or rejecting cookies and subsequent processing of their personal data. The proposed rules seek to simplify and streamline the decision steps precisely to allow data subjects to make genuine choices and benefit from all the protections the rules have in place.

Giving users the possibility to set their cookie preferences centrally coupled with the obligation for providers of online interfaces to accept such signals would further strengthen users' rights and offer a real choice and increased autonomy to decide what can be done with their data. In

fact, since most consumers (76%) want to be able to choose how much data devices can collect[98], this amendment would place the user at the centre, allowing them to make modern choices with modern tools and respond to such demands by consumers.

The proposed amendment will bring relief to users who will no longer be exposed to a large number of pop-up banners when visiting websites. Second, the proposal protects citizens from repetitive pop-up banners, providing that a choice made will need to be respected during a time period of six months. This will reduce nuisance for citizens, especially on websites that they visit on a regular basis.

The proposal further addresses the issue that some entities make cookie pop-up banners complex and hard to understand by design. The single click requirement will render pop-up banners easier to navigate where they are being used for consent. This will reduce nuisance created by having to click on multiple buttons to refuse or accept all choices.

The reform does not touch upon the high level of protection of citizens. The consent requirement is maintained as a general rule for accessing the device. The proposed amendments do not affect the protection of citizens against the illegal use of spyware, since the rules of the GDPR including its strong safeguards against such activities continue to apply. Furthermore, users remain protected against placing of malware on their devices under the rules of the ePrivacy Directive. The protection of the interests of legal persons under Article 5(3) continues to apply equally.

Moreover, moving the current rules from a Directive to a Regulation will further help to decrease fragmentation across Member States and will thus help to provide more legal clarity to businesses operating in the Union. Finally, the proposed amendments will also place the enforcement under the supervision of national data protection authorities. This will support a more uniform and consistent interpretation and enforcement, providing more certainty and clarity to entities.

All in all, the proposed amendments will contribute and strengthen the policy goal of guaranteeing a strong legal framework, for users and society as a whole. They preserve the right to privacy as well as the right to data protection enshrined under the Charter, while also taking into consideration the needs of businesses.

[98] BEUC (2023) *Connected, but unfairly treated: consumer survey results on the fairness of the online environment.* Available at: BEUC-X-2023-113_Fairness_of_the_digital_environment_survey_results.pdf.

2. INCIDENT REPORTING

The Digital Omnibus will introduce a single-entry point (SEP) through which entities can simultaneously fulfil their incident reporting obligations under multiple legal acts. Through fostering a "report once, share many" principle, the single-entry point will reduce administrative burdens for entities, while ensuring effective and secure flow of information about security incidents to the recipients defined in the respective legislation.

Under the current EU cybersecurity regulatory framework, the same event may lead to multiple incident reporting obligations for different purposes. For example, a mid-sized company facing a ransomware attack that disrupts services and extorts customers' personal data may have to report the same incident with separate forms and procedures stemming from several legal acts. This may include reporting to one or more competent authorities or Computer Security Incident Response Teams (CSIRTs) under the NIS2 Directive[99], as well as reporting to sectorial authorities under sectorial legislation (for example Digital Operational Resilience Act (DORA[100]), Electricity Network Code on Cybersecurity (NCCS[101]), aviation security and safety rules[102]). In particular, companies that provide multiple services face various cybersecurity-related obligations under horizontal instruments such as the NIS2 Directive and – with regard to personal data breaches - the GDPR[103], as well as abovementioned sectorial legislation. Moreover, an incident may trigger reporting obligations related to cybersecurity and physical security, notably under the CER Directive[104]. The resulting incident reports often have to be sent to different authorities across various Member States, as well as to different authorities within the same Member State, using different formats.

2.1. Analysis of the problems and opportunities

The rules and main issues. Multiple EU legal instruments contain reporting requirements for incidents relevant to cybersecurity. The **NIS2 Directive** serves as a horizontal framework for regulating the cybersecurity of essential and important entities in 18 critical sectors, including by setting an obligation to report significant incidents to the CSIRT or, as applicable, to the competent authority under NIS2. The Directive has several interlinkages with the **CER Directive**, which sets out obligations for critical entities in 11 sectors[105] regarding their resilience. In particular, the NIS2 Directive applies to all entities that are identified as critical entities under the CER Directive. Regarding incident reporting, the CER Directive requires critical entities to notify to the CER competent authority incidents that significantly disrupt or have the potential to significantly disrupt the provision of essential services. Under the **GDPR**, controllers are required to notify personal data breaches to the competent supervisory authority under GDPR. The **Cyber Resilience Act**[106] (CRA) sets out rules for the cybersecurity of

[99] Directive (EU) 2022/2555.
[100] Regulation (EU) 2022/2554.
[101] Commission Delegated Regulation (EU) 2024/1366.
[102] Commission Implementing Regulation (EU) 2023/203, Commission Delegated Regulation (EU) 2022/1645
[103] Regulation (EU) 2016/679.
[104] Directive (EU) 2022/2557.
[105] Each of the 11 sectors in scope of the CER Directive are also in scope of the NIS2 Directive.
[106] Regulation (EU) 2024/2847.

products with digital elements in the internal market, including notification obligations. For example, the CRA requires manufacturers to notify any actively exploited vulnerability contained in the product with digital elements that it becomes aware of, as well as to notify any severe incident having an impact on the security of the product with digital elements. Each of these notifications are to be made to the CSIRT designated as coordinator and are made available simultaneously to the European Union Agency for Cybersecurity (ENISA). The CRA requires ENISA to establish a single reporting platform, which is, among other types of notifications, used for the purposes of the abovementioned notifications.

The **EU Digital Identity Regulation**[107] sets reporting requirements for different types of actors, including trust service providers (TSPs) and qualified trust service providers (QTSPs). For example, under the Regulation, non-qualified TSPs and QTSPs are obliged to notify security breaches or disruptions in the provision of the service.

In addition to the abovementioned instruments, certain pieces of EU *acquis* set out cybersecurity-related reporting requirements for entities active in particular sectors. The **DORA** requires financial entities to report major ICT-related incidents to the relevant competent authority under DORA. Moreover, the relevant requirements also apply to operational or security payment-related incidents and to major operational or security payment-related incidents, where they concern credit institutions, payment institutions, account information service providers, and electronic money institutions. Although DORA is *lex specialis* to the NIS2 Directive, incidents reportable under DORA are also often reportable under other Union legal acts such as NIS2 or the GDPR.[108]

In the electricity sector, the **NCCS** requires critical-impact and high-impact entities to share relevant information related to a reportable cyber-attack with its CSIRTs and its competent authority. Regarding the aviation sector, the **Commission Implementing Regulation (EU) 2023/203** and **Commission Delegated Regulation (EU) 2022/1645** set requirements for certain types of organisations to report to the competent authority any information security incident or vulnerability which may represent a significant risk to aviation safety.

As regards providers of publicly available electronic communications services, the **ePrivacy Directive**[109] sets reporting requirements in case of a particular risk of a breach of the security of the network, and in case of a personal data breach[110]. Besides the obligation to notify incidents under different legal instruments, it should be noted that there are partial overlaps in the content of information to be notified to relevant authorities under those instruments. The contents of incident reports are defined through different means depending on the legal act.

[107] Regulation (EU) 910/2014 as amended by Regulation (EU) 2024/1183 and Directive (EU) 2022/2555.
[108] In particular, where the entity provides financial services in parallel with other types of services subject to the NIS2 Directive, the NIS2 Directive applies in parallel.
[109] Directive 2002/58/EC.
[110] After a repeal of Article 4 of the ePrivacy Directive, the reporting of data breaches would continue to be carried out under the GDPR framework.

For example, for DORA, incident reporting templates are defined in a Commission Implementing Regulation[111], while for NIS2, the Commission has an empowerment to adopt implementing acts to further specify the type of information, the format and the procedure of notification[112]. Under legal acts including the GDPR[113], CER[114], the legal act mandates certain contents for the incident notification, although an EU-wide template has not been defined. The abovementioned legal acts, using varying terminologies and criteria, require entities to notify information related to aspects such as an overall description or assessment of the incident, the cause of the incident, the severity and impact of the incident, and mitigating measures that the entity has taken to address the incident. The Digital Omnibus provides a basis for creating common EU-wide reporting templates for CER and for the GDPR. However, as regards instruments which take the form of delegated and implementing acts such as NCCS and relevant instruments for the aviation sector, separate amendments of the respective acts would be needed in order to create common reporting templates for incidents notified under those acts, and for ensuring the use of the single-entry point for those acts.

In addition to the Digital Omnibus, the upcoming revision of the Cybersecurity Act will contribute to streamlining the EU cybersecurity legislative framework. While the Digital Omnibus will introduce a single-entry point for incident notifications, the Cybersecurity Act will address other areas with simplification potential. Coherent implementation of the Digital Omnibus and the simplification-related provisions of the Cybersecurity Act will contribute to reducing administrative burden for entities, while guaranteeing a high level of cybersecurity in the Union.

The objectives. Cutting duplicate costs for entities that need to report the same incident under multiple frameworks and tackling underreporting. Furthermore, it provides a basis for further streamlining the contents of incident reports by enabling the definition of EU-wide reporting templates for CER and for GDPR, and by ensuring the adoption of common templates for the NIS2 Directive. By doing so, the Digital Omnibus will streamline the notification of incident information to the recipients defined in respective Union legal acts.

Stakeholder views

Stakeholder contributions related to the implementation of EU cybersecurity legislation have widely called for streamlining of incident reporting mechanisms. Business stakeholders of various sizes and sectors called in the Call for Evidence for the Digital Omnibus for a general principle of "one incident, one report, one mechanism", while highlighting the need to streamline duplicated incident reporting requirements. Frequent reference was made to the overlapping requirements between NIS2, DORA, the Cyber Resilience Act, and the GDPR. Recommended solutions varied as to their level (with some urging for a stronger role for ENISA, at European level, and others favoring an approach at national level), and the extent to which reporting templates, timelines and thresholds should be aligned.

Notably, the European Cybersecurity Organisation – European public-private partnership on cybersecurity – called for designating one point of reporting for all cybersecurity incidents, as well as for

[111] Commission Implementing Regulation (EU) 2025/302.

[112] Article 23(11) of the NIS2 Directive. Required contents of reports on significant incidents under the NIS2 Directive are defined in Article 23(4) of the Directive.

[113] Article 33(3) of GDPR.

[114] Article 15(2) of the CER Directive.

standardising templates and data formats[115]. Likewise, one of the main findings of the Implementation Dialogue on Cybersecurity Policies held by Executive Vice-President Henna Virkkunen on 15 September 2025 was that many companies (of all sectors) face hindrances in their compliance with incident reporting, and would support a more streamlined solution.
Consumer protection organisations also expressed support for a more streamlined approach which would benefit users, notably in a reality check on cybersecurity incident reporting organised by Commission services on 2 October 2025.
Altogether, available stakeholder feedback strongly supports simplification of cybersecurity incident reporting. A single-entry point covering multiple legal acts receives the most support, with some stakeholders arguing for a European-level platform and others favouring national-level single-entry points.

2.2. Simplification measures and impacts

The measures. The Digital Omnibus Regulation will simplify entities' compliance with their incident reporting obligations by providing for a single-entry point for incident notifications. The single-entry point will be managed by ENISA, and will serve as a gateway, that channels and delivers to the competent authorities notifications of certain types of incidents under the NIS2 Directive, DORA, CER Directive, NCCS, relevant aviation *acquis*, GDPR and the EU Digital Identity Regulation. The introduction of the single-entry point does not modify the addressees of incident reports defined under the respective legal acts, nor does it change the substance of the reporting obligations. While ENISA maintains the single-entry point, the introduction of the SEP thereby does not amount to adding ENISA as a recipient of the reported information as the SEP will not be a data processing platform, Moreover, the SEP will simplify reporting obligations without deregulating and thereby maintain a high level of cybersecurity.

To guarantee secure treatment of sensitive data arising from incident reporting, ENISA will define specifications on the technical, operational and organisational measures regarding the establishment, maintenance and secure operation of the single-entry point. The single-entry point will be interoperable and compatible with European Business Wallets, which will further facilitate the use of the single-entry point by entities. Furthermore, the single-entry point will reduce the administrative burden for entities arising from incident reporting by ensuring that a single notification submitted via the single-entry point can be used to fulfil reporting obligations under several Union legal acts. This will be facilitated by the inter-operability with other platforms and databases.

The legislation concerned by the SEP sets reporting obligations for some of the most critical infrastructure of Member States, which calls for advanced security guarantees and risk management measures. Building on the expertise of ENISA and the experience with the CRA single reporting platform, these measures would include a secure-by-design approach as well as pre-deployment and post-deployment penetration testing of the platform and the conditioning of the implementation of the SEP on successful piloting and testing.

The single-entry point should ensure that information notified by an entity under one legal act contributes towards fulfilling the entity's reporting obligations under any of the legal acts which

[115] ECSO (2024) *Streamlining Regulatory Obligations of EU Cybersecurity Policies*. Available at: Streamlining Regulatory Obligations of EU Cybersecurity Policies - ECSO

provide for reporting via the single-entry point. Furthermore, in the longer term, the introduction of the single-entry point may facilitate identifying possibilities for convergence between the contents of incident reports under different legal acts. Where the contents of incident reports are defined in legally binding acts, modifications of the reporting obligations would be subject to amendment of the respective legal acts.

The Digital Omnibus will streamline the implementation of the NIS2 Directive by requiring the Commission to adopt implementing acts that specify the type of information, the format and the procedure of incident notifications. These implementing acts will reduce complexity in the regulatory framework, in particular by ensuring that the same information is required as part of NIS2 incident notifications in all Member States.

Moreover, the Digital Omnibus will repeal Article 4 of the ePrivacy Directive. Whereas the Article sets requirements for providers of publicly available electronic communications services as regards safeguarding the security of their services and notification requirements, the NIS2 Directive provides for requirements as regards cybersecurity risk-management measures and incident reporting for those providers. Therefore, the repeal will reduce overlapping obligations for entities in the electronic communications sector.

The benefits. Considering the multiple reporting requirements arising from the abovementioned EU *acquis*, establishing a single-entry point for incident notifications represents an opportunity to reduce administrative burden for entities falling in scope of these obligations. The single-entry point streamlines the implementation of relevant legislation, thereby facilitating entities' compliance with their reporting obligations. Furthermore, it is expected to bring savings for Member State authorities by reducing administrative overheads related to establishing, maintaining and operating separate reporting platforms for different legal acts.

The single-entry point is expected to be particularly beneficial for operators that are active in multiple Member States and in multiple economic sectors. According to one study, 82% of surveyed entities reported that they have to notify more than one authority in case of a cybersecurity incident, with 21% of respondents stating that they had to notify 5 authorities.[116] For instance, in the case of an incident on a financial institution providing managed security services and for which the incident involved the breach of personal data, the stakeholder would potentially need to notify the competent authorities under DORA, NIS2, CER and GDPR. If this concerns a group stakeholder of entities subject to the jurisdiction of several Member States, this would entail the multiplication of reporting for the group as a whole. In such a case where all authorities are notified through separate means, a single-entry point for reporting would consequently be able to reduce the reporting effort by at least 50% for a large majority of entities - insofar as they would only notify once instead of (at least) twice for the same incident, while for one fifth of entities, the single-entry point could reduce reporting burden by 66-80%, as they would reduce from at least 3-5 notifications to a single one.

Operators that are subject to multiple Union legal acts are particularly likely to report incidents to multiple authorities, resulting in a multiplication of reporting burden in cases where the same

[116] Ibid.

incident is reported through different channels. In the case of operators that are active in multiple Member States, an incident that spreads across different entities in the same group may additionally result in multiple incident reporting obligations under the same legal act, such as the NIS2 Directive or GDPR as per the EDPB's Guidelines[117]. As another example, under the NIS2 Directive, providers of public electronic communications networks and providers of publicly available electronic communications services fall under the jurisdiction of all Member States in which they provide their services, including as regards incident reporting obligations under the Directive. More broadly, the single-entry point would particularly benefit SMEs, which often lack administrative capacity to navigate multiple reporting regimes. In such cases, reporting duties usually fall under the responsibilities of incident response teams, and the time spent on several notifications represents an opportunity cost in terms of the effectiveness of incident management.

All in all, the presence of multiple reporting platforms, which in the context of many legal acts are replicated at national level in each Member State, and require providing comparable information via multiple templates, represents untapped potential for savings.

2.3. Estimated impacts

The establishment of a single-entry point for reporting would result in significant savings for entities subject to incident reporting requirements under the relevant Union legal acts and for Member States.

Costs for developing the single-entry point. Notifying incidents via single-entry points is recognised as a potential means to decrease the administrative burden for entities[118], and contributes to reducing the number of reporting platforms that must be maintained by relevant national authorities. However, if single-entry points for each Member State are developed at the national level, the cost could range from EUR 150,000–200,000 and up to EUR 1.3–1.5 million[119] per Member State to achieve EU-wide coverage. With a moderate estimate of an average cost of EUR 550,000 per Member State, the total cost of development of national single-entry points across the Union would reach EUR 15,000,000. Wherever no national platform is yet in place, a single-entry point at the EU level is expected to bring savings by reducing administrative overheads related to establishing, maintaining and operating separate reporting platforms for different legal acts. The additional costs foreseen to operate and maintain the single-entry points would be estimated to equal to 2–4 FTEs per Member State. Overall, these costs reflect the additional complexity of mandating national incident single-entry points and legislative revisions. Therefore, even the establishment of national single-entry

[117] European Data Protection Board, Guidelines 9/2022 on personal data breach notification under GDPR, 28 March 2023.
[118] See Recital 106 of the NIS2 Directive.
[119] In the past (ENISA evaluation Report, 2017) the cost for implementing platform integration / adaptation aimed at producing real-time situational awareness and dynamic (live) threat reports was estimated to cost around EUR 869 208 to 1.3 million for the initial set-up and require around 4 FTE for management and maintenance. Similarly, discussions with the developer of a national cybersecurity platform highlighted the need of around 4 FTE for platform management.

points, which should be seen as a cost-reducing measure, would result in higher costs than putting in place a European-wide single-entry point.

At an EU level, the estimated initial cost for the development of the single-entry point is EUR 6 million, while maintaining the single-entry point would require 8 FTEs within ENISA[120]. The cost of onboarding each additional legal act into the single-entry point is estimated at EUR 500,000. Compared to the implementation of national single-entry points within each Member State, the overall implementation cost of a single-entry point at the EU level would be significantly lower, as only one centralised single-entry point would be developed and maintained at EU level.

Cost savings from streamlined reporting though the single-entry point. According to one study[121], 40% of the more than 4,000 surveyed organisations active in European markets face at least one incident annually. 44% of those experience more than 4 incidents, resulting in a weighted average of 1.18 incidents per entity per year. Assuming that the full process of reporting one incident takes 12 hours of staff time[122], the staff costs for incident reporting would be approximately EUR 440[123]. This estimate can be taken as comparatively conservative, since it omits the costs of other associated internal compliance processes to report an incident, such as in-house IT tools or external legal support on how to comply with different regulatory authorities. In an SME Panel consultation run by the Commission in September-October 2025[124], responding SMEs estimated that the overall cost of reporting an incident could range between EUR 500 and EUR 35,000 (when taking into account additional implied costs), depending on the nature of the incident and on the company profile. However, when directly asked about the costs of incident reporting, stakeholders consulted as part of the 'reality check' carried out on 2 October 2025 raised the different expenses associated with the aforementioned aspects of incident reporting, but were unable to produce a quantified estimation.

At the same time, it is estimated that at least 160,000 entities are regulated under NIS2[125], while approximately 1 million entities meet the definition of data controller under the GDPR and are

[120] The cost estimates are similar to the cost estimates for the development of a centralised reporting solution under DORA, provided by the European Supervisory Authorities (ESAs). See Report on the feasibility for further centralisation of reporting of major ICT-related incidents, p. 56. Available at https://www.esma.europa.eu/press-news/esma-news/esas-publish-study-feasibility-further-centralisation-major-ict-related.

[121] Cloudflare (18 June 2024) *European Businesses Anticipate More Cybersecurity Attacks, But Feel Unprepared for Them. Press release.* Available at https://www.cloudflare.com/press-releases/2024/european-businesses-anticipate-more-cybersecurity-attacks-but-feel/.

[122] Staff time required for reporting an incident is understood to include tasks including an internal assessment by the entity whether the incident is reportable and under which legal bases; collecting data required for filling the applicable incident reporting templates; and submitting the reports. These tasks may involve more than one staff member in the entity, making this assumption a conservative one. Moreover, where incident reporting takes place in multiple stages, staff time is required at each stage in the process.

[123] Based on an average mid-level compliance or cybersecurity staff salary of EUR 60 000 – EUR 80 000 per year, the hourly wage of a professional is calculated at EUR 36.5 (annual salary of EUR 70 000, with 48 working weeks a year at 40 hours/week).

[124] See Annex I, Chapter III.

[125] Based on an extrapolation of the number of essential and important entities notified by Member States pursuant to Article 3 of the NIS2 Directive by September 2025, it is estimated that 160 000 entities fall under the scope of NIS2. Considering that the single-entry point also covers other Union legal acts, the estimate should be considered conservative.

established or operating in more than one Member State[126]. Consequently, assuming that all entities under the NIS2, DORA and CER are also data controllers, at least 160,000 entities fall under the scope of multiple legal acts covered by the single-entry point, while even a larger number of entities would benefit from easier cross-border reporting of incidents.

Provided each of these entities faces 1.18 incidents per year, on the basis of the forementioned study, it can thereby be extrapolated that the total cost for entities arising from reporting each of the incidents faced is EUR 83,072,000 per year. With the estimate that the single-entry point can reduce the costs by 50% as described in the previous section, it would therefore result in approximately EUR 41.5 million of savings each year. This figure represents a conservative estimate that does not account for additional savings from simplification of reporting under the GDPR.

Although estimates suggest that incidents are common, under-reporting of incidents has long been recognised as an issue hindering the successful implementation of the EU cybersecurity framework[127]. According to the 2024 incident reporting data on the CIRAS (Cybersecurity Incident Reporting and Analysis System) platform[128] managed by ENISA, a total of 1 340 cybersecurity incident reports were collected. With the estimated cost of EUR 440 for reporting an incident, the cost involved in reporting these incidents would amount to EUR 589,600, while savings of 50% arising from simplified means of incident reporting would total EUR 294,800 per year. However, as the overall number of incidents occurring in the EU is estimated as larger, with full reporting of relevant incidents, the savings arising from the single-entry point should be assessed as higher than EUR 294 800 per year[129]. By its induced simplicity for stakeholders, the single entry-point is expected to further incentivise the reporting of incidents.

The below Table 7 presents the overview estimated savings, based on the outlined explanations and taking into consideration the ongoing transposition of the NIS2 directive by Member States as well as the scarcity of quantified empirical data available on the number and cost of incidents under the relevant legislations.

Regulation with incident reporting implications	**Estimated number of entities subject to the regulation**	**Estimated number of entities subject to multiple incident reporting obligations**	**Cost of reporting per business**
NIS2	160,000	All entities subjected to CER and part of entities subject to DORA are also subject to	

[126] The Impact Assessment for the GDPR (SEC(2012)72) estimated the number of data controllers established and processing data cross-border at 927,272.

[127] European Court of Auditors (2019) *Challenges to effective EU cybersecurity policy*, available at https://www.eca.europa.eu/lists/ecadocuments/brp_cybersecurity/brp_cybersecurity_en.pdf.; ENISA (2024) *EU Cybersecurity Index 2024: EU-level insights and next steps*, available at https://www.enisa.europa.eu/sites/default/files/202506/The%20EU%20Cubersecurity%20Index%202024_en_0.pdf.

[128] CIRAS (2025) *CIRAS Incident reporting dashboard 2024*. Available at: https://ciras.enisa.europa.eu/

[129] This sum should also not be aggregated to the EUR 41.5 million estimate presented above, which builds from different assumptions. Were all incidents reported, it would be included within the same total.

DORA	21,000[130]	NIS2. It is assumed that all entities subject to NIS2 are also subject to GDPR. Consequently, the number of entities subject to multiple reporting obligations is estimated at **160,000**. The present estimate covers only NIS2, DORA and CER. It excludes the EU Digital Identity Regulation, NCCS and relevant aviation acquis. Given the above considerations, 160,000 should be regarded as a conservative estimate of the number of entities subject to reporting obligations under at least two Union legal acts.	Incident reporting costs have been estimated at EUR 440 per notification.
CER	5,000[131]		
GDPR	11,000,000[132]	It is estimated that **1,000,000** entities are subject to reporting obligations in multiple Member State[133].	The cost of reporting a data breach under GDPR is estimated at EUR 100 – EUR 500.[134]

Table 7: Estimated cost savings for the introduction of a Single-Entry Point

Item	**Unit**	**Assumptions**	**Formula (stylised)**	**Estimated administrative cost savings**	
				Businesses	
Incident reporting	EUR	Current level of incident reporting continues: 1340 incidents at an estimated	0,5 x (1340 incidents x EUR 440)	**One-off**	**Recurring**

[130] Impact Assessment Report accompanying the Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector (DORA), p. 8. SWD(2020) 198 final. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020SC0198.

[131] Impact Assessment Report accompanying the Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities. SWD(2020) 358 final. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020SC0358.

[132] Schulze Brock, P., Katsinis, A., Lagüera Gonzalez J., Di Bella, L., Odenthal L., Hell M., Lozar B., Secades Casino B. (2025) *Annual Report on European SMEs 2024/2025, SME performance review*. Publications Office of the European Union, Luxembourg. Available at: https://publications.jrc.ec.europa.eu/repository/handle/JRC142263. According to the Joint Research Centre, as of 2023, there were 25,851,156 companies in the EU. In turn, according to the impact assessment of the GDPR, "it can be assumed that approximately 42% of the total number of companies can be practically considered as data controllers within the meaning of the Directive", hence 42% of 26 million is approximately 11 million entities.

[133] This number is the result of extrapolation of calculations made in the GDPR impact assessment to estimate the number of companies/ data controllers active in more than one Member State.

[134] These estimates are conservative and refer to results from the SME consultation carried out for the GDPR impact assessment, dating from 2012.

		price of EUR 440, halved through the introduction of a Single-Entry Point[135]		N/A	≈ **EUR 294,800** per year
Incident reporting	EUR	All incidents are reported (N.B. savings as regards reporting under GDPR in multiple Member States are not included in the calculations): 188 800 incidents at an estimated price of EUR 440, halved through the introduction of a Single-Entry Point	0,5 x (188 800 incidents x EUR 440)	N/A	≈ **EUR 41,536,000** per year
Development and maintenance of single-entry points	EUR	***Development:*** ENISA develops a single-entry point, at a cost of EUR 6 million. Member States therefore do not need to develop national single-entry points. ***Maintenance:*** Member States would require 2-4 FTEs yearly for these purposes, whereas ENISA would require 8 FTEs. The cost savings calculation is made at EU level.	EUR 15 million – EUR 6 million (EUR 70,000 x 2-4 FTE x 27 Member States) – (EUR 70,000 x 8 FTE)	*Public authorities* **One-off** ≈ **EUR 9,000,000**	**Recurring** ≈ **EUR 3,220,000 – 7,000, 000** per year

Stakeholder views

The stakeholders consulted from the private sector and civil society expressed strong support for a single-entry point solution, converging on the need to streamline the notification of incidents under various legislations as well as the templates and data. However, they presented different preferences regarding the organisation of incident reporting channels, and the role ENISA should have in this mechanism.

In response to the Open Public Consultation for the revision of the Cybersecurity Act[136] carried out in April–June 2025, the Commission received feedback from 194 respondents, of which 79 were companies or businesses, and 54 were business associations. Among other themes, the consultation

[135] N.B. The assumption is mutually exclusive with the assumption presented in the below row. Therefore, the estimated cost savings presented on each row should be regarded as separate estimates based on differing assumptions, rather than as cumulative savings.

[136] European Commission (2025) *Call for evidence and public consultation on the revision of the Cybersecurity Act*. Available at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14578-The-EU-Cybersecurity-Act/public-consultation_en.

addressed simplification of cybersecurity legislation. On average, these types of respondents rated the effectiveness of a single reporting platform at EU level for the compliance with reporting obligations from all relevant EU legislation with the score of 4.62 on a scale of 1–6. Of the 105 respondents that answered the question, 45 (43%) gave the maximum score of 6. By contrast, companies, businesses and business associations gave an average score of 4.30 for a single reporting platform at EU level for the compliance with reporting obligations from NIS2, with 32 of the 107 respondents answering the question (30%) giving the maximum score. Finally, as regards a single reporting platform at national level for the compliance with reporting obligations stemming from relevant EU legislation, these types of respondents gave an average score of 4.78, with 55 of 122 respondents (45%) giving the maximum score.

All in all, the survey responses show that businesses find a single reporting platform to be beneficial for reducing administrative burden. Although all the three abovementioned options receive broad support, an important number of stakeholder contributions argue for a European-level single entry point. This was also reflected in the Call for Evidence to the Digital Omnibus, where most contributions and submitted position papers on the topic (primarily from companies – mainly large ones, with cross-border operations, public authorities, and business associations, but also from some consumer organisations and citizens) advocated the establishment of a single EU-wide reporting portal. Proposed solutions differed regarding the appropriate level of implementation: some respondents called for a stronger coordinating role for ENISA at the European level, while others favoured a stronger role for Member States. A limited number of stakeholders in the financial sector expressed some caution as to the specific interplay of such a solution with the DORA reporting framework in place.

Alongside the broad support for simplified incident notification to alleviate the administrative burden of reporting under multiple legal acts in multiple Member States, stakeholders also raised the potential security benefits of a single-entry point. In the 'Reality check' carried out on 2 October 2025 by Commission services, industry actors expressed concerns regarding the time spent by incident response resources on reporting duties during the emergency. The "report once, share many" model could improve the efficiency of their incident management and consequently their security by optimising the time of relevant staff.

Some stakeholders, particularly businesses, expressed concerns about the potential burden incurred by adapting to yet a new reporting mechanism. Others raised security concerns, by the centralisation of all reporting via one platform.

Taking note of this, the SEP proposal is expected to incur minimal additional costs, such as a one-off in-house short training for relevant staff and a limited one-off change to the entity's internal reporting procedures, with the broader advantage of enabling a single reporting tool across various legal acts and Member States. On the security level, and as outlined earlier in this chapter, the initiative would be tied from its inception to rigorous security and pre-testing requirements, building from ENISA's expertise.

2.4. Preserving the objectives of the rules and other impacts

The proposed measures will fully preserve the rights and competences of the authorities empowered by the respective legal framework to receive incident reports channelled through the single-entry point.

Moreover, the system will support a more effective application of the underlying reporting obligations. Complex reporting requirements and limited awareness are among the perceived drivers for underreporting of cybersecurity incidents[137]. A single-entry point for incident notifications would contribute to addressing these issues, thereby incentivising more comprehensive reporting of incidents. In turn, receiving a larger number of incident reports

[137] ENISA (2024) *EU Cybersecurity Index 2024: EU-level insights and next steps*, p. 6. Available at: The EU Cybersecurity Index 2024 | ENISA

enables the recipients of the reports to gain a fuller and more accurate picture of the landscape of incidents, which enables better drawing of lessons from incidents. Over time, the process is expected to result in increased cyber resilience of the critical sectors concerned, thereby enhancing Europe's security[138]. Furthermore, as a larger number of incidents are reported through a single-entry point, cost savings arising from simpler incident reporting vis-à-vis separate entry points will increase.

Establishing the single-entry point also contributes to the digital-by-default principle by ensuring a fully digitised solution for reporting incidents under the relevant Union legal acts. Interoperability of the single-entry point with the European Business Wallets will contribute to digitalisation by providing one use case for the Business Wallets, thereby incentivising the uptake of the Business Wallets. More broadly, the single-entry point contributes to the interoperability of ICT systems used by Member State authorities by ensuring that information notified through the single-entry point is channelled to the recipients defined in the relevant Union legal acts.

The single-entry point will support the protection of fundamental rights as regards the right to the protection of personal data. By providing streamlined means for reporting incidents that, in many cases, involve breaches of personal data, the single-entry point will increase the speed and consistency of response to such breaches.

The single-entry point also has a limited positive impact on the environment. Consolidating incident reporting into a single-entry point is expected to save energy consumption compared to separate incident reporting entry points operated at the level of Member States for various Union legal acts.

ENISA will be mandated to establish and maintain the Single-Entry Point and ensure its security, proper functioning, reliability, integrity and confidentiality. It should pilot the functioning and consult the Commission and the relevant Member State authorities prior to enabling the reporting under any legal act.

[138] See also Recital 101 of the NIS2 Directive.

3. TARGETED AMENDMENTS TO THE ARTIFICIAL INTELLIGENCE ACT

The Commission is committed to a clear, simple and innovation-friendly implementation of the AI Act, as set out in the AI Continent Action Plan [139] and the Apply AI Strategy [140]. Initiatives such as the launch of the AI Act Service Desk [141] and the preparation of guidelines and other support tools build clarity regarding the applicable rules and support their application. The Commission will continue these efforts and is preparing further guidelines. The commitment to a successful implementation also includes building on the lessons learned during the progressive roll-out of the AI Act and continuously stepping up efforts to facilitate a smooth application. In this regard, the Commission has identified implementation challenges that jeopardise the AI Act's successful and innovation-friendly general entry into application on 2 August 2026. These challenges should be addressed through legislative amendments.

3.1. Analysis of the problems and opportunities

The rules. The AI Act, which entered into force on 1 August 2024, creates a single market and harmonised rules for trustworthy and human-centric AI in the EU. It aims to promote innovation and uptake of AI, while also ensuring a high level of protection of health, safety and fundamental rights, including democracy and the rule of law. The AI Act's entry into application occurs in stages, with all rules entering into application until 2 August 2027.

The rules for high-risk AI systems are the most comprehensive body of rules in the AI Act and will apply as of 2 August 2026 or 2 August 2027. High-risk AI systems must be developed to meet requirements in relation to data and data governance; documentation and record keeping; transparency and provision of information to users; human oversight; robustness; accuracy and security. Providers of high-risk AI systems have to ensure that the systems comply with these requirements and must themselves comply with certain obligations. They must in particular carry out a conformity assessment of the high-risk AI system before it is being placed on the market or put into service. Standardisation should play a key role in the provision of technical solutions to providers, so as to ensure that high-risk AI systems comply with the requirements of the AI Act. In May 2023, the Commission requested the European standardisation organisations CEN-CENELEC to develop such standards [142]. In June 2025, it updated this request in order to take account of the final text of the AI Act [143], which CEN-CENELEC accepted. The Commission takes note that CEN-CENELEC has been unable to deliver the standards by the deadline of 31 August 2025.

The AI Act also sets out a regime for the supervision, monitoring and enforcement of its rules on AI systems. In line with its regulatory design as a product safety legislation, much of the AI Act's supervision and enforcement will take place at the national level. For this purpose,

[139] COM(2025) 165 final.
[140] COM(2025) 723 final.
[141] https://ai-act-service-desk.ec.europa.eu/
[142] C(2023)3215.
[143] C(2025)3871.

Member States have to establish or to designate national competent authorities and lay down rules to empower those authorities and provide for penalties. The deadline for Member States to notify the Commission of the designated authorities and laws on penalties was 2 August 2025, with the objective that the infrastructure related to the governance and the conformity assessment system should be operational well before 2 August 2026 [144]. Many Member States have not been able to meet this deadline, and these delays suggest that the governance and conformity assessment system may not be operational on time.

A key feature of the AI Act is its regulatory design as a horizontal product safety legislation, that is consistent with the 'New Legislative Framework', following the approach of and ensuring coherence with existing EU product legislation and other relevant EU legislation. This horizontal nature means that it is essential to have clarity as regards the AI Act's interplay in order to ensure a smooth interplay with other EU laws. However, the application of the AI Act's rules in parallel and coherently with other applicable EU legislation raises questions in their practical application. Uncertainty about how to apply those rules risks discouraging the adoption of AI systems and undermining the AI Act's objective of fostering the uptake of AI.

Main issues. Most of the AI Act has not yet entered into application, and even those parts that have entered into application have only done so recently [145]. Therefore, there are no reliable calculations for compliance costs arising from the existing framework for businesses. Moreover, the AI Act only introduces rules for certain AI applications, so the cost of compliance with the AI Act varies greatly.

In the impact assessment accompanying the proposal for the AI Act (hereafter: the 'initial AI Act impact assessment') [146] estimated that the theoretical maximum compliance costs and administrative burden amount to around EUR 10 000 for companies that follow standard business procedures. This is applicable only to those companies that are provide high-risk AI systems (estimated at no more than 5-15% of all AI applications [147]). There would also be between EUR 3,000-7,500 of verification costs for a subset of such high-risk applications [148]. Compliance costs would significantly increase if harmonised standards were not available to demonstrate compliance. This is especially true for smaller companies with limited legal resources. The application of harmonised standards is voluntary, and companies can seek compliance with the AI Act without them. However, standards do provide clear guidance and a presumption of compliance, and they can in certain cases enable self-assessment (thus avoiding the costs of seeking an external conformity assessment). In a survey of AI Pact signatories [149], 20% of respondents estimated that their compliance costs would be at least 80% higher, while 26.67% estimated that their compliance costs would increase by 20-50% in the absence of harmonised standards or similar tools for compliance with the high-risk AI systems [150]. The

[144] Recital 179 AI Act.
[145] The general provisions (definitions, prohibited practices and obligations regarding AI literacy) on 2 February 2025 and the obligations for providers of general-purpose AI models on 2 August 2025.
[146] SWD(2021) 84 final.
[147] SWD(2021) 84 final, pp. 67, 68.
[148] SWD(2021) 84 final, p. 69.
[149] Described in detail below, in the section 'Stakeholder views'.
[150] Following a survey of signatories of the AI Pact, which is described in detail in the section on 'Stakeholder views'.

costs for business from the delayed establishment of national competent authorities is expected to be mostly indirect. The most significant cost could arise from a delay in designating conformity assessment bodies as a result of the delayed establishment of notifying authorities. This is because such a delay could delay companies being able to place products on the market or oblige them to incur extra cost by switching to conformity assessment bodies in other Member States.

Additional compliance costs arise from obligations that were only introduced during the interinstitutional negotiations and were therefore not part of the initial AI Act impact assessment. This is particularly the case for the obligation for providers and deployers of AI systems to ensure a sufficient level of AI literacy for their staff, due to its horizontal application (regardless of the level of risk actually posed by those providers' or deployers' AI systems). This obligation has already applied since 2 February 2025. In the survey amongst AI Pact signatories mentioned above, 54.05% of respondents said that they have incurred additional costs in order to comply with the new obligation in Article 4 AI Act because of the uncertainty what is required, despite already taking measures to foster AI literacy among their staff before being obliged to do so. The respondents' answers varied when they were asked how much additional costs they had incurred: 36.11% estimated that their additional annual compliance cost reaches up to EUR 10 000, but 16.67% stakeholders even estimated it at up to EUR 50 000 annually to comply with this obligation.

The objectives. The AI Act's successful implementation is a priority of the Commission, and the Commission's commitment to a clear, simple and innovation-friendly has been reaffirmed in the AI Continent Action Plan and Apply AI Strategy. The progressive roll-out of the AI Act allows that the experience gathered in implementing the first parts of the rules can feed into the preparations for the parts that are still to apply. This includes taking measures that are necessary to overcome challenges in the implementation. The objective of this intervention is to address those implementation challenges that jeopardize the successful transition of the AI Act's next entry into application milestone on 2 August 2026 and that require legislative measures.

Stakeholder views

The Commission has run a **public consultation [151] to identify implementation challenges with the AI Act**. This was launched as part of a consultation that would feed into the preparation of the Apply AI Strategy and of the Digital Omnibus. The public consultation shows that companies developing AI identified the **lack of available standards, guidance documents, or other tools to support compliance as the main obstacle to implementing the AI Act** (62 replies), followed by uncertainty about the scope and which rules will apply to them (52 replies) [152]. When asked which aspects cause particular difficulty in the implementation so far, respondents identified a **lack of harmonised standards, the capacity of notified bodies, and the potential for fragmented interpretations and enforcement across the EU**, as well as the complex interplay between the AI Act and other EU regulations, with potential overlaps and conflicts between these frameworks [153]. Similar responses were given by organisations using AI (including academic/research institutions, companies/businesses, public authorities), which also consider

[151] European Commission, *Call for evidence and public consultation on the Apply AI Strategy*, 2025, Apply AI Strategy – strengthening the AI continent

[152] Page 9 of the Summary report: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14625-Apply-AI-Strategy-strengthening-the-AI-continent/public-consultation_en

[153] Ibid, p. 10.

as the most significant challenge to AI Act implementation the lack of available standards, guidance documents, or other tools to support compliance (69 replies), as well as uncertainty about the scope and which rules will apply (57 replies) [154].

The Commission also launched a call for evidence [155]. The **findings of the call for evidence support those of the public consultation** referred in the paragraph above. In the call for evidence, stakeholders across all groups highlighted elements that make implementation of the AI Act challenging for them. Most business stakeholders again flagged as the main challenge the lack of availability of standards, other guidance and the national governance. With regard to simplifying the obligations and requirements of the AI Act, stakeholders across all groups called for a **targeted approach and no significant overhaul of the AI Act**, which they consider crucial for legal certainty. NGOs, citizens and trade unions expressed broad concern about lowering the level of protection from risks of AI that is provided by the AI Act and cautioned against amendments. Many stakeholders across all groups also call for **non-legislative measures to simplify compliance with the AI Act,** notably through guidelines, communication and practical support tools. In this regard, businesses particularly mentioned the need for guidance on the interplay with the GDPR.

The **reality check** on the AI Act on 16 September 2025 [156] further confirmed these findings. During the round-table discussion, stakeholders stated that the absence of clear standards and the interplay between the AI Act and other regulations (e.g. the GDPR) are substantial challenges in the implementation. During the reality check, stakeholders also expressed their concern that **the compliance requirements for the horizontal AI literacy obligation are uncertain**. Participants also highlighted the difficulties in implementing post-market monitoring. The participants emphasized the need for more support tools, standards, and notified bodies to facilitate compliance with the AI Act. The Commission also launched a **survey of signatories of the AI Pact** [157], which are companies who have pledged to anticipate certain requirements of the AI Act ahead of their entry into application. This survey was conducted to **gather evidence on compliance costs from companies that have already undertaken efforts towards compliance with the AI Act's rules**, bearing in mind that most of the AI Act's rules do not yet apply and that evidence of compliance costs is otherwise limited. The survey ran between 16 and 30 September 2025 and followed a multiple-choice template in which respondents were able to self-select which sections were relevant to them. 44 responses, out of which 25.58% respondents with fewer than 10 employees, 25.58% with 10-249 employees and 48.84% with more than 750 employees. One of the survey questions was whether and what challenges the respondents were facing challenges in the implementation. The most frequent answers were **ambiguity in regulatory requirements and lack of** guidance (75%) and **delays in the standardisation processes** (52.50%).

The Commission acknowledges the need to pay particular attention to the needs of SME. It therefore conducted an SME panel[158] to gather input about SMEs' business operations linked to digital rules. SMEs were, inter alia, asked to identify the challenges they experience in the implementation of the AI Act. The greatest difficulties reported were **uncertainty about the legislation's scope and applicable rules** (30%) and **access to standards, guidance documents, or other compliance tools** (18%), while 13% reported uncertainty regarding the responsible supervisory authorities. 12% referred to resource constraints, and 8% cited bureaucratic hurdles or duplication with existing procedural requirements.

Specific concerns expressed:

The following concerns were expressed regarding the implementation timeline:

- The main stakeholder concern, particularly by businesses of all sizes, business associations and public authorities, is the **challenge of meeting the implementation timeline for the high-risk AI system rules –** in view of the delayed availability of standards, other guidance tools and competent authorities' enforcement capacity. In the Apply AI Consultation, 77.5% of companies

[154] Ibid, p. 11.
[155] See Annex I, Chapter I.
[156] See Annex I, Chapter IV.
[157] European Commission (2025) *AI Pact*, https://digital-strategy.ec.europa.eu/en/policies/ai-pact
[158] See Annex I, Chapter III.

developing AI named this their main implementation challenge and 52.50% respondents to the AI Pact signatories' survey. It was also the most frequent response to the call for evidence. At the same time, NGOs (especially consumer associations), as well as some standardisation bodies and citizens, argued that the implementation work should not slow down, lest companies be discouraged from investing in compliance with the new rules.

- Moreover, in the call for evidence, many stakeholders (in particular businesses) were concerned about facing **retroactive requirements**, due to the technical complexity of implementation. In particular, stakeholders expressed concern about the cost and technical difficulty of retroactively applying technical solutions that enable the marking of AI system outputs as artificially generated or manipulated, as required by Article 50(2) of the AI Act.

The following concerns were expressed regarding specific obligations:

- Several stakeholders (particularly businesses and public authorities) called for greater overall proportionality of rules that apply to AI systems that do not fall under the risk categories of the AI Act. During the reality check, it was revealed that stakeholders are particularly concerned by the **uncertainty around the compliance requirements for the horizontal AI literacy obligation**, which gives market surveillance authorities considerable margin of discretion to determine what is a 'sufficient level of AI literacy' and creating a deterrent effect for businesses and public authorities.
- In the call for evidence, several business stakeholders called for **more flexibility in post-market monitoring of high-risk AI systems**. This was also confirmed as a concern in the reality check, where businesses explained that the approaches vary greatly across sectors and the prospect that the Commission will introduce harmonised conditions through an implementing act raises concerns.
- Stakeholders also expressed concerns in the call for evidence about the **administrative burden implied by registering in the EU database AI systems that have been exempted from being considered as high-risk**(as provided for by Article 49(2) of the AI Act).

The following concerns were expressed regarding the governance:

- A particular concern is the **fragmentation of governance**, both across different laws as well as within the AI Act. This concern has been aggravated as the first Member States have established their national competent authorities, with many of them dividing market surveillance over multiple national authorities. In the survey of AI Pact signatories, 57.49% respondents identified this as a challenge they foresee once the AI Act starts to apply, Inconsistencies in implementation may arise across sectors as well as among countries, in particular when systems are present in several countries or are based on large models that are supervised at the EU level.
- In the call for evidence, businesses call to simplify the allocation of responsibilities, and some specifically call to **centralise more oversight with the AI Office and empower it better**.
- Centralising more oversight with the AI Office is also a **request of many Member States** [159], which report financial and human resource challenges in the national implementation, in particular because **AI oversight requires expertise and skills for which there is a shortage** and for which the public sector is in competition with the private sector.

The following views were expressed regarding measures in support of compliance and innovation:

- Extending the **processing of special categories of personal data for the purposes of training and testing all AI systems and models** was frequently mentioned in the call for evidence as a possibility to facilitate compliance with data protection law. Businesses called for the threshold

[159] At the time of negotiations, this was also a strong request by the European Parliament.

for the use of that legal basis to be aligned with that of the GDPR (i.e. that the data processing should be 'necessary' rather than 'strictly necessary').
- Stakeholders (particularly businesses and business associations) called for an **additional focus on sandboxing**. This was a call that was brought forward by smaller and larger businesses alike.

The following concerns were expressed on the complexity of the interplay of the AI Act with other EU law:

- All stakeholder groups expressed concerns about the **complexity of the interplay of the AI Act with other EU law**. Uncertainty, duplication of requirements and governance create burden in the practical application of the rules. Companies and business association frequently called for the introduction of **more mechanisms of mutual recognition of compliance** across laws.

3.2. Simplification measures and impacts

The simplification measures proposed by the Commission are **targeted amendments** to the existing regulatory framework that aim to provide relief for identified implementation challenges, while at the same time **preserving legal certainty and predictability** for stakeholders. These efforts are **complemented by several non-legislative initiatives**, including the setting-up of an AI Act Service Desk and the provision of guidance.

First, the Commission proposes to **align the application timelines for certain rules** to address the challenge posed by the delay of standards and the establishment of national competent authorities. Building on the lessons learned, it is appropriate to put in place a mechanism that links the entry into application to the availability of measures in support of compliance with the AI Act's high-risk rules, such as harmonised standards, common specifications, and Commission guidelines. However, this flexibility should apply only for a limited time and a definite date by which the rules apply in any case should be set. Moreover, it is appropriate to distinguish between the two types of AI systems that classify as high-risk and extend a longer transition period to AI systems that classify as high-risk pursuant to Article 6(1) and Annex I AI Act. The Commission also proposes to respond to the challenge of retroactively introducing technical solutions to generative AI systems in order to ensure that outputs from the AI system are marked in a machine-readable format and are detectable as artificially generated or manipulated in accordance with Article 50(2) of the AI Act, by introducing a **transition period of 6 months for Article 50(2) of the AI Act**. This would allow AI systems that are already on the market on 2 August 2026 to be made compliant by 2 February 2027.

Second, it is necessary **to simplify certain obligations** with a view to ensuring that the burden of complying with them is proportionate to their objectives. **Certain privileges for SMEs should be extended to SMCs** in line with the objectives set out in the Commission's proposal for a regulation of the European Parliament and of the Council as regards the extension of certain mitigating measures available for SMEs to SMCs and further simplification measures [160]. In other words, simplified technical documentation, a quality management system that takes account of their size, to receive special consideration of their interests in the calculation of fines for violations, special consideration of their needs in the preparation of voluntary codes of

[160] COM(2025) 501 final.

conduct and guidelines, and additional regulatory privileges should be considered. In addition, an existing privilege granted to microenterprises, namely simplified quality management, should be extended to all SMEs. In the light of the finding that the horizontal obligation to ensure a sufficient level of AI literacy does not achieve its objective but does cause serious compliance concerns, the **obligation on companies to ensure a sufficient level of AI literacy should be replaced with an obligation on the Commission and Member States**, to encourage providers and deployers to ensure that their staff and other users have an adequate level of AI literacy. The obligation for deployers of high-risk AI systems to assign human oversight only to staff with the necessary training, competence and support remains [161]. Moreover, there should be **flexibility for providers of high-risk AI systems to implement a post-market monitoring system** that works for their organisation. The Commission should accordingly not adopt harmonised conditions that prevent such flexibility but should rather offer voluntary guidance for those who seek it. Providers of **AI systems that are exempted from classification as high-risk should not be obliged to register** in the EU database for high-risk AI systems – so as to remove an administrative burden that is not justified because these AI systems do not pose significant risk.

Third, it is crucial to **improve the effectiveness of the governance system.** The AI Act already foresees that the AI Office assumes the supervisory role for large and capable general-purpose AI models, and general-purpose AI systems built on these models in certain cases. This is due to the complex and evolving nature of these models, for which there are few experts, rendering it most efficient to centralise the oversight at the AI Office rather than requiring 27 Member States to build such capabilities. As general-purpose AI models proliferate and an increasing number of systems are built on these models, including AI agents, the **AI Office's powers should be reinforced to oversee AI systems built on general-purpose AI models**, to ensure their effectiveness. This will not only reduce fragmentation of governance but also contribute to a coherent application of rules for AI systems, including prohibitions, high-risk and transparency, offering guidance for national authorities who oversee other AI systems. It will allow the respective providers to only deal with one regulatory authority; it would thus reduce cost on the side of the providers as well for national authorities (for example, only one authority would be responsible for the post market monitoring instead of 27). However, this should not apply for AI systems related to products covered under Union harmonisation legislation listed in Annex I of the AI Act, for which the oversight should remain with the sectoral market surveillance authorities in the Member States. Where AI systems constitute or are embedded in VLOPs or VLOSEs within the meaning of Regulation (EU) 2022/2065 (Digital Services Act), the oversight should also be allocated to the Commission's AI Office, to make a coherent and synergetic application of the AI Act and Digital Services Act easier. Finally, the existing mechanism of the AI Act to **facilitate cooperation of market surveillance authorities and authorities or bodies that supervise or enforce EU law protecting fundamental rights** should be strengthened in order to enable the smooth functioning of the AI Act governance, while also ensuring that operators do not face duplicate requests for information.

[161] Article 26(2) AI Act.

Fourth, the scope of the **measures that support stakeholders in the compliance** should be extended. Article 10(5) of the AI Act **allows providers of high-risk AI systems to exceptionally use sensitive personal data –** which is otherwise prohibited by the GDPR **–** for the purpose of bias detection and correction. This facilitates effective AI training and testing. The possibility of relying on this legal basis should be extended to providers of all AI systems and general-purpose AI models. AI regulatory sandboxes are a crucial measure for supporting AI innovators in the development of trustworthy and compliant high-risk AI systems. Their roll-out should be supported by reinforcing the cooperation at EU-level. Moreover, the **AI Office should be enabled to establish an AI regulatory sandbox at EU level** for AI systems under its supervision. It is also necessary to broaden the scope of the real-world testing of high-risk AI systems so that this instrument can be used for the high-risk AI systems listed in Annex I to the AI Act. Leveraging these infrastructures and facilitating cross-border collaboration will result in better streamlining of the coordination and optimisation of resources.

Fifth, **operational changes and technical corrections** should be made to contribute to an overall improved application of the AI Act. With regard to the **interplay of the AI Act with the Union harmonisation legislation listed in Section A of Annex I**, it is necessary to streamline the procedure for conformity assessment bodies to apply for and be assessed in order to become notified bodies. There is also need for a transitional rule for the first time after the AI Act's governance system has been established, to reduce the risk of a gap in availability of notified bodies when the rules start to apply. Moreover, an Annex to the AI Act should be created with the codes according to which notified bodies under the AI Act are classified and which they can use to register in the Commission's New Approach Notified and Designated Organisations (NANDO) information system, supporting the rapid establishment of notified bodies and their integration into the existing frameworks. It is also necessary to amend parts of the EU's common rules in the field of civil aviation [162] so that the AI Act's high-risk requirements can smoothly be integrated into those rules by means of implementing or delegated acts. In light of the objective to reduce implementation challenges for citizens, businesses and public administrations, it is also essential that harmonised conditions for the implementation of certain rules are adopted only where strictly necessary. For that purpose, it is appropriate to remove certain empowerments bestowed on the Commission to adopt such harmonised conditions by means of implementing acts in cases where this is not strictly necessary [163].

Sixth and finally, it is important to make it clear that many implementation challenges cannot be addressed through legislative amendments and that **stakeholders are also calling for non-legislative support measures**. For example, 72.09% of respondents of the survey of AI Pact signatories said they saw the establishment of a centralised platform to bring together all

[162] Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91.

[163] It is proposed to remove empowerments set out in Article 50(7), 56(6), 69(2) and 72(3) AI Act.

guidance and compliance support tool as the most helpful measure that the Commission could take. The recently published AI Act Single Information Platform caters to this [164]. The Commission will therefore continue to step up its efforts to facilitate and support compliance through other means. In particular, further **concerns related to the interplay with other EU law will be addressed in guidance** on the practical application of the rules. This includes the requests to provide guidance on the interplay with the GDPR, which the Commission is preparing jointly with the European Data Protection Board.

The **Commission has also noted that many challenges stem from the uncertainty surrounding the practical application** of certain concepts, such as the 'safety component' concept, the high-risk classification, and the scope for exemption of AI systems used for research and development. The Commission will clarify these concepts in forthcoming guidelines [165] and continue to work on different forms of additional guidance [166].

3.3. Estimated impacts

The proposed simplification measures are expected to **reduce compliance costs and make implementation easier** for businesses (especially SMEs and small mid-caps) and public authorities. Aligning timelines and introducing a transition period will allow operators to adapt gradually. It will also avoid the need for costly retroactive adjustments. Extending SME privileges, simplifying documentation, and providing guidance from authorities will lower administrative burden. Clarifying how the AI Act interacts with other EU laws will further reduce duplication and uncertainty. Supporting innovation through AI regulatory sandboxes and real-world testing will also help firms develop and test AI safely and facilitates their compliance efforts.

A **direct reduction of compliance cost** can be expected and estimated for the following measures:

- extension of certain regulatory privileges of microenterprises to SMEs and of SMEs to SMCs
- alignment of the implementation timeline for the rules related to high-risk AI systems
- replacing the obligation on operators to ensure a sufficient level of AI literacy of their staff with an obligation on the Commission and Member States to encourage such measures
- removing the obligation on providers of AI systems that are exempted from classification as high-risk to register those systems (which may for instance only carry out preparatory tasks) in the EU database

[164] European Commission, *AI Act Single Information Platform*, 2025, https://ai-act-service-desk.ec.europa.eu/en
[165] See section 1.2.3.
[166] For example, the AI Office is planning a workshop with independent experts with recognised expertise in the field of AI for a technical assessment of AI systems in the financial sector used for creditworthiness assessments. The findings of this workshop should assist in determining whether those AI systems are within the meaning of the AI Act, as specified through the Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act).

There is **no reliable evidence or estimate of compliance cost that allow a cost calculation** of other measures to simplify the future implementation. Moreover, several measures are expected to have indirect effects.

The **extension of some regulatory privileges regarding risk management systems for microenterprises to SMEs** is expected to benefit many companies. Extending the simplified quality management system requirement of Article 63, which currently applies only to microenterprises, which constitute 94% of the 26.1 million SMEs in the EU [167], to SMEs would theoretically bring benefits to 1 566 000 companies. Eurostat data indicate that 13.5% of enterprises with 10 or more employees in the in the EU use AI [168]. Assuming that a third of them are (also) developers of AI systems, of which 5% to 15% (median 10%) are concerned by the AI Act's requirements, this results in an estimated number of 7 000 additional companies.

The **extension of some regulatory privileges granted to SMEs regarding documentation requirements to SMCs would equally bring significant benefits.** Although the provisions for which regulatory privileges are granted do not yet apply, a conservative estimate would be a cost reduction by about 25% of the two categories 'administrative burden regarding documentation and traceability' and 'administrative burden regarding provision of information' which were calculated at about EUR 8 000 combined in the initial AI Act impact assessment. Thus, the regulatory costs for compliance of a high-risk AI system would decrease on average by EUR 2 000 for an SMC. In the Commission Staff Working Document on small mid-cap companies [169], the Commission services have estimated that 38 000 companies classify as small mid-caps in the EU. In the Eurostat survey on AI usage, SMCs are part of the category large companies, which have a significantly higher AI adoption rate of 41%. Assuming again that a third of them also develop AI, and that 5% to 15% (median 10%) are concerned by the AI Act's requirements, this results in an estimated number of 1 250 additional companies, with corresponding **savings of EUR 2 500 000**.

In the initial impact assessment for the AI Act, the Commission estimated maximum aggregate compliance costs for the obligations for providers of high-risk AI systems at EUR 100 - EUR 500 million per year, with around EUR 100 million of verification costs, if harmonised standards are available. Without harmonised standards, according to the survey amongst AI Pact Signatories [170], 20% of stakeholders expect costs to increase by over 80%, 13.33% expect a 50-80% increase, 26.67% expect a 20-50% increase and others were not able to disclose. One can thus estimate an average of 34% increase in compliance and verification costs. Taking as a baseline the Commission's initial impact assessment, this would lead to an additional estimated maximum aggregate cost of **EUR 68–204 million per year,** which an alignment of the implementation timeline to the availability of harmonised standards (or alternative tools) would avoid. In addition, one can expect positive cost reductions for Member States' competent

[167] Schulze Brock, P., Katsinis, A., Lagüera Gonzalez J., Di Bella, L., Odenthal L., Hell M., Lozar B. and Secades Casino B., *Annual Report on European SMEs 2024/2025, SME performance review*. Publications Office of the European Union, Luxembourg, 2025, p. 11, https://publications.jrc.ec.europa.eu/repository/handle/JRC142263.

[168] Eurostat (2025) *Artificial intelligence by size class of enterprise*. Available at: https://ec.europa.eu/eurostat/databrowser/view/isoc_eb_ai/default/table?lang=en

[169] SWD(2025) 501 final, page 8.

[170] Referred to above, in the section 'Stakeholder views'.

authorities who would otherwise incur additional cost by having to perform oversight without a clear guidance what is deemed compliant through harmonised standards or alternative tools.

The co-legislators introduced the **obligation on operators to ensure AI literacy** (Article 4 of the AI Act). This was not part of the Commission's proposal and therefore was not covered by the impact assessment. It is difficult to estimate average training costs across 27 Member States, particularly given the natural variety among different company sizes. 36.11% of respondents of the survey amongst AI Pact signatories estimated that their additional annual compliance cost ranges from EUR 0-10,000 [171]. However, the average cost will be considerably lower because the obligation relates to staff training and is therefore more costly for larger companies, which were overrepresented in the survey [172]. Moreover, companies do provide AI training even without a legal obligation (and are still encouraged to do so) in order to ensure that the AI systems are deployed and used responsibly and effectively. Thus, an estimate could be that the additional compliance with Article 4 costs on average up to EUR 1 000 per company, on top of efforts carried out independently to foster AI literacy. As previously mentioned, Eurostat data indicate that 13.5% of the 1.65 million enterprises with 10 or more employees in the EU use AI (i.e. around 222 750). Applying the above estimate, the simplification measure would thus result in **cost savings of up to EUR 222,75 million**. Meeting the Digital Decade target of 75% of enterprises using AI in 2030 could result in savings of up to EUR 1.24 billion by 2030.

The obligation to **register AI systems in the EU high-risk database** involves inputting into the online database some information which is readily available to the provider of an AI system. No more than 2.5 working hours should be required on average considering the need to understand the requirements, the once-off registration of the provider and the uploading of information for each AI systems that has been developed. The average labour cost in information services (Sector J of the Eurostat classification [173]) was EUR 37.19 in 2020 (the results from the 2024 survey are not yet available). Under these circumstances, EUR 40 per hour appears a relevant approximation. Hence, the costs would be EUR 100 per company. Taking the above-mentioned 222 750 companies using AI as an upper limit of companies that might have to register AI systems, assuming again that a third of them also develop AI, and that between 5 and 15% (median 10%) of AI applications would be high-risk as a proxy for the number of companies affected, there could be up to 7425 companies which need to register potential high-risk AI applications. If one assumes that at most 20% of these systems could be exempted under Article 6(3) of the AI Act, then a maximum of 1485 companies affected. Thus, total **savings could be up to EUR 148,500 per year**.

The below table 7 outlines all the above calculations, with their underlying assumptions.

[171] The other responses were: 16.67% estimated the additional annual compliance cost at between EUR 10 000 and 50 000; 2.78% estimated it at between EUR 50 000 and 10 000; and 8.33% estimated it at more than EUR 100 000.

[172] 25.58% enterprises had fewer than 10 employees, 25.58% had between 10 and 249 employees and the largest group of 48.84% had more than 750 employees.

[173] Eurostat (2023) *Labour cost, wages, and salaries, direct remuneration by NACE Rev. 2 activity*. Available at: [lc_ncost_r2] Labour cost, wages and salaries, direct remuneration (excluding apprentices) by NACE Rev. 2 activity

Table 8: Estimated cost savings for targeted changes to the Artificial Intelligence Act

Item	Unit	Assumptions	Formula (stylised)	Estimated administrative cost savings	
				Businesses	
Extension of certain regulatory privileges of SMEs to SMCs	EUR	25% reduction of EUR 8,000 cost related to documentation and provision of information for an additional amount of 1,250 companies	0.25 x 8,000 x 1250	**One-off**	**Recurring**
				N/A	≈ **EUR 2.5 million** per year
Alignment of implementation timeline for high-risk rules	EUR	34% increase of aggregate compliance and verification costs of EUR 100-500 and EUR 100 million per year, if harmonised standards are not available	0.34 x (100-500 mio. + 100 mio.)	N/A	≈ **EUR 68-204 million** per year
Transformation of obligation on AI literacy in Art. 4	EUR	1.65 million companies in the EU, 13.5% of which use AI, i.e. around 222,750, have an average EUR 1,000 additional costs for AI literacy compliance	1.65 million x 0,135 x EUR 1,000	N/A	≈ **EUR 222.75 million** per year
Remove registration in EU database for AI systems exempted according to Art. 6(3)	EUR	222,750 companies using AI of which a third develop AI (see above), of which 10% are providers of high-risk AI systems and of which 20% could be exempted, thus subject to the obligation to have an average cost of 2.5 working hours at EUR 40/per hour for the registration	(222,750 / 3) x 0.1 x 0.2 x 2.5h x EUR 40	N/A	≈ **EUR 148,500** per year
	EUR			*Public authorities*	

Reallocate supervision of AI systems based on GPAI models to AI Office		At least 1 FTE per MS and 10 in some MS (117 FTE in total) at EUR 30/hour no longer required in case of centralisation that in turn requires 55 FTE at EU level	(117 - 55) x EUR 30/h x 8h x 250 working days/year	N/A	≈ **EUR 3.7 million** per year
TOTAL	EUR			≈ **EUR 297.2 – 433.2 million**	

The **reinforcement of the AI Office's oversight over certain AI systems** is expected to lead to indirect positive impacts for businesses, including **reducing the governance fragmentation across authorities and contributing to the coherent application of the AI Act**'s AI systems rules, as national authorities will be able to take the AI Office's approach as guidance for their enforcement work, as well as offering **new pathways to compliance support through an EU level AI regulatory sandbox**. These measures have resource implications for the Commission, due to the volume and high complexity of tasks requiring specific technical and legal expertise as well as specialised tools and methodologies. According to the Commission's estimates, the AI Office's supervisory powers would encompass at least 230 AI systems and up to 100 platform-embedded AI systems built on general-purpose AI models, as well as hundreds of small-scale AI systems not embedding such models, used by platforms,[174] in addition to the supervision it already exercises over general-purpose AI models. The rapid evolution of AI technology, particularly the development and deployment of agentic AI becoming increasingly sophisticated, makes it challenging to accurately estimate the number of entities that will fall under our enforcement purview under Article 75(1) of the AI Act, which could likely also be significantly higher. Moreover, the **EU-level AI regulatory sandbox** will require additional resources. These tasks are estimated to require additional 53 FTEs (50 FTE for enforcement activities and 3 FTE for the operation of the EU-level AI regulatory sandbox). These implications have to be weighed against **reduced budgetary requirements for Member States**, who would otherwise be responsible to ensure the oversight for those AI systems. In this context, it has to be recalled that AI systems based on large general-purpose AI models are typically made available in all EU Member States at the same time. The counterfactual scenario, whereby the oversight and enforcement of these AI systems would be allocated to Member States would require at least 1 technical FTE in all Member States and for the 5 largest Member States and 5 Member States with active AI ecosystems at least a team of 10 FTE each. Thus, at the absolute minimum, 117 FTE would be required, i.e. more than twice the 55 FTE at EU level. With an average hourly cost of around EUR 30 per hour, i.e. EUR 60 000 per year, the extra 62 staff would amount to a minimum of EUR 3.7 million per year additional costs for Member States.

[174] Based on publicly available data and growth rates estimated by EpochAI.

3.4. Preserving the objectives of the rules and other impacts

The initial AI Act impact assessment considered other types of impacts, such as societal impacts, impacts on safety, impacts on fundamental rights and environmental impacts.

Regarding **societal impacts** [175], the initial AI Act impact assessment concluded that (i) there could be labour market impacts due to increased trust in – and therefore uptake of AI applications – (ii) the AI Act would reduce involuntary discrimination by AI systems; and (iii) promoting the uptake of AI would accelerate the development of socially beneficial applications. The targeted nature of the envisaged amendments means that they are not expected to modify such impact. The alignment of the AI Act's implementation timeline could slightly delay the attainment of such impacts, although it must be considered that they affect only part of the rules that cumulatively lead to the expected societal impact. Conversely, the extended measures in support of innovation could positively contribute to accelerating the development of socially beneficial applications.

Regarding **impacts on safety** [176], the initial AI Act impact assessment concluded that the AI Act would fill gaps in relation to the specific safety and security risks posed by AI embedded in products in order to minimize the risks of death, injury and material. The targeted nature of envisaged amendments would not affect the scope of AI systems covered by the AI Act or the substantive requirements for the different risk levels, so they are not expected to modify this impact.

Regarding **impacts on fundamental rights**, the initial AI Act impact assessment considered that the AI Act would boost the protection of fundamental rights. The Commission's explanatory memorandum to the proposal states that the AI Act is expected to enhance and promote the protection of many rights set out in the Charter [177], as well as positively affect the rights of a number of special groups [178]. The AI Act proposal was also found to impose some restrictions on certain rights [179], but these were assessed as proportionate and limited to the minimum necessary. The envisaged alignment of the timeline of entry into application could delay the attainment of the positive effects on the protection of fundamental rights. This impact must be weighed against the alternative of no postponement, with the risk that an application of the rules would practically not be feasible or extremely costly. Such situation would conversely aggravate the restriction of certain rights, notably the freedom to conduct business. Against this background, this delayed attainment of the positive effects on the protection of fundamental rights appears proportionate.

---

[175] Section 6.3.

[176] Section 6.4.

[177] The right to human dignity (Article 1), respect for private life and protection of personal data (Articles 7 and 8), non-discrimination (Article 21), equality between women and men (Article 23), freedom of expression (Article 11) and freedom of assembly (Article 12), effective remedy and a fair trial, defence and the presumption of innocence (Articles 47 and 48) and right to a high level of environmental protection and the improvement of the quality of the environment (Article 37).

[178] Workers' rights to fair and just working conditions (Article 31), the right to a high level of consumer protection (Article 28), the rights of the child (Article 24) and the right to integration of persons with disabilities (Article 26).

[179] The freedom to conduct business (Article 16) and the freedom of art and science (Article 13).

Regarding **environmental impacts**, the initial AI Act impact assessment found that the direct environmental impacts that could be expected from the AI Act were limited. However, it also identified some possible negative indirect impacts due to the increased uptake of AI that could cancel out the positive effects of increased energy efficiency through AI use. The targeted nature of the envisaged amendments means that they are not expected to modify this impact.

The initial monitoring framework of the initial AI Act impact assessment remains the reference base for the continuous implementation of the legislation and achievement of the unchanged broader policy objectives.

4. REPEAL OF THE PLATFORM-TO-BUSINESS REGULATION

The 2019 Platform-to-Business Regulation ('P2B Regulation') was the first step towards providing a comprehensive legal framework for the platform economy. It was the initial general framework applicable to what are called 'online intermediation services'. These services intermediate for a very large number of both large and small undertakings, or 'business users', within the internal market. However, the entry into application of the Digital Markets Act (DMA) and Digital Services Act (DSA) in 2023 and 2024 respectively significantly reinforced the set of rules for online intermediation services and online platforms. This has led to questions over the implementation of the P2B. The Digital Omnibus proposes to repeal large parts of the latter, underlining that the P2B Regulation's significant provisions are already taken on in other legal acts. This will increase legal clarity for stakeholders over the application of the rules, and a more streamlined digital rulebook. A transitory period to 2032 is foreseen to ensure legal certainty for acts containing cross-references to certain provisions of the P2B Regulation.

4.1. Analysis of the problems and opportunities

The rules. Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services (the platform-to-business or 'P2B Regulation') has been in application since 12 July 2020. The P2B Regulation was the first step towards providing a comprehensive legal framework for the platform economy. It was the initial general framework applicable to what are called 'online intermediation services'. These services intermediate for a very large number of both large and small undertakings, or 'business users', within the internal market. The P2B requirements were designed to ensure that business users, in particular SMEs that can have limited bargaining power relative to the online platforms, should be able to conduct their business in a predictable manner (e.g. relying on transparency as regards rankings) and are not exposed to unnecessary costs when facing issues with the online platform (e.g. suspension of the business account, or products and services being blocked by the platform). In addition, the P2B Regulation was also designed as a tool to ensure that fairness and transparency help smaller platforms to grow and innovate in a common legal framework shared with larger platforms, in a levelled playing field. To ensure that online intermediation services comply with the P2B requirements, its enforcement lies with the competence of the Member States.

To assist with implementation, the Commission published a notice on ranking guidelines[180] pursuant to Article 5(7) of the P2B Regulation, which should remain as a reference including after the repeal of the Regulation.

[180] Commission Guidelines on ranking transparency pursuant to Regulation (EU) 2019/1150 of the European Parliament and of the Council (2020/C 424/01).

The main issues. Since its entry into application, other acts of EU law have come to regulate online intermediation services and online platforms. These include the Digital Markets Act (DMA)[181] and the Digital Services Act (DSA)[182].

A preliminary assessment of the state of implementation of the P2B Regulation was published on 21 September 2023[183].

The report observed initial positive effects when it comes to contractual transparency for business users and due process in complaint-handling for instance. However, the report also evidenced that there was a lack of awareness among business users as well as providers of online intermediation services and of online search engines of their respective rights and obligations under the P2B Regulation. This was also coupled to insufficient compliance with the P2B Regulation and led to a lack of implementation. Hardly any complaints were received under the P2B Regulation until 2023. The report concluded that "the full potential of the P2B Regulation [was] not achieved at present".

This first preliminary review of the P2B Regulation of 2023 was published when the DSA and DMA had just entered into force. In the meantime, the EU regulatory framework for online intermediary services and online platforms has become more complete and more robust.

The DMA became applicable on 2 May 2023. Its purpose is to contribute to the proper functioning of the internal market by laying down harmonised rules ensuring for all businesses, contestable and fair markets in the digital sector across the Union where gatekeepers are present, to the benefit of business users and end users. With a view to protecting contestability and innovation in digital markets, the DMA prohibits certain unfair practices by so-called gatekeeper platforms that have proven harmful. Among the practices addressed are ranking transparency obligations, fair general conditions for access to gatekeeper services, data portability, access to data and self-preferencing.

Since its entry into application on 17 February 2024, the DSA aims to contribute to the proper functioning of the internal market, while also ensuring a safe, predictable, and trusted online environment that facilitates innovation and in which fundamental rights enshrined in the Charter are effectively protected. The DSA fully harmonises the obligations imposed, among others, on providers of intermediary services, including online platforms and online search engines, therefore pre-empting national rules in this area. It contains rules on terms and conditions, recommender systems, complaint-handling systems, out-of-court dispute settlement and codes of conduct. Enforcement of the rules lies with national authorities of Member States for online platforms established in their territory, and with the Commission for Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs).

The objectives. By repealing the P2B Regulation, the regulatory framework applicable to online platforms and business users is simplified by eliminating overlaps and multiple layers of regulation. This minimises legal uncertainty and reduces unnecessary compliance costs which

[181] Regulation (EU) 2022/1925.
[182] Regulation (EU) 2022/2065.
[183] COM(2023)525.

contribute to business trust in the legal framework and encourages new entrants into the EU market. This simplification also contributes to more robust and more targeted enforcement of existing rules.

4.2. Simplification measures and impacts

The Digital Omnibus proposes to repeal the P2B Regulation, with provisions largely covered in other legal texts as outlined below.

Transparency and fairness of terms and conditions by providers of online intermediation services (Articles 3 and 8 P2B Regulation) is granted now by the eponymous Article 14 of the DSA, covering also conditions for restrictions on the use of their service. Similarly, obligations on intermediation service providers as regards restriction, suspension and termination (Article 4 P2B Regulation) are largely covered by the obligation on hosting service providers to provide a statement of reasons for restrictions (Article 17 DSA) and, to some extent, conditions for measures and protection against misuse (Article 23 DSA). However, there is a difference in scope on the types of restrictions covered by the two regimes, in particular as regards specific situations for self-employed platform workers.

When it comes to transparency on differentiated treatment, ranking and self-preferencing (Articles 5 and 7 P2B Regulation), both the DSA and the DMA contain clear rules. Online platforms have to be transparent about the parameters used in their recommender systems as per Article 27 DSA, and VLOPs/VLOSEs have to consider the design of any of their algorithms in their risk assessment (Article 34(2) DSA). Under DMA, in turn, gatekeepers are prohibited from positively discriminating in favour of their own services and products in ranking results, and apply transparent, fair and non-discriminatory conditions to such ranking (Article 6(5) DMA). Additionally, gatekeepers are required to apply fair, reasonable an non-discriminatory general conditions of access for business users to its designated core platform services.

As regards access to relevant data by business users, the P2B Regulation provides for transparency obligations in the terms and conditions of the online intermediary service provider, including on the absence of such an access (Article 9 P2B Regulation). The DMA obliges gatekeepers to provide effective and free of charge data portability rights to its users and free-of-charge, continuous and real-time access to relevant data by users (Articles 6(9) and (10) DMA).

When it comes to the "most favoured nation clauses" (restricting business users to offer the same goods and services under different conditions through other means than through the services of the intermediation service provider) (Article 10 P2B Regulation), the P2B imposed an obligation of transparency on the platform. The DMA establishes a prohibition for gatekeepers to impose such clauses (Article 5(3) DMA).

The P2B Regulation contains obligations for online platforms to allow for complaint-handling, mediation and specialized mediators (Articles 11, 12 and 13 P2B Regulation). This largely overlaps with the DSA's provisions on internal complaints systems, out-of-court dispute settlement, complemented by transparency and reporting obligations (Articles 20, 21, 15, 24, 42 DSA). To be noted that certain categories of persons performing platform work, as regulated

by Directive (EU) 2023/2831 on improving working conditions in platform work, rely on these provisions in the P2B Regulation. Specific mediation mechanisms are also foreseen in the P2B Regulation for very large online platforms as regards media content by the European Media Freedom Act (Article 18 EMFA).

The right for representative action for organisations and associations of business users (Article 14 P2B Regulation) is mirrored in the DSA (Articles 86 and 90), and importantly now covered by Directive (EU) 2020/1828 on representative actions for the protection of the collective interests of consumers[184].

Finally, the possibility for developing codes of conduct under the P2B Regulation (Article 17) is largely covered by Article 45 of the DSA, allowing for the drawing up of codes of conduct to be developed to contribute to the application of the DSA.

4.3. Estimated impacts

This strengthened EU regulatory framework has largely overtaken the provisions of the P2B Regulation. The P2B Regulation, by providing for more transparency for business users of online platforms, implicitly aimed at practices by larger platforms where a difference in bargaining power exists. In this context, the DSA and the DMA provide for stronger protections for SMEs vis-à-vis larger actors. This is especially the case when it comes to unfair practices related to transparency and self-preferencing, data access and dispute resolution where the DSA and the DMA go further than the mere transparency obligations under the P2B Regulation.

Simplification of the regulatory framework for online platforms will reduce compliance costs due to layered and overlapping rules. Online intermediary service providers will benefit from increased clarity of legal provisions.

Repealing large parts of the P2B Regulation will also contribute to a more coherent and robust enforcement vis-à-vis larger platforms by clearly identified regulators, avoiding potential duplications. Regulators, such as DSCs for all intermediaries established in their respective Member States, and the Commission for VLOPs/VLOSEs and gatekeepers, will be able to focus their resources to the benefit of a more consistent and harmonised enforcement.

Arguably, repealing the P2B Regulation may lead to fragmentation since Member States will be allowed to regulate other aspects relating to online intermediary service providers. This was indeed recognized as a risk in the Impact Assessment preparing the P2B Regulation: "the uncoordinated adoption of national legislations - whether platform-specific or covering B2B issues in general but applicable to platform businesses – may result in divergent regulatory measures across the EU"[185]. However, the EU digital rulebook is now more robust with the

[184] Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC.

[185] Commission Staff Working Document Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services {COM(2018) 238 final} - {SEC(2018) 209 final} - {SWD(2018) 139 final} part 2.5, p.31.

entry into application of the DMA and the DSA, complementing the e-Commerce Directive, which are of maximum harmonization and align therefore with the P2B Regulation's objective to create a harmonised legal framework[186].

This risk for fragmentation is considered to be particularly low given that the regulatory space for national measures is very narrow. Indeed, the e-Commerce Directive, the DSA and the DMA almost exhaustively cover the aspects related to online intermediary service providers that are regulated by the P2B Regulation. For instance, the Court of Justice has stated that the e-Commerce Directive must be interpreted as precluding measures adopted by a Member State, with the stated aim of ensuring the adequate and effective enforcement of the Platforms-to-Business Regulation, under which, on pain of penalties, providers of online intermediation services established in another Member State are subject, with a view to providing their services in the first Member State, to the obligation to be entered in a register maintained by an authority of that Member State, to communicate to that authority certain detailed information about their organisation and to pay a financial contribution to that authority[187]. Therefore, the country-of-origin principle will nevertheless remain as an indispensable instrument to protect the single market.

Based on these considerations, it can be concluded that the P2B Regulation is only of **residual relevance** and should be repealed. At the same time, there is a need to ensure a transitory phase allowing that, where the P2B rules are complementary to or cross-referenced by other legislations, those elements of complementarity are preserved. This is the case for certain definitions pioneered by the P2B Regulation in EU law, as well as certain protections offered in particular to self-employed platform workers, in complementarity to the Platform Workers Directive[188], in course of transposition.

Stakeholder views

Some Member States pointed to existing overlaps of the P2B Regulation with other legislation, such as the DSA or the DMA. Similarly, several businesses reported having experienced legal uncertainty and duplications resulting from overlapping provisions of the P2B Regulation and other EU rules. For instance, some European platforms have pointed to specific overlaps regarding obligations on the setting up of an internal complaint-handling system (Art. 11 P2B Regulation) and the DSA – with the latter codifying a more comprehensive framework. Other degrees of overlaps were noted as regards to transparency obligations (ranking, terms and conditions), or rules on mediation. Business associations generally questioned the P2B Regulation's added value, and articulation with other laws. Nevertheless, the precedence taken by the DSA and the DMA on platform rules, as described in the above sections, generally limited the amount of stakeholder attention to the P2B Regulation in the last years.

[186] Commission Staff Working Document Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services {COM(2018) 238 final} - {SEC(2018) 209 final} - {SWD(2018) 139 final} part 7.1.4, p.72.

[187] See Judgements of 30 May 2024 in cases C-662/22 (Joined Cases C-662/22, C-667/22), Case C-666/22 (Joined Cases C-664/22, C-666/22), Case C-665/22, Case C-664/22 (Joined Cases C-664/22, C-666/22) and Case C-663/22.

[188] Directive (EU) 2024/2831.

CONCLUSION

The Digital Omnibus is an ambitious burden reduction proposal. It contributes directly to the Commission's target objective of cutting recurring administrative costs by EUR 37.5 billion by the end of the mandate[189].

On aggregate, and on the basis of initial estimates, it could lead up to EUR 1,335,634,500 in administrative cost savings per year for businesses, on top of EUR 1,043,943, 500 in estimated one-off savings. Provided the proposal enters into force by early 2027, this would amount to at least EUR 5 billion by the end of the Commission mandate in 2029. In addition, a further EUR 1 billion are estimated to be saved for public administrations by 2029. An overview of all estimated savings can be found in Annex II.

Several of the measures put forward in this Omnibus, by their very targeted nature, were not immediately quantifiable in terms of direct cost reduction on the basis of available data when preparing this proposal. Similarly, the cost of adaptation could not always be quantified, but is overall expected to be limited due to the targeted nature of the amendments. The latter are largely expected to create more favourable business conditions, for companies of all sizes in Europe, and stimulate innovation. The overall beneficial cost impact of this proposal is thereby expected to be higher than estimated at this stage.

On a more qualitative level, the Omnibus also leads to distinct cross-regulatory simplification by clarifying certain interplays between laws. This delivers better clarity in the engagement with the European digital rulebook. The amendments are 'optimising' changes, that seek to deliver the same, or better results, at a lower cost. Their impact on the underlying objective of the rules is expected to be positive. In particular, they are expected to support the highest standards of protections for fundamental rights, not least the right to privacy, the right to data protection, the right to non-discrimination, as well as the right to conduct a business.

The Digital Omnibus, as part of the broader Digital Simplification Package, is only the first step of a larger set of actions. The Commission will pursue its digital simplification agenda through the Digital Fitness Check across the mandate – with a view of delivering further regulatory clarity for businesses, citizens, and administrations across Europe.

[189] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A simpler and faster Europe: Communication on implementation and simplification. COM/2025/47 final.

ANNEXES

Annex I - Stakeholder consultations

Introduction

Numerous consultation streams were carried out in the context of the proposal. Each were conceived as complementary to one another, addressing either different topical aspects or stakeholder groups concerned by the initiative.

In the initial scoping phase of the Digital Omnibus, three public consultations and calls for evidence were published on the key pillars of the proposal in the spring of 2025. A consultation ran on the Apply AI Strategy from 9 April to 4 June[190], another on the revision of the Cybersecurity Act from 11 April to 20 June[191], and finally another on the European Data Union Strategy from 23 May to 20 July[192]. Each questionnaire had a dedicated section (or at times multiple) on implementation and simplification concerns, directly related to the reflexions on the Digital Omnibus. Taken together, 718 unique responses were obtained as part of this first consultation stream.

A Call for Evidence on the Digital Omnibus was further published from 16 September to 14 October 2025[193]. Its aim was to cover the entirety of the initiative, and give the opportunity to stakeholders to comment on a more targeted set of proposals in a consolidated stream. 512 responses were received, by diverse stakeholder categories.

With a view of raising awareness on the Digital Omnibus among small and medium-sized enterprises (SMEs), and collect their feedback, a dedicated SME Panel was run via the Enterprise Europe Network (EEN) between 4 September to 16 October 2025. The EEN is the world's largest support network for small and medium-sized enterprises, and is implemented by the European Commission's European Innovation Council and SMEs Executive Agency (EISMEA). SME Panels are a consultation stream falling under this framework, whereby small and medium-sized enterprises have the opportunity to contribute their views to an upcoming policy initiative. In addition to the online written consultation (where 106 SME responses were gathered), the Commission also presented the Digital Omnibus proposal to SME associations part of the network, in a dedicated meeting on 1 October.

---

[190] European Commission (2025) *Call for evidence and public consultation on the Apply AI Strategy*. Available at: Apply AI Strategy – strengthening the AI continent

[191] European Commission (2025) *Call for evidence and public consultation on the revision of the Cybersecurity Act.* Available at: The EU Cybersecurity Act

[192] European Commission (2025) *Call for evidence and public consultation on the European Data Union Strategy*. Available at: European Data Union Strategy

[193] European Commission (2025) *Call for evidence on the digital package and omnibus*. Available at: Simplification – digital package and omnibus

Two other consultation streams were organized, with a focus on direct exchanges with stakeholders. At political level, two implementation dialogues were held by the Executive Vice-President Henna Virkkunen: the first on data policy[194] (1 July 2025), and the second on cybersecurity policy[195] (15 September). Another was held by Commissioner McGrath on the implementation of the GDPR on 16 July 2025[196]. At technical level, five reality checks were organized by Commission services with stakeholders between 15 September and 6 October 2025 to deep dive into different implementation barriers on specific sets of rules considered for simplification under the Digital Omnibus.

Finally, a large number of bilateral meetings were organized by Commission services with stakeholders throughout the year of 2025, to address specific concerns. Discussions were also held with Member States. In addition to bilateral exchanges, dedicated agenda points on the Digital Simplification Package where discussed at Council Working Parties in June and September 2025 where the Commission presented the state of play and asked for Member States' views.

Overall, stakeholder feedback converged as to the need for a simplified application of some of the digital rules. Better coherence, and a focus on optimisation of compliance costs, is largely welcome by stakeholders of all nature. Some divergence exists as to some of the more tailored measures. While discrepancies between stakeholder categories were noted across the Digital Omnibus span of targeted amendments, they are to be viewed through the prism of the specific legal change considered. This Annex presents an overview of each consultation, highlighting the key findings.

I. Call for Evidence on the Digital Omnibus

The consultation ran from 16 September to 14 October 2025. In total, 512 responses were submitted online by a diverse group of stakeholders. In addition, several others sent their contributions directly to the Commission services. Most feedback was received by business associations (35.9%) and companies (27.2%), with SMEs representing 66% of the latter respondents. This was followed by NGOs (9.4%), citizens (8.8% EU citizens and 1% non-EU citizens), academic/research institutions (3.9%), public authorities (3.5%), trade unions (2.2%), consumer organisations (1.6%), as well as others (6.6%).

In terms of geographical distribution, most of the respondents were based in the EU, with a majority of contributions coming from Belgium (25.8%), Germany (15.4%), and France (10.0%), who together account for a share of over half of all the contributions. Countries like

[194] European Commission (2025) *Implementation dialogue – data policy*. Available at : Implementation dialogue – data policy - European Commission

[195] European Commission (2025) *Implementation dialogue on cybersecurity policy with Executive Vice-President Henna Virkkunen*. Available at: Implementation dialogue on cybersecurity policy with Executive Vice-President Henna Virkkunen - European Commission

[196] European Commission (2025) *Implementation dialogue on the application of the general data protection regulation, with Commissioner Michael McGrath*. Available at: Implementation dialogue on the application of the general data protection regulation with Commissioner Michael McGrath - European Commission

the Netherlands (6.8%), Italy (4.9%), and Czech Republic (4.9%) also showed notable engagement.

Internationally, the highest share of respondents that participated were from the United States (4.7%) and the United Kingdom (2.9%). The companies and business organizations that participated showed a high EU-establishment rate: 80.6% specified that they were established in the EU. Overall, 78.5% of all submissions included an attachment (non-paper or other type of paper).

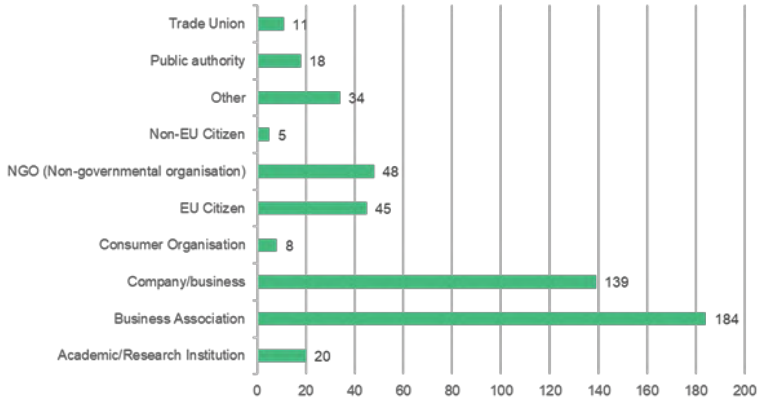

Figure 1: Stakeholder Categories

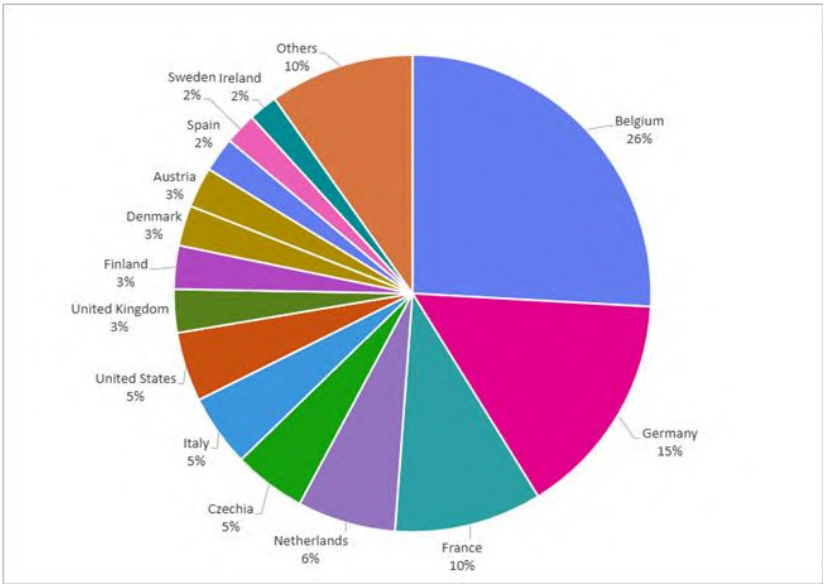

Figure 2: Country of Origin

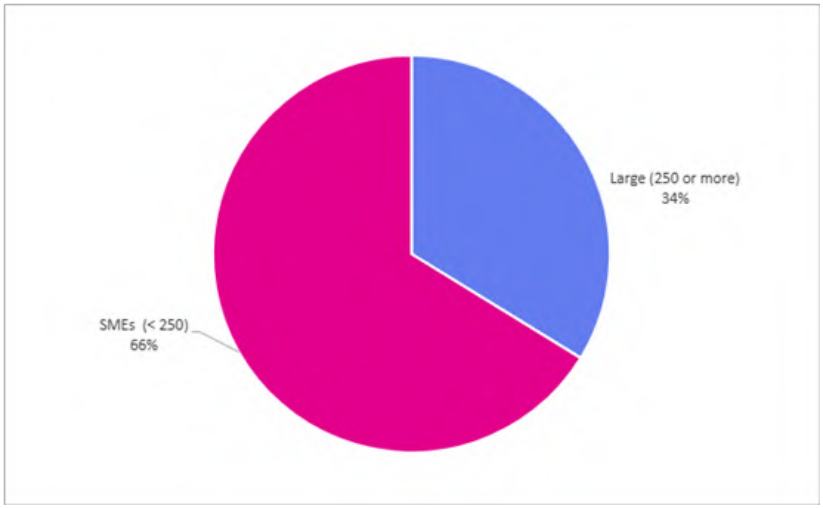

Figure 3: SMEs Among Business Type

Summary of results

Most stakeholders strongly voiced support for the simplification agenda. A large majority of respondents across different stakeholder types converged on the view that the EU's digital regulatory landscape has become overly complex, and that simplification should focus on coherence, consistency, and proportionality, reducing unnecessary burdens for businesses while delivering and maintaining effective standards for consumer protection. This was often accompanied by a widespread call to harmonize definitions and rules (with recurring calls for centralized glossaries, for instance), and offer better guidance on legal interplays, such as between the GDPR and other acts (AI Act, Data Act, Data Governance Act, Cyber Resilience Act and EHDS).

A majority of responding NGOs and several citizens, however, pressed to not water down the EU's established high regulatory and social standards in the simplification effort. Rules around privacy and artificial intelligence were particularly singled out in this purpose. Many SME associations similarly stressed that simplification should not affect essential rules which have created a level-playing field for them.

While most of the received feedback focused on the core areas under consideration in the Call for Evidence (rules relating to the data acquis, artificial intelligence, cybersecurity and digital identity[197]), a limited amount of business stakeholders also contributed on the application of other types of digital legislation, such as telecommunications and platform rules. Across topical areas, many stakeholders called for further harmonization between horizontal and sectoral rules – with some suggesting future work on that in the future, for instance via the Digital Fitness Check or via sector-specific Omnibuses.

<u>Feedback on the data acquis</u>

[197] Ultimately, this last policy area was not maintained as part of the set of rules addressed under the Digital Omnibus.

A large proportion of respondents gave feedback on the data acquis elements under consideration in the Digital Omnibus. The topic of cookie banners, and more generally potential simplification of the GDPR, attracted most of the feedback. Among business stakeholders, as well as some public authorities, there was broad support for better alignment between the GDPR and ePrivacy Directive (Art. 5(3)) regarding consent fatigue, fragmentation and proportionality - with additional specific support for broader legal grounds to access terminal equipment in alignment with the GDPR's risk-based approach. Many NGOs and privacy groups countered this by stating it would weaken the protection level that is intended by the ePrivacy directive, prioritizing preservation of user protection. EU-citizens frequently mentioned cookie fatigue, from a user perspective, with several calling for simpler, browser-based (standardized) consent mechanisms as a solution to cookie fatigue (also joined by many business stakeholders). Publishers and media representatives called strongly against centralized browser solutions, with concerns that it would reinforce the control of a limited set number of companies.

On the GDPR more broadly, most stakeholders across categories argued for better guidance on interplays with other rules. The AI Act was the most frequently cited legislation, followed closely by the Data Act. Other clarifications were also asked regarding alignment of rules with the Data Governance Act, the Cyber Resilience Act, and the EHDS. Some business stakeholders (especially large associations and companies) expressed additional support as to allow AI training on personal or pseudonymised data under legitimate interest, as well as a plea for additional consideration of privacy-enhancing technologies (PETs) as a proportionate safeguard for low-sensitivity data. Overall, the 'risk-based' approach of the GDPR was raised as something to be strengthened by business stakeholders of all sizes. SMEs notably called for further exemptions, in the continuity of the Fourth Omnibus Package from the European Commission.

Feedback on the Data Act, Data Governance Act (DGA) and the Open Data Directive (ODD) featured prominently across the consultation, particularly among business stakeholders. Overall, stakeholders converged on the view that both the DGA and the ODD are conceptually relevant but operationally fragmented: some stakeholders therefore called for merging of the ODD, DGA and also Free Flow of Non Personal Data Regulation (FFDR). Stakeholders advocated for further harmonization between the ODD, DGA and Data Act to boost clarity, predictability, and reduce costs in order to achieve consistent data sharing in machine-readable format. Many stakeholders additionally noted persistent uncertainty about the distinction between personal and non-personal data, and the conditions for lawful data reuse.

Specifically on the Data Act, SMEs and SME associations (both sectoral and horizontal) strongly urged for a forceful implementation of the rules. Some SME and startup associations further encouraged for dedicated funding for SMEs to incentivize participation in common data spaces, as well as better guidance on general applicability of the data acquis. On the other hand, large companies and associations called for a postponement of the Data Act application – with suggestions ranging from 12 to 24 months. Additionally, they urged for a review of the trade secrets framework under the Data Act, arguing that it jeopardized established business models, and less stringent Business to Government (B2G) data requests. Respondents from the automotive and railway industry at European level (joined by several other large companies)

particularly encouraged as to the exclusion of B2B contracts from the Data Act, and to avoid retroactive application of legacy contracts. German industrial stakeholders, joined by several other business associations across sectors, explicitly supported a number of exemptions for Small Mid-Caps.

Non-EU respondents (notably from the US, Japan, and Switzerland), joined by some large European business stakeholders, urged for clearer alignment of international data transfer rules and interoperability standards, warning that fragmented approaches could hinder transatlantic and global cooperation.

Feedback on implementation of artificial intelligence rules

Feedback was also substantial on the artificial intelligence mentions under the Call for Evidence. The implementation of high-risk rules under the AI Act was the most debated topic. A broad majority of business stakeholders (especially large ones) called for a revision of the implementation timeline for the AI Act's high-risk provisions. Within this group, the types of postponement mechanisms varied considerably:

- Some advocated for a grace period, generally of 1 year, meaning temporary relief from penalties while voluntary compliance continues;
- Others opted for full postponement of the application of the rules until harmonised standards are formally adopted and published, with suggestions ranging from 6 to 24 months;
- And the remaining contributions favoured sectoral rules (or guidance) and sectoral frameworks, some proposing a (sector-based) phased entry into force where certain high-risk categories would come into effect later than others (particularly put forward by stakeholders in the medical devices industry, for instance, as well as in the machinery and construction, railway, and automotive sectors).

Almost all responding NGOs (especially consumer associations), as well as some standardization bodies and citizens, strongly contested this phased approach. They urged to not slow down the implementation work, which may provide a negative signal to companies about to invest into compliance with the new rules.

SMEs highlighted the challenges faced by smaller players with the AI Act's high-risk rules. Many SMEs called for more support tools, subsidized conformity assessment, guidance and simplified compliance, rather than legal changes necessarily. Other innovation support measures, such as AI regulatory sandboxes and real-world testing, were further called for by larger business stakeholders as well. Several large businesses or associations (especially non-European) specifically called for a revision of the threshold for General Purpose AI systemic risk, and a closer alignment on international standards. The railway industry was vocal, across several contributions, as for B2B ('business to business') requirements to be less stringent than for B2C ('business to consumer'), as well as a general exemption for legacy systems.

A transversal matter of concern across business stakeholders of all sizes related to the assessed lack of clarity in certain definitions under the AI Act, as well a call for better tailoring of the high-risk categorization and more flexibility around low-risk products. Many respondents also

called for additional clarification of the AI Act's interplay with other digital laws, namely the GDPR and the Digital Services Act.

Finally, some industry stakeholders (many of them based in the US), pointed to the restrictions under data protection law affecting AI training and testing under legitimate interest. This was also supported by some European startups. Overall, in many contributions, a need for clearer guidance on the use of legitimate interest when it comes to consent for AI training, was underlined. Publishers and media representatives expressed general caution as to the potential dilution of the copyright principles under the AI Act, as part of the simplification agenda.

Feedback on cybersecurity rules

A significant proportion of contributions addressed cybersecurity matters. Respondents across companies of all sized, public authorities, business groups but also consumer organisations overwhelmingly supported streamlined cyber incident reporting, citing heavy overlaps between NIS2, DORA, CRA, and the GDPR. Calls for a single EU reporting portal were widespread across stakeholder categories. Recommended solutions varied as to their level (with some urging for a stronger role for ENISA, at European level, and others favoring an approach at national level), and the extent to which reporting templates, timelines and thresholds should be aligned.

A number of business contributions called for clarification of scope and interplay with other frameworks under the Cyber Resilience Act (CRA). SMEs in particular requested better guidance on implementation, clearer definitions and proportional requirements, noting that certification costs can be disproportionately high for smaller firms.

Moreover, several business associations and standardization organisations underlined the importance of standardisation, calling for leveraging and relying on existing industry standards rather than developing more overlapping security frameworks.

Finally, some feedback from business stakeholders focused on NIS2's implementation. Almost all stakeholders commenting on this point called for a more harmonized approach, and consistent enforcement across Member States (with notable concerns about auditing costs).

Feedback on digital identity rules

The contributions on the topic of digital identity were very limited in this Call for Evidence. Most of the contributions on digital identity were submitted by companies in the digital identity industry. Some stakeholders underlined the fragmented compliance landscape and advocated for a single-audit framework for QTSPs, recognized by all competent authorities (supervisory bodies, NIS2, GDPR, DORA). In line with this, contributions generally called for aligning the eIDAS-revision (EUDI framework) with the European Business Wallet proposal, (global) standards, SDG, DPP and PSD2 (for the payments authentication process). Some SME stakeholders further expressed concern on some of the standardization work being pursued for the EUDI Wallet, assessing it as potentially too prescriptive.

Additionally, some stakeholders (especially SMEs) called for clear and multilingual onboarding guidelines for all businesses (including those outside of the EU) to make the European Business Wallet an attractive and accessible tool. Some respondents stressed that the European Business

Wallet should be a market driven initiative. Relatedly, a large European SME association called for the use of the Business Wallet and EUDI Wallet to remain optional for businesses and citizens.

II. Public consultations on the Apply AI Strategy, the revision of the Cybersecurity Act, and the Data Union Strategy

As aforementioned in the introduction, to support the development of the Digital Omnibus proposal, three public consultations and related calls for evidence were launched in spring 2025. Each addressed one of the Digital Omnibus' key pillars: the Apply AI Strategy consultation, the Cybersecurity Act revision and the European Data Union Strategy consultation.

Each consultation had a respective section centered on simplification concerns. The below subsections provide an overview of the main findings that directly relate to simplification topics.

Apply AI Strategy consultation

The public consultation took place between 9th of April and 4th of June 2025. It aimed to gather information about the current state of AI adoption and development in the EU, with a specific focus on implementation challenges, to guide the Apply AI Strategy as well as further potential support actions for stakeholders.

The public consultation gathered 230 responses, and the associated Call for Evidence 287. Responses came from companies or businesses (90 out of 230), EU citizens (42), business associations (41), academic/research institutions (15), NGOs (14) and public authorities (10), trade unions (3), one consumer organisation, one non-EU citizen and 13 respondents who chose the option 'Other'. The vast majority of the respondents were from EU member states, with Belgium on the lead.

Among the several topics addressed, regulatory uncertainty emerged as a particularly relevant issue. One of the academic/research institutions, and 29 of the companies indicated that regulatory uncertainty is a barrier to AI (both for AI users and non-users) and mentioned that difficulty in identifying applicable rules and accessing information in relation to those rules as one of their main concerns. Uncertainty about future or upcoming legislation was mentioned by 27 companies and the burden of adapting internal procedures to ensure compliance with applicable rules was mentioned by 25 companies. Additionally, 14 companies pointed out heavy administrative burden as the main factor to not use any of the support initiatives provided by the EU such as CEDS, EDIHs, TEFs and AI on Demand.

Among AI developers, 52 stressed uncertainty about the scope and rules under the AI Act implementation as the major obstacles to compliance, particularly for small and medium-sized enterprises, which may not have the necessary resources or expertise to navigate the complex regulatory landscape. The absence of clear guidelines and standards was cited as a significant challenge, and the use of regulatory sandboxes was suggested as a potential solution. The complexity of the regulatory framework was criticised, with multiple regulations, such as the Digital Services Act, NIS2, and the AI Act, imposing overlapping and sometimes conflicting

requirements. The need for a more risk-based approach was emphasised, as well as the importance of providing clear and practical guidance to support the implementation of the AI Act.

The administrative burden imposed by the AI Act was seen as a significant hurdle, particularly for global companies with multiple AI-based solutions. The lack of harmonised standards, the capacity of Notified Bodies, and the potential for fragmented interpretations and enforcement across the EU were also identified as major challenges. The interplay between the AI Act and other EU regulations, such as the GDPR, MDR, and Machinery Directive, was noted as an area of uncertainty, with potential overlaps and conflicts between these frameworks. The requirements for high-risk AI systems, including fundamental rights impact assessments and conformity assessments, were seen as duplicative and burdensome, with some respondents arguing that these requirements do not deliver material benefits to customers. The lack of clarity and legal certainty surrounding the AI Act was a recurring theme. The need for international alignment and the use of international standards was also highlighted to reduce trade barriers and facilitate the development of AI in the EU.

Revision of the Cybersecurity Act consultation

The Public Consultation was conducted in the context of the ongoing revision of the Cybersecurity Act (Regulation (EU) 2019/881), running from 11 April to 20 June 2025. It aimed to gather feedback from a wide range of stakeholders on the effectiveness of the current legislative framework and potential areas for improvement. A total of 193 responses were received, with partial responses accepted. Among the respondents, 40.9% represented companies or businesses, 28% business associations, 13.5% EU citizens, 4.1% public authorities, 4.1% Other, 3.6% academic/research institutions, 3.1% non-governmental organisation, 2.1% trade union and 0.5% non-EU citizen. Responses were received from across 26 countries, including all EU Member States and a few non-EU countries.

According to written submissions in the associated Call for Evidence, there was a strong consensus among stakeholders on the need to reduce complexity and administrative burden, particularly for SMEs. Several contributors highlighted the challenges faced by smaller entities in navigating the current regulatory landscape and called for simplified compliance procedures. Stakeholders stressed the importance of clearer, harmonised guidelines to avoid fragmented implementation and ensure consistent application across the EU. Others emphasised the disproportionate impact of complex obligations on SMEs and advocated for tailored support mechanisms, including exemptions and simplified reporting frameworks. Several contributors also proposed the development of centralised EU platforms for reporting and compliance tracking, which would enhance efficiency and reduce duplication across different legislative instruments.

National authorities and ENISA representatives provided practical perspectives on implementation barriers, highlighting the need for streamlined reporting mechanisms, clearer guidance, and improved coordination across legislative instruments. They stressed the importance of making compliance processes more efficient and responsive to the needs of both Member States and industry.

This Public Consultation showed that NIS2 was the most frequently cited applicable EU legislation, with many respondents indicating multiple frameworks (GDPR, DORA, CER, AI Act) apply to their entities. Cross-sectoral associations and digital service providers highlighted the growing complexity and called for a more integrated legislative approach.

Stakeholders expressed strong concern about the diversity of incident reporting tools and processes at the national level, with medium-sized, small, and micro enterprises reporting the highest difficulty. The lack of harmonised reporting thresholds across EU legislations was a major challenge, especially for SMEs and business associations.

Implementation of cybersecurity risk-management measures showed varied responses, reflecting differences in organisational capacity. Overlap of requirements and the burden of proving compliance were significant issues, particularly for medium-sized, small, and micro enterprises, as well as trade unions. Calls for clearer guidance and streamlined processes were frequent.

Open-ended responses emphasised the need for simplified regulations, standardised templates, and centralised platforms. Stakeholders described the current system as fragmented and resource-intensive, with overlapping obligations diverting resources from operational cybersecurity efforts. There was strong support for cross-sector harmonisation, especially in banking, energy, transport, and public administration.

Overall, the analysis revealed a consistent call for simplification, harmonisation, and clarity in EU cybersecurity legislation. Medium-sized companies reported the highest concern, particularly regarding reporting thresholds, tool diversity, and compliance burdens. Small and micro enterprises also express significant concern, while large companies tend to be more moderate. Business associations advocated strongly for harmonisation, and public authorities, EU citizens, and other stakeholders highlight the need for coordination and sector-specific guidance. These findings underscore the importance of a coordinated and inclusive approach to cybersecurity governance that balances regulatory ambition with practical feasibility for all entities.

Data Union Strategy consultation

The public consultation on the European Data Union Strategy ran from 23 May to 20 July 2025. The strategy aimed to explore options to increase the availability of high-quality data, streamline existing data rules, potentially creating a simplified, clearer, and more coherent legal framework for businesses and administrations to share data more seamlessly and at scale, and address the international aspects of data flows.

In total, 171 contributions were received, of which 99 were on behalf of a company or business organisation / association, 28 from public authorities, 16 from citizens (all EU citizens), 16 from non-governmental organisations, 4 on behalf of academic / research institutions, 2 from consumer organisations, 1 from a trade union and 5 identifying as “other”. Amongst the 52 companies, 27% were small and medium-sized enterprises. Overall, 88% of the replies came from the EU-27. Around 66 position papers were submitted, either in addition to questionnaire

answers (62) or as stand-alone contributions (4). The below gives an overview of the consultation areas with a direct link to simplification.

1. Main simplification concerns expressed in the consultation

A wide majority of stakeholders thinks that consolidation of the data legislation is necessary due to **uncertainties regarding their interplay**. Out of 149 respondents, 30% completely agree with this finding, 29% to a large extent and 26% to a certain extent, while only 7% of stakeholders answer "not at all".

Concretely, 62% of 142 respondents support consolidation across the Data Act, Data Governance Act, Open Data Directive, Free Flow of non-personal data Directive, sector-specific rules, and ePrivacy Directive. Moreover, 27% want to include the GDPR in the consolidation efforts.

A majority of stakeholders is **uncertain** whether the **benefits of data legislation outweigh the costs** associated with its introduction (70% of 110 responding stakeholders). On the ePrivacy Directive, almost 80% opt for this option.

When asked about the balance between privacy protection and innovation, the respondents express mixed opinions. Regarding the processing of the **content** of electronic communications for other purposes than providing the service, 28% of the 125 respondents are opposed, 22% agree provided they have actively consented, and 34% want to limit the use of such data to legitimate interests. Regarding the processing of **metadata** of electronic communications, 20% oppose, 19% only with active consent, and 46% want to limit the use of such data to legitimate interests. Regarding data originating from terminal equipment, using **cookies and other tracking techniques**, 36% agree with the use of such data for legitimate interests related to the service provision, 20% agree to the use of such data but only when having actively consented, while 24% state they do not want to be tracked in any form.

Regarding the processing of IoT data for professional/industrial use, around 45% of 114 respondents **do not think that the current ePrivacy rules provide a good balance and do reflect well the technical situation**, as opposed to 11% who think this is the case. 44% say they do not know. Many stakeholders believe the ePrivacy framework is outdated or call for an alignment with the GDPR. While businesses call for more flexibility for processing purposes, users and civil society express the wish for modernised rules that effectively protect users from tracking and provide a real choice for their privacy settings.

When asked about the main **challenges in balancing data protection with innovation and technological advancements** (multiple-choice question, 146 respondents), the most chosen answers were "ensuring consistent enforcement of data protection laws within the EU" (29% of the responses) and "guidance on interplay with other legislation" (28%), followed by the "absence of regulatory sandboxes or means to discuss solutions with supervisory authorities" (16%). Among respondents who give more detail to their answers, the majority reports that the **inconsistent enforcement and one-sided interpretation of regulations by data protection authorities** is a significant issue. Key areas for clarification include the **interplay of the GDPR with the Data Act and the AI Act,** and the **interpretation of "personal data",** especially in

the context of IoT. Roughly 20% call for better defining the limits of the definition of personal data, especially in an industrial and IoT context, and including a criterium of reasonable risk of reidentification.

On the **preferred future governance structure on data sharing**, 32% of 129 respondents state to prefer one single EU governance body to be set up, whereas 15% want governance to be left to the member States, with stronger cooperation rules between them, and 15% prefer several EU governance bodies with strong cooperation rules. 14% answer "I don't know".

When asked about how to **improve the current legal framework** as regards access and use of Data for AI and innovation (multiple-choice question), the most chosen answers among the 154 responding stakeholders were to harmonize the legal terminology (68%), to provide guidelines on the interaction of laws (66%), to reduce administrative burden (62%) and to streamline governance structures at EU level (59%).

62% of the respondents indicated **reducing administrative burden** as the way to improve **the current legal framework.** Environmental reporting (22% of responses) and financial reporting (20%) stood out as the areas where over 70% of the 123 participants believed that existing rules could be enforced more efficiently through automated data exchanges, followed by trade/customs declarations (15%), product safety/standards (14%), AI contracting (13%) and workplace/labour law compliance (10%).

Out of 134 respondents, a clear majority (63 %; 39%: high potential, 24%: moderate) showed potential in **data spaces** to cut red tape by automating compliance procedures. Several respondents argue that the primary burden is **overly complex compliance steps**; they urged the Commission to streamline or eliminate these before layering automation on top. Nearly two-thirds of respondents (65 % of 130 respondents) wanted the EU to make it a high priority to fund digital tools that simplify regulations. In general, the respondents proposed to start with **high-burden and high impact sectors** where regulations are complex and data flows already exists, and to avoid new fragmentation. They proposed to **review and simplify the underlying rules first**, highlighting the fact that digital tools should support, not substitute regulatory clarity. Several submissions called for a **one-stop-shop EU portal** where firms lodge all regulatory reports ("report once, comply many"), or to use existing building blocks such as the **European Digital Identity Wallet**. Civil society organisations cautioned that "simplification" such as automation **must not erode** fundamental rights, cybersecurity, or environmental safeguards.

Moreover, when asked about **data localisation requirements**, 28% of 90 responding stakeholders confirmed considerable **costs**, and 19% to some extent. The answers given in the free-text section (28%) highlighted the burdens imposed by **varying and overlapping legal data regimes** on international operations. 54% of 89 respondents were worried (completely or to a large extent) about the insufficient clarity of the interaction between the regulatory framework of the EU and third countries, and 51% were concerned about compliance or **administrative burdens** linked to **international data transfers**. Criticisms uttered in the free-text section included perceived regulatory burdens, especially for **small and medium enterprises**, legal fragmentation and complexity, and a perceived protectionism, which might

restrict innovation. Stakeholders repeatedly highlighted the importance of international cooperation and adequacy decisions to **simplify GDPR-compliance**. Additionally, when asked about the **obstacles to engage in data altruism**, the most chosen answer was "administrative or legal complexity" (21% of 103 respondents).

2. Data availability and AI training

Most of the 136 responding stakeholders think the EU should **re-examine legal regimes to facilitate data usage for AI training** (yes: 70%; no: 30%). Of those saying "yes", 34 respondents identify the GDPR, 15 the Copyright Directive, 12 the AI Act, 9 the Data Act and 4 the ePrivacy Directive as the main legal regimes to be re-examined. The majority reports the need to strike a **balance between protecting personal data and enabling the use of data for AI**.

Among 130 stakeholders, there are similar views about the solutions which the EU should financially support to **enhance data availability** (create synthetic data; facilitating market access to articulated data needs; establish data intermediation services supporting not-for-profits, researchers and SMEs; negotiate and acquire collective data usage licences, with access limited to not-for-profits, researchers and SMEs). All proposed answers enjoy broad support, ranging between 56% and 60% approval rates, while between 14% and 20% of respondents answer "I don't know".

On the role of **public service broadcasters** in making data available for AI (multiple-choice question), many of the 108 responding stakeholders think that public service broadcasters **should make their content available to EU organisations for AI training** (50%), while 29% do not see a specific role for such broadcasters. A majority further reports that public broadcasters should have the sovereignty to decide about making their content available, with copyright clearance indicated by some as a major challenge.

On the role of **national deposit libraries** in making data available for AI (multiple-choice question), a majority thinks that these libraries should negotiate specific licences with copyright holders to make data available for AI (58% of 112 respondents), while 18% do not see any role for such libraries. Most of the 29 responses in the free-text section highlight the danger of national libraries and archives circumventing copyright laws.

On **synthetic data**, most stakeholders are in favour of the EU financially supporting the production of synthetic data (among 126 stakeholders, 18% see this as highly beneficial, 17% as somewhat beneficial and 26% as useful). Similarly, a majority agrees that the EU should mandate Member States to make certain synthetic data assets publicly available (17%: highly beneficial, 11%: somewhat beneficial, 29%: useful).

3. Specific focus on the Data Governance Act, the Free Flow of Non-Personal Data Regulation, and the Open Data Directive

(i) Data Governance Act

Regarding the Data Governance Act (DGA), many of the responding stakeholders report that they are **very familiar** with it (43% out of 134) or know most of its objectives and content

(33%). Familiarity is especially high among respondents from Germany (70% of respondents) and Belgium (78% of respondents), and within large organisations (250+ employees), where 48% report being "very familiar". 77% of 134 respondents indicate some form of **direct relevance** of the DGA for their organisation: 38 identify as organisations wanting to re-use public sector data (33%), 29 as public sector bodies (25%), and 17 as organisations engaged in data-sharing activities involving data intermediation service providers (15%).

Responses to the question about the **effectiveness** of the DGA are **mixed**. Only 8% of 125 respondents indicate that the DGA has achieved completely or to a large extent its objective of making more public sector data available. Similarly, only 9% feel that the DGA has met its objective of facilitating the collection of data for public use. Just 10% indicate that the DGA has fully or largely achieved its objective of reinforcing data sharing. On average, 46% of respondents express mixed views on the extent to which the DGA's objectives have been achieved, answering "somewhat" or "to some extent."

About half of the 119 responding stakeholders are either strongly (33%) or slightly (18%) in favour of **applying stricter conditions for reuse of public sector documents** covered by the DGA to '**gatekeepers'** under the Digital Markets Act or **'very large online platforms'** under the Digital Services Act. 22%, many of which being business associations, disagree to such suggestion. Similarly, 47% of 121 respondents are in favour of applying different rules to non-EU companies

A majority of stakeholders (52% of 116 respondents) would wish that the public sector makes more efforts to **allow processing of confidential data** as described in the DGA. 21% indicate having "recently worked with a public sector body that provided for a mechanism to re-use confidential data with privacy/confidentiality safeguards." On **data intermediation services**, half of the 121 respondents express support for the current strict regime of the DGA aiming to ensure the trustworthiness of such services, while 20% do not see the need for such legal framework. 12% favour a differentiated regime based on the market power of service providers. Only 2 stakeholders indicate that a voluntary certification of such services would be sufficient. The question on experiences with **data altruism** attracted 12 responses, of which 17% express positive views based on their experience working with data made available voluntarily by individuals through consent or by organisations through permission. When asked about the obstacles to engage in data altruism, the most chosen answer was "administrative or legal complexity" (21% of 103 respondents), followed by a lack of "trust that data will be used for the common good only" (16%) and "financial sustainability" (14%).

(ii) Free Flow of Non-Personal Data Regulation

Among the 113 respondents, 48 % demonstrate **strong familiarity** with the Free Flow of Non-Personal Data Regulation (FFDR): 27 are very familiar (24%) and another 27 know most of its objectives and content (24%). A further 30 respondents (26%) say they know some of its objectives. Only 16% of 101 respondents have encountered being subject to a written rule in an EU Member State preventing them from storing certain data outside that state, while 57% answer "no" and 27% "I don't know".

Asked about the **effectiveness** of the FFDR, views are **mixed** and **uncertainty remains high**. Fewer than four in ten respondents believe any FFDR objective is already fully met, and a consistent one-third cannot yet assess the Regulation's impact. Confidence is strongest where the FFDR directly tackles localisation rules (38% of 103 respondents agreeing that the FFDR is already easing localisation barriers); it is weakest on trust, security (26%), and practical switching between providers (28% perceiving benefits). Out of 104 respondents, 45% think the FFDR has been effective (13%), somewhat effective (29%) or very effective (3%) in facilitating cross-border data flow within the EU, while 43% choose the answer "I don't know".

Uncertainty is also high when asked about whether the mechanisms for **monitoring compliance** with the FFDR are sufficient. Among 101 respondents, almost two-thirds do not know whether the current monitoring set-up is sufficient. 20% of stakeholders deem it sufficient, whereas 14% do not see it as sufficient. Similarly, 68% of 103 respondents do not know whether the **enforcement mechanism** of the FFDR is sufficient, and 62% of 88 respondents do not know whether they would suggest **reforming** the rules of the FFDR.

(iii) Open Data Directive

Among the 114 respondents, 39 % report **being highly familiar** with the Open Data Directive (ODD). A further 29 % say they know most of its objectives, while 18 % indicate familiarity with both the directive's objectives and its detailed provisions. Respondents from Germany, France and Belgium show above-average familiarity with the ODD, and within large organisations (250 + employees) the share of highly familiar respondents is about 21.4 %.

Asked about the **need to modify the ODD**, the largest share (39% of 107 respondents) feels that the ODD should be modified, while a smaller group (25%) believes no changes are needed. Around 37% say they do not know. Answers in the free-text section highlight the need to eliminate national and cross-legislative inconsistencies by creating a consolidated legal framework, the need for a higher quality of open data and more high-value datasets, and missing legal clarity vis-à-vis data protection.

Of the 105 respondents, 46% say they use public-sector data frequently, 35% use it only to a limited extent, and just 8% have never used it at all. The groups most relevant to the ODD are businesses, business associations, and public-sector organisations. By country, the largest shares of respondents come from Germany, Belgium, France, Sweden, Italy, and the Netherlands.

Most respondents have a **positive view on the effects of the ODD** in practice. 68% of 104 respondents either slightly (47%) or strongly (21%) agree that more public sector data has become available for reuse, especially for SMEs. Similarly, 66% of 100 respondents agree slightly (44%) or strongly (22%) that the implementing act on high-value datasets has had a positive impact on the availability of such data. Around 57% of 103 respondents are in favour of transforming the ODD into a directly applicable Regulation (31% strongly, 26% slightly).

III. SME Panel on the Digital Omnibus

The European Commission conducted an SME Panel to gather input about business operations linked to digital rules among small and medium-sized enterprises (SMEs). The consultation was run online from 4 September to 16 October. It was complemented by an in-person meeting with SME associations on 1 October, to present the Digital Omnibus initiative to SMEs.

With a total of 106 contributions to the consultation, 94 respondents provided information regarding their company size, distributed across five categories. The largest group of respondents represented micro enterprises (1-9 employees), accounting for 44 responses, followed by small enterprises (10-49 employees) with 21 entries. Medium-sized enterprises (50-249 employees) with 16 responses, while 10 respondents identified as self-employed (owner-only, no employees). Finally, three responses came from larger enterprises employing more than 750 people.

Most participating businesses were based in Greece (34%), Poland (19%), and Spain (19%), followed by Portugal (6%), France (4%), Bulgaria (4%), and Hungary (4%). A smaller number of responses came from Cyprus (3%) and Sweden (1%). The geographical distribution shows a strong representation from Southern and Eastern Europe, with Greece providing over one-third of all responses.

Overall, 60% of participating companies indicated that they provide services or products in more than one EU Member State, reflecting a strong cross-border dimension among respondents. The questionnaire was structured into four sections covering different areas of law explored under the Digital Omnibus: cybersecurity incident reporting, data sharing, artificial intelligence, and digital identity framework. It aimed to explore how to help reduce daily compliance-related operational costs.

Summary of Results

Cybersecurity incident reporting

This section focused on the obligations of companies in the event of cybersecurity incidents such as cyberattacks or data breaches. It explored the challenges companies may have encountered in complying with EU legislation and its national transpositions.

Respondents were asked whether their company had ever submitted an incident report under several regulatory frameworks, including the Network and Information Security Directive (NIS2), Digital Operational Resilience Act (DORA),, General Data Protection Regulation (GDPR), Network Code on cybersecurity of cross-border electricity flows (NCCS). Most of the respondents (79%) indicated that they had never submitted an incident report under the regulatory frameworks considered. Among the companies that did report incidents, the most frequent case (9%) concerned companies designated as ‘essential’ or ‘important’ under NIS2, reflecting the critical role of companies in sectors such as energy, transport, health, manufacturing and ICT service management. On the contrary, no incidents were reported under regulations like NCCS.

The results suggest that reporting obligations to different regulatory authorities remain relatively uncommon for SMEs, with 55 respondents stating that this was not the case for their company. Nevertheless, five companies reported being required to notify the same incident to multiple authorities (with one company from Portugal stating, for instance, that it reports each year in Portugal, Poland, France, Czechia, Germany and Spain), with a further 32 respondents unsure. This uncertainty highlights a possible lack of awareness concerning overlapping reporting obligations. In their qualitative responses, participants pointed out that this is for instance, the case when it comes to GDPR compliance, national data protection authorities, and in some cases, sectoral regulations.

Despite this, several companies estimated that the cost of their company linked to the reporting of a cybersecurity incident could range from €500 to €35.000 (including cost of labor, and necessary in-house tools). Such range could be explained by factors such as the company size, sector, and nature of the incident.

Regarding the frequency of the incidents faced and reported per year, 19% of the companies participating in the survey experience between 0 to 10 reportable incidents annually, while 2% faced between 10 and 20 incidents per year, and only one company reported more than 20 incidents per year. Therefore, cybersecurity incidents seem to remain relatively infrequent among the surveyed companies (78% did not face or report any incident).

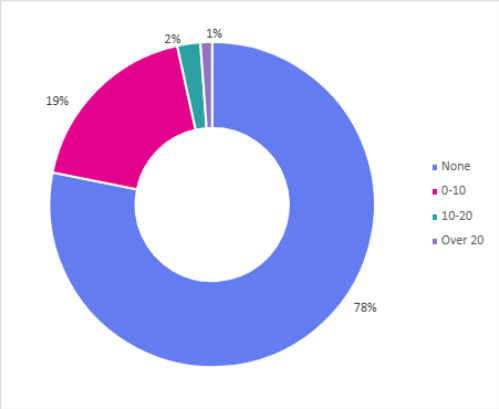

Figure 4: Reported and Faced Incidents per Year

Data sharing

Most respondents indicated not being aware of which legislative frameworks governing data sharing and access were applicable to their work model and operations. The most frequently recognised framework was the ePrivacy Directive, with 19 companies indicating that it applies to them. Eleven respondents stated that their company falls under the Data Act, followed by nine under the Free Flow of Non-Personal Data Regulation, and six each under the Open Data Directive and the Data Governance Act.

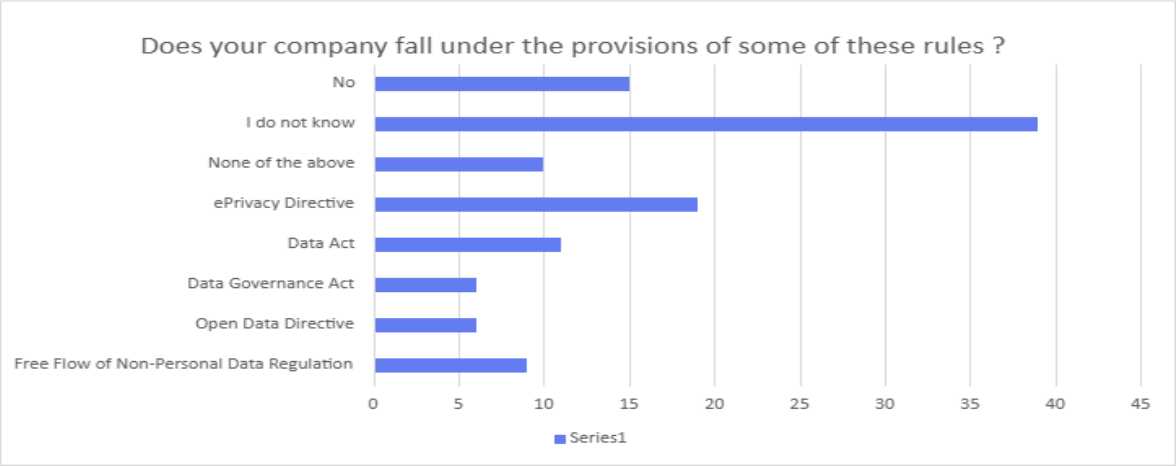

Figure 5: EU Data Related Legislation Applicable to Respondents

In addition, the great majority of the respondents considered that accessing data held by public sector bodies to re-use it for their own business activities was too complex as a process or that the data available was not relevant to their business.

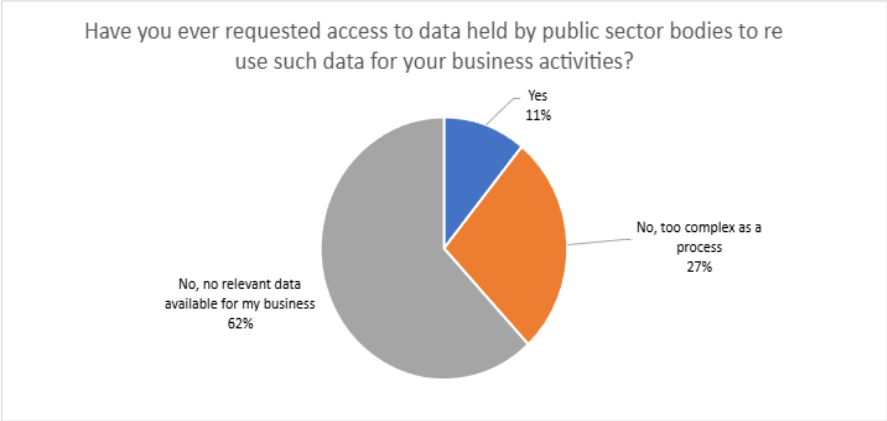

Figure 6: Respondents Accessing Data Held by Public Sector

Of those who reported having requested this type of data (11%, 23 respondents), 15 considered that the cost of such request was low compared to the value created by such data. Five stated that it was moderate or proportionate, while only three reported that the cost was high in comparison to the added value. Some companies further added cost estimates for such requests, but with broad and inconclusive ranges (from €100 to €50.000 for one micro-sized company from Greece)

When asked specifically about cookies (regulated under the ePrivacy Directive), 66% of the respondents indicated that they did not use them for other purposes than the technically necessary functions envisioned in the ePrivacy Directive, such as for sending a message over a network or for providing a service the user has specifically asked for. On the contrary, 34% of the respondents affirmed using cookies for other purposes. Website statistics were reported as the most common among these alternative practices.

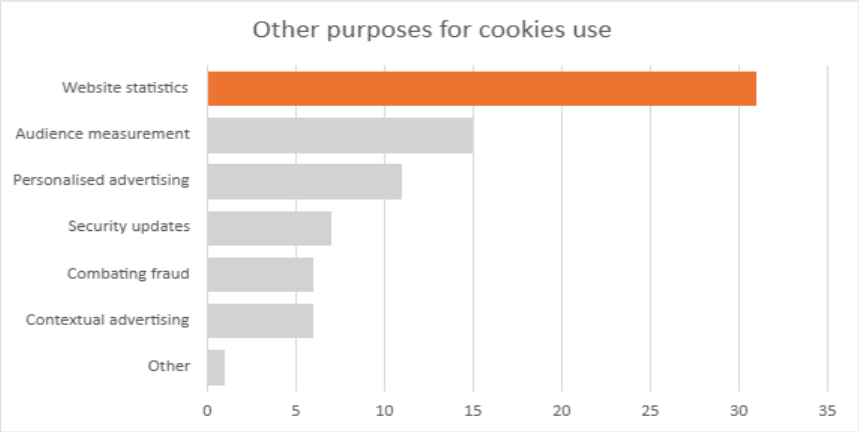

Figure 7: Other Purposes for Cookies Use

Responses regarding the average annual cost of creating and maintaining cookie banners varied significantly. Twenty SMEs provided quantitative data. While some respondents indicated that they do not use such banners, most others reported expenses ranging from €50 to € 1500 per year, A small number of respondents reported considerably higher costs, between €2,000-€5000 annually. Furthermore, respondents were asked whether they would continue to rely on cookie banners if the collection of personal data for audience measurement and website statistics no longer required user consent. The results suggest that, even if consent were no longer mandatory for audience measurement, a majority of companies (37 out of 61) would still rely on some form of cookie banner, either to ensure transparency or to safeguard against legal uncertainty.

Artificial Intelligence

While SMEs already benefit from a simplified regulatory regime under the AI Act, this section explored whether further supporting measures could be useful for a smoother implementation. In this regard, the greatest difficulties reported were uncertainty about the scope of the legislation and which rules apply (30%) and access to standards, guidance documents, or other compliance tools (18%), while 13% reported uncertainty regarding the responsible supervisory authorities. This was followed by 12% who pointed out resource constraints, and 8% cited bureaucratic hurdles or duplication with existing procedural requirements.

Companies indicated that templates and toolkits for SMEs (33%), staff training (23%), and access to a contact point for free compliance advice (27%) would most reduce the burden of implementing the AI Act, while 12% requested more guidance documents and 4% reported no support needed.

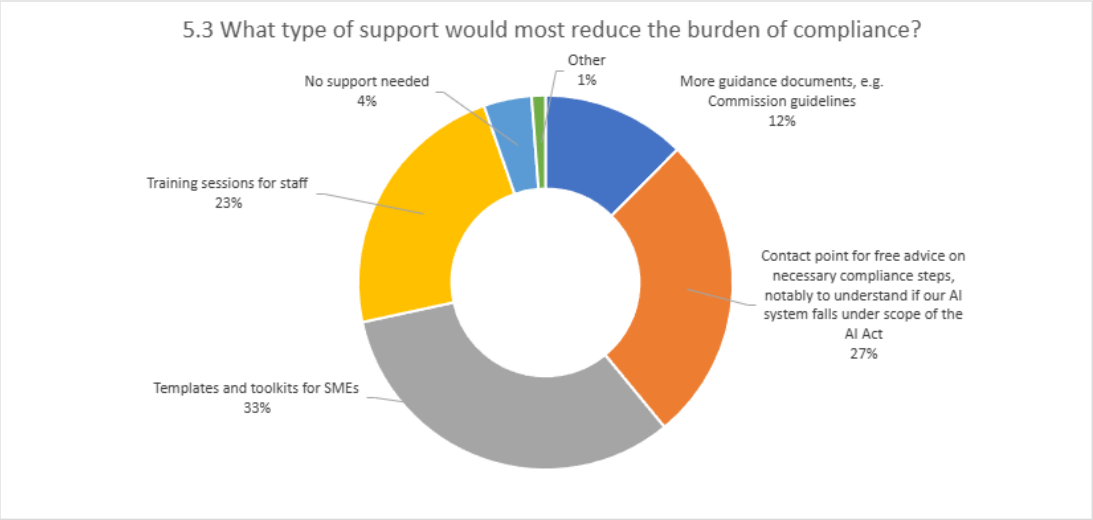

Figure 8: Type of Support to Reduce Compliance Burden

Additionally, respondents listed hiring or training staff for compliance, legal and consultancy fees and updating technical processes or systems as top cost drivers, while certification and conformity assessment and ongoing monitoring and reporting were considered lower cost factors. A small number of respondents shared an estimate of their overall compliance costs with the AI Act, ranging between €150 and €50.000 for some.

Finally, on the matter of regulatory overlap, respondents identified interactions between the AI Act and the General Data Protection Regulation (GDPR) as the principal cause of legal uncertainty for their business. Smaller impact was reported for other laws such as the Digital Services Act (DSA) or the EU Copyright Directive.

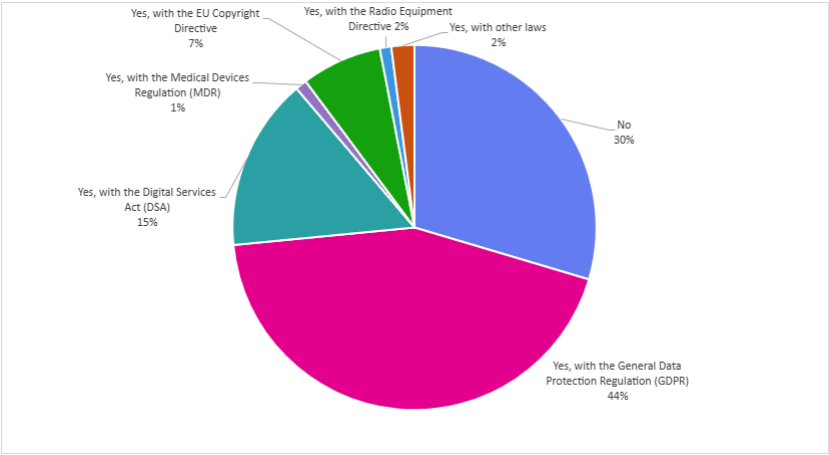

Figure 9: Cases of Uncertainty between the AI Act and Other Laws

Digital Identity Framework

The last section of the consultation focused on the application of the eIDAS Regulation. Respondents whose organisations are subject to regular compliance audits under this Regulation stated that they destinate 74% of the costs for external audits services, and 26% to other services. Besides the external audit fees, respondents listed specialised staff and external

legal or consultancy fees as the typical costs involved, headed by IT systems costs. Other types of costs mentioned were AI subscriptions and server costs.

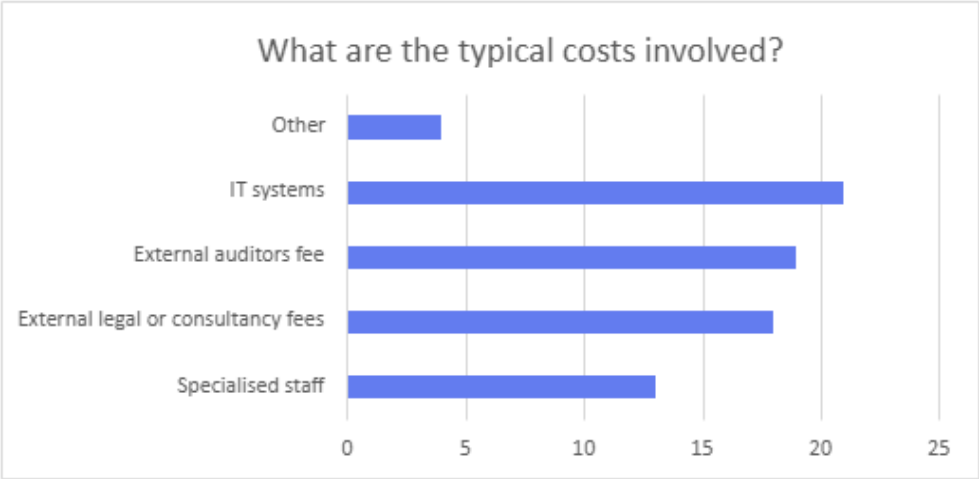

Figure 10: Typical Costs Involved for Auditing Under eIDAS 2

While arguments such as additional cost savings, less workload, and fewer disruptions to operations were brought forward as support for a longer audit cycle, most respondents (52%) stated that they didn't know whether prolonging the audit cycle would bring direct benefits for their organisation. 22% of the respondents considered that prolonging the audit cycle would bring direct benefits for their organisation, with 26% of the respondents indicating that it would not bring any benefits. It should however be noted that auditing under the eIDAS 2 concerns a very limited amount of qualified trust service providers in Europe, leading to potential additional qualification of the responses. In addition, support in the form of simplified guidance was pointed out to make compliance audits more manageable.

Overall, while the eIDAS Regulation ensures secure cross-border digital transactions, compliance audits remain resource-intensive. Clearer and simplified guidance is viewed as key to easing the compliance burden.

IV. Reality checks

The European Commission's services held a series of five reality checks between 15 September and 6 October 2025.

Reality checks are a consultation method whereby Commission services meet with a set of business stakeholders at technical level to discuss implementation of specific rules, and test potential simplification avenues. Where relevant, non-business stakeholders can also be invited to the meetings to share specific knowledge or expertise.

With regards to the Digital Omnibus, the objective was to seek detailed views on cookie banners, the implementation of artificial intelligence rules, the availability of protected public

sector information for reuse, cybersecurity incident reporting, and auditing under the EU's digital identity regulatory framework[198].

These meetings were organised under a 'focus group' format, with Chatham House rules. They were held online in order to facilitate the participation of stakeholders across Europe. A registration page was created on EU Survey, and shared via the Enterprise Europe Network, European Digital Innovation Hubs, and the AI Pact. Respondents had the option to indicate their meeting of interest. Commission services then proceeded to the applicants' selection, with a view of ensuring a balanced representation of profiles. Number of participants was limited to a maximum of 15-20 stakeholders per meeting, in order to facilitate in-depth exchanges and sharing of technical knowledge.

A summary of discussions for each of the five reality checks can be found below.

1. Reality check on the cookie policy framework under Article 5(3) ePrivacy Directive

The reality check took place on 15 September 2025, from 14:00-16:30. It focused on Article 5(3)ePrivacy Directive, particularly on the cookie policy framework. A background note with guiding questions was circulated before the meeting.

Around 20 stakeholders were present, representing businesses and civil society. While business representatives largely agreed on the problem of "cookie fatigue" and the lack of user having a meaningful choice, civil society insisted that the cookie fatigue was caused by the industry using confusing and complicated banners on purpose.

A majority of stakeholders (including one civil society representative) considered the current consent requirement under Art. 5(3) ePrivacy Directive unnecessary. They favoured a risk-based approach, with more exemptions for low-risk activities such as fraud prevention, web analytics, security purposes, contextual advertising, improving the customer journey, and purposes not involving personal data. At the same time, they stressed that personalised advertising cannot be considered low-risk and should remain subject to consent. One business stakeholder proposed reforming Art. 5(3) to require consent only for personalised advertising.

Participants discussed also whether audience measurement should be exempt: one business association argued it serves the public interest (e.g. supporting enforcement of online child protection rules, allocation of press revenues), while a civil society representative underlined that some audience measurement practices are privacy-intrusive. However, the latter agreed that limiting consent banners to invasive practices like targeted advertising could improve user choice, as banners would then act as genuine warnings. It was also noted that most websites (e.g. NGOs or consumer brands) do not need personal data to provide their services, a view supported by others.

Stakeholders also discussed whether to regulate centralised consent management systems, such as allowing cookie settings via browsers. Some businesses raised competition law concerns about the dominance of a few browser providers and the importance of understanding website

[198] Ultimately, this last policy area was not maintained as part of the set of rules addressed under the Digital Omnibus.

use. Others, particularly from civil society, supported this as user-centric and simplifying choice. They argued competition risks could be addressed through instruments like the DMA, supported by open standards. Alternative solutions mentioned included using trusted third parties or certification schemes for cookie banner providers. A civil society representative also highlighted California's regulation of global privacy control as a positive example.

Asked about the greatest challenge in complying with Art. 5(3) ePD and GDPR, many stakeholders from the business side highlighted the expansive interpretation of what constitutes personal data and consent requirements under the ePD by some DPAs and particularly recent EDPB guidelines, and the inconsistent enforcement and interpretation throughout Europe.

Civil society repeatedly insisted, however, that the focus on personal/non-personal data would be misguided as the right to privacy (which the current ePrivacy Directive protects) was a different fundamental right (Art. 7 Charter) from data protection (Art. 8), protecting notably the confidentiality of communications and not only personal data. Accordingly, even without personal data-relevance, terminal equipment should be protected against unauthorized access.

Participants identified scenarios in which the subscriber in the sense of the current ePrivacy Directive could be a legal person, e.g. in IoT scenarios. The user and subscriber could be different persons and obtaining consent can be challenging. On the other hand, one stakeholder representing a law firm questioned whether this necessarily means maintaining the integrity of the terminal equipment, and suggested focussing on the protection of the data obtained from it, potentially restricting particularly invasive tracking or analysis methods instead.

On the topic of privacy-enhancing technologies (PET), there was a large agreement on the importance of incentivizing the use of PETs. While not being perfect, PETs could significantly reduce privacy-related risks of tracking and other technologies. Several stakeholders pointed out that under the current approach, investing in PETs was unattractive, as Art. 5(3) requires consent even if using a PET. Civil society cautioned against an overly reliance on PETs due to "privacy washing"-risk, as the effectiveness of PETs heavily depended on their design. One business stakeholder therefore highlighted the importance of independent audits and certification of PETs.

Regarding compliance costs, one business association stated that maintaining a cookie banner for a middle-sized publisher would bring about costs of 100.000-500.000 EUR/year. The representativeness of this figure was questioned by civil society, which held that the price of maintaining a standard 3rd party cookie banner was negligible and that there are service suppliers on the market that would charge much less for more complex cookie consent situations. One business stakeholder estimated that their company incurs a cost of 2 million EUR/year to comply with the ePD, based on 20 full-time employees working on the topic.

On the use cases for placing and processing of information on terminal equipment that are unrelated to personal data, there were only a few responses. One representative from civil society put forward the problematic examples of blockchain mining and unauthorized exploitation of devices, besides the legitimate uses cases (e.g. setting the font style of a website), which are already allowed under Art. 5(3) today. A business association pointed out that any

communication with a website will require the storage of information on the device (e.g. the user highlighting text in a website).

2. Reality check on AI Act implementation

On September 16, 2025, the AI Office hosted an online roundtable event, bringing together stakeholders to discuss the implementation and implications of the AI Act. This event was part of a broader initiative by the European Commission to conduct a series of "reality checks", focus-group discussions aimed at evaluating the practical application of digital legislation, particularly the previously mentioned AI Act, across various industries. The feedback from these discussions will be crucial in refining the Digital Omnibus Package, ensuring it meets business needs while maintaining regulatory objectives. This report will cover the following aspects of the discussion: approach, organisation, participants, and topics.

Organisational structure:

The event was conducted virtually, from 3 PM to 5:30 PM CET, lasting approximately 2 hours and 30 minutes. The virtual format allowed for the inclusion of companies across the EU and based in third countries, ensuring a diverse range of experiences and perspectives. The session was divided into a welcome and scene-setter segment, followed by an in-depth roundtable discussion.

Participants:

10 participants representing individual companies were selected among applicants, following an open call for registration. The selection ensured a diverse range of sectors and company sizes to provide a comprehensive view of the AI Act's application experience and cost. One participant introduced broader stakeholder views as a business association. To ensure diversity of perspectives, with particular regard to the broader implications of AI, two civil society organisations were invited.

Types of Questions Discussed:

Two main topics were addressed by the participants during the discussions:

1. Experiences preparing compliance: Participants shared their challenges and pressure points in preparing for the 2 August 2026, deadline for implementing high-risk and transparency rules under the AI Act. They also discussed the resources dedicated towards AI Act compliance, including full-time equivalents (FTEs) and estimated costs.

2. Experience with applicable requirements: Participants provided feedback on their experiences with implementing the AI Act's AI literacy requirements and prohibitions. This included discussions on challenges encountered and the resources allocated towards achieving AI literacy within their organizations.

Summary:

The roundtable discussion on the AI Act revealed several key themes and challenges faced by companies and stakeholders. One of the main concerns is the significant compliance cost

associated with high-risk AI systems, which some participants estimated to be at least €100,000 per system. The absence of clear standards and the interplay between the AI Act and other regulations, such as GDPR, pose substantial challenges to stakeholders.

Additionally, there is a strong demand for more guidance on AI literacy and the need for better clarification on what constitutes a "sufficient level of AI literacy". Participants also highlighted the difficulties in implementing post-market monitoring strategies, as well as the complexities involved in different types of AI systems, including GPAI and downstream applications.

Furthermore, the roundtable underscored the importance of simplified compliance procedures and the need for harmonized standards to facilitate practical implementation. The participants emphasized the need for more support tools, standards, and notified bodies to facilitate compliance with the AI Act.

Overall, the reality check event provided a valuable opportunity for stakeholders to share their challenges regarding the AI Act's implementation. The event underscored the importance of ongoing engagement and collaboration between regulators, industry stakeholders, and experts to ensure that the AI Act is effective in promoting trust, innovation, and responsible AI development and deployment.

Quoted costs in the Meeting and Related Explanations

Participant	Figure	Explanation
Business association	100.000€	Estimated compliance cost for every high-risk AI project
Business association	25.000€	Cost of integration of external high-risk AI systems
Business association	150.000€	Compliance cost for AIA incurred so far
Private Enterprise (1)	100.000 – 150.000€	AI literacy trainings for staff (mainly internally developed)
Private Enterprise (1)	20.000-30.000€	Price of governance tools to make record of AI use-cases and follow-up
Private Enterprise (2)	70.000-100.000€	Quotes of external pricing for AI Literacy training

Quoted FTEs in the Meeting and Related Explanations

Participant	Number of FTEs	Explanation
Private Enterprise (1)	10	Staff dedicated towards AIA compliance and coordination
Private Enterprise (3)	20	Estimation of FTEs working on AIA compliance (maybe more, but not full time)
Private Enterprise (4)	2	Half the legal team is responsible of AIA compliance, necessity to expand

3. Reality check on the availability of protected public sector information for reuse

This meeting was held on 16 September 2025, from 10:00-12:30. Around 15 stakeholders were present, representing the public sector (national data coordinators and data holders) and businesses both on individual and association level. A background note with guiding questions was circulated before the meeting.

The meeting explored the potential streamlining of rules on availability of protected public sector information for reuse. The latter are currently regulated in two different, complementary instruments. First, the Open Data Directive sets out rules for the re-use of accessible public sector information but excludes from its scope certain categories of data that are not generally open due to their confidentiality (e.g. statistical confidentiality, protection of IP rights and trade secrets) or personal data protection concerns. Secondly, Chapter II of the Data Governance Act sets our common rules (e.g. non-discrimination, reasonable fees) for situations when public sector bodies decide to make also their non-open data available for reuse under specific conditions.

The discussion highlighted the importance of creating a more coherent, streamlined framework for public sector data reuse. Participants stressed the need for improved awareness among authorities, harmonized legislation, and a supportive European-wide structure that enables better data sharing and reuse without compromising data protection and security concerns. The key conclusions were the following:

i. Challenges in Complying with Requests for Data Reuse and in Making Public Sector Datasets Available

- Data Protection Concerns: Authorities often cite GDPR and other data protection rules as reasons to withhold public sector data, though Article 86 provides leeway that isn't fully utilized. Also, clearing personal data from datasets prior to release is labour-intensive, and authorities sometimes lack the awareness of their roles within data governance.

- Identification of Users: Difficulty in identifying data users hampers data sharing, especially sensitive datasets in today's geopolitical context.
- Publication Costs: Administrations face significant expenses in making data available proactively, acting as a deterrent to publication.
- API Development Costs: The development and maintenance of APIs are financially burdensome, creating barriers to data sharing in some Member States (MS). It hinders proactive data publication.
- Complexity from the Data Governance Act (DGA): The Act's novelty introduces complexity and overlaps, resulting in confusion in some MS.
- Access Restrictions on Specific Data: For instance, treating Vehicle Identification Numbers (VIN) as personal data severely limits useful dataset access.
- Reluctance to Share Data: There exists a cultural hesitation to share data due to fear of favouritism or infringement on competition laws.
- Fragmented Responsibilities and Limited Capacity: Especially in Central/Eastern Europe, limited resources and decentralised data holding complicates data access decisions.
- Lack of Clarity and Awareness: There is often a lack of understanding among public bodies about what constitutes a dataset and what information can be re-used, compounded by inadequate metadata.

ii. Potential for Harmonisation of Reuse Rules

- Improving Awareness and Accessibility: Harmonised rules would enhance understanding for companies regarding data availability and usage processes.
- One-Stop Shop for Data Access: Establishing central access points in each MS could streamline data availability, potentially with EU support.
- Uniformity Across MS: Varied data availability across MS calls for harmonization, possibly through regulation, ensuring consistent access and usability.
- Unified Framework: A unified EU legislative framework for data would bridge the Open Data Directive (ODD) and DGA while respecting specific sectoral laws.

iii. Simplification for Small-Mid Caps

- Benefiting from Harmonised Rules for all: Clear, universal rules will ease navigation for all companies, irrespective of size.
- Focus on Data Quality and Formats: Emphasizing standardization in data quality and formats is deemed more beneficial than differential treatment.
- Avoiding Discrimination Against Large Companies: The focus should remain on accessible data, rather than discriminating based on company size or type.

iv. Obstacles in Accessing or Reusing Public Sector Data

- Variability in National Implementation of Rules: Different national implementations lead to varying data quality, impacting cross-border usability.
- Resource and Procedural Challenges: Public sector bodies often lack the necessary resources, resulting in delays and inconsistent procedures for data access.
- Need for Sustainable Funding: Continued public funding is necessary to sustain the availability and quality of data provisions.

v. Differences in Reuse Rules Across Member States

- Issues with Interoperability: Variations in data granularity and availability lead to challenges in cross-border interoperability.
- Successful Access Models: Adopting successful models, like those under the HVD implementing act for weather data, could inspire improvements in other sectors.

4. Reality check on cybersecurity incident reporting

The meeting was held on 2 October 2025, from 14:00-15:30. A background note with guiding questions was circulated before the meeting. Twelve stakeholders were present, representing small and large enterprises as well as civil society organisations.

The reality check was aimed at collecting quantified feedback on the impact of EU legislation and compliance with cybersecurity incident reporting requirements. However, participants raised the difficulty of producing data requested. They were encouraged to share, where possible, any additional quantified information in writing following the meeting.

Businesses raised concerns about the burden associated with reporting to multiple authorities following different channels and formats while the incident management is ongoing. This often requires relevant teams to step away from their duties to comply with notification obligations which can impact the timeliness and efficiency of the response. Some Member States' delay in transposing the NIS2 directive as well as not entirely repealing Articles 40 and 41 of the European Electronic Communications Code (EECC) was brought to the attention of the Commission.

The **"report once, share many" model** received wide support from stakeholders, while **some** discussed whether submitting incident reports to the Member States with which they are used to cooperating would not be more appropriate.

Main conclusions:

(i) Stakeholders all face compliance obligations from multiple EU rules and regulations:
- Multiple EU legal acts relevant to cybersecurity incidents apply to companies directly and/or are required by contracts with third parties. In this context most commonly were mentioned NIS2, GDPR and DORA.
- Concerns were raised about the continued applicability at the national level of policies that should have been repealed by subsequent European legislation (e.g. EECC Articles 40 and 41), increasing the compliance burden.

(ii) Cybersecurity incident reporting modalities are fragmented:
- Participants voiced difficulties with notifying multiple authorities in different reporting modalities (e.g. uploading documents, using different platforms) to provide different information in various formats.
- It was also mentioned that the reporting burden extends to additional efforts to answer follow-up questions.
- Concerns were also raised about the burden of identifying the adequate authorities in different markets to notify.

- It was highlighted that the vast majority of the incident reports submitted concern the GDPR and increasingly NIS2.

(iii) Cybersecurity incident reporting incurs costs that are identified but difficult to quantify:

- Participants did not provide data on the estimated costs of incident reporting.
- Current incident reporting may require teams in charge of incident management to step away from their duties and take time to fulfil the compliance obligations at the cost of time spent solving the incident and minimizing consequences.
- Additional costs are incurred by the external resources needed to set up and maintain the underlying processes that will enable reporting during the emergency, such as enabling the assessment of the incident's significance, if and under which legislation it should be reported.

(iv) Broad support for the "report once, share many" model with divergence on the most appropriate level of reporting:

- From the perspective of telecom operators, reporting to one authority per market at the national level could help alleviate the burden and help foster a relationship of trust.
- Some participants suggested ENISA could provide a guiding document on different practices across Member States and facilitate the reporting process, including for critical entities.
- If the reporting is made before a single authority which disseminates the report further, several participants stressed there should not be follow-up questions from all the authorities that receive the report.
- There should be harmonized templates, timelines and terminologies to be used by all Member States. Additionally, regarding the data and information requested, more context and justification of the purpose for collecting more detailed information should be considered.
- One suggestion was to adopt a reporting approach that accommodates the urgent character of incident management in the spirit of the 112 European emergency number and combine this with assistance provided by response teams.
- Reporting should also be simplified and streamlined when the obligations extend to suppliers.
- Participants generally agreed ENISA should have a role but did not agree on what the role should be (e.g. provide guidance or oversight).

5. Reality check on trust services and the European Digital Identity Wallets

This meeting was held on 6 October 2025, from 15:30-17:30. It focused on the auditing process for qualified trust service providers (QTSPs), as well as on different use cases for the European Digital Identity Wallets (EUDIW) across various sectors. Half a dozen stakeholders, most of them European QTSPs, participated.

On the auditing process for QTSPs, the participating concerned entities first highlighted the need to define the concept of a "high level of confidence", which is not currently specified in the Implementing Act or the main regulation. The absence of a clear definition could lead to market fragmentation, with each TSP implementing services differently. TSPs requested clarification on the level of confidence and how it differs from the level of assurance (LoA). As possible alternatives, stakeholders suggested either postponing the timeline or focusing instead on the substantial LoA.

Participating QTSPs also underlined that the high number of Implementing Acts, with different application deadlines, it make it very difficult for them to know when the regulation needs to be applied and when they need to "stop doing what". One stakeholder suggested the creation of a summary in form of a White Paper that specifies requirements.

Participants noted that an audit requires around 100 days to be completed, requiring a lot of resources. In some cases, it is also more complex as auditors usually request additional information which makes the process even longer. Additionally, some stakeholders expressed the need to have a standard to be made mandatory to have clear guidelines for auditors with regards to ensuring compliance with overlapping regulations to eIDAS 2.0 (DORA, NIS2, Cyber Resilience Act…).

Finally, some stakeholders suggested that auditing could be further automatized, to accelerate and simplify processes.

On the European Digital Identity Wallets, more generally, participants stressed the need for a unified business model. While the framework is useful to European society, one QTSP from Italy for instance expressed skepticism about the effective uptake as the bar has been set too high. This is because there is no EUDIW today, and the other option is to have EDIWs subsidized by Member States on the citizens – which will create inconsistencies across countries. Reaching consensus will all ecosystem stakeholders was perceived to be difficult.

Furthermore, achieving a high level of assurance (LoA) was deemed complex. Conformity assessment bodies (CABs) are currently lacking, affecting the user experience. The overall certification scheme is not yet in place despite an ambitious timeline, which will create problems to meet the deadline.

Some participants suggested to adopt a risk-based approach for the level of assurance – not necessarily to change the high LoA itself, but rather to allow the substantial level to be applied within a risk-based framework. A unified approach across Member States was also called for, and support from ENISA could help achieve this alignment.

Some participants suggested the need to set up a monitorization scheme around the data and credential exchange, especially to find a way to maintain privacy.

Stakeholders expressed that there is at times a lack of understanding with regards to article 5f of eIDAS 2.0, and whether it is about the provision of the wallets or the usage itself. The Commission acknowledged that public services have to accept EUDIW when providing their services, with regards to authentication and identification according to the regulation. Stakeholders also inquired if the wallets should be accepted in the payments systems. They

emphasized that the article is not clear, especially for banks, leaving the door open to interpretation.

Participants also inquired about the potential consequences of non-compliance. The Commission outlined the infringement procedure process. However, in most cases, such situations do not lead to a formal infringement procedure; rather, the issue is flagged to the concerned Member State, which then takes the necessary corrective measures.

Finally, on the topic of free digital signatures for non-professional use, participants underlined the need to clearly define what non-professional use/professional use means, to ensure alignment and a common understanding across Member States.

V. Implementation dialogues

Implementation dialogues are a new consultation tool for the European Commission at the political level, launched in the spring of 2025. Their objective is to seek feedback from stakeholders in order to facilitate the implementation of EU policies.

Each Commissioner is to hold two meetings a year. Executive Vice-President Henna Virkkunen held a first dialogue on data policy on 1 July 2025, followed by a second on 15 September 2025. Commissioner McGrath also hosted an implementation dialogue on the application of the GDPR on 16 July 2025. A summary of these meetings can be found below.

Data Policy

The Implementation Dialogue took place on 1 July 2025. It was chaired and moderated by EVP Henna Virkkunen. The goal was to present and discuss the state of play and level of implementation of the current 'data acquis'. It was specifically aimed at identifying solutions for streamlining and simplifying certain parts of the 'data acquis' in the context of the Digital Omnibus planned for November 2025. Relevant feedback could also inform the European Data Union strategy planned for October 2025.

The list of participating stakeholders is in the Annex.

i. Main findings

The roundtable discussion was structured according to four themes:

-
- Theme I - Public sector data re-use under the current Open Data Directive and chapter II Data **Governance Act**
- Theme II - Data intermediation services as a facilitator of voluntary B2B data sharing (DGA Chapter III)
- Theme III: Rights to access and use data from connected products (Data Act Chapter II/III)
- Theme IV - Feedback on other data rules

Theme I - Public sector data re-use under the current Open Data Directive and chapter II Data Governance Act

The guiding questions asked to participants were:

- What potential lies in the re-use of data held by the public sector? In which areas should more data be made available? What are the bottlenecks?
- How are public sector bodies supporting industry with access to relevant data, in particular sensitive data (e.g. personal data, data representing commercial secrets)?

Public sector stakeholders reported ongoing efforts to publish high-quality data under open licences (Open Data Directive) and to enable access to sensitive data under controlled conditions (DGA Chapter II), with statistical offices now helping other public bodies take on this role. Cadastral offices flagged the difficulty of funding cross-country data harmonisation from national budgets and called for EU support.

Two AI start-ups reported difficulties accessing legal data (laws, regulations, case law) and language resources in some Member States. They suggested turning the Open Data Directive into a Regulation to reduce national divergences and expanding the list of high-value datasets to include legal, health, and financial data. They also supported the development of a European legal data space. GDPR and trade secrets are often used as pretexts to deny access, they argued. For protected data, secure processing environments and regulatory sandboxes could offer solutions.

EU statistical offices also aim to **reduce burden** on companies having to fill in **statistical surveys** by using mechanisms for on-demand access to privately-held data. In this context, the Financial Data Access Regulation was mentioned as a lost opportunity to reduce the number of surveys. The Data Act is a stepping stone in this direction.

Theme II - Data intermediation services as a facilitator of voluntary B2B data sharing (DGA Chapter III)

The guiding questions asked to participants were:

- What role do you see for data intermediation services in voluntary data sharing, in particular in common European data spaces?
- What legislative obligations are necessary for companies to trust them? What could be achieved through voluntary labelling?

Representatives of the emerging ecosystem of **data intermediation services** and technologies highlighted the importance of a European framework for B2B data sharing for the Union's competitiveness.

A service provider described itself as the "PayPal" of the data economy, enabling permissioning flows and empowering end-users while improving efficiency. For instance, a French bank automated 75% of consumer loan processes, reducing credit checks from 5 days to 6 minutes. Such data intermediation services, aligned with the Data Act and Chapter III of the DGA (if based on neutral business models), can support compliant and efficient data sharing. The provider opposed making the regime voluntary.

The French data intermediation association supports the mandatory regime but recommends: (1) expanding the categories of allowed value-added services (e.g. data preparation that doesn't

retain data or extract undue value), and (2) enhancing the label's attractiveness by granting privileges, such as acting on behalf of users in dealings with public authorities. Intermediaries can also help assess data value for inclusion in company balance sheets—a practice already regulated in China.

Theme III: Rights to access and use data from connected products (Data Act Chapter II/III)

The following guiding questions were put to the stakeholders:

- Do you consider it important to ensure that users have a right to access and use data from connected products they own/operate?
- How can perceived risks to data holders' trade secrets, such as misappropriation or loss of competitive advantage, be addressed?

Company representatives from various sectors - aviation, energy, automotive, agriculture, insurance, and SMEs - view the Data Act as a major milestone. It increases transparency about available data, fosters innovation and efficiency, and enhances competition by allowing users to share data with providers of their choice, helping avoid vendor lock-ins. It also empowers customers and smaller market players, supporting rights such as repair and connectivity.

The Act is expected to enable faster, more efficient maintenance - for instance, allowing a farmer to repair machinery during harvest without waiting for a technician. Cross-brand interoperability was highlighted as essential, especially when using equipment from multiple vendors. However, some types of data - those derived through proprietary algorithms - may fall outside the Act's scope.

Several participants warned that manufacturers might overuse the "trade secrets" clause (the so-called 'handbrake') to restrict data access. They called for enforcement by authorities with sector expertise, and welcomed model contract terms and clearer guidance on the trade secrets provision.

Companies obliged to adapt their data systems under the Data Act acknowledged compliance costs but saw the requirements as manageable, especially when building on existing data-sharing infrastructure. They rejected calls to replace the Act with sector-specific rules, favouring a unified framework to avoid regulatory fragmentation. The consistent rules across sectors for IoT products are seen as a key strength of the legislation.

Consumer advocates stressed that the Act's success depends on data holders acting in good faith. Without cooperation, IoT-based services will not develop. Protection under GDPR and the ePrivacy Directive must be upheld. They also warned against excessive tracking and default data-sharing features in connected devices, which consumers largely oppose.

Theme IV - Feedback on other data rules

The guiding questions were:

- Is the EU 'data acquis' innovation-friendly enough, in particular in view of developing AI in Europe?

- What is the interaction with sector-specific legislation?
- What are the specific hurdles for small and medium enterprises?
- What simplification would you recommend strengthening competitiveness?

This last session helped raise awareness on a wide range of issues.

"EU regulation simplifies"

A consumer organisation pointed to a study undertaken by the European Investment Bank, according to which, the **highest hurdle is not regulation** and certainly not EU regulation. EU regulation harmonising a certain area of law is rather simplifying as it replaces potentially diverging national legislations. The highest hurdle is the lack of skilled labour, followed by energy costs. Regulation only would come fourth. In other words, EU regulation simplifies.

Complexity due to overlap, "without prejudice" clauses and cascading effect in contractual clauses

While participants acknowledged the legitimacy of various regulations, they highlighted the complexity caused by overlapping regimes and "without prejudice" clauses, which create regulatory silos. This is especially problematic for service providers operating across sectors, where obligations placed on larger players often cascade down to smaller ones via contracts, complicating business operations. To address this, one participant called for a risk-based regulatory approach and greater use of exploratory tools like sandboxes. The absence of cross-regulatory guidance further exacerbates complexity.

An insurance sector representative noted overlaps between the AI Act and existing insurance regulations. Although the Commission had initially suggested insurers wouldn't fall under the AI Act's high-risk category, these obligations now appear to apply regardless. Another participant observed that in some countries, AI enforcement bodies assume non-compliance by default—an approach that stifles innovation. SMEs, in particular, need fast-track support and a more coordinated, constructive enforcement environment.

Areas for simplification

One area in which access to more privately-held data could be provided would be health and cybersecurity. This could help insurance companies to offer better tailored insurance policies and premiums. Others considered the European Health Data Space Regulation to be good in principle, but requiring strong enforcement.

Some other stakeholders suggested that certain legislation could further be simplified, including sectorial legislation such as the financial data access regulation (FIDA), with suggestions from the representative of the insurance industry as to its scope and potential effects.

Diverging GDPR enforcement and low degree of harmonisation of interpretations by the European Data Protection Board were seen as a hindrance to develop pan-European AI solutions. Also, the AI Act mandates keeping training data whereas that would normally not be possible under GDPR, thus calling for better alignment of the two acts.

Simplification should make compliance easier. Regulation also should aim to achieve interoperability and thus trigger standardisation. Innovation and regulatory sandboxes were also

seen as very useful, and could be tailored to the needs of SMEs and SMCs. To further support such companies, rules on public procurement should be revised to include more companies in EU R&I funding actions. The focus of such actions should be on applied research that leads to actual products or services.

Synthetic data was mentioned as a good compliance tool whenever data is too sensitive to be shared. However, a common definition and standards are still lacking. One participant mentioned a positive experience with a certification scheme under the GDPR.

The coordinator of the European tourism data space highlighted the lack of sufficient granularity in public sector data, which hinders the development of viable business cases—an issue also seen in private sector data. Companies active in the data economy struggle with compliance challenges, particularly around consent management and confidentiality.

Support is especially needed for SMEs and micro-enterprises, such as tourist guides, through technical tools for data use and sharing. Interoperability of data space architectures and common standards is essential.

Participants also raised concerns about the dominance of non-European big tech firms. One called for a sovereign EU cloud solution for strategic data and suggested mandating EU data localisation in public procurement to safeguard data sovereignty.

One stakeholder reported that Member States have different regimes for accessing language data with challenges often relating to copyright and data protection. The organisation perceived the legal regime in the United States under the so-called "fair use" doctrine as a more permissive, which they believe offers a competitive advantage to US-based organisations. In the EU, one would have to go through many and complex licensing negotiations. **Collective licensing agreements** with media companies and broadcasters could provide a solution.

The Data Union strategy would be an excellent opportunity to provide industry stakeholders with unified vision on how to use data as an asset in the economy.

ii. Links with ongoing or future policy initiatives, stress tests and reality checks

This Implementation Dialogue is linked to the on-going evaluation and potential revision of the Open Data Directive, the Data Governance Act, as well as to support the implementation of the Data Act. It links with the ongoing public consultation for the Data Union Strategy. It is also relevant for the monitoring of the roll-out of common European data spaces. As there are many legal regim regulating horizontal aspects of (certain) data (data protection, copyright, trade secrets), but also sectoral regimes, the dialogue showed that there are many interlinkages between legal regimes. This may be taken up during the GDPR dialogue.

The input will be used to inform the Digital Omnibus proposal, planned for Q4 of 2025. It will further be assessed in the preparation of the Data Union Strategy communication planned for Q3. Going beyond these measures, input may also influence the questions asked in the course of the Digital Fitness Check to be launched as a further step towards stress testing the digital acquis.

iii. Next steps and possible future initiatives

The findings serve as insights for targeted amendments to the Data Governance Act to be undertaken as part of the Digital Simplification Omnibus package, other measures to be announced in the Data Union strategy as well as considerations for more substantial Digital Fitness Check and potentially, more substantial amendments to the 'data acquis'.

Participants

Name of the organisation or company	Name of the participant
Aindo	Daniele Panfilo, CEO
AnySolutions	Dolores Ordoñez Martinez, Director General
Association pour l'intermédiation de données	Xavier Drilhon, President
BEUC	Maryant Fernández Pérez, Head of Digital Policy
BMW	Dr. Fathi El-Dwaik, Vice President Electrics/Electronics Systems
Central Union of Agricultural Producers and Forest Owners of Finland (MTK)	Kimmo Tammi, Legal Advisor
DataSpace Europe Oy	Jaana Sinipuro, CEO
DAWEX	Fabrice Tocco, co-CEO
Doctrine	Hugo Ruggieri, Directeur juridique et affaires publiques et DPO
Elastic NV	Zoltan Precsenyi
EnBW	René Deist, Chief Digital and Information Officer
Eurogeographics	Sallie Payne Snell, Secretary General and Executive Director
European Digital SME Alliance	Sebastiano Toffaletti, Secretary-General
Federation of German companies in the Arts and Crafts sector (ZDH)	Dr.Ing. Fabian Schnabel, Advisor
Innopay	Mariane ter Veen, Director

Insurance Europe	William Vidonja, Head of Conduct of Business
Lufthansa	Joern Messner, Vice President Innovation & Tech Factory
Mistral AI	Cyriaque Dubois, Associate Global Public Affairs & Communications
Mobivia	Stéphane Derville, Technical and Innovation Director
QUIBIM	Ángel Alberich-Bayarri, CEO and co-founder
Statistics Netherlands (CBS)	Angelique Berg, Director-General
Tilde	Andrejs Vasiļjevs, CIO
Volvo Trucks	Niklas Gustafsson, VP of Public Policy and Regulatory Affairs

Implementation Dialogue on Cybersecurity Policy

Executive Vice-President Henna Virkkunen held an Implementation Dialogue on Cybersecurity Policy in Brussels on 15 September 2025. The aim was to share insights and experience on implementation and simplification in the area of cybersecurity, while maintaining the required high level of cybersecurity. The Implementation Dialogue was organised in particular in the context of the preparations of the digital package on simplification as well as the revision of the Cybersecurity Act planned for later this year.

1. Main Findings (from the stakeholders' perspectives)

Potential for Implementation and Simplification:

- **Simplification of legislation**: Many stakeholders stressed the need to simplify the EU legal framework governing cybersecurity. The current regulatory landscape, shaped by a number of horizontal and sectorial rules, such as NIS2, CRA, DORA, CER or GDPR is seen as complex, at times with overlapping requirements, and divergences in national implementation, creating compliance challenges for businesses. Stakeholders are calling for a single, cohesive framework that would minimise administrative burden and provide clarity. This suggestion includes efforts to align and harmonise legislation across EU Member States, reducing discrepancies and facilitating easier compliance, especially for small and medium-sized enterprises which may lack the resources to navigate complex legal environments. Large stakeholders highlighted how their vast network of suppliers (10.000 suppliers for some), among which many SMEs, is confronted with significant compliance challenges due to the EU's fragmented regulatory environment.

- **Rationalised reporting mechanisms**: Many stakeholders suggested moving towards a "report once – share many" approach, for example via a single reporting platform, to simplify the processes and reduce duplication. NIS2, GDPR and DORA were most referred to in this context. Such a system could use standardised templates or digital platforms to streamline compliance with multiple regulatory requirements. This way, organisations could focus on risk management, allocating their attention and resources more effectively, improving their ability to respond to incidents without being caught up by redundant compliance requirements. Aligned timelines and reporting requirements across the EU, would make it easier for companies operating in multiple countries to adhere to one set of rules rather than adapting to multiple, potentially conflicting requirements.
- **Enhancing ENISA's role**: The European Union Agency for Cybersecurity (ENISA) was identified as a potential central actor in the effort to simplify cybersecurity frameworks and support implementation. Several stakeholders suggested ENISA could serve as a central hub for situational awareness and report consolidation and information sharing. Such responsibilities for ENISA would reduce fragmentation in reporting channels and provide companies with a single point of contact for cybersecurity issues, thereby streamlining processes and allowing quicker response time in the event of incidents.
- **Sharing of compliance information**: Many stakeholders suggested that a shared, EU-wide, unified "evidence package" would help streamline regulatory compliance processes. Such a package would allow companies to compile compliance documentation once and share it across national competent authorities and jurisdictions, saving time and resources. This would allow organisations to "comply once and share across Europe", thereby enhancing efficiency.
- **Harmonisation of frameworks:** overall, stakeholders called for a streamlined cybersecurity framework across the EU, harmonising existing frameworks to reduce duplication and enhance mutual recognition between Member States. Stakeholders also suggested to harmonise compliance through non-regulatory tools and advocated for an "online cybersecurity library" with relevant resources that could be administered by ENISA. This library could compile relevant information regarding the implementation, guidelines on implementation especially for SMEs and a toolbox for companies.
- **Simplifying certification processes:** Several stakeholders highlighted the challenge of coping with differing certification processes across Member States, and the resulting cost. They advocated for the introduction of mutual recognition rules, emphasising how harmonising these processes could exempt companies from going through multiple, often very costly, certifications in different jurisdictions. This approach would significantly reduce compliance costs and allow businesses to focus their resources on enhancing cyber defence rather than addressing bureaucratic processes.
- **Internal market sovereignty:** The internal market remains fragmented due to inconsistent implementation of EU rules at national level. This inconsistency shifts the focus to compliance instead of building strong capabilities and crisis management. Strengthening the cybersecurity sector requires boosting the demand for solutions developed within the

European Union. Stakeholders highlighted that EU needs to stop relying on high-risk vendors, that businesses need to secure their supply chains and focus on developing EU-based cyber solutions. Additionally, the EU-wide market rules should promote innovation, research and investment. ENISA can contribute by creating standards that enhance market sovereignty and address limitations posed by existing frameworks. Coordinating the efforts of various authorities is crucial for enabling companies to grow and innovate. This coordination will ensure that regulations support, rather than restrict, market expansion. By prioritising technical expertise over simple compliance with rules, a more dynamic and adaptable market can be developed. This approach will position the market to lead advancements in cybersecurity.

Obstacles Relating to Existing Rules and Their Implementation:

- **Regulatory complexity and overlap**: Overall, stakeholders repeated concerns about the complexity and overlap in the existing EU cybersecurity regulations. This network of legislation, composed of acts like NIS2, the CRA, the Cyber Solidary Act, sectoral cybersecurity rules like DORA for the financial sector, and their interplay with the GDPR, for instance in case of personal data breaches, has created a burdensome compliance environment. SMEs, in particular, are struggling to interpret which rules apply to them and to ensure compliance without exhausting their resources. Stakeholders noted the difficulty in determining compliance scope given national discrepancies, which can lead to different interpretations and applications of the rules. This fragmentation increases administrative overhead and distracts from a unified EU market approach.
- **Lack of clarity and consistency**: The current regulatory framework lacks clarity, which produces inconsistency in implementation, in particular the scope of NIS2 Directive. This discrepancy is further exacerbated by the difference in how rules are enacted across the EU's Member States. Stakeholders have highlighted that inconsistent reporting timelines, authorities and certification requirements across Member States further complicate compliance efforts.
- **High reporting burden**: Reporting obligations under existing regulations are extensive and often duplicative. The requirement for firms to file multiple, often similar reports across different regulatory bodies for the same event is not only time-consuming but is seen as distracting resources away from incident management and resolution efforts. This misallocation of resources becomes especially pronounced during crisis situations, further weakening the organisation's response capabilities.

Best Practices:

- **Single reporting entry point**: Many stakeholders pointed out the benefits of a centralised reporting system or entity where a single submission could fulfil the obligations of multiple requirements. This approach could reduce procedural redundancy and alleviate the burden currently felt by entities navigating multi-layered bureaucratic requirements.
- **Sharing information**: Stakeholders reported successful information-sharing practices based on open-source standards (such as STIX and TAXII) and emphasised the value of

collaborative threat intelligence networks for situational awareness and collective cybersecurity defences.

- **Unified Control Sets**: The establishment of common control sets fulfilling the requirements of multiple laws is a viable method of streamlining compliance. This strategy could be expanded and standardised across the EU to promote a more coherent regulatory environment and reduce redundant compliance efforts.
- **Automation of compliance tools**: Some stakeholders highlighted that efficiency gains can be achieved through automating compliance tasks. Automation can alleviate the burden of manual compliance processes and improve the speed and accuracy of reporting.

2. Next Steps and Possible Future Initiatives (from the stakeholders' perspectives)

- **Support measures**: The European Commission could take action to provide better guidance and support for businesses, helping them understand and meet current regulatory requirements. This could include comprehensive guidelines, templates, and training programmes focusing on the specifics of EU regulation.
- **Investing in digital compliance tools**: Encouraging the development and implementation of digital solutions to automate compliance processes could significantly reduce administrative burdens.
- **Expanding ENISA's role**: Several stakeholders recommended expanding the role of ENISA as a central point for cybersecurity information exchange, reporting on threat landscape, and standard-setting. This expansion could foster a more streamlined approach to incident management and regulatory compliance across the EU.
- **Education and awareness-raising initiatives**: Enhancing the cybersecurity education and awareness of stakeholders, particularly SMEs, was recommended by many. Facilitating access to information about regulatory requirements and compliance processes could empower businesses to more effectively manage their cybersecurity obligations.

3. Links with Ongoing or Future Policy Initiatives (from the DGs perspective)

- **Alignment with the ongoing initiatives (Digital Omnibus and Cybersecurity Act revision)**: The simplification ideas presented in the Implementation Dialogue would feed into the ongoing initiatives and largely support the Commission's vision and ambition.
- **Call for evidence on the Digital omnibus**: the call for evidence on the digital omnibus run from 16 September to 14 October and gather over 500 submissions by stakeholders. The call for evidence and the public consultation are important tools used by the European Commission to ensure that policymaking is transparent, inclusive, and evidence-based. Through these instruments, the Commission gathers input from a wide range of stakeholders — including citizens, businesses, NGOs, and public authorities — at an early stage of the policy cycle. The call for evidence helps identify key problems, objectives, and potential policy options, while the public consultation allows for deeper feedback on specific proposals. Together, they help the Commission assess the likely impacts of initiatives,

improve the quality and legitimacy of EU legislation, and ensure that new measures reflect real needs and practical experiences across the Union.

Implementation Dialogue on the application of the general data protection regulation

The Implementation Dialogue on the Application of the General Data Protection Regulation was held on 16 July 2025 in Brussels.

The meeting was attended by representatives of selected stakeholders, representing business, civil society, and academia, from different sectors and fields of life. The objective of the Implementation Dialogue was to collect stakeholders' views and ideas on the possible need and ways to simplify and improve the application of the GDPR, keeping in mind that these should not result in lowering the high level of data protection in the EU. The feedback from stakeholders can be summarised as follows:

• Overall, stakeholders consider that the GDPR is a balanced legal framework which has met its objectives.

• While stakeholders cautioned against a general reopening of the GDPR, some industry representatives suggested targeted measures including possible amendments to the rules to enhance clarity of certain concepts or simplifying obligations for data controllers, insisting on the respect of the GDPR risk-based principle, notably as regards AI and other new technologies.

• Businesses also underlined that they have invested in compliance and a general reopening could create uncertainty, including in the context of international data transfers.

• Civil society organisations strongly opposed any amendment of the GDPR, highlighting that the GDPR is an expression of the fundamental right to data protection.

• Stakeholders share the view that there is a need to ensure consistent and harmonised enforcement and application.

• All stakeholders underlined the need for more practical guidance and increased stakeholder engagement from the national data protection authorities and the European Data Protection Board.

• They also called for tailor-made support, such as templates and checklists, especially for SMEs. Several stakeholders referred to the codes of conduct as a useful compliance tool, but their development and adoption procedure were considered cumbersome.

• The importance of clear articulation of different pieces of EU legislation was raised by most stakeholders, who mainly referred to the interplay between the GDPR and the AI Act, and many considered that this could be achieved through guidance and enhanced cooperation of different regulatory authorities. Commissioner McGrath reaffirmed the Commission's commitment to high standards of data protection and to a balanced approach that both fosters innovation and protects fundamental rights.

List of participating entities: Bundesverband Digitale Wirtschaft (BVDW), Bureau Européen des Unions de Consommateurs (BEUC), Business Europe, Cloud Infrastructure Services

Providers in Europe (CISPE), Confederation of European Data Protection Organisations (CEDPO), Connect Europe/GSMA, Digital Europe, Ecommerce Europe, European AI Forum (EAIF), European Automobile Manufacturers' Association (ACEA), European Banking Federation (EBF), European Centre for Digital Rights, NoyB, European Digital Rights (EDRi), European Federation of Pharmaceutical Industries and Associations (EFPIA), European School Heads Association (ESHA), Federation of European Direct and Interactive Marketing (FEDMA), France Digitale, IAB Europe, Insurance Europe, Irish Council for Civil Liberties (ICCL), Privacy International, SMEunited, Stiftung Digitale Chancen (SDC), Transatlantic Consumer Dialogue (TACD), Union Fédérale des Consommateurs - Que Choisir (UFC - Que Choisir), Verbraucherzentrale Bundesverband (vzbv), Prof. Gloria González Fuster, Prof. Christopher Kuner.

VI. List of meetings

In addition to its engagement in the different settings laid out above (either at political or technical level), the Commission services held bilateral meetings with the following stakeholders in the preparation of its proposal for the Digital Omnibus:

1. Confederation of Swedish Enterprises
2. Digital Europe
3. European DIGITAL SME Alliance
4. Google
5. Swedish National Board of Trade
6. BritCham
7. European Tech Alliance
8. AmCham
9. German Insurance Association
10. Automobile Manufacturers Association
11. European Startups Network
12. Berthelsmann Foundation
13. APPLIA
14. Move EU
15. BEUC
16. IBM
17. IKEA
18. Amadeus
19. Delivery Platforms Europe
20. Association Financial Markets Europe
21. EDRI
22. Access Now
23. Centre for Democracy & Technology
24. MEDEF
25. Federation of Finnish Enterprises

26. Noyb
27. Law & Innovation
28. MagazineMedia Europe
29. European Publishers Council
30. Axel Springer SE
31. ID Side
32. Deutscher Anwaltsverein
33. Danish Chamber of Commerce
34. Cloudflare
35. NetApp
36. European Cybersecurity Organisation (ECSO)
37. World Economic Forum (WEF)
38. ITI – The Information Technology Industry Council
39. Uber
40. Orgalim
41. VDMA
42. French Business Confederation
43. Black Forest Labs
44. Insurance Europe
45. Aerospace, Security & Defence Industries Association of Europe

Annex II – Summary of cost savings estimates

Proposed simplification measures	Estimated administrative cost savings			
	Businesses		*Public authorities*	
	One-off	**Recurring**	**One-off**	**Recurring**
Reduction of administrative costs by avoiding information gathering by public authorities in the Free Flow of Non-Personal Data Regulation	N/A		N/A	EUR 846,612
Deletion of requirements under the Data Governance Act for data intermediation service providers to offer services through a separate legal entity	EUR 318,750	EUR 6 million	N/A	
Narrowing the scope of Chapter V of the Data Act from "exceptional need" to "public emergencies"	EUR 27,625 million	EUR 19,7 million	N/A	
Specific lighter regime under the Data Act for data processing services which are custom-made	EUR 1,016 billion	N/A	N/A	
Extension to Small Mid-Caps of the possibility to benefit from cheaper access to data from protected public databases	N/A	EUR 4,75 – 19 million	N/A	
Amendments to the cookie banners regime	N/A	EUR 820 million	N/A	EUR 320 million
Creation of a Single-Entry Point for cybersecurity incident reporting	N/A	EUR 41,536 million	EUR 9 million	EUR 3,22 – 7 million

Extension of certain regulatory privileges of SMEs to SMCs under the AI Act	N/A	EUR 2,5 million	N/A	
Alignment of implementation timeline for high-risk rules under the AI Act	N/A	EUR 68-204 million	N/A	
Transformation of obligation on AI literacy under the AI Act	N/A	EUR 222,75 million	N/A	
Remove registration in EU database for AI systems exempted according to Art. 6(3) of the AI Act	N/A	EUR 148,500	N/A	
Reallocate supervision of AI systems based on GPAI models to AI Office	N/A		N/A	EUR 3,7 million
TOTAL	*Per year* **Up to EUR 1,335,634,500** *By 2029* **Up to EUR 5,050,847,000**		*By 2029* **Up to EUR 1,003,639,836**	

** Cost savings that could not be directly assessed in quantitative terms by the Commission due to insufficiently specific available data are not included in this table. More targeted identified cost savings that may overlap within the broader business category (eg. for SMEs) are also not reflected in the aggregate, to avoid duplication. For a more detailed overview of impacts on SMEs, see Annex IV. These estimates assume the measures proposed under the Digital Omnibus come into application early 2027, on the basis of data available to the Commission in the preparation stage of the proposal.

Annex III - Competitiveness Check

1. Overview of impacts on competitiveness

Dimensions of Competitiveness	Impact of the initiative (++ / + / 0 / - / -- / n.a.)	References to sub-sections of the main report or annexes
Cost and price competitiveness	++	Subsections 1.1, 1.3., 2.3, and 3.3 of the main report.
International competitiveness	+	Subsection 1.1.2.4. of the main report.
Capacity to innovate	++	Subsections 1.1., 1.2., and 3.3. of the main report.
SME competitiveness	+	Subsections 1.1.2.6., 1.1.2.8., and 3.3. of the main report.

2. Synthetic Assessment

Overall, the proposed measures are expected to yield **significant benefits to the competitiveness** of the EU industry.

On **data policy,** the Digital Omnibus seeks to pull into one coherent law (the Data Act) the rules supporting a competitive single market for data sharing. The proposed changes to the GPDR, namely the clarifications around the processing of personal data for the development and operation of AI models and systems under a legitimate interest, are an additional means for increased competitiveness of EU businesses. The proposed amendments would also clarify the scope of personal data and when information falls outside the scope of GDPR, enhancing legal certainty for all companies. Proposed modifications to the ePrivacy directive will directly cut the operational and maintenance costs of cookie banners for businesses, representing another strong competitiveness gain. **The Single-Entry Point**, by streamlining and thus reducing the cost of cybersecurity incident reporting, also supports businesses compliance processes. Last, the **targeted amendments to the Artificial Intelligence Act** both increase legal certainty and reduce administrative burdens on companies, such as obligations relating to AI literacy. All in all, simplifying the above rules and further harmonising their interpretations and application are expected to have a definite positive impact on European competitiveness, particularly benefiting SMEs and SMCs.

- In terms of **cost and price competitiveness** the amendments are expected to have a positive impact. By reducing administrative burdens throughout the proposal (see Annex II for the full overview), this will translate into businesses able to operate at lower costs – thus improving their own cost and price competitiveness. The deletion of the requirement of setting up a separate legal person for data intermediation service providers, for instance, is estimated to lead to EUR 318,750 one-off savings for such businesses, with an additional

EUR 6 million on an annual basis. The narrowing of the scope of Chapter V of the Data Act will also reduce one-off infrastructure costs (EUR 27,625 million), as well as recurrent annual expenses (EUR 19,7 million). The creation of a specific lighter regime for data processing services would entail one-off savings in the magnitude of EUR 1 billion, by avoiding the heavy cost of contract renegotiation. The changes on cookie banners are also expected to significantly enhance cost and price effectiveness by reducing administrative and compliance burdens for businesses, particularly SMEs. It is estimated that approximately 50% of European websites would not rely on consent and thereby use cookie banners anymore. Companies would thereby save substantial resources on legal compliance and banner management, with overall cost savings estimated at EUR 820 million per year. On cybersecurity, the introduction of the Single-Entry Point is expected to reduce by EUR 41.5 million per year the cost of incident reporting for businesses across Europe. Last, on artificial intelligence several amendments are expected to reduce up to EUR 429,5 million in administrative burden per year – by both increasing legal certainty (for instance via the changes to the application timelines for rules on high-risk AI), and directly streamlining certain administrative obligations (AI literacy, registration in EU database for high-risk AI systems, etc.).

- When it comes to the impact on **international competitiveness** and trade, the Digital Omnibus also includes provisions in that direction. For instance, the proposed change on trade secrets is expected to enhance EU businesses' global competitiveness, reducing financial losses and improving operational stability. The amendment strengthens the EU's international competitiveness by enhancing the protection of trade secrets against unlawful disclosure to entities under potentially weaker third-country jurisdictions. This reinforces the EU's position as a trusted and secure data ecosystem, making it more attractive for investment, cross-border collaboration, and digital innovation within its borders. It also levels the global playing field by mitigating the competitive disadvantage EU firms face when foreign competitors benefit from laxer legal regimes.

- The EU's **capacity to innovate** is significantly strengthened by the proposed measures. Specifically, the additional emphasis on regulatory sandboxes (under the AI Act) helps create a safe and collaborative environment for businesses to experiment with new technologies. This reduces uncertainty and the risk of costly non-compliance, while also encouraging greater investment in research and development. Additionally, the proposed amendments to the current conditions for re-use under the Open Data Directive and the Data Governance Act will facilitate compliance with those rules as they will be easier to understand and implement. High-value datasets will be more easily accessible for re-use, supporting innovation and representing a key driver for Europe's competitiveness. Last, the changes to the GDPR regarding the processing of personal data for the development and operation of AI models and systems under a legitimate interest will significantly bolster AI innovation for all entrepreneurs.

- In terms of **SME competitiveness**, aforementioned proposals contain multiple aspects that could directly or indirectly generate a positive impact on SMEs as well as SMCs (small mid-caps), e.g. a lighter regime for data processing services provided by SMEs and SMCs, additional exemptions under the consolidated Data Act regarding re-use of public sector data, and new provisions under the Artificial Intelligence Act. All these initiatives would enhance the competitive positioning of SMEs. More details on the latter can be found in Annex IV.

3. Competitive position of the most affected sectors

Despite its ICT grounding, the Digital Omnibus' impact is largely cross-sectoral. Many of its core provisions affect companies of all sectors, using digital tools or means for their own business or compliance operations (e.g. cookies, requirements for cybersecurity incident-reporting, rules on personal data handling, re-use of data, AI in the workplace). The Call for Evidence to the Digital Omnibus reflected this, with contributions from all types of sectors. Therefore, no particular sector can be singled out as significantly benefitting or being hindered by the proposed measures. Overall, the impact is expected to be beneficial across sectors.

Annex IV - SME Check

OVERVIEW OF IMPACTS ON SMES

Relevance for SMEs
This initiative is considered relevant to SMEs. It proposes several targeted amendments to legal acts that were, at the time of their initial impact assessments, considered as having both direct and indirect impacts on SMEs. The proposed changes generally apply to all types of companies regardless of size (for instance on cookie rules, personal data rules, or incident reporting). However, specific provisions on cloud switching under the Data Act propose a direct exemption to both SMEs and Small Mid-Caps (SMCs). Regulatory privileges granted to micro enterprises under the Artificial Intelligence Act are also extended to SMEs. Last, the proposal also lays out specific measures extending exemptions that were already granted to SMEs under the current legal framework (in the Data Governance Act, the Open Data Directive, and the Artificial Intelligence Act) to SMCs.

(1) IDENTIFICATION OF AFFECTED BUSINESSES AND ASSESSMENT OF RELEVANCE
Are SMEs directly affected? In which sectors?
Yes – across sectors.
Estimated number of directly affected SMEs
Eurostat data from 2022 shows that the EU is home to approximately 1.4 million enterprises in the sector of ICT services[199]. Since over 99 % of all EU enterprises are considered to be SMEs, it can be considered that approximately 1.386 million ICT-relevant SMEs could be in scope of this initiative's various targeted amendments on several pieces of the digital acquis, depending on their exact nature. The exact number may vary however based on the specific considered amendment. For instance, regarding the proposed changes on a lighter cloud switching regime for SMEs and SMCs within the Data Act, it is estimated that this would positively affect 5000 of such companies. Several of the other provisions would directly beneficially affect many SMEs in Europe, but could not be quantified on the basis of the data available when preparing the proposal. Other measures pertain to the extension of regulatory privileges granted to SMEs equally to SMCs, where a specific company population could be identified. For instance, for the specific changes under the AI Act's Article 63, 1250 SMCs are estimated to benefit. However, due to the cross-cutting nature of the Digital Omnibus proposal, it should be noted that several of the targeted amendments would affect SMEs of all sectors indistinctively – not only companies in the ICT sector. For instance, the simplification of information requirements in the proposed changes to the General Data Protection Regulation (GDPR) would directly

[199] Eurostat (2022) *Businesses in the information and communication services sector*. Available at: Businesses in the information and communication services sector - Statistics Explained - Eurostat

affect SMEs such as craftspersons, hairdressers, or bakers, relieving them from the obligation to prepare privacy notices. While there is no exact number of SMEs handling personal data that would be directly affected by these specific changes, the number can be expected to be higher than the sole 1.386 million SMEs active in the ICT sector. Similarly, cybersecurity attacks typically affect companies of all sizes and across sectors[200]. The effects of the newly introduced Single Entry Point, streamlining the reporting of such incidents, would affect SMEs beyond the ICT sector. Last, the introduction of new rules on cookie banners would positively affect any SME with a website (exact number of which could not be quantified), regardless of the sector the company operates in.

Estimated number of employees in directly affected SMEs

In 2022, Eurostat estimated that 7.2 million employees were employed within SMEs in the ICT sector. Based on the above considerations regarding the wide-ranging scope of effect of several of the proposals put forward in the Digital Omnibus, it can be considered that at minimum such amount of employees could similarly be positively affected by the proposal's various amendments. This number could be higher for certain of the more horizontal provisions discussed above, which reach beyond the sole ICT sector.

Are SMEs indirectly affected? In which sectors? What is the estimated number of indirectly affected SMEs and employees?

See above considerations on the number of SMEs directly affected by the proposal. A large proportion of SMEs would equally be indirectly affected in one way or another, across sectors due to the horizontal nature of several of the amendments. However, due to the burden reduction nature of the proposal such impacts are estimated to be positive on SMEs.

(4) CONSULTATION OF SME STAKEHOLDERS

How has the input from the SME community been taken into consideration?

A dedicated SME Panel consultation was organised via the Enterprise Europe Network (EEN) between 4 September and 16 October. The EEN is the world's largest support network for small and medium-sized enterprises, and is implemented by the European Commission's European Innovation Council and SMEs Executive Agency (EISMEA). Its findings can be found in Annex I of this Staff Working Document. Additionally, several meetings were held with SME stakeholders in the making of the proposal. The Call for Evidence to the Digital Omnibus also gathered 121 responses from companies identifying as SMEs, as well as a number of SME associations. Previously held public consultations on some of the specific pillars of the Omnibus (data sharing, artificial intelligence, and cybersecurity) also led to direct contributions from SMEs.

Their input was duly taken into consideration for the preparation of the initiative. Some SME exemptions were provided, and even extended to SMCs in some cases in order to address the reality that some SMEs that may 'outgrow' their status can face a sudden increase in compliance burden. Overall, the measures were carefully weighed in order to limit the

[200] ENISA (2021) *Cybersecurity for SMEs*. Available at: Cybersecurity for SMEs - Challenges and Recommendations | ENISA

potential burdens on companies, and maximise positive outcomes (see below for specific cases).

Are SMEs' views different from those of large businesses?

SMEs' views broadly aligned with those of large businesses on a number of the provisions put forward in the Omnibus. For instance, the streamlining of cybersecurity incident reporting was widely called for, by companies of all sizes, due to the horizontal nature of the problem. Similarly, issues related to cookie banners were assessed in a broadly similar way between SMEs and larger companies as to the essence of the problem; the only variable factor noted was the importance of the cost burden between the two (with larger companies claiming higher operating costs for compliance with the existing rules in the organised reality check on cookie rules, as compared to the results of the SME panel on the same question[201]).

On some other provisions however, the views from SMEs differed largely. On a general note, results of the conducted SME Panel highlight that the specificities of many of the legal acts addressed under the Digital Omnibus are not well known by a majority of SMEs. This contrasts greatly with the high degree of policy engagement noted by larger stakeholders in the consultation process.

Some more specific distinctions can also be noted. On the question of trade secrets under the Data Act, for instance, SMEs put a strong emphasis on limiting the capacity of data holders (often larger companies) of invoking trade secrets as a means to refrain from data sharing obligations under the Data Act's Chapter II. Ultimately, the issue of trade secrets was addressed as regards to third-country jurisdictions, but the proposal preserved the Business-to-Business (B2B) essence of the Data Act called for by SMEs. Regarding compliance with the Artificial Intelligence Act, while larger companies tended to focus on direct legal amendments, SMEs heavily emphasised the need for support tools, subsidised conformity assessments, guidelines and toolkits. Taking note of this, the Commission has already prepared and will continue delivering such support instruments, adjacently to the Digital Omnibus. For instance, the AI Act Service Desk was set up, with a particular emphasis on supporting SMEs with their compliance with the AI Act[202].

Last, some of the proposed provisions in the Omnibus build directly from contributions of startups and SMEs. For instance, the measures on cloud switching under the Data Act – outlaying a specific lighter regime for SMEs and SMCs – stem from noted concerns from smaller providers on the need to guarantee predictable revenues over a fixed period of time (something that was limited by the existing legal framework). The changes limit the right to switch contracts, thereby better protecting smaller companies that tend to depend more on these types of fixed-term contracts.

(4) ASSESSMENT OF IMPACTS ON SMES

What are the estimated direct costs for SMEs of the preferred policy option?

Qualitative assessment

[201] See Annex I.

[202] European Commission (2025) *AI Act Service Desk*. Available at: AI Act Service Desk | AI Act Service Desk

No direct costs are estimated for SMEs as a result of this proposal, which is by its nature designed to reduce administrative burdens on companies.
Quantitative assessment
N/A.
What are the estimated direct benefits/cost savings for SMEs of the preferred policy option?
Qualitative assessment
Due to the cross-cutting nature of the initiative, and as outlined in the first subsection to this Annex, all estimated cost-savings are applicable to SMEs and larger companies without discrimination. Quantifiable cost savings can be found in Annex II to this Staff Working Document.
Quantitative assessment
See Annex II for the aggregate estimate, which applies to companies of all sizes and thereby including a majority of SMEs. More specifically, EUR 588,450,000 is expected to be saved for SMEs and SMCs, as a non-incurred cost, due to the introduced lighter regime for data processing services. Some other quantitative cost savings estimates are further provided in cases where existing regulatory privileges for SMEs are extended to SMCs. This is for instance the case under the Data Act, where the possibility to benefit from access to data from protected public databases at cheaper rate is expected to represent savings of up to EUR 19 million, as well as under the AI Act, where the extension of privileges granted to SMEs on documentation requirements would correspond to savings of EUR 2,500,000.
What are the indirect impacts of this initiative on SMEs?
SMEs may need to face some limited adjustment costs with some of the specific proposals of the Digital Omnibus. Namely, regarding the introducing of the Single-Entry Point, some limited one-off upskilling of staff on the changes to the entities' internal reporting procedures can be expected. However, these limited impacts are significantly outweighed by the expected benefits.

(4) MINIMISING NEGATIVE IMPACTS ON SMES
Are SMEs disproportionately affected compared to large companies? **If yes, are there any specific subgroups of SMEs more exposed than others?**
No.
Have mitigating measures been included in the preferred option/proposal?

No mitigating measures have been taken within the proposal as such, since the latter does not entail any foreseen negative impact. However, as outlined earlier above, a certain number of provisions were directly tailored to take into account SME interests.

CONTRIBUTION TO THE 35% BURDEN REDUCTION TARGET FOR SMES
Are there any administrative cost savings relevant for the 35% burden reduction target for SMEs?
Due to the cross-cutting nature of the initiative, and as outlined in the first subsection to this Annex, all estimated cost-savings are applicable to SMEs and larger companies without discrimination. Quantifiable cost savings can be found in Annex II to this Staff Working Document.

Annex V - Detailed list of reporting obligations in the digital acquis

In her confirmation hearing of 12 November 2024 at the European Parliament[203], Executive Vice-President Henna Virkkunen pledged to deliver a full list of reporting obligations applicable to companies as a basis for potential simplification.

This annex presents this list, identified in the full digital acquis as of 15 October 2025.

It is broken into three main parts:

- Regular reporting;
- Incident reporting;
- Reporting upon request.

Each section presents the relevant legislative act under which the reporting requirement stems from, with further details on the specific Article it is derived from, the frequency of reporting, the addressees, and recipients of the reporting obligation.

Some of these reporting obligations have been addressed in the Digital Omnibus. This is notably the case with the proposal to streamline cybersecurity incident-reporting and related incidents, and for certain reporting obligations under the repealed Platform-to-Business Regulation.

Further reporting obligations addressed in the below may be addressed via other means by the Commission, notably in the context of the Digital Fitness Check. In the public consultation launched as part of the Digital Simplification Package[204], companies and public sector bodies are asked to provide their views to this list. This will support the Commission's qualification of future measures to be taken, in view of lowering the administrative burden linked to reporting obligations all the while preserving the rationale of certain measures underpinning the transparency and accountability of policies.

[203] European Parliament (2024) *Verbatim of confirmation hearing of Henna Virkkunen, Executive Vice-President-designate of the European Commission*. Available at: virkkunen_verbatimreporthearing-original.pdf

[204] European Commission (2025) *Have your Say: Digital fitness check – testing the cumulative impact of the EU's digital rules*. Available at: Digital fitness check – testing the cumulative impact of the EU's digital rules

REGULAR REPORTING

Legislative act	Art.	Extracts of the legal text describing the reporting obligation	Frequency of reporting	Addressees	To whom the information needs to be reported
Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance)	26(10)	Deployers shall submit annual reports to the relevant market surveillance and national data protection authorities on their use of post-remote biometric identification systems, excluding the disclosure of sensitive operational data related to law enforcement. The reports may be aggregated to cover more than one deployment.	Annually	Company Public authority	National competent authority
Commission Delegated Regulation (EU) 2023/444 of 16 December 2022 supplementing Directive (EU) 2018/1972 of the European Parliament and of the Council with measures to ensure effective access to emergency services through emergency communications to the single European emergency number '112' (Text with EEA relevance)	7(1)	Member States shall regularly report to the Commission the performance of the routing to the most appropriate PSAP under Article 5, implemented for emergency communications and caller location information.	Regularly (i.e. every 2 years)	Member States	European Commission
Decision 676/2002/EC of the European Parliament and of the Council of 7 March 2002 on a regulatory framework for radio spectrum policy in the European Community (Radio Spectrum Decision)	9	The Commission shall report on an annual basis to the European Parliament and the Council on the activities developed and the measures adopted pursuant to this Decision, as well as on future actions envisaged pursuant to this Decision.	Annually	European Commission	European Parliament and Council
Decision No 626/2008/EC of the European Parliament and of the Council of 30 June 2008 on the selection and authorisation of systems providing mobile satellite services (MSS) (Text with EEA relevance)	9(2)	Member States shall ensure that rules on enforcement, including rules on penalties applicable in the event of breaches of the common conditions provided	Annually, upon certain conditions	Member States	European Commission

		for in Article 7(2), are in accordance with Community law, in particular Article 10 of Directive 2002/20/EC. Penalties must be effective, proportionate and dissuasive. Member States shall ensure monitoring of compliance with these common conditions and take appropriate measures to address non-compliance. Member States shall inform the Commission of the results of such monitoring on an annual basis, in the event that any common conditions have not been complied with and in the event that any enforcement measures have been taken. The Commission may, with the assistance of the Communications Committee referred to in Article 10(1), examine any alleged specific breach of the common conditions. Where a Member State informs the Commission of a particular breach, the Commission shall examine the alleged breach with the assistance of the Communications Committee.	being fulfilled		
Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast)Text with EEA relevance.	8(2)	National regulatory authorities shall report annually, inter alia, on the state of the electronic communications market, on the decisions they issue, on their human and financial resources and how those resources are	Annually	Member States	General public

		attributed, as well as on future plans. Their reports shall be made public.			
Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast)Text with EEA relevance.	17(2)	Where undertakings providing public electronic communications networks or publicly available electronic communications services are not subject to the requirements of company law and do not satisfy the small and medium-sized enterprise criteria of Union law accounting rules, their financial reports shall be drawn up and submitted to independent audit and published. The audit shall be carried out in accordance with the relevant Union and national rules. The first subparagraph of this paragraph shall also apply to the separate accounts required under point (a) of the first subparagraph of paragraph 1.	Upon certain conditions being fulfilled	Undertakings	General public
Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast)Text with EEA relevance.	103(1)	Competent authorities in coordination, where relevant, with national regulatory authorities shall ensure that, where providers of internet access services or publicly available interpersonal communication services make the provision of those services subject to terms and conditions, the information referred to in Annex IX is published in a clear, comprehensive, machine-	One-off with regular updating	Companies	National regulatory authority General public

		readable manner and in an accessible format for end-users with disabilities in accordance with Union law harmonising accessibility requirements for products and services, by all such providers, or by the competent authority itself in coordination, where relevant, with the national regulatory authority. Such information shall be updated regularly. Competent authorities in coordination, where relevant, with national regulatory authorities may specify additional requirements regarding the form in which such information is to be published. That information shall, on request, be supplied to the competent authority and, where relevant, to the national regulatory authority before its publication.			
Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast)Text with EEA relevance.	104(1)	National regulatory authorities in coordination with other competent authorities may require providers of internet access services and of publicly available interpersonal communications services to publish comprehensive, comparable, reliable, user-friendly and up-to-date information for end-users on the quality of their services, to the extent that they control at least some elements of the network	One-off with regular updating	Companies	NRAs/general public

		either directly or by virtue of a service level agreement to that effect, and on measures taken to ensure equivalence in access for end-users with disabilities. National regulatory authorities in coordination with other competent authorities may also require providers of publicly available interpersonal communication services to inform consumers if the quality of the services they provide depends on any external factors, such as control of signal transmission or network connectivity.			
Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')	5(1)	In addition to other information requirements established by Community law, Member States shall ensure that the service provider shall render easily, directly and permanently accessible to the recipients of the service and competent authorities, at least the following information: (a) the name of the service provider; (b) the geographic address at which the service provider is established; (c) the details of the service provider, including his electronic mail address, which allow him to be contacted	One-off, with possible updating	Service provider	Recipients of said service Competent authorities

rapidly and communicated with in a direct and effective manner;

(d) where the service provider is registered in a trade or similar public register, the trade register in which the service provider is entered and his registration number, or equivalent means of identification in that register;

(e) where the activity is subject to an authorisation scheme, the particulars of the relevant supervisory authority;

(f) as concerns the regulated professions:

- any professional body or similar institution with which the service provider is registered,

- the professional title and the Member State where it has been granted,

- a reference to the applicable professional rules in the Member State of establishment and the means to access them;

(g) where the service provider undertakes an activity that is subject to VAT, the identification number referred to in Article 22(1) of the sixth Council Directive 77/388/EEC of 17 May 1977 on the harmonisation of the laws of the

		Member States relating to turnover taxes - Common system of value added tax: uniform basis of assessment(29).			
Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)	4(4)	Subject to any technical implementing measures adopted under paragraph 5, the competent national authorities may adopt guidelines and, where necessary, issue instructions concerning the circumstances in which providers are required to notify personal data breaches, the format of such notification and the manner in which the notification is to be made. They shall also be able to audit whether providers have complied with their notification obligations under this paragraph, and shall impose appropriate sanctions in the event of a failure to do so. Providers shall maintain an inventory of personal data breaches comprising the facts surrounding the breach, its effects and the remedial action taken which shall be sufficient to enable the competent national authorities to verify compliance with the provisions of paragraph 3. The inventory shall only include the information necessary for this purpose	Following national authorities' guidelines	Provider of a publicly available electronic communication service	Competent national authority

Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) (Codified version) (Text with EEA relevance)	2(5a)	Member States shall ensure that media service providers inform the competent national authorities or bodies about any changes that may affect the determination of jurisdiction in accordance with paragraphs 2, 3 and 4.	Upon any relevant changes	Member States Media service providers	Competent national authorities or bodies
Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) (Codified version) (Text with EEA relevance)	7(2)	Member States shall ensure that media service providers report on a regular basis to the national regulatory authorities or bodies on the implementation of the measures referred to in paragraph 1 [accessibility measures]. By 19 December 2022 and every three years thereafter, Member States shall report to the Commission on the implementation of paragraph 1.	Every three years	Member States Media service providers	National regulatory authorities or bodies
Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) (Codified version) (Text with EEA relevance)	7(3)	Member States shall encourage media service providers to develop accessibility action plans in respect of continuously and progressively making their services more accessible to persons with disabilities. Any such action plan shall be communicated to national regulatory authorities or bodies.	Upon developme nt of action plans	Member States Media service providers	National regulatory authorities or bodies
Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in	13(4)	Member States shall report to the Commission by 19 December 2021 and every two	Every two years	Member States	Commission

Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) (Codified version) (Text with EEA relevance)		years thereafter on the implementation of paragraphs 1 and 2 [share of European works and prominence measures in VOD services].			
Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) (Codified version) (Text with EEA relevance)	16(3)	Member States shall provide the Commission every 2 years, starting from 3 October 1991, with a report on the application of this Article [share of European works in broadcasting] and Article 17 [share of independent productions in broadcasting]. That report shall in particular include a statistical statement on the achievement of the proportion referred to in this Article and Article 17 for each of the television programmes falling within the jurisdiction of the Member State concerned, the reasons, in each case, for the failure to attain that proportion and the measures adopted or envisaged in order to achieve it.	Every two years	Member States	Commission
Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) (Codified version) (Text with EEA relevance)	33a(2)	By 19 December 2022 and every three years thereafter, Member States shall report to the Commission on the implementation of paragraph 1 [media literacy measures].	Every three years	Member States	Commission
Directive 2014/26/EU of the European Parliament and of the Council of 26 February 2014 on collective management of copyright and related rights and multi-territorial licensing of rights	39	By 10 April 2016, Member States shall provide the Commission, on the basis of the	One-off, after this	Member States	European Commission

in musical works for online use in the internal market Text with EEA relevance		information at their disposal, with a list of the collective management organisations established in their territories. Member States shall notify any changes to that list to the Commission without undue delay. The Commission shall publish that information and keep it up to date.	upon changes		
Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (Text with EEA relevance.)	12(5)	Where a Member State provides in its national law for a licensing mechanism in accordance with this Article, that Member State shall inform the Commission about the scope of the corresponding national provisions, about the purposes and types of licences that may be introduced under those provisions, about the contact details of organisations issuing licences in accordance with that licensing mechanism, and about the means by which information on the licensing and on the options available to rightholders as referred to in point (c) of paragraph 3 can be obtained. The Commission shall publish that information.	Upon certain conditions being fulfilled	Member States	European Commission
Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the term of protection of copyright and certain related rights (codified version)	11(1)	Member States shall immediately notify the Commission of any governmental plan to grant new related rights, including the basic reasons for their	Upon certain conditions being fulfilled	Member States	European Commission

		introduction and the term of protection envisaged.			
Directive 2014/26/EU of the European Parliament and of the Council of 26 February 2014 on collective management of copyright and related rights and multi-territorial licensing of rights in musical works for online use in the internal market Text with EEA relevance	22(1)	Member States shall ensure that a collective management organisation, irrespective of its legal form under national law, draws up and makes public an annual transparency report, including the special report referred to in paragraph 3, for each financial year no later than eight months following the end of that financial year. The collective management organisation shall publish on its website the annual transparency report, which shall remain available to the public on that website for at least five years. [Further paragraphs specifying form and content of the reporting.]	Annually	Collective Management Organisations	Publicly available
Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union (Text with EEA relevance)	5(1)	National regulatory authorities shall publish reports on an annual basis regarding their monitoring and findings and provide those reports to the Commission and to BEREC.	Annually	National regulatory authorities	European Commission and BEREC
Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services (Text with EEA relevance)	11(4) and (5)	Providers of online intermediation services shall establish and make easily available to the public information on the functioning and effectiveness of their internal complaint-handling	One-off with annual update	Providers of online intermediation services (except small enterprises)	General public

		system. They shall verify the information at least annually and where significant changes are needed, they shall update that information. That information shall include the total number of complaints lodged, the main types of complaints, the average time period needed to process the complaints and aggregated information regarding the outcome of the complaints.			
Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance)	3(3)	3. Where an undertaking providing core platform services meets all of the thresholds in paragraph 2, it shall notify the Commission thereof without delay and in any event within 2 months after those thresholds are met and provide it with the relevant information identified in paragraph 2. That notification shall include the relevant information identified in paragraph 2 for each of the core platform services of the undertaking that meets the thresholds in paragraph 2, point (b). Whenever a further core platform service provided by the undertaking that has previously been designated as a gatekeeper meets the thresholds in paragraph 2, points (b) and (c), such undertaking shall notify the Commission thereof within 2 months after those thresholds are satisfied.	Upon certain conditions being met	Undertakings providing core platform services (potential gatekeepers)	Commission

Where the undertaking providing the core platform service fails to notify the Commission pursuant to the first subparagraph of this paragraph and fails to provide within the deadline set by the Commission in the request for information pursuant to Article 21 all the relevant information that is required for the Commission to designate the undertaking concerned as gatekeeper pursuant to paragraph 4 of this Article, the Commission shall still be entitled to designate that undertaking as a gatekeeper, based on information available to the Commission.

Where the undertaking providing core platform services complies with the request for information pursuant to the second subparagraph of this paragraph or where the information is provided after the expiration of the deadline referred to in that subparagraph, the Commission shall apply the procedure set out in paragraph 4.

Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance)	11(2)	Within the deadline referred to in paragraph 1, the gatekeeper shall publish and provide the Commission with a nonconfidential summary of that report. [11(3) details that the gatekeeper shall update that report and that non-confidential summary at least annually.]	One-off with annual update	Gatekeeper	General public European Commission
Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance)	15(3)	The gatekeeper shall make publicly available an overview of the audited description referred to in paragraph 1. In doing so, the gatekeeper shall be entitled to take account of the need to respect its business secrets. The gatekeeper shall update that description and that overview at least annually.	One-off with annual update	Gatekeeper	European Commission
Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance)	28(6)	Gatekeepers shall communicate the name and contact details of the head of the compliance function to the Commission.	One-off, with possible updates	Gatekeeper	European Commission
Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance)	15(1)	Providers of intermediary services shall make publicly available, in a machine-readable format and in an easily accessible manner, at least once a year, clear, easily comprehensible reports on any content moderation that they engaged in during the relevant period. Those reports shall include, in particular, information on the following, as	At least annually	Providers of intermediary services	General public

applicable:

(a) for providers of intermediary services, the number of orders received from Member States' authorities including orders issued in accordance with Articles 9 and 10, categorised by the type of illegal content concerned, the Member State issuing the order, and the median time needed to inform the authority issuing the order, or any other authority specified in the order, of its receipt, and to give effect to the order;

(b) for providers of hosting services, the number of notices submitted in accordance with Article 16, categorised by the type of alleged illegal content concerned, the number of notices submitted by trusted flaggers, any action taken pursuant to the notices by differentiating whether the action was taken on the basis of the law or the terms and conditions of the provider, the number of notices processed by using automated means and the median time needed for taking the action;

(c) for providers of intermediary services, meaningful and comprehensible information about the content moderation engaged in at the

providers' own initiative, including the use of automated tools, the measures taken to provide training and assistance to persons in charge of content moderation, the number and type of measures taken that affect the availability, visibility and accessibility of information provided by the recipients of the service and the recipients' ability to provide information through the service, and other related restrictions of the service; the information reported shall be categorised by the type of illegal content or violation of the terms and conditions of the service provider, by the detection method and by the type of restriction applied;

(d) for providers of intermediary services, the number of complaints received through the internal complaint-handling systems in accordance with the provider's terms and conditions and additionally, for providers of online platforms, in accordance with Article 20, the basis for those complaints, decisions taken in respect of those complaints, the median time needed for taking those decisions and the number of instances where those decisions were reversed;

(e) any use made of automated

		means for the purpose of content moderation, including a qualitative description, a specification of the precise purposes, indicators of the accuracy and the possible rate of error of the automated means used in fulfilling those purposes, and any safeguards applied.			
Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance)	24(2)	By 17 February 2023 and at least once every six months thereafter, providers shall publish for each online platform or online search engine, in a publicly available section of their online interface, information on the average monthly active recipients of the service in the Union, calculated as an average over the period of the past six months and in accordance with the methodology laid down in the delegated acts referred to in Article 33(3), where those delegated acts have been adopted.	Every six months	Online platforms	Publicly available
Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance)	37(1)	Providers of very large online platforms and of very large online search engines shall be subject, at their own expense and at least once a year, to independent audits to assess compliance with the following: (…)	At least annually	Providers of VLOP & VLOSE	European Commission

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance)	39(1)	Providers of very large online platforms or of very large online search engines that present advertisements on their online interfaces shall compile and make publicly available in a specific section of their online interface, through a searchable and reliable tool that allows multicriteria queries and through application programming interfaces, a repository containing the information referred to in paragraph 2, for the entire period during which they present an advertisement and until one year after the advertisement was presented for the last time on their online interfaces. (...)	Upon certain conditions being fulfilled	Providers of VLOP & VLOSE	General public
Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance)	42(4)	Providers of very large online platforms or of very large online search engines shall transmit to the Digital Services Coordinator of establishment and the Commission, without undue delay upon completion, and make publicly available at the latest three months after the receipt of each audit report pursuant to Article 37(4): (a) a report setting out the results of the risk assessment pursuant to Article 34; (b) the specific mitigation measures put in place pursuant to Article 35(1); (c) the audit report provided for	At least annually	Providers of VLOP & VLOSE	European Commission DSC General public

		in Article 37(4); (d) the audit implementation report provided for in Article 37(6); (e) where applicable, information about the consultations conducted by the provider in support of the risk assessments and design of the risk mitigation measures.			
Regulation (EU) 2022/612 of the European Parliament and of the Council of 6 April 2022 on roaming on public mobile communications networks within the Union (recast) (Text with EEA relevance)	6(2)	[Paragraph 1: In specific and exceptional circumstances, with a view to ensuring the sustainability of its domestic charging model, where a roaming provider is not able to recover its overall actual and projected costs of providing regulated roaming services in accordance with Articles 4 and 5, from its overall actual and projected revenues from the provision of such services, that roaming provider may apply for authorisation to apply a surcharge. That surcharge shall be applied only to the extent necessary to recover the costs of providing regulated retail roaming services, having regard to the applicable maximum wholesale charges.] Where a roaming provider decides to avail itself of paragraph 1 of this Article, it shall without delay submit an application to the national regulatory authority and provide it with all necessary information in accordance with the implementing acts referred	One-off with annual update	Operators	NRA (BEREC optional)

		to in Article 7. Every 12 months thereafter, the roaming provider shall update that information and submit it to the national regulatory authority.			
Regulation (EU) 2022/612 of the European Parliament and of the Council of 6 April 2022 on roaming on public mobile communications networks within the Union (recast) (Text with EEA relevance)	7	1. In order to ensure consistent application of Articles 5 and 6, the Commission shall, after consulting BEREC, adopt implementing acts laying down detailed rules on the following: (a) the application of fair use policies; (b) the methodology for assessing the sustainability of the provision of retail roaming services at domestic prices; and (c) the application to be submitted by a roaming provider for the purposes of the assessment referred to in point (b). The implementing acts referred to in the first subparagraph of this paragraph shall be adopted in accordance with the examination procedure referred to in Article 20(2). The Commission shall, after consulting BEREC, review the implementing acts referred to in the first subparagraph periodically in light of market developments. [...] The national regulatory authority and, where applicable, other competent authorities shall inform the Commission annually concerning the	Periodically	BEREC	European Commission

		application of Articles 5 and 6, and of this Article.			
Regulation (EU) 2022/612 of the European Parliament and of the Council of 6 April 2022 on roaming on public mobile communications networks within the Union (recast) (Text with EEA relevance)	7(4)	The national regulatory authority and, where applicable, other competent authorities shall inform the Commission annually concerning the application of Articles 5 and 6, and of this Article.	Annually	NRA	European Commission
Regulation (EU) 2022/612 of the European Parliament and of the Council of 6 April 2022 on roaming on public mobile communications networks within the Union (recast) (Text with EEA relevance)	21(2)	In order to assess competitive developments in Union-wide roaming markets, BEREC shall collect data regularly from national regulatory authorities on developments in retail and wholesale charges for regulated voice, SMS and data roaming services, including wholesale charges applied for balanced and unbalanced roaming traffic respectively, on the impact of the roll-out and implementation of next generation mobile communications networks and technologies on the roaming market, on the use of trading platforms and similar instruments, on the development of machine-to-machine roaming and IoT devices, and on the extent to which wholesale roaming agreements cover quality of service and give access to different network technologies and generations. Where applicable, the national	Regularly (i.e. annually)	NRA and BEREC	BEREC and Commission

regulatory authorities may provide such data in coordination with other competent authorities. BEREC shall also collect data regularly from national regulatory authorities on the application of fair use policies by operators, the developments of domestic-only tariffs, the application of the sustainability mechanisms and complaints on roaming and compliance with the quality of service obligations. Where appropriate, national regulatory authorities shall coordinate with and collect such data from other competent authorities. BEREC shall regularly collect and provide additional information on transparency, on the application of measures on emergency communication, on value-added services and on roaming on non-terrestrial public mobile communications networks. BEREC shall also collect data on the wholesale roaming agreements not subject to the maximum wholesale roaming charges provided for in Article 9, 10 or 11 and on the implementation of contractual measures at wholesale level aiming to prevent regulated roaming services to roaming providers' customers while the latter are periodically travelling within the Union. (…) pursuant to this paragraph shall be notified to the Commission at

		least once a year. The Commission shall make them public.			
Regulation (EU) 2024/1309 of the European Parliament and of the Council of 29 April 2024 on measures to reduce the cost of deploying gigabit electronic communications networks, amending Regulation (EU) 2015/2120 and repealing Directive 2014/61/EU (Gigabit Infrastructure Act) (Text with EEA relevance)	3(2)	(...) Operators and legal persons referred to in the first subparagraph of this paragraph shall inform the national regulatory authority of the conclusion of agreements reached in accordance with the first subparagraph, including the agreed price.	Upon said agreement	Operators and legal persons who are primarily active as tenants of land, or as holders of rights over land, other than property rights, on which facilities are planned to be or have been installed with a view to deploying elements of VHCNs, or who manage lease contracts on behalf of land owners	NRAs
Regulation (EU) 2024/1309 of the European Parliament and of the Council of 29 April 2024 on measures to reduce the cost of deploying gigabit electronic communications networks, amending Regulation (EU) 2015/2120 and repealing Directive 2014/61/EU (Gigabit Infrastructure Act) (Text with EEA relevance)	7(10)	The Commission shall monitor the application of this Article in Member States. To that end, Member States shall report every three years to the Commission on the status of implementation of this Article	Every three years	Member States	Commission

		and on whether the conditions listed therein have been met.				
Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance)	13(23)	A manufacturer that ceases its operations and, as a result, is not able to comply with this Regulation shall inform, before the cessation of operations takes effect, the relevant market surveillance authorities as well as, by any means available and to the extent possible, the users of the relevant products with digital elements placed on the market, of the impending cessation of operations.	One-off	Manufacturer	Market Surveillance Authority, as well as, by any means available and to the extent possible, the users of the relevant products with digital elements	
Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC	20(1)	Qualified trust service providers shall be audited at their own expense at least every 24 months by a conformity assessment body. […] Qualified trust service providers shall submit the resulting conformity assessment report to the	At least once every two years	Qualified trust service providers	Supervisory body	

		supervisory body within three working days of receipt			
Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC	20(1a)	Qualified trust service providers shall inform the supervisory body at the latest one month before any planned audits and shall allow the supervisory body to participate as an observer upon request.	Ahead of any planned audit	Qualified trust service providers	Supervisory body
Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC	30(3)(b)	Public or private certification bodies shall notify to the Commission any alternative procedures they use to certify qualified signature creation devices (QSCD) for compliance with Annex II requirements.	Unspecified	Certification bodies (public or private)	European Commission
Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC	24(2)(a)	Inform the supervisory body at least one month before implementing any change in the provision of its qualified trust services or at least three months in case of an intention to cease those activities.	Upon any (intention to) change in the provision of qualified trust services	Qualified trust service providers	Supervisory body
Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC	20(1)	Qualified trust service providers shall be audited at their own expense at least every 24 months by a conformity assessment body. […] Qualified trust service providers shall submit the resulting conformity assessment report to the supervisory body within three working days of receipt.	At least once in two years	Qualified trust service providers	Supervisory body

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC	20(1a)	Qualified trust service providers shall inform the supervisory body at the latest one month before any planned audits and shall allow the supervisory body to participate as an observer upon request	Ahead of any planned audit	Qualified trust service providers	Supervisory body
Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC	30(3)(b)	Public or private certification bodies shall notify to the Commission any alternative procedures they use to certify qualified signature creation devices (QSCD) for compliance with Annex II requirements.	Unspecified	Certification bodies (public or private)	European Commission
Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC	24(2)(a)	Inform the supervisory body at least one month before implementing any change in the provision of its qualified trust services or at least three months in case of an intention to cease those activities.	Upon any (intention to) change in the provision of qualified trust services	Qualified trust service providers	Supervisory body
Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC	5a(18)	Notification of information about the provided EUDIW by the Member State to the Commission.	Unspecified	Member States	Commission
Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC	5c(7)	Member States shall communicate to the Commission the names and addresses of the Conformity Assessment Bodies (CABs) designated to carry out EUDIW certification.	One-off, periodical updating	Member States	Commission

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC	5d(1)	Member States shall notify the Commission and the Cooperation Group about certified EUDI Wallets and relevant certification information.	Unspecified	Member States	Commission Cooperation Group
Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC	48a(4)	Submission by Member States to the Commission of a report on the statistics collected in relation to the functioning of the EUDIW and QTSP.	Unspecified	Member States	Commission
Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC	12a(6)	Member States must notify the Commission of the names and addresses of CABs certifying eID schemes.	One-off, periodical updating	Member States	Commission
Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance)	20(2)	A recognised data altruism organisation shall draw up and transmit to the relevant competent authority for the registration of data altruism organisations an annual activity report which shall contain at least the following: (a) information on the activities of the recognised data altruism organisation; (b) a description of the way in which the objectives of general interest for which data was collected have been promoted during the given financial year; (c) a list of all natural and legal persons that were allowed to process data it holds, including a summary description of the objectives of	Annually	Data altruism organisations that voluntarily apply for a trust label under the Regulation	General public and competent authority

		general interest pursued by such data processing and the description of the technical means used for it, including a description of the techniques used to preserve privacy and data protection; (d) a summary of the results of the data processing allowed by the recognised data altruism organisation, where applicable; (e) information on sources of revenue of the recognised data altruism organisation, in particular all revenue from allowing access to the data, and on expenditure.			
Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) (Text with EEA relevance)	10(10)	Dispute settlement bodies shall draw up and make publicly available annual activity reports. Such annual reports shall include, in particular, the following general information: (a) an aggregation of the outcomes of disputes; (b) the average time taken to resolve disputes; (c) the most common reasons for disputes.	Annually	Dispute settlement bodies	General public
Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC	20(1b)	Member States must notify the Commission of the names, addresses, and accreditation details of CABs for auditing QTSPs	One-off, periodical updating	Member States	Commission
Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust	30(2)	Member States notify the Commission about public or	One-off	Member States	Commission

services for electronic transactions in the internal market and repealing Directive 1999/93/EC		private bodies designated to certify QSCDs.			
Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC	31(1)	Notification by Member States to the Commission on certification or cancellation of QSCDs.	Periodical	Member States	Commission
Commission Implementing Regulation (EU) 2016/2286 of 15 December 2016 laying down detailed rules on the application of fair use policy and on the methodology for assessing the sustainability of the abolition of retail roaming surcharges and on the application to be submitted by a roaming provider for the purposes of that assessment (Text with EEA relevance)	5(2)	Fair use policies in accordance with this Regulation shall be notified by the roaming provider to the national regulatory authority.	One-off	Operators	NRA
Commission Implementing Regulation (EU) 2016/2286 of 15 December 2016 laying down detailed rules on the application of fair use policy and on the methodology for assessing the sustainability of the abolition of retail roaming surcharges and on the application to be submitted by a roaming provider for the purposes of that assessment (Text with EEA relevance)	6(1)	Applications for authorisation to apply a roaming surcharge filed by a roaming provider pursuant to Article 6c(2) of Regulation (EU) No 531/2012 in order to ensure the sustainability of its domestic charging model (‘application’) shall be assessed on the basis of data on the overall volumes of regulated retail roaming services provided by the applicant roaming provider projected over a period of 12 months starting at the earliest on 15 June 2017. For the first application, these volume projections shall be estimated using one or a combination of the following options: (a) actual volumes of regulated retail roaming services provided	Upon the operator's application for a derogation	Operators	NRA

by the applicant at the applicable regulated retail roaming price prior to 15 June 2017;

(b) projected volumes of regulated retail roaming services after 15 June 2017, where the projected volumes of regulated retail roaming services over the period in question are estimated based on actual domestic retail consumption of mobile services and time spent abroad in the Union by the roaming customers of the applicant;

(c) projected volumes of regulated retail roaming services after 15 June 2017, where the volumes of regulated retail roaming services are estimated based on the proportional change in the volumes of regulated retail roaming services experienced in the applicant's tariff plans representing a substantial part of the customer base on which the prices of regulated retail roaming services were set by the applicant at the domestic level for a period of at least 30 days, in accordance with the methodology set out in Annex I.

In the event of updates to the application being submitted pursuant to Article 6c(2) of Regulation (EU) No 531/2012,

		the projected overall volumes of regulated roaming services shall be updated on the basis of the actual average pattern of consumption of domestic mobile services multiplied by the observed number of roaming customers and the time they have spent in visited Member States in the previous 12 months.			
Commission Implementing Regulation (EU) 2016/2286 of 15 December 2016 laying down detailed rules on the application of fair use policy and on the methodology for assessing the sustainability of the abolition of retail roaming surcharges and on the application to be submitted by a roaming provider for the purposes of that assessment (Text with EEA relevance)	6(2)	Any data on the applicant's costs and revenues shall be based on financial accounts, which shall be made available to the national regulatory authority, and may be adjusted according to volume estimates pursuant to paragraph 1. Where costs are projected, deviations from figures resulting from past financial accounts shall be considered only if supported by proof of financial commitments for the period covered by the projections.	Upon the operator's application for a derogation	Operators	NRA
Commission Implementing Regulation (EU) 2016/2286 of 15 December 2016 laying down detailed rules on the application of fair use policy and on the methodology for assessing the sustainability of the abolition of retail roaming surcharges and on the application to be submitted by a roaming provider for the purposes of that assessment (Text with EEA relevance)	6(3)	The applicant shall provide all necessary data used to determine the mobile services margin and the overall actual and projected costs and revenues of providing regulated roaming services over the relevant period.	Upon the operator's application for a derogation	Operators	NRA
Commission Implementing Regulation (EU) 2016/2286 of 15 December 2016 laying down detailed rules on the application of fair use policy and on the methodology for assessing the	11	In order to monitor the consistent application of Articles 6b and 6c of	Regularly (at least	Operators and NRA	NRA and European Commisison

sustainability of the abolition of retail roaming surcharges and on the application to be submitted by a roaming provider for the purposes of that assessment (Text with EEA relevance)		Regulation (EU) No 531/2012 and of this Regulation, and with a view to informing the Commission annually of applications pursuant to Article 6d(5) of Regulation (EU) No 531/2012, the national regulatory authorities shall regularly collect information concerning: (a) any action they take to supervise the application of Article 6b of Regulation (EU) No 531/2012 and the detailed rules laid down in this Regulation; (b) the number of applications to apply a roaming surcharge filed, authorised and renewed in the course of the year pursuant to Article 6c(2) and (4) of Regulation (EU) No 531/2012; (c) the extent of negative roaming retail net margins recognised in their decisions to authorise the roaming surcharge and the arrangements concerning a surcharge declared in the applications for authorisation to apply a roaming surcharge filed by a roaming provider pursuant to Article 6c(2) of Regulation (EU) No 531/2012 in order to ensure the sustainability of its domestic charging model.	once a year)		
Commission Implementing Regulation (EU) 2020/1070 of 20 July 2020 on specifying the characteristics of small-area wireless access	4	Member States shall regularly monitor and report to the	Annually	Member States	European Commission

points pursuant to Article 57 paragraph 2 of Directive (EU) 2018/1972 of the European Parliament and the Council establishing the European Electronic Communications Code (Text with EEA relevance)		Commission, the first time by 31 December 2021, and each year thereafter, on the application of this Regulation, in particular on the application of Article 3(1), including on the technologies used by the small-area wireless access points deployed.			
Commission Implementing Regulation (EU) 2024/2979 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 as regards the integrity and core functionalities of European Digital Identity Wallets	6(3)(a)	Wallet providers shall inform wallet users of their rights and obligations in relation to their wallet unit.	Unspecified	EUDIW providers	Directly to wallet users.
Commission Implementing Regulation (EU) 2024/2981 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 as regards the certification of European Digital Identity Wallets	5(4)	The holder of the certificate of conformity shall notify the certification body of vulnerabilities and changes affecting the wallet solution based on defined impact criteria.	One-off with periodical updates	Holders of certificates of conformity (EUDIW solution providers after certification)	Certification bodies (which issued the certificate)
Commission Implementing Regulation (EU) 2025/848 of 6 May 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the registration of wallet-relying parties	5(3)	Wallet-relying parties shall update any information previously registered in the national register of wallet-relying parties without undue delay.	Periodically	Wallet Relying Parties	National competent authority maintaining the registration
Commission Implementing Regulation (EU) 2025/849 of 6 May 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the submission of information to the Commission and to the Cooperation Group for the list of certified European Digital Identity Wallets	3(1-3)	Member States shall submit the information set out in the Annex to the Commission and to the Cooperation Group (information about a provided and certified wallet).	Unspecified	Member States	Commission and the Cooperation Group

Commission Implementing Regulation (EU) 2024/2980 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards notifications to the Commission concerning the European Digital Identity Wallet ecosystem	4(1-3)	Member States shall submit the information set out in the Annex II to the Commission (notifications of information on wallet providers and on the mechanisms by which to validate the authenticity and validity of wallet units)	Unspecified	Member States	Commission
Commission Delegated Regulation (EU) 2021/654 of 18 December 2020 supplementing Directive (EU) 2018/1972 of the European Parliament and of the Council by setting a single maximum Union-wide mobile voice termination rate and a single maximum Union-wide fixed voice termination rate (Text with EEA relevance)	76(3)	National regulatory authorities shall closely monitor, and ensure compliance with, the application of the Union-wide voice termination rates by providers of voice termination services. National regulatory authorities may, at any time, require a provider of voice termination services to amend the rate it charges to other undertakings if it does not comply with the delegated act referred to in paragraph 1. National regulatory authorities shall annually report to the Commission and to BEREC with regard to the application of this Article.	Annually	National Regulatory Authorities (NRAs)	European Commission and BEREC
Commission Delegated Regulation (EU) 2023/1127 of 2 March 2023 supplementing Regulation (EU) 2022/2065 of the European Parliament and of the Council with the detailed methodologies and procedures regarding the supervisory fees charged by the Commission on providers of very large online platforms and very large online search engines (Text with EEA relevance)	6(2)	At the latest by 31 August of each year, any provider of designated service or services subject to the supervisory fee pursuant to Article 3 shall provide to the Commission its latest financial statement, and any other supporting document for the determination of the	Annually	Providers of VLOPs & VLOSEs	European Commission

		maximum overall limit pursuant to Article 5 as well as, where applicable, any information necessary for the application of the fee. Where a provider does not provide the documents necessary for the determination of the maximum overall limit, it shall be presumed that this limit is not reached by that provider in that calendar year.			
Commission Delegated Regulation (EU) 2024/436 of 20 October 2023 supplementing Regulation (EU) 2022/2065 of the European Parliament and of the Council, by laying down rules on the performance of audits for very large online platforms and very large online search engines	5(1)	At a time agreed with the auditing organisation, and in any event prior to the performance of any audit procedure, the audited provider shall transmit to the selected auditing organisation at least the following information: (a) a description of the internal controls put in place with respect to each audited obligation and commitment, including related indicators and all present and historical measurements, and benchmarks used by the audited provider to assert or monitor compliance with the audited obligations and commitments, as well as any supporting documentation; (b) its preliminary analysis of inherent and control risks, where the audited provider has performed such an analysis, and any supporting documentation; (c) information about any relevant decision-making structures, competences of	Upon any audit procedure	Providers of VLOPs & VLOSEs	Auditing Organisation

		departments of the provider, including the compliance function pursuant to Article 41 of Regulation (EU) 2022/2065, relevant IT systems, data sources, processing and storage, as well as explanations of relevant algorithmic systems and their interactions.(...)			
Commission Delegated Regulation (EU) 2024/436 of 20 October 2023 supplementing Regulation (EU) 2022/2065 of the European Parliament and of the Council, by laying down rules on the performance of audits for very large online platforms and very large online search engines	17(1)	The audited provider shall make available to the auditing organisation: (a) a list and the text of all codes of conduct referred to in Articles 45 and 46 of Regulation (EU) 2022/2065 and crisis protocols referred to in Article 48 of that Regulation, to which the audited provider is a signatory; (b) a detailed list of commitments within those codes of conduct and crisis protocols that the audited provider has taken; (c) where applicable, the key performance indicators agreed under each code of conduct and crisis protocol; (d) where applicable, any available measurements, data and documentation, and any reports prepared by the audited provider with respect to the compliance of the audited provider with the commitments taken, including access to all relevant information and data related to the functioning of the	Upon any audit procedure	Providers of VLOPs & VLOSEs	Auditing Organisation

		services offered by the audited provider relevant to the implementation of the code of conduct or the crisis protocol; (e) where applicable, other measurements, data and documentation prepared by signatories of the code of conduct or the crisis protocol, and the assessments by the Commission or the Board referred to in Article 45(4) of Regulation (EU) 2022/2065.			
Directive (EU) 2016/2102 of the European Parliament and of the Council of 26 October 2016 on the accessibility of the websites and mobile applications of public sector bodies	8(1)	By 23 December 2021, and every three years thereafter, Member States shall submit to the Commission a report on the outcome of the monitoring including the measurement data. That report shall be drawn up on the basis of the arrangements for reporting referred to in paragraph 6 of this Article. The report shall also cover information on the use of the enforcement procedure set out in Article 9.	Every three years	Member States	European Commission
Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) (Text with EEA relevance)	3(2)	Before concluding a contract for the purchase, rent or lease of a connected product, the seller, rentor or lessor, which may be the manufacturer, shall provide at least the following information to the user, in a clear and comprehensible manner: (a) the type, format and estimated volume of product	One-off	Seller, rentor or lessor of a connected product	User of said connected product

		data which the connected product is capable of generating; (b) whether the connected product is capable of generating data continuously and in real-time; (c) whether the connected product is capable of storing data on-device or on a remote server, including, where applicable, the intended duration of retention; (d) how the user may access, retrieve or, where relevant, erase the data, including the technical means to do so, as well as their terms of use and quality of service.			
Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) (Text with EEA relevance)	3(3)	Before concluding a contract for the provision of a related service, the provider of such related service shall provide at least the following information to the user, in a clear and comprehensible manner: (a) the nature, estimated volume and collection frequency of product data that the prospective data holder is expected to obtain and, where relevant, the arrangements for the user to access or retrieve such data, including the prospective data holder's data storage arrangements and the duration of retention; (b) the nature and estimated volume of related service data to be generated, as well as the arrangements for the user to access or retrieve such data, including the prospective	One-off	Provider of a service related to a connected product	User of said service

data holder’s data storage arrangements and the duration of retention; (c) whether the prospective data holder expects to use readily available data itself and the purposes for which those data are to be used, and whether it intends to allow one or more third parties to use the data for purposes agreed upon with the user; (d) the identity of the prospective data holder, such as its trading name and the geographical address at which it is established and, where applicable, of other data processing parties; (e) the means of communication which make it possible to contact the prospective data holder quickly and communicate with that data holder efficiently; (f) how the user can request that the data are shared with a third party and, where applicable, end the data sharing; OJ L, 22.12.2023 EN 38/71 ELI: http://data.europa.eu/eli/reg/2023/2854/oj (g) the user’s right to lodge a complaint alleging an infringement of any of the provisions of this Chapter with the competent authority designated pursuant to Article 37; (h) whether a prospective data holder is the holder of trade secrets contained in the data that is accessible from the connected product or generated during the provision of a related service, and, where the

		prospective data holder is not the trade secret holder, the identity of the trade secret holder; (i) the duration of the contract between the user and the prospective data holder, as well as the arrangements for terminating such a contract.			
Commission Decision 2007/116/EC of 15 February 2007 on reserving the national numbering range beginning with 116 for harmonised numbers for harmonised services of social value (notified under document number C(2007) 249) (Text with EEA relevance)	6	Member States shall report periodically to the Commission on the actual use of numbers listed in the Annex for the provision of the related services within their territory.	Periodically	Member States	European Commission
Commission Recommendation (EU) 2021/1970 of 10 November 2021 on a common European data space for cultural heritage	Ch. IV	Member States should inform the Commission 24 months from the publication of this Recommendation in the Official Journal of the European Union, and every 2 years thereafter, of actions taken in response to the Recommendation.	Every two years	Member States	European Commission

INCIDENT REPORTING

Legislative act	Art.	Extracts of the legal text describing the reporting obligation	Frequency of reporting	Addressees	To whom the information needs to be reported
Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU)	22(4)	The authorised representative shall terminate the mandate if it considers or has reason to consider the provider to be acting contrary to its obligations pursuant to this Regulation. In such a case, it shall immediately inform the relevant market surveillance authority, as well as, where applicable, the relevant notified body, about the termination of the mandate and the reasons therefor.	Upon certain conditions being fulfilled	Company Public authority	National competent authority

2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance)					
Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance)	23(2)	Where an importer has sufficient reason to consider that a high-risk AI system is not in conformity with this Regulation, or is falsified, or accompanied by falsified documentation, it shall not place the system on the market until it has been brought into conformity. Where the high-risk AI system presents a risk within the meaning of Article 79(1), the importer shall inform the provider of the system, the authorised representative and the market surveillance authorities to that effect.	Upon certain conditions being fulfilled	Company Public authority	National competent authority Relevant company Public authority
Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance)	24(4)	A distributor that considers or has reason to consider, on the basis of the information in its possession, a high-risk AI system which it has made available on the market not to be in conformity with the requirements set out in Section 2, shall take the corrective actions necessary to bring that system into conformity with those requirements, to withdraw it or recall it, or shall ensure that the provider, the importer or any relevant operator, as appropriate, takes those corrective actions. Where the high-risk AI system presents a risk within the meaning of Article 79(1), the distributor shall immediately inform the provider or importer of the system and the authorities competent for the high-risk AI system concerned, giving details, in particular, of the non-compliance and of any corrective actions taken.	Upon certain conditions being fulfilled	Company Public authority	National competent authority Relevant company Public authority
Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance)	26(5)	Deployers shall monitor the operation of the high-risk AI system on the basis of the instructions for use and, where relevant, inform providers in accordance with Article 72. Where deployers have reason to consider that the use of the high-risk AI system in accordance with the instructions may result in that AI system presenting a risk within the meaning of Article 79(1), they shall, without undue delay, inform the provider or distributor and the relevant market surveillance authority, and shall suspend the use of that system. Where deployers have identified a serious incident, they shall also immediately inform first the provider, and then the importer or distributor and the relevant market surveillance authorities of that incident. If the deployer is not	Upon certain conditions being fulfilled	Company Public authority	National competent authority Relevant company Public authority

		able to reach the provider, Article 73 shall apply mutatis mutandis. This obligation shall not cover sensitive operational data of deployers of AI systems which are law enforcement authorities.			
Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance)	23(1)	Each Member State shall ensure that essential and important entities notify, without undue delay, its CSIRT or, where applicable, its competent authority in accordance with paragraph 4 of any incident that has a significant impact on the provision of their services as referred to in paragraph 3 (significant incident). Where appropriate, entities concerned shall notify, without undue delay, the recipients of their services of significant incidents that are likely to adversely affect the provision of those services. Each Member State shall ensure that those entities report, inter alia, any information enabling the CSIRT or, where applicable, the competent authority to determine any cross-border impact of the incident. The mere act of notification shall not subject the notifying entity to increased liability. Where the entities concerned notify the competent authority of a significant incident under the first subparagraph, the Member State shall ensure that that competent authority forwards the notification to the CSIRT upon receipt. In the case of a cross-border or cross-sectoral significant incident, Member States shall ensure that their single points of contact are provided in due time with relevant information notified in accordance with paragraph 4.	a) Early warning: without undue delay and in any event within 24 hours of becoming aware of the significant incident b) Incident notification: without undue delay and in any event within 72 hours of becoming aware of the significant incident c) Upon the request of a CSIRT or, where applicable, the competent authority, an intermediate report d) Final report not later than one month after the submission of the incident notification under point (b)	Essential and important entities (18 critical sectors)	CSIRT or competent authority, as applicable
Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance)	23(2)	Where applicable, Member States shall ensure that essential and important entities communicate, without undue delay, to the recipients of their services that are potentially affected by a significant cyber threat any measures or remedies that those recipients are able to take in response to that threat. Where appropriate, the entities shall also inform those recipients of the significant cyber threat itself.	Once per incident	Essential and important entities (18 critical sectors)	Recipients of services that are potentially affected by a significant cyber threat

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)	4(2)	In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.	Upon incident	Provider of a publicly available eletronic communication service	Subscribers to said electronic communications service
Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)	4(3)	In the case of a personal data breach, the provider of publicly available electronic communications services shall, without undue delay, notify the personal data breach to the competent national authority. When the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall also notify the subscriber or individual of the breach without undue delay. Notification of a personal data breach to a subscriber or individual concerned shall not be required if the provider has demonstrated to the satisfaction of the competent authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the security breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it. Without prejudice to the provider's obligation to notify subscribers and individuals concerned, if the provider has not already notified the subscriber or individual of the personal data breach, the competent national authority, having considered the likely adverse effects of the breach, may require it to do so. The notification to the subscriber or individual shall at least describe the nature of the personal data breach and the contact points where more information can be obtained, and shall recommend measures to mitigate the possible adverse effects of the personal data breach. The notification to the competent national authority shall, in addition, describe the consequences of, and the measures proposed or taken by the provider to address, the personal data breach.	Upon incident	Provider of a publicly available electronic communication service	Competent national authority Subscriber to service/individual
Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending	14(1)	A gatekeeper shall inform the Commission of any intended concentration within the meaning of Article 3 of Regulation (EC) No 139/2004, where the merging entities or the target of concentration provide core platform services or any other	One-off, prior to implementing a concentration	Gatekeeper	European Commission

Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance)		services in the digital sector or enable the collection of data, irrespective of whether it is notifiable to the Commission under that Regulation or to a competent national competition authority under national merger rules. A gatekeeper shall inform the Commission of such a concentration prior to its implementation and following the conclusion of the agreement, the announcement of the public bid, or the acquisition of a controlling interest.			
Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance)	14(3)	If, following any concentration referred to in paragraph 1 of this Article, additional core platform services individually meet the thresholds in Article 3(2), point (b), the gatekeeper concerned shall inform the Commission thereof within 2 months from the implementation of the concentration and provide the Commission with the information referred to in Article 3(2).	One-off, within 2 months from the implementation of the concentration	Gatekeeper	European Commission
Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance)	18	Where a provider of hosting services becomes aware of any information giving rise to a suspicion that a criminal offence involving a threat to the life or safety of a person or persons has taken place, is taking place or is likely to take place, it shall promptly inform the law enforcement or judicial authorities of the Member State or Member States concerned of its suspicion and provide all relevant information available. (...)	Upon certain conditions being fulfilled	Hosting service provider	Law enforcement or judicial authorities
Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance)	36(1)(c)	Where a crisis occurs, the Commission, acting upon a recommendation of the Board may adopt a decision, requiring one or more providers of very large online platforms or of very large online search engines to take one or more of the following actions: (...) (c) report to the Commission by a certain date or at regular intervals specified in the decision, on the assessments referred to in point (a), on the precise content, implementation and qualitative and quantitative impact of the specific measures taken pursuant to point (b) and on any other issue related to those assessments or	One-off or at regular intervals	Providers of VLOP & VLOSE	European Commission

		those measures, as specified in the decision. When identifying and applying measures pursuant to point (b) of this paragraph, the service provider or providers shall take due account of the gravity of the serious threat referred to in paragraph 2, of the urgency of the measures and of the actual or potential implications for the rights and legitimate interests of all parties concerned, including the possible failure of the measures to respect the fundamental rights enshrined in the Charter.			
Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the internal market and amending Directive 2010/13/EU (European Media Freedom Act)	22(1)	Member States shall lay down, in national law, substantive and procedural rules which allow for an assessment of media market concentrations that could have a significant impact on media pluralism and editorial independence. Those rules shall: (…) (b) require the parties involved in such a media market concentration to notify the concentration in advance to the relevant national authorities or bodies or provide such authorities or bodies with appropriate powers to obtain information from those parties which is necessary to assess the concentration; (...) (d) set out in advance objective, non-discriminatory and proportionate criteria for notifying such media market concentrations ...	One-off, before a media market concentration that could have a significant impact on media pluralism and editorial independence	Member States Relevant national authorities or bodies Parties involved in media market concentrations that could have a significant impact on media pluralism and editorial independence	Relevant national authorities or bodies
Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance)	14(1)	A manufacturer shall notify any actively exploited vulnerability contained in the product with digital elements that it becomes aware of simultaneously to the CSIRT designated as coordinator, in accordance with paragraph 7 of this Article, and to ENISA. The manufacturer shall notify that actively exploited vulnerability via the single reporting platform established pursuant to Article 16	Upon certain conditions being fulfilled	Manufacturer	CSIRT designated as coordinator, ENISA
Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive	14(3)	A manufacturer shall notify any severe incident having an impact on the security of the product with digital elements that it becomes aware of simultaneously to the CSIRT designated as coordinator, in accordance with paragraph 7 of this Article, and to ENISA. The manufacturer shall notify that incident via the single reporting platform established pursuant to Article 16.	Upon certain conditions being fulfilled	Manufacturer	CSIRT designated as coordinator, ENISA

(EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance)					
Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance)	14(8)	After becoming aware of an actively exploited vulnerability or a severe incident having an impact on the security of the product with digital elements, the manufacturer shall inform the impacted users of the product with digital elements, and where appropriate all users, of that vulnerability or incident and, where necessary, of any risk mitigation and corrective measures that the users can deploy to mitigate the impact of that vulnerability or incident, where appropriate in a structured, machine-readable format that is easily automatically processable. Where the manufacturer fails to inform the users of the product with digital elements in a timely manner, the notified CSIRTs designated as coordinators may provide such information to the users when considered to be proportionate and necessary for preventing or mitigating the impact of that vulnerability or incident	Upon certain conditions being fulfilled	Manufacturer	Impacted users , and where appropriate all users
Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance)	19(3)	Where an importer considers or has reason to believe that a product with digital elements or the processes put in place by the manufacturer are not in conformity with this Regulation, the importer shall not place the product on the market until that product or the processes put in place by the manufacturer have been brought into conformity with this Regulation. Furthermore, where the product with digital elements presents a significant cybersecurity risk, the importer shall inform the manufacturer and the market surveillance authorities to that effect. Where an importer has reason to believe that a product with digital elements may present a significant cybersecurity risk in light of non-technical risk factors, the importer shall inform the market surveillance authorities to that effect. Upon receipt of such information, the market surveillance authorities shall follow the procedures referred to in Article 54(2).	Upon certain conditions being fulfilled	Importer	Manufacturer and market surveillance authorities
Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity	19(5)	Importers who know or have reason to believe that a product with digital elements which they have placed on the market is not in conformity with this Regulation shall immediately take	Upon certain conditions being fulfilled	Importer	Manufacturer and market surveillance authorities, as applicable

requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance)		the corrective measures necessary to ensure that the product with digital elements is brought into conformity with this Regulation, or to withdraw or recall the product, if appropriate. Upon becoming aware of a vulnerability in the product with digital elements, importers shall inform the manufacturer without undue delay about that vulnerability. Furthermore, where the product with digital elements presents a significant cybersecurity risk, importers shall immediately inform the market surveillance authorities of the Member States in which they have made the product with digital elements available on the market to that effect, giving details, in particular, of non-compliance and of any corrective measures taken.			
Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance)	19(8)	Where the importer of a product with digital elements becomes aware that the manufacturer of that product has ceased its operations and, as result, is not able to comply with the obligations laid down in this Regulation, the importer shall inform the relevant market surveillance authorities about this situation, as well as, by any means available and to the extent possible, the users of the products with digital elements placed on the market	Upon awareness of a manufacturer's ending of operations	Importer	Market surveillance authorities
Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance)	20(3)	Where a distributor considers or has reason to believe, on the basis of information in its possession, that a product with digital elements or the processes put in place by the manufacturer are not in conformity with the essential cybersecurity requirements set out in Annex I, the distributor shall not make the product with digital elements available on the market until that product or the processes put in place by the manufacturer have been brought into conformity with this Regulation. Furthermore, where the product with digital elements poses a significant cybersecurity risk, the distributor shall inform, without undue delay, the manufacturer and the market surveillance authorities to that effect.	Upon certain conditions being fulfilled	Distributor	Manufacturer and market surveillance authorities
Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity	20(4)	Distributors who know or have reason to believe, on the basis of information in their possession, that a product with digital elements, which they have made available on the market, or the	Upon certain conditions being fulfilled	Distributor	Manufacturer and market surveillance authorities, as applicable

requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance)		processes put in place by its manufacturer are not in conformity with this Regulation shall make sure that the corrective measures necessary to bring that product with digital elements or the processes put in place by its manufacturer into conformity, or to withdraw or recall the product, if appropriate, are taken. Upon becoming aware of a vulnerability in the product with digital elements, distributors shall inform the manufacturer without undue delay about that vulnerability. Furthermore, where the product with digital elements presents a significant cybersecurity risk, distributors shall immediately inform the market surveillance authorities of the Member States in which they have made the product with digital elements available on the market to that effect, giving details, in particular, of the non-compliance and of any corrective measures taken.			
Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance)	20(6)	Where the distributor of a product with digital elements becomes aware, on the basis of information in its possession, that the manufacturer of that product has ceased its operations and, as result, is not able to comply with the obligations laid down in this Regulation, the distributor shall inform, without undue delay, the relevant market surveillance authorities about this situation, as well as, by any means available and to the extent possible, the users of the products with digital elements placed on the market.	Upon awareness of a manufacturer's ending of operations	Distributor	Market surveillance authorities
Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC	19a(1)(b)	Notify the supervisory body, the identifiable affected individuals, the public if it is of public interest and, where applicable, other relevant competent authorities, of any security breaches or disruptions in the provision of the service or the implementation of the measures […] that have a significant impact on the trust service provided or on the personal data maintained therein, without undue delay and in any case no later than 24 hours of having become aware of any security breaches or disruptions.	Upon awareness of breach or disruption	Non-qualified trust service providers	Supervisory body Identifiable affected individuals Public (if necessary in the public interest) Other competent authorities (where applicable)
Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and	24(2)(fb)	Notify the supervisory body, the identifiable affected individuals, other relevant competent bodies where applicable and, at the request of the supervisory body, the public if it is of	Upon awareness of breach or disruption	Qualified trust service providers	Supervisory body, identifiable affected individuals, general public (if necessary in the public interest), other

trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC		public interest, of any security breaches or disruptions in the provision of the service […] that have a significant impact on the trust service provided or on the personal data maintained therein, without undue delay and in any event within 24 hours of the incident.			competent authorities (where applicable)
Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC	19a(1)(b)	Notify the supervisory body, the identifiable affected individuals, the public if it is of public interest and, where applicable, other relevant competent authorities, of any security breaches or disruptions in the provision of the service or the implementation of the measures […] that have a significant impact on the trust service provided or on the personal data maintained therein, without undue delay and in any case no later than 24 hours of having become aware of any security breaches or disruptions.	Upon awareness of breach or disruption	Non-qualified trust service providers	Supervisory body Identifiable affected individuals Public (if necessary in the public interest) Other competent authorities (where applicable)
Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC	24(2)(fb)	Notify the supervisory body, the identifiable affected individuals, other relevant competent bodies where applicable and, at the request of the supervisory body, the public if it is of public interest, of any security breaches or disruptions in the provision of the service […] that have a significant impact on the trust service provided or on the personal data maintained therein, without undue delay and in any event within 24 hours of the incident.	Upon awareness of breach or disruption	Qualified trust service providers	Supervisory body Identifiable affected individuals Public (if necessary in the public interest) Other competent authorities (where applicable)
Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC	45a(3)	Notification by a provider of a web-browser to the Commission where the provider takes precautionary measures in the event of substantiated concerns related to security breaches or the loss of integrity of an identified certificate or set of certificates. The provider shall notify its concerns in writing together with a description of the measures taken to mitigate those concerns.	Upon concerns related to security breach of loss of integrity of (an) identified certificate(s)	Web-browser providers	Commission Supervisory body Certificate holder QTSP
Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in	5e(1-3)	Member States shall notify the Commission, affected users and relying parties about any suspension, remedy, or withdrawal of an EUDI Wallet following a security breach or compromise.	Upon security breach or compromise	Member States	Commission Affected users

the internal market and repealing Directive 1999/93/EC					
Commission Implementing Regulation (EU) 2024/2977 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 as regards person identification data and electronic attestations of attributes issued to European Digital Identity Wallets	5(3)	Where providers of person identification data have revoked person identification data, they shall, through dedicated and secure channels, inform wallet users subject of those person identification data within 24 hours of the revocation and of the reasons for the revocation. This shall be done in a manner that is concise, easily accessible and using clear and plain language	Upon revocation of person identification data	Providers of person identification data	Directly to the affected wallet users
Commission Implementing Regulation (EU) 2024/2979 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 as regards the integrity and core functionalities of European Digital Identity Wallets	7(3)	Where wallet providers have revoked wallet unit attestations, they shall inform affected wallet users within 24 hours of the revocation of their wallet units, including the reason for the revocation and the consequences for the wallet user. This information shall be provided in a manner that is concise, easily accessible and using clear and plain language.	Upon revocation of wallet unit attestations	EUDIW providers	Directly to the affected wallet users.
Commission Implementing Regulation (EU) 2025/848 of 6 May 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the registration of wallet-relying parties	6(7)	When a wallet-relying party no longer intends to rely upon wallet units for the provision of public or private services under a specific registration, it shall notify the relevant registrar without undue delay and request the cancellation of that registration.	Upon withdrawal from wallet units reliance	Wallet Relying Parties	National registrar

REPORTING UPON REQUEST

Legislative act	Art.	Extracts of the legal text describing the reporting obligation	Frequency of reporting	Addressees	To whom the information needs to be reported
Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU)	6(4)	A provider who considers that an AI system referred to in Annex III is not high-risk shall document its assessment before that system is placed on the market or put into service. Such provider shall be subject to the registration obligation set out in Article 49(2). Upon request of national competent authorities, the provider shall provide the documentation of the assessment.	Upon certain conditions being fulfilled	Company Public authority	National competent authority

2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance)					
Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance)	21(1)	Providers of high-risk AI systems shall, upon a reasoned request by a competent authority, provide that authority all the information and documentation necessary to demonstrate the conformity of the high-risk AI system with the requirements set out in Section 2, in a language which can be easily understood by the authority in one of the official languages of the institutions of the Union as indicated by the Member State concerned.	Upon request	Company Public authority	National competent authority
Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance)	21(2)	Upon a reasoned request by a competent authority, providers shall also give the requesting competent authority, as applicable, access to the automatically generated logs of the high-risk AI system referred to in Article 12(1), to the extent such logs are under their control.	Upon request	Company Public authority	National competent authority
Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance)	22(3)	The authorised representative shall perform the tasks specified in the mandate received from the provider. It shall provide a copy of the mandate to the market surveillance authorities upon request, in one of the official languages of the institutions of the Union, as indicated by the competent authority.	Upon request	Company Public authority	National competent authority
Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU)	23(6)	Importers shall provide the relevant competent authorities, upon a reasoned request, with all the necessary information and documentation, including that referred to in paragraph 5, to demonstrate the conformity of a high-risk AI system with the requirements set out in Section 2 in a language which can be easily understood by them. For this purpose, they shall also ensure that the technical documentation can be made available to those authorities.	Upon request by competent authority	Company Public authority	National competent authority

2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance)					
Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance)	24(5)	Upon a reasoned request from a relevant competent authority, distributors of a high-risk AI system shall provide that authority with all the information and documentation regarding their actions pursuant to paragraphs 1 to 4 necessary to demonstrate the conformity of that system with the requirements set out in Section 2.	Upon request by competent authority	Company Public authority	National competent authority
Commission Delegated Regulation (EU) 2023/444 of 16 December 2022 supplementing Directive (EU) 2018/1972 of the European Parliament and of the Council with measures to ensure effective access to emergency services through emergency communications to the single European emergency number '112' (Text with EEA relevance)	8(2)	Member States shall provide the Commission with the information referred to in this article and Article 7 without prejudice to the initial deadlines provided therein, in the context of each data gathering that the Commission initiates for the purposes of fulfilling its obligation to report to the European Parliament and the Council pursuant to Article 109(4) of Directive (EU) 2018/1972.	At Commission's initiative	Member States	European Commission
Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030 (Text with EEA relevance)	2	Member States shall provide to the Commission in a timely manner the necessary statistics and data required for the effective monitoring of the digital transformation and of the degree of achievement of the digital targets. Those data shall, where possible, be disaggregated by gender and by region, in accordance with Union and national law. Where the relevant statistics from Member States are not available, the Commission may use an alternative data collection methodology, such as studies or direct collection of data from the Member States, in consultation with the Member States, including in order to ensure that the regional level is properly documented. The use of that alternative data collection methodology shall not affect the tasks of the Commission (Eurostat) as laid down in Commission Decision 2012/504/EU	Upon Commission's request	Member States	Commission
Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic	20(1)	Member States shall ensure that undertakings providing electronic communications networks and services, associated facilities, or associated services, provide all the information, including financial information, necessary for	Upon certain conditions being fulfilled	Undertakings	Member States

Communications Code (Recast)Text with EEA relevance.		national regulatory authorities, other competent authorities and BEREC to ensure conformity with the provisions of, or decisions or opinions adopted in accordance with, this Directive and Regulation (EU) 2018/1971 of the European Parliament and of the Council (1). In particular, national regulatory authorities and, where necessary for performing their tasks, other competent authorities shall have the power to require those undertakings to submit information concerning future network or service developments that could have an impact on the wholesale services that they make available to competitors, as well as information on electronic communications networks and associated facilities, which is disaggregated at local level and sufficiently detailed to enable the geographical survey and designation of areas in accordance with Article 22. Where the information collected in accordance with the first subparagraph is insufficient for national regulatory authorities, other competent authorities and BEREC to carry out their regulatory tasks under Union law, such information may be inquired from other relevant undertakings active in the electronic communications or closely related sectors. Undertakings designated as having significant market power on wholesale markets may also be required to submit accounting data on the retail markets that are associated with those wholesale markets. National regulatory and other competent authorities may request information from the single information points established pursuant to Directive 2014/61/EU. Any request for information shall be proportionate to the performance of the task and shall be reasoned. Undertakings shall provide the information requested promptly and in accordance with the timescales and level of detail required.			
Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast)Text with EEA relevance.	20(2)	Member States shall ensure that national regulatory and other competent authorities provide the Commission, after a reasoned request, with the information necessary for it to carry out its tasks under the TFEU. The information requested by the Commission shall be proportionate to the	Upon certain conditions being fulfilled	Member States	European Commission

		performance of those tasks. Where the information provided refers to information previously provided by undertakings at the request of the authority, such undertakings shall be informed thereof. To the extent necessary, and unless the authority that provides the information has made an explicit and reasoned request to the contrary, the Commission shall make the information provided available to another such authority in another Member State. Subject to the requirements of paragraph 3, Member States shall ensure that the information submitted to one authority can be made available to another such authority in the same or different Member State and to BEREC, after a substantiated request, where necessary to allow either authority, or BEREC, to fulfil its responsibilities under Union law.			
Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast)Text with EEA relevance.	21	Without prejudice to any information requested pursuant to Article 20 and information and reporting obligations under national law other than the general authorisation, national regulatory and other competent authorities may require undertakings to provide information with regard to the general authorisation, the rights of use or the specific obligations referred to in Article 13(2), which is proportionate and objectively justified in particular for the purposes of: (a) verifying, on a systematic or case-by-case basis, compliance with condition 1 of Part A, conditions 2 and 6 of Part D, and conditions 2 and 7 of Part E, of Annex I and of compliance with obligations as referred to in Article 13(2); (b) verifying, on a case-by-case basis, compliance with conditions as set out in Annex I where a complaint has been received or where the competent authority has other reasons to believe that a condition is not complied with or in the case of an investigation by the competent authority on its own initiative; (c) carrying out procedures for and the assessment of requests for granting rights of use;	Upon request	Undertakings	National regulatory authorities

		(d) publishing comparative overviews of quality and price of services for the benefit of consumers; (e) collating clearly defined statistics, reports or studies; (f) carrying out market analyses for the purposes of this Directive, including data on the downstream or retail markets associated with or related to the markets which are the subject of the market analysis; (g) safeguarding the efficient use and ensuring the effective management of radio spectrum and of numbering resources; (h) evaluating future network or service developments that could have an impact on wholesale services made available to competitors, on territorial coverage, on connectivity available to end-users or on the designation of areas pursuant to Article 22; (i) conducting geographical surveys; (j) responding to reasoned requests for information by BEREC. The information referred to in points (a) and (b), and (d) to (j) of the first subparagraph shall not be required prior to, or as a condition for, market access. BEREC may develop templates for information requests, where necessary, to facilitate consolidated presentation and analysis of the information obtained.			
Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast)Text with EEA relevance.	30	Member States shall ensure that their relevant competent authorities monitor and supervise compliance with the conditions of the general authorisation or of rights of use for radio spectrum and for numbering resources, with the specific obligations referred to in Article 13(2) and with the obligation to use radio spectrum effectively and efficiently in accordance with Article 4, Article 45(1) and Article 47.	Upon request	Undertakings	Member States
Directive (EU) 2017/1564 of the European Parliament and of the Council of 13 September 2017 on certain permitted uses of certain works	6(2)	Member States shall provide the information they have received pursuant to paragraph 1 to the Commission. The Commission shall make such information publicly	Upon request	Member States	European Commission

and other subject matter protected by copyright and related rights for the benefit of persons who are blind, visually impaired or otherwise print-disabled and amending Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society		available online on a central information access point and keep it up to date.			
Regulation (EU) 2018/1971 of the European Parliament and of the Council of 11 December 2018 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Agency for Support for BEREC (BEREC Office), amending Regulation (EU) 2015/2120 and repealing Regulation (EC) No 1211/2009 (Text with EEA relevance)	40(4)	Where information is not made available by the NRAs in a timely manner, BEREC or the BEREC Office may address a reasoned request either to other NRAs and other competent authorities of the Member State concerned, or directly to the relevant undertakings providing electronic communications networks, services and associated facilities.	Upon request	Companies	BEREC
Regulation (EU) 2018/1971 of the European Parliament and of the Council of 11 December 2018 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Agency for Support for BEREC (BEREC Office), amending Regulation (EU) 2015/2120 and repealing Regulation (EC) No 1211/2009Text with EEA relevance.	Article 5, Article 9, Article 10	The BEREC Office shall have the following tasks: (...) (b) to collect information from NRAs and to exchange and transmit information in relation to the regulatory tasks assigned to BEREC pursuant to Article 4;	Upon request	National regulatory authorities	BEREC
Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance)	11(1)	Within 6 months after its designation pursuant to Article 3, and in accordance with Article 3(10), the gatekeeper shall provide the Commission with a report describing in a detailed and transparent manner the measures it has implemented to ensure compliance with the obligations laid down in Articles 5, 6 and 7.	Upon designation as a gatekeeper	Gatekeeper	European Commission
Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937	15(1)	Within 6 months after its designation pursuant to Article 3, a gatekeeper shall submit to the Commission an independently audited description of any techniques for profiling of consumers that the gatekeeper applies to or across its core platform services listed in the designation	One-off, within 6 months after designation	Gatekeeper	European Commission

and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance)		decision pursuant to Article 3(9). The Commission shall transmit that audited description to the European Data Protection Board.			
Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance)	9	Upon the receipt of an order to act against one or more specific items of illegal content, issued by the relevant national judicial or administrative authorities, on the basis of the applicable Union law or national law in compliance with Union law, providers of intermediary services shall inform the authority issuing the order, or any other authority specified in the order, of any effect given to the order without undue delay, specifying if and when effect was given to the order.	Upon request	Intermediary service providers	Authority issuing the order or any other authority specified in the order
Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance)	10	Upon receipt of an order to provide specific information about one or more specific individual recipients of the service, issued by the relevant national judicial or administrative authorities on the basis of the applicable Union law or national law in compliance with Union law, providers of intermediary services shall, without undue delay inform the authority issuing the order, or any other authority specified in the order, of its receipt and of the effect given to the order, specifying if and when effect was given to the order. (...)	Upon request	Intermediary service providers	Authority issuing the order or any other authority specified in the order
Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance)	24(3)	Providers of online platforms or of online search engines shall communicate to the Digital Services Coordinator of establishment and the Commission, upon their request and without undue delay, the information referred to in paragraph 2, updated to the moment of such request. That Digital Services Coordinator or the Commission may require the provider of the online platform or of the online search engine to provide additional information as regards the calculation referred to in that paragraph, including explanations and substantiation in respect of the data used. That information shall not include personal data	Upon request	Online platforms and search engines	Digital Services Coordinators and the Commission

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance)	24(5)	Providers of online platforms shall, without undue delay, submit to the Commission the decisions and the statements of reasons referred to in Article 17(1) for the inclusion in a publicly accessible machine-readable database managed by the Commission. Providers of online platforms shall ensure that the information submitted does not contain personal data.	Upon request	Providers of online platforms	European Commission
Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance)	34(3)	Providers of very large online platforms and of very large online search engines shall preserve the supporting documents of the risk assessments for at least three years after the performance of risk assessments, and shall, upon request, communicate them to the Commission and to the Digital Services Coordinator of establishment.	Upon request	Providers of VLOPS and VLOSES	Digital Services Coordinators and the Commission
Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance)	41(4)	Providers of very large online platforms or of very large online search engines shall communicate the name and contact details of the head of the compliance function to the Digital Services Coordinator of establishment and to the Commission.	One-off, with periodical updating	Providers of VLOP & VLOSE	European Commission, DSC
Regulation (EU) 2022/612 of the European Parliament and of the Council of 6 April 2022 on roaming on public mobile communications networks within the Union (recast) (Text with EEA relevance)	3(6)	The visited network operator may terminate the wholesale roaming agreement unilaterally on grounds of permanent roaming or anomalous or abusive use of wholesale roaming access only upon prior authorisation of the visited network operator's national regulatory authority. Within three months of receipt of a request by the visited network operator for authorisation to terminate a wholesale roaming agreement, the national regulatory authority of the visited network operator shall, after consulting the national regulatory authority of the home network operator, decide whether to grant or refuse such authorisation and shall inform the Commission accordingly. The national regulatory authorities of the visited network operator and of the home network operator may each request BEREC to adopt an opinion with regard to the action to be taken in accordance with this Regulation. BEREC shall adopt its opinion within one	Upon certain conditions being fulfilled	Operators	NRA (BEREC optional)

		month of receipt of such a request. Where BEREC has been consulted, the national regulatory authority of the visited network operator shall await and take the utmost account of BEREC's opinion before deciding, subject to the three-month deadline referred to in the sixth subparagraph, whether to grant or refuse authorisation for the termination of the wholesale roaming agreement. The national regulatory authority of the visited network operator shall make information concerning authorisations to terminate wholesale roaming agreements available to the public, subject to business confidentiality. The fifth to ninth subparagraphs of this paragraph shall be without prejudice to the power of a national regulatory authority to require the immediate cessation of a breach of the obligations set out in this Regulation pursuant to Article 17(7) and to the right of the visited network operator to apply adequate measures in order to combat fraud.			
Regulation (EU) 2022/612 of the European Parliament and of the Council of 6 April 2022 on roaming on public mobile communications networks within the Union (recast) (Text with EEA relevance)	16	By 31 December 2022, BEREC shall establish, and subsequently maintain: (a) a single, Union-wide database of numbering ranges for value-added services in each Member State, to be made accessible to operators, national regulatory authorities and, where applicable, to other competent authorities; and (b) a single, Union-wide database of means of access to emergency services that are mandated in each Member State and that are technically feasible to be used by roaming customers, to be made accessible to operators and national regulatory authorities and, where applicable, to other competent authorities. For the purposes of the establishment and maintenance of the databases referred to in the first paragraph, the national regulatory authorities or other competent authorities shall provide the necessary information and the relevant updates to BEREC by electronic means without undue delay. Without prejudice to Article 13, the databases referred to in the first paragraph shall enable national regulatory authorities and other competent authorities, on an optional basis, to provide additional information.	Upon request	NRA	BEREC

Regulation (EU) 2022/612 of the European Parliament and of the Council of 6 April 2022 on roaming on public mobile communications networks within the Union (recast) (Text with EEA relevance)	17	National regulatory authorities and, where applicable, other competent authorities shall have the power to require undertakings subject to obligations under this Regulation to supply all information relevant to the implementation and enforcement of this Regulation. Those undertakings shall provide such information promptly on request and in accordance with time limits and level of detail required by the national regulatory authority and, where applicable, other competent authorities.	Upon request	Operators / undertakings	NRA
Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance)	13(22)	Manufacturers shall, upon a reasoned request from a market surveillance authority, provide that authority, in a language which can be easily understood by that authority, with all the information and documentation, in paper or electronic form, necessary to demonstrate the conformity of the product with digital elements and of the processes put in place by the manufacturer with the essential cybersecurity requirements set out in Annex I. Manufacturers shall cooperate with that authority, at its request, on any measures taken to eliminate the cybersecurity risks posed by the product with digital elements which they have placed on the market.	Upon request	Manufacturer	Market surveillance authority
Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance)	18(3)(b)	An authorised representative shall perform the tasks specified in the mandate received from the manufacturer. The authorised representative shall provide a copy of the mandate to the market surveillance authorities upon request. The mandate shall allow the authorised representative to do at least the following: [...] further to a reasoned request from a market surveillance authority, provide that authority with all the information and documentation necessary to demonstrate the conformity of the product with digital elements	Upon request	Authorised representative	Market surveillance authority
Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024	19(7)	Importers shall, further to a reasoned request from a market surveillance authority, provide it with all the	Upon request	Importer	Market surveillance authority

on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance)		information and documentation, in paper or electronic form, necessary to demonstrate the conformity of the product with digital elements with the essential cybersecurity requirements set out in Part I of Annex I as well as of the processes put in place by the manufacturer with the essential cybersecurity requirements set out in Part II of Annex I in a language that can be easily understood by that authority. They shall cooperate with that authority, at its request, on any measures taken to eliminate the cybersecurity risks posed by a product with digital elements, which they have placed on the market.			
Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance)	20(5)	Distributors shall, further to a reasoned request from a market surveillance authority, provide all the information and documentation, in paper or electronic form, necessary to demonstrate the conformity of the product with digital elements and the processes put in place by its manufacturer with this Regulation in a language that can be easily understood by that authority. They shall cooperate with that authority, at its request, on any measures taken to eliminate the cybersecurity risks posed by a product with digital elements which they have made available on the market.	Upon request	Distributor	Market surveillance authorities
Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance)	24(2)	Open-source software stewards shall cooperate with the market surveillance authorities, at their request, with a view to mitigating the cybersecurity risks posed by a product with digital elements qualifying as free and open-source software. Further to a reasoned request from a market surveillance authority, open-source software stewards shall provide that authority, in a language which can be easily understood by that authority, with the documentation referred to in paragraph 1, in paper or electronic form.	Upon request	Open-source stewards	Market surveillance authorities
Commission Decision 2005/50/EC on the harmonisation of the 24 GHz range radio spectrum band for the time-limited use by automotive short-	7	Each Member State shall determine the relevant national radio astronomy stations to be protected pursuant to Article 6(2) in its territory and the characteristics of the	Upon Commission request	Member States	European Commission

range radar equipment in the Community. Implementation table (15/01/2020) as amended by Commission Implementing Decision (EU) 2017/2077 of 10 November 2017		exclusion zones pertaining to each station. This information, supported by appropriate justification, shall be notified to the Commission within six months of adoption of this Decision, and published in the Official Journal of the European Union.			
Commission Decision 2007/98/EC of 14 February 2007 on the harmonised use of radio spectrum in the 2 GHz frequency bands for the implementation of systems providing mobile satellite services (notified under document number C(2007) 409) (Text with EEA relevance)	4	Member States shall keep the use of the relevant bands under scrutiny and report their findings to the Commission to allow for a review of this Decision if necessary.	Upon Commission's request	Member States	European Commission
Commission Decision 2008/294/EC as amended by commission implementing decision 2013/654/EU of 12 November 2013, Commission Implementing Decision (EU) 2016/2317 of 16 December 2016, commission implementing decision (EU) 2022/2324 of 23 November 2022 mobile communications services on aircraft (MCA services)	5	Member States shall keep use of spectrum by MCA services under scrutiny, in particular with regard to actual or potential harmful interference and to the continued relevance of all the conditions specified in Article 3, and shall report their findings to the Commission to allow a timely review of this Decision if necessary.	Upon Commission's request	Member States	European Commission
Commission Decision 2008/411/EC of 21 May 2008 on the harmonisation of the 3400 - 3800 MHz frequency band for terrestrial systems capable of providing electronic communications services in the Community (notified under document number C(2008) 1873) (Text with EEA relevance) as amended by commission implementing decision 2014/276/EU of 2 May 2014 and commission implementing decision (EU) 2019/235 of 24 January 2019	4	Member States shall keep the use of the 3 400-3 800 MHz band under scrutiny and report their findings to the Commission to allow regular and timely review of the Decision.	Upon Commission's request	Member States	European Commission
Commission Decision 2009/766/EC on the harmonisation of the 900 MHz and 1800 MHz frequency bands for terrestrial systems capable of providing pan-European electronic	6	Member States shall keep the use of the 900 MHz and 1 800 MHz bands under permanent review to ensure the efficient use thereof, and in particular report as soon as	Upon Commission's request	Member States	European Commission

communications services in the Community as regards relevant technical conditions for the Internet of Things. Implementation table (21/03/2022) as repealed by commission implementing decision (EU) 2022/173 of 7 February 2022		necessary to the Commission any need for a revision of this Decision, in compliance with EU law.			
Commission Decision 2010/166/EU, in order to introduce new technologies and frequency bands for mobile communication services on board vessels (MCV services) in the European Union as repealed by commission implementing decision (EU) 2024/340 of 22 January 2024	5	Member States shall submit a report to the Commission on their findings with regard to the review referred to in Article 4. The European Commission shall, where appropriate, proceed to a review of this Decision.	Upon Commission's request	Member States	European Commission
Commission Decision 2010/267/EU of 6 May 2010 on harmonised technical conditions of use in the 790-862 MHz frequency band for terrestrial systems capable of providing electronic communications services in the European Union	3	Member States shall keep the use of the 800 MHz band under scrutiny and report their findings to the Commission upon request. The Commission shall, were appropriate, proceed to a review of this Decision.	Upon Commission's request	Member States	European Commission
Commission Implementing Decision (EU) 2016/339 of 8 March 2016 on the harmonisation of the 2 010-2 025 MHz frequency band for portable or mobile wireless video links and cordless cameras used for programme making and special events	4	Member States shall keep the use of the 2 010-2 025 MHz frequency band under scrutiny and report their findings to the Commission, including any information on the amendment or withdrawal of rights of use, in order to allow a timely review of this Decision if necessary.	Upon Commission's request	Member States	European Commission
Commission Implementing Decision (EU) 2016/687 of 28 April 2016 on the harmonisation of the 694-790 MHz frequency band for terrestrial systems capable of providing wireless broadband electronic communications services and for flexible national use in the Union (notified under document C(2016) 2268) (Text with EEA relevance)	6	Member States shall monitor the use of the 700 MHz frequency band and report their findings to the Commission upon request or at their own initiative in order to allow timely review of this Decision, as appropriate.	Upon Commission's request	Member States	European Commission

Commission Implementing Decision (EU) 2018/1538 of 11 October 2018 on the harmonisation of radio spectrum for use by short-range devices within the 874-876 and 915-921 MHz frequency bands (notified under document C(2018) 6535) (Text with EEA relevance.)	4	Member States shall monitor the use of the 874-876 MHz and 915-921 MHz frequency bands, including the potential use of the 874,4-876 MHz and 919,4-921 MHz sub-bands for the future railway mobile communications system (FRMCS), and report their findings to the Commission upon request or at their own initiative in order to allow regular and timely review of the Decision.	Upon Commission's request	Member States	European Commission
Commission Implementing Decision (EU) 2019/784 of 14 May 2019 on harmonisation of the 24,25-27,5 GHz frequency band for terrestrial systems capable of providing wireless broadband electronic communications services in the Union (notified under document C(2019) 3450) (Text with EEA relevance.) as amended by Commission Implementing Decision (EU) 2020/590 of 24 April 2020	7	(…) Member States shall monitor the use of the 24,25-27,5 GHz frequency band, including the progress on co-existence between the terrestrial systems referred to in Article 1 and other systems using the band, and report their findings to the Commission upon request or at their own initiative to allow a timely review of this Decision.	Upon Commission's request	Member States	European Commission
Commission Implementing Decision (EU) 2019/785 of 14 May 2019 on the harmonisation of radio spectrum for equipment using ultra-wideband technology in the Union and repealing Decision 2007/131/EC (notified under document C(2019) 3461) (Text with EEA relevance.) as amended by Commission Implementing Decision (EU) 2024/1467	4	Member States shall monitor the use of the bands identified in the Annex by equipment using ultra-wideband technology, in particular to ensure that all the conditions laid down in Article 3 of this Decision continue to be relevant, and report their findings to the Commission.	Upon Commission's request	Member States	European Commission
Commission Implementing Decision (EU) 2021/1730 of 28 September 2021 on the harmonised use of the paired frequency bands 874,4-880,0 MHz and 919,4-925,0 MHz and of the unpaired frequency band 1900-1910 MHz for Railway Mobile Radio (notified under document C(2021) 6862) (Text with EEA relevance)	4	(…) Member States shall monitor the use by RMR of the frequency bands subject to this Decision and report their findings, including any impacts on interoperability related to spectrum issues, to the Commission upon request or at their own initiative to allow a timely review of this Decision, where needed.	Upon Commission's request	Member States	European Commission

Commission Implementing Decision (EU) 2022/173 of 7 February 2022 on the harmonisation of the 900 MHz and 1800 MHz frequency bands for terrestrial systems capable of providing electronic communications services in the Union and repealing Decision 2009/766/EC (notified under document C(2022) 605) (Text with EEA relevance)	6	Member States shall keep the use of the 900 MHz and 1 800 MHz bands under permanent review to ensure the efficient use thereof, and in particular report as soon as necessary to the Commission any need for a revision of this Decision, in compliance with EU law.	Upon Commission's request	Member States	European Commission
Commission Implementing Decision (EU) 2022/179 of 8 February 2022 on the harmonised use of radio spectrum in the 5 GHz frequency band for the implementation of wireless access systems including radio local area networks and repealing Decision 2005/513/EC (notified under document C(2022) 628) (Text with EEA relevance)	4	Member States shall monitor the evolution of standards and technology in relation to the use of the 5 150-5 250 MHz, 5 250-5 350 MHz and 5 470-5 725 MHz frequency bands for WAS/RLANs and report their findings to the Commission at the latter's request or on their own initiative in order to allow for a timely review of this Decision.	Upon Commission's request	Member States	European Commission
Commission Implementing Decision 2013/195/EU defining the practical arrangements, uniform formats and a methodology in relation to the radio spectrum inventory established by Decision No 243/2012/EU of the European Parliament and of the Council establishing a multiannual radio spectrum policy programme	6	In order to assist the Commission in reporting on the functioning of the radio spectrum inventory, Member States shall provide the Commission with information on the application and effectiveness of this decision.	Upon Commission's request	Member States	European Commission
Commission Implementing Decision (EU) 2024/1983 on the harmonisation of the 40,5-43,5 GHz frequency band for terrestrial systems capable of providing wireless broadband electronic communications services in the Union	7	Member States shall provide the Commission with all necessary information on the implementation of this Decision immediately after the adoption of the relevant national measures.	Upon Commission's request	Member States	European Commission
Commission Implementing Decision (EU) 2024/340 of 22 January 2024 on harmonised conditions for the use of radio spectrum for mobile communication services on board vessels in the Union, repealing Decision 2010/166/EU	5	Member States shall submit a report to the Commission on their findings with regard to the review referred to in Article 4. The European Commission shall, where appropriate, proceed to a review of this Decision.	Upon Commission's request	Member States	European Commission

Commission Implementing Decision 2012/688/EU of 5 November 2012 on the harmonisation of the frequency bands 1920 - 1980 MHz and 2110 - 2170 MHz for terrestrial systems capable of providing electronic communications services in the Union (notified under document C(2012) 7697) Text with EEA relevance as amended by Commission Implementing Decision (EU) 2020/667 of 6 May 2020		Member States shall keep the use of the paired terrestrial 2 GHz band under scrutiny and report their findings to the Commission to allow regular and timely review of this Decision.	Upon Commission's request	Member States	European Commission
Commission Decision 2006/771/EC on harmonisation of the radio spectrum for use by short-range devices as amended by commission decision 2008/432/EC of 23 May 2008, COMMISSION DECISION 2009/381/EC of 13 May 2009, Commission decision 2010/368/EU of 30 June 2010, commission implementing decision 2011/829/EU of 8 December 2011, commission implementing decision 2013/752/EU, of 11 December 2013 Commission Implementing Decision (EU) 2017/1483 of 08 August 2017, COMMISSION IMPLEMENTING DECISION (EU) 2019/1345 of 2 August 2019, commission implementing decision (EU) 2022/180 of 8 February 2022 and commission implementing decision (EU) 2025/105 of 22 January 2025 [to be checked if separate Acts or amendments of the same Act]	4	Member States shall keep the use of the relevant bands under scrutiny and report their findings to the Commission to allow regular and timely review of the Decision.	Upon Commission's request	Member States	European Commission
Commission Delegated Regulation (EU) 2023/1127 of 2 March 2023 supplementing Regulation (EU) 2022/2065 of the European Parliament and of the Council with the detailed methodologies and procedures regarding the supervisory fees charged by the Commission on providers of very large online platforms and very large online search engines (Text with EEA relevance)	6(3)	At the latest by 30 September of each year, the Commission shall communicate to each provider of designated service or services identified pursuant to Article 3 the provisional determination of the amount of supervisory fee for all designated services provided by that provider calculated in accordance with the methodology set out in Articles 4 and 5. The provider shall communicate to the Commission any observation on such calculation within two weeks from receipt of the communication of that provisional determination.	Annually	Providers of VLOPs & VLOSEs	European Commission