Council of the European Union

Brussels, 20 November 2025
(OR. en)

15698/25

Interinstitutional File:
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.:	COM(2025) 837 final
Subject:	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)

Delegations will find attached document COM(2025) 837 final.

Encl.: COM(2025) 837 final

EUROPEAN
COMMISSION

Brussels, 19.11.2025
COM(2025) 837 final

2025/0360 (COD)

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)

{SWD(2025) 836 final}

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

• Reasons for and objectives of the proposal

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 the EU acquis, as a key measure to support the EU's competitiveness.

This vision reflects the broader plan 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'. They also 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 emphasised the need for simplification to facilitate business compliance without compromising the EU's core policy objectives.

In the Commission's consultation and engagement activities around the simplification agenda, stakeholders representing different interests have called for targeted amendments of certain

---

[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)

digital rules, to both streamline compliance costs and clarify interplays between rules in their sector.

With a value added of EUR 791 billion across the European Union in 2022[9], the ICT sector plays a crucial role in driving the EU's competitiveness across all sectors of the economy, both through the growth of digital businesses and offering key digital solutions across the board. Digital rules have been instrumental in framing a fair business environment in the EU. They established a true single market for digital services. The EU has pioneered digital regulation, and has set the golden standard for the highest level of protections for fundamental rights, consumer safety and the protection of European values.

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.

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[10]), 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

[10] As per separate legal proposal

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 legislation and Regulation (EU) 2024/1689 (the Artificial Intelligence Act[11]), 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.

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.

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 initiatives, the Commission is expecting to publish in 2026 a review of the

[11] As per separate proposal

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 an 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.

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 regulatory framework, 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, and guidelines for clarifying definitions.

To support the application of the Artificial Intelligence Act, the Commission continues to prioritise issuing guidelines on several aspects, as further detailed in the explanatory memorandum for the Digital Omnibus proposal amending the Artificial Intelligence Act.

Proposals in the Digital Omnibus

The 'data legislative acquis' was extended over the past years to a range of regulations, creating legal complexity, including some overlaps, not perfectly aligned definitions and questions on the interplay of the instruments. Notably, Regulation (EU) 2018/1807 (Free Flow of Non-Personal Data Regulation) was adopted and was designed to create a single market for cloud services. It has been partially superseded by Chapter VI of Regulation (EU) 2023/2854 (Data Act) which lays down obligations on switching between data processing services.

Another case in point is Chapter II of Regulation (EU) 2022/868 (the Data Governance Act) which complements the rules on re-use of public sector information in Directive (EU) 2019/1024 (the Open Data Directive) for data that cannot be re-used without restrictions. In addition, other chapters of Regulation (EU) 2022/868 (the Data Governance Act) created rules on data intermediation services, data altruism, requirements for foreign government access requests to non-personal data and created the European Data Innovation Board. Regulation (EU) 2023/2854 (the Data Act), on the other hand, created material obligation on manufacturers of connected devices and providers of related services to share data with their users, or on business to share data with government agencies as well as rules on fair data sharing contracts.

To address this, the Omnibus proposes to repeal outdated rules, especially current rules of Regulation (EU) 2018/1807 (the Free Flow of Non-personal Data Regulation (FFDR) with the exception of the prohibition of data localisation requirements in the Union and consolidate and streamline rules in Regulation (EU) 2022/868 (Data Governance Act, DGA), such as the rules on data altruism and data intermediation services to boost the attractiveness of those data sharing mechanisms. At the same time, the Data Governance Act's rules on the re-use of protected data is merged with the rules of Directive (EU) 2019/1024 (the Open Data Directive) to create a single framework for re-use of data held by public sector bodies reflected into Regulation (EU) 2023/2854 (the Data Act Regulation). 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.

The proposal further introduces the possibility for public sector bodies to set out different conditions and charge higher fees for the re-use by very large enterprises and in particular undertakings designated as gatekeepers, as defined under Article 3 of Regulation (EU) 2022/1925 (Digital Markets Act), 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.

The proposal includes the consolidated and streamlined rules of Regulation (EU) 2024/1689 (Free Flow of Data Regulation), Regulation (EU) 2022/868 (Data Governance Act) and Directive (EU) 2019/1024 (the Open Data Directive) in Regulation (EU) 2023/2854 (Data Act), creating one single consolidated instrument for Europe's data economy. Regulation (EU) 2024/1689) (Free Flow of Data Regulation), Directive (EU) 2019/1024 (Open Data Directive) and Regulation (EU) 2022/868 (Data Governance Act) are repealed. The rules across all four instruments are better aligned and streamlined to enhance clarity and consistency, thereby increasing their effectiveness and supporting businesses in driving innovation. This initiative is in accordance with the Data Union Strategy, which fundamentally aims to drive the simplification of the legislative framework.

In addition, to further assist smaller businesses, the rules that facilitate compliance with the EU data legislation for small and medium-sized enterprises (SMEs) are extended to include small mid-cap companies (SMCs). Regulation (EU) 2023/2854 (Data Act), which entered into application on 12 September 2025, marks a significant step towards a fair and competitive data economy in the EU. The changes put forward in this proposal do not intend to introduce changes to the achievements of Regulation (EU) 2023/2854 (Data Act).

However, to fully achieve its objective of balancing innovation and data availability with the protection of data holders' rights and interest, four key elements require calibration. Specifically, it is crucial to ensure Regulation (EU) 2023/2854 (Data Act) not only reduces burdens but also boosts legal clarity and drive competitiveness. First, there is an urgent need to strengthen safeguards against the risk of trade secret leaks to third countries in the context of the mandatory IoT data-sharing provisions. Second, the extensive scope of the business-to-government framework could potentially result in legal ambiguity. Third, legal uncertainty could result from the provisions on essential requirements for smart contracts executing data sharing agreements. Finally, the provisions of Regulation (EU) 2023/2854 (the Data Act) provisions on switching between data processing services retain their relevance as a central contribution towards a more open and competitive cloud market. Nevertheless, these provisions did not sufficiently account for the specific situation of services that to be usable are significantly customised to the needs of a customer or are provided by SMEs and SMCs. The amendments contained in this proposal will maintain the ambition of removing vendor lock-in, particularly switching and egress charges, while reducing the administrative burden on providers of the aforementioned services. The proposal thus puts forward amendments that enhance legal clarity and are strongly aligned with the overall objectives of Regulation (EU) 2023/2854 (the Data Act).

In addition, to further assist smaller businesses the rules that facilitate compliance with the EU data acquis for small and medium-sized enterprises (SMEs) are extended to include small mid-cap companies (SMCs).

As regards personal data, Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and free movement of such data (General Data Protection Regulation GDPR) became applicable on 25 May 2018, creating Union wide standards, rules and safeguards for the processing of individuals' personal data, the rights of data subjects as well as a general legal framework for those processing personal data. While stakeholders have in general found Regulation (EU) 2016/679 (General Data Protection Regulation) balanced and sound and which continues to be fit for purpose, some entities, especially smaller companies and associations with a low number of non-intensive, often low-risk data processing operations, expressed concerns regarding the application of some obligations of the General Data Protection Regulation. Some of these concerns can be addressed through a more consistent and harmonised interpretation and enforcement across Member States, while others require targeted amendments of the legislation. In this context, the amendments contained in this proposal aim to address those concerns notably by clarifying certain key definitions, for instance the notions of personal data; by facilitating compliance, for instance by supporting controllers with respect to the criteria and means to determine whether data resulting from pseudonymisation does not constitute personal data, in relation to information requirements and data breach notifications to supervisory authorities; as well as by clarifying certain aspects as to the processing of data for AI training and development. The proposed amendments address also the lack of clarity about the conditions for scientific research by providing a definition of scientific research, further clarifying that further processing for scientific purposes is compatible with the initial purpose of processing and by clarifying that scientific research constitutes a legitimate interest. It is also proposed to extend the exceptions from the information obligation for processing. Where relevant, this proposal reflects the changes to the General Data Protection Regulation 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.

Further, a regulatory solution on the consent fatigue and proliferation of cookies banners is long-overdue. Directive (EU) 2002/58/EC on privacy and electronic communications ('ePrivacy Directive'), last revised in 2009 provides a framework for protecting the confidentiality of communications and specifies the Regulation (EU) 2016/679 ('General Data Protection Regulation GDPR') where processing of personal data is involved in the context of electronic communications. It also protects the terminal equipment of users which may be used to invade their privacy and collect information relating to those users. An essential part of the use of terminal equipment – such as phones and personal computers – is to consume content and use online services. Many of these online services rely on the revenue from advertising, including personalised advertising. This is also the case for media services. Online service providers rely on the so-called cookies or similar technologies that make use of the processing and storage capabilities of terminal equipment thereby accessing, for example, information stored in or emitted from the terminal equipment. This is used for a variety of purposes, such as to optimise the provision of the service for the particular terminal equipment, ensure the security of the terminal equipment and the overall service, but also to track individual's behaviour and interaction with different online services to provide personalised advertisement.

When use of such technologies is not necessary for technical storage or access 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, Directive (EU) 2002/58/EC (the ePrivacy Directive) requires consent. Such consent is typically requested via pop-up banners displayed on the website or mobile application. Such banners contain information on purposes of processing, often linked to types of cookies, recipients of data, and they are not always easy for individuals to understand. For these reasons they might not achieve their aim – to inform the individual and give control over protecting their privacy and processing of their personal data, but instead are perceived as a nuisance to internet users. At the same time, the providers of online service incur considerable costs to design compliant banners.

Increasing complexity, Article 5(3) of Directive (EU) 2002/58/EC (ePrivacy Directive) applies to the placement of cookies or similar technologies to gain information from a user's terminal equipment, while the subsequent processing of personal data is subject to Regulation (EU) 2016/679 (General Data Protection Regulation). While consent is required to ensure data subjects' control, it is not always the most appropriate legal basis for subsequent processing, for example, when processing is necessary for performance of other service than the information society service. This has led to legal uncertainty and higher compliance costs for controllers that process personal data obtained from terminal equipment. Moreover, the dual regime of ePrivacy and General Data Protection Regulation led to different national authorities being competent to supervise the rules of the two legal frameworks.

For these reasons, it is proposed to immediately simplify the interplay of the applicable rules. Processing of personal data on and from terminal equipment should be governed only by Regulation (EU) 2016/679 (General Data Protection Regulation), absorbing also the clear requirement for consent for accessing the terminal equipment of a natural person when personal data is collected. The proposed amendments also provide for certain purposes where it should not be necessary to obtain consent and where the subsequent processing should be considered lawful, in particular where they pose a low risk to the rights and freedoms of the data subjects or where the placement of such technologies is necessary for the provision of a service requested by the data subject.

Finally, the proposal paves the way for automated and machine-readable indications of individual choices and respect of those indications by website and mobile application providers and providers of mobile phone applications once standards are available. This builds on the 2009 amendment to Directive (EU) 2002/58/EC (ePrivacy Directive) (cf. Recital 66 of Directive 2009/136/EC) that already encouraged to allow expressing the user's consent by using the appropriate settings of a browser or other application where it is technically possible and effective and Article 21(5) of Regulation (EU) 2016/679 (General Data Protection Regulation), as well as the 2017 proposal of the Commission on a Regulation on Privacy and Electronic Communications (COM(2017)10) which proposed user choice management by web-browser settings. It gives the Commission a mandate to request the standardisation bodies to develop a set of standards for encoding automated and machine-readable indication of data subject's choices, and the communication of those choices from browsers to websites and from mobile phone applications to web services. Once these are available, and after a six-month grace period, controllers using website and mobile applications to provide their service are obliged to respect those encoded automated and machine-readable indications. Where controllers ensure that their websites or mobile phone applications comply with such standards, they should benefit from a presumption of compliance. On this basis, it is expected that browsers also develop relevant settings. The provisions are formulated in a technological neutral manner so that also other tools, e.g. agentic AI, could support users in making consent choices, should they be fit for ensuring compliance with the requirements of the GDPR. Considering the importance of online

revenue streams for independent journalism as an indispensable pillar of a democratic society, media service providers as defined in Regulation (EU) 2024/1083 (European Media Freedom Act) should not be obliged to respect such signals, allowing them to have a direct interaction with users in informing them and enabling them to make their consent choices..

The amendments presented in this Regulation will introduce a **single-entry point 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 burden for entities, while ensuring effective and secure flow of information about security incidents to the recipients defined in respective legislation.

The proposal establishes the obligation on ENISA to develop the single entry-point, taking into account the single-reporting platform for notifications of actively exploited vulnerabilities and sever incidents under Regulation (EU) 2024/2847 (the Cyber Resilience Act (CRA)). It mandates specific requirements for the tool, as a secure conduit of information reported by entities and dispatched to the competent authorities. It leaves unchanged the underlying legal requirements for incident reporting but optimizes significantly the workflow and the resources required from entities.

The proposal also mandates the use of the single-entry point for a series of closely interconnected incident reporting obligations set in the Directive (EU) 2022/2555 (NIS2 Directive), Regulation (EU) 2016/679 (GDPR), Regulation (EU) 2022/2554 (DORA), Regulation (EU) 910/2014 (eIDAS Regulation), and Directive (EU) 2022/2557 (CER Directive). Other sectorial reporting obligations, such as those set out in the framework of the network code on cybersecurity aspects of cross-border electricity flows (NCCS) and the relevant instruments for the aviation sector, will also be brought under the single-entry point through amendments to the respective delegated and implementing acts that establish the reporting obligations under those frameworks.

The proposal also aims at streamlining the contents of reported information by introducing empowerments for several legal acts, where such do not exist. The proposal clarifies that when developing common reporting templates for Directive (EU) 2022/2555, Directive (EU) 2022/2557 or Regulation (EU) 2016/679, in order to ensure consistency, promote synergies and reduce administrative burden on entities by minimizing the number of data fields that entities are required to complete, the Commission should take due account of the experience gained and the common templates developed under Regulation (EU) 2022/2554 (DORA).

In addition to these core changes, the proposal takes the opportunity to repeal 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'). The Regulation has been in application since 12 July 2020 and was the first step towards providing a comprehensive legal framework for the platform economy. Since its entry into application, other acts of EU law have come to regulate online intermediation services and online platforms. These include Regulation (EU) 2022/1925 (the Digital Markets Act (DMA) and Regulation (EU) 2022/2065 (the Digital Services Act (DSA) which largely overtake the provisions in the P2B Regulation. Selected provisions of the P2B Regulation will remain in place in order to ensure legal certainty for acts containing cross-references to these provisions, for instance Directive (EU) 2023/2831 on improving working conditions for platform work. In general, simplification of the regulatory framework for online platforms will reduce compliance costs due to layered and overlapping rules, as called for by stakeholders. Online intermediary service providers will benefit from increased clarity of legal provisions. Enforcement will be more targeted.

- **Consistency with existing policy provisions in the policy area**

The proposal is accompanied by a second proposal amending Regulation (EU) 2024/1689 (AI Act), composing together the 'Digital Omnibus' and marking the first, immediate step in simplifying the digital rulebook. In addition to the Digital Omnibus, the proposal for a revision of Regulation (EU) 2019/881 (Cybersecurity Act) will include among others the updated mandate of the European Union Agency for Cybersecurity (ENISA) as well as measures aiming at simplifying compliance with cybersecurity requirements.

The Digital Omnibus is part of a wider strategy for regulatory simplification announced through the Digital Package, presented more in detail in the introductory section of this explanatory memorandum.

- **Consistency with other Union policies**

The proposal is part of the Commission's agenda for the simplification of the EU's regulatory framework. The wide-scope of amended acts shows the clear potential for simplification by addressing the interplay between different rules, including where they pertain to different policy areas. This is the case for example in the digital simplification solution developed under the single-entry point for incident reporting, that leaves untouched the underlying regulatory obligations, but brings together in the same interface cybersecurity rules that apply to essential entities, those applicable to the financial sector, data protection rules, and other.

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

- **Legal basis**

The proposal is based on Articles 114 and 16 of the Treaty on the Functioning of the European Union, reflecting the legal basis of the amended acts. The appropriate legal basis for the provisions amending Regulation (EU) 2016/679 (General Data Protection Regulation) and Regulation (EU) 2018/1725 is Article 16 of the Treaty. As all other amended acts are based on Article 114 of the Treaty, the same legal basis is also appropriate for the corresponding amending provisions of this Regulation.

- **Subsidiarity (for non-exclusive competence)**

Given that the amended rules are Union rules, they can only be amended at Union level. The technical adjustments presented in this Regulation preserve the logic of subsidiarity that underpins the amended acts.

As regards Regulation (EU) 2023/2854 (Data Act), the amendments reinforce the objective of the Regulation to remove barriers in the single market for the data-driven economy. They do so by appending into the Regulation existing rules. The targeted amendments made to those rules seek to simplify, provide clarity and reduce administrative burdens for both the private sector and for national authorities. They do not interfere with the competence of the Member States or the EU institutions.

This is equally the case for the repeal of Directive (EU) 2019/1024 (Open Data Directive), noting that its substantive rules are absorbed into Regulation (EU) 2023/2854 (Data Act) without substantially modifying the competences afforded to Member States). A significant part of public sector data is today already subject to the directly applicable Implementing Regulation (EU) 2023/138 on high-value datasets[12]. The transformation into a Regulation will facilitate uniform application of the proposed changes across all Member States. It will particularly support public administrations holding public sector data, but also re-users of such data, by streamlining processes and reducing the administrative burden associated with interpreting and implementing diverse national laws. Enforcement of directly applicable rules will likely become more consistent. The proposal does not change national access regimes and aims at providing enough flexibility for national solutions – a prerogative underlined by Member States.

As regards Regulation (EU) 2016/679 (General Data Protection Regulation) and Regulation (EU) 2018/1725, the proposed amendments seek to provide clarity and predictability in the application of the existing rules, and to reduce administrative burden, where possible, without undermining the high level of data protection under Regulation (EU) 2016/679 (General Data Protection Regulation) and Regulation (EU) 2018/1725. Similarly, they leave unchanged the competence of the Member States and of EU bodies and institutions.

With the introduction of the single-entry point for incident reporting, a Europe-wide solution is proposed to provide one conduit for multiple legal obligations imposed on businesses for reporting essentially the same incident. The solution does not alter in any way the rights and competences of national authorities to receive such reports. Instead, it incentivises reporting by providing a single-entry point in an easy-to-use interface to seemingly file one report, whereas responding to multiple legal obligations at the same time. Given that many of the services concerned are provided cross-border and providers are present in multiple Member States, a European solution is necessary.

- **Proportionality**

The proposal includes technical amendments that are necessary to achieve the objectives of reducing administrative burdens and providing regulatory clarity, while at the same time preserving and optimising the underlying objectives of the amended legislation. They are proportionate, in imposing negligible, if any, transitional and adaptation costs to businesses and authorities, but facilitating a high cost-savings return over the next years.

Several of the amendments presented in this Regulation pursue the simplification objective by primarily providing legal certainty and clarifying the application of the rules - for example as regards clarifications for data holders on protections for trade secrets in Regulation (EU) 2023/2854 (Data Act), or clarifications on training AI models and systems that include personal data regulated by Regulation (EU) 2016/679 (General Data Protection Regulation), or the notion of personal data in Regulation (EU) 2016/679 (General Data Protection Regulation) and Regulation (EU) 2018/1725. Some of the provisions seek to codify interpretations of the Court of Justice of the European Union, such as with regard to

[12] Implementing Regulation (EU) 2013/138.

pseudonymisation of personal data further clarified in Regulation (EU) 2016/679 (General Data Protection Regulation). As such, they include very targeted amendments to the rules, while expecting a high impact in providing legal certainty to businesses and investors.

Amendments proposed in this Regulation also seek to cut direct costs on businesses and authorities, observing that the same regulatory objectives can be reached with lower burdens and ensuring the proportionality of the rules. For example, the mandatory regime for data intermediary services provided for in Regulation (EU) 2022/868 (Data Governance Act) is transformed into a voluntary, trust-enhancing regime in Regulation (EU) 2023/2854 (Data Act).

With the extension to small mid-caps of certain provisions applicable to small and medium enterprises, the simplification measures are targeted and make minimal changes to the scope of those obligations, while providing legal certainty to a wider scope of enterprises with a high potential for supporting the EU's competitiveness. The proposals are limited to those changes necessary to ensure that SMCs benefit from the same legal framework as SMEs.

The single-entry point for incident reporting and data breach notifications brings high cost-savings for businesses, while also tackling the generalised issue of underreporting. It is not just a proportionate solution, but it brings a key simplification solution through a digital tool and supports the effectiveness of the reporting obligations covered under the entry point.

The repeal of Regulation (EU) 2019/1150 (P2B Regulation) is necessary to eliminate the duplication of rules; the Regulation has only residual value, and, in view of a proportionate regulatory approach in the regulation of online platforms, it is necessary to eliminate double obligations.

- **Choice of the instrument**

The amendments are proposed through a Regulation, given the nature of the amended rules. Where Directives are amended, the provisions are addressed to European bodies, or make targeted modifications in particular to carve out provisions further developed in Regulations.

3. RESULTS OF EX-POST EVALUATIONS, STAKEHOLDER CONSULTATIONS AND IMPACT ASSESSMENTS

- **Ex-post evaluations/fitness checks of existing legislation**

Most of the legislation under consideration in this proposal is relatively recent, subject to an ongoing evaluation of results. Key observations are summarised in the accompanying staff working document.

An exception from this is the 2023 preliminary review of Regulation (EU) 2019/1150 (the Platform to Business (P2B) Regulation[13]). The report observed initial positive effects when it

[13] Commission Staff Working Document, Report from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions on the first

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 Regulation (EU) 2019/1150 (P2B Regulation). This was also coupled to insufficient compliance with Regulation (EU) 2019/1150 (P2B Regulation) and led to a lack of implementation. Very limited complaints were received under Regulation (EU) 2019/1150 (P2B Regulation) until 2023. The report concluded that "the full potential of Regulation (EU) 2019/1150 (P2B Regulation) [was] not achieved at present". In the meantime, Regulation (EU) 2022/2065 (DSA) and Regulation (EU) 2022/1925 (DMA) started applying fully and have largely overtaken the provisions in Regulation (EU) 2019/1150 (P2B Regulation).

- **Stakeholder consultations**

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 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[14], another on the revision of Regulation (EU) 2019/881 (the Cybersecurity Act) from 11 April to 20 June[15], and finally another on the European Data Union Strategy from 23 May to 20 July[16]. 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[17]. Its aim was to give the opportunity to stakeholders to comment on a consolidated proposal for the scope of the Digital Omnibus. 513 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.

Executive Vice-President Henna Virkkunen hosted two implementation dialogues on the key topics addressed in the Digital Omnibus: the first on data policy[18] (1 July 2025), and the second on cybersecurity policy[19] (15 September).

---

preliminary review on the implementation of Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services {SWD(2023) 300 final}

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

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

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

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

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

Commissioner McGrath hosted an implementation dialogue on the application of the GDPR (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 collect their feedback, a dedicated SME Panel was run via the Enterprise Europe Network (EEN)[20] 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.

Overall, stakeholder feedback converged as to the need for a simplified application of some of the digital rules. Stakeholders welcomed a focus on coherence and consolidation of the rules, and a focus on optimisation of compliance costs.

There was a clear call for streamlining the data acquis and consolidating the rules. This is addressed in the proposal, together with targeted amendments supported by stakeholders, including as regards the General Data Protection Regulation and the fatigue generated by the cookie banners. In addition, businesses have pointed to further assessments of the interplay between the data rules that warrant a deeper analysis through the Better Regulation tools, notably the forthcoming digital fitness check.

Businesses across different sectors have also pointed to the unjustified burdens stemming from double reporting of incidents across multiple legal frameworks. This call for action is addressed through the proposal of a single-entry point for incident reporting.

As regards the Artificial Intelligence Act, stakeholders have pointed to the need for legal certainty in the application of the rules, and have in particular stressed the need for available standards and guidance ahead of applying the rules. The separate regulatory proposal under the Digital Omnibus addresses their concerns.

Finally, stakeholders have not been vocal about the impact of the Platform-to-Business Regulation, confirming the results of the interim evaluation report that the rules are neither well-known, nor effective in achieving their objective. This Regulation proposes a repeal of the Platform-to-Business rules, notably in light of their overlap with more recent rules.

A detailed overview of these stakeholder consultations, and how they were reflected upon in the proposal, can be found in the Staff Working Document supporting the Digital Omnibus.

---

[19] 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

[20] 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).

- **Collection and use of expertise**

In addition to the consultation streams outlined above, the Commission mainly relied on internal analysis for the purpose of this proposal. Two studies were also contracted in support of the analysis on the data chapters of the proposal. The first one focused on the implementation of Regulation (EU) 2018/1807 (Free Flow of Non-Personal Data Regulation), Directive (EU) 2019/1024 (Open Data Directive) and Regulation (EU) 2022/868 (the Data Governance Act). The second study, more closely linked to the Data Union Strategy Communication (adopted as part of the same Simplification Package alongside the Digital Omnibus), focused on data policy developments linked to generative AI, regulatory compliance, and international dimensions. Both studies are being finalised, and will be published at a later stage.

The Commission's services have also run a study on the interplay between Regulation (EU) 2022/2065 (Digital Services Act) and other legislative acts, including Regulation (EU) 2019/1150 (the P2B Regulation). The Commission is releasing as part of the Digital Package, the report describing the interplay between Regulation (EU) 2022/2065 (Digital Services Act) and other related rules, pursuant to the requirement of Article 91 of Regulation (EU) 2022/2065 (Digital Services Act).

- **Impact assessment**

The amendments put forward in this Regulation are targeted and technical in their nature. They are designed to ensure a more efficient implementation of rules. They are not prone to multiple policy options that could meaningfully be tested and compared and, in alignment with the Better Regulation guidelines, are not underpinned by a full impact assessment report.

The attached Staff Working Document goes in depth into the intervention logic for the amendments, the stakeholder views on the different measures, and presents the cost benefit analysis for the proposals, including the cost savings generated and other types of impacts. In many cases it builds on the respective Impact Assessments that were originally done for the different acts.

- **Regulatory fitness and simplification**

The proposed Regulation entails very strong burden reduction for businesses, as well as for public administrations and citizens. Initial estimates foresee possible savings of at least EUR 1 billion annually, from moment of entry into force, with an additional EUR 1 billion savings in one-off costs, amounting to a total of at least EUR 5 billion over 3 years by 2029. Non quantifiable benefits are also largely expected, notably from a streamlined set of rules which will facilitate their engagement and compliance thereof. The calculations also exclude the business opportunities created through the regulatory approach proposed.

While SMEs are already exempted under a certain number of provisions in the legal acts amended in the Digital Omnibus, further support measures are put forward in the area of cloud switching. Within the chapter on harmonised data sharing rules, some exemptions already provided to SMEs are extended to small mid-caps (SMCs).

The proposal is also fully consistent with the Commission's 'Digital Check', aimed at ensuring the adequate alignment of policy proposals with digital environments. More details on this can be found in the attached Legislative and Financial Digital Statement's Chapter 4.

- **Fundamental rights**

The proposed amendments support the innovation opportunities for businesses in the single market, and thus promote the right to conduct a business in the Union.

Certain provisions are also related to the protection and promotion of other fundamental rights, notably the right to privacy and protection of personal data and were calibrated to preserve the highest standard of protections, and to support individuals in effectively exercising their rights, while optimising costs and creating further innovation opportunities. By doing so the proposal follows strictly the principle of proportionality enshrined in Article 52 of the Charter.

In the specific case of the targeted amendments to Regulation (EU) 2016/679 (General Data Protection Regulation) and Regulation (EU) 2018/1725, the proposed amendments would simplify requirements for low-risk processing, harmonise certain standards and clarify certain key concepts of Regulation (EU) 2016/679 (General Data Protection Regulation) and Regulation (EU) 2018/1725 allowing controllers to implement more effective data protection policies. This would allow them to concentrate their resources towards more data-intensive and high-risk activities for which the measures to protect personal data are most critical.

As regards the privacy of communication, the proposal preserves the highest standard of protection, including consent-based access to terminal equipment. The amendment to Directive (EU) 2002/58/EC (ePrivacy Directive) does not alter the substantive protections. It aligns the rules for processing of personal data on and from terminal equipment with those of Regulation (EU 2016/679 (General Data Protection Regulation). Rules on the integrity of the terminal equipment under the Directive are maintained where non-personal data is processed.

4. BUDGETARY IMPLICATIONS

The budgetary implications of setting up and maintaining the single-entry point for incident reporting by the European Union Agency for Cybersecurity (ENISA) are detailed in the revision of Regulation (EU) 2019/881 (Cybersecurity Act), as part of the resources for ENISA.

5. OTHER ELEMENTS

- **Implementation plans and monitoring, evaluation and reporting arrangements**

N.A.

- **Detailed explanation of the specific provisions of the proposal**

Amendments to Regulation (EU) 2023/2854 – the Data Act

The amendments to the data legal framework consolidate into Regulation (EU) 2023/2854 (the Data Act) in a robustly streamlined manner the provisions of Regulation (EU) 2018/1807 (the Free Flow of Data Regulation), Regulation (EU) 2022/868 (Data Governance Act) and Directive (EU) 2019/1024 (Open Data Directive). Chapter I also includes targeted amendments to adjust the current rules of Regulation (EU) 2023/2854 (Data Act).

Article 1 covers amendments to Regulation (EU) 2023/2854 (Data Act) on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828.

In Article 1:

Paragraph (1) updates the scope of Regulation (EU) 2023/2854 (Data Act) into which new chapters will be inserted as explained further below.

Paragraph (2) amends definitions and inserts new ones.

Paragraph (3) creates a new rule under Article 4(8) of Regulation (EU) 2023/2854 (Data Act) that allows data holders to refuse disclosure of trade secrets to a user when there is a high risk of unlawful acquisition, use, or disclosure to third countries, or entities under their control, that are subject to jurisdictions with weaker protections than those available in the Union.

Paragraph (5) introduces the same rule for Article 5(11) of Regulation (EU) 2023/2854 (Data Act), concerning data holders disclosing trade secrets to third parties.

Paragraphs (5) to (19) narrow the scope of Chapter V from 'exceptional needs' only to 'public emergencies'. It deletes Article 14 and 15, and creates a new Article 15a, which becomes the sole Article for requesting during public emergencies under the B2G regime of Regulation (EU) 2023/2854 (Data Act). The requests can be made when necessary to respond to a public emergency (Article 15a(2)), or to mitigate or support the recovery from a public emergency (Article 15a(3)). Cross-references are adjusted accordingly, language simplified and clarified. Article 1 paragraph (21) creates a new Article 22a that frames the complaints regime under Chapter V, merging previously repeated provisions.

Paragraphs (20) to (22) include certain exemptions to Chapter VI of Regulation (EU) 2023/2854 (Data Act) (switching between data processing services): In Article 31, a lighter specific regime is inserted for data processing services that are custom-made, i.e. data processing services that are not off-the-shelf and would not function without prior adaptation to the needs and ecosystem of the user, where these are provided based on contracts concluded before 12 September 2025. Similarly, in Article 31, a new lighter specific regime is inserted for data processing services provided by SMEs and SMCs on the basis of contracts concluded before 12 September 2025, accompanied by a clarification that these providers can include early-termination penalties in fixed-term contracts.

Paragraphs (23) to (25) include modifications to Article 32 of Regulation (EU) 2023/2854 (Data Act) resulting from the integration of bodies currently governed under Regulation (EU) 2022/868 (Data Governance Act) into Regulation (EU) 2023/2854 (Data Act).

Paragraph (26) removes obligations on providers of smart contracts to comply with essential requirements with an empowerment for the Commission to adopt harmonised standards.

Paragraphs (27) integrates two legal regimes currently in Regulation (EU) 2022/868 (Data Governance Act), a Regulation that shall be repealed once the Omnibus enters into force. This point reforms current rules in chapter III and IV of the Data Governance Act that provide for a compulsory notification regime for data intermediation services providers and for a voluntary registration regime for data altruism organisations. The two regimes shall be inserted as a new Chapter VIIa into Regulation (EU) 2023/2854 (Data Act). In light of the emerging nature of the market for data intermediation services, the obligations of regulation (EU) 2022/868 (Data Governance Act) shall be made more flexible for this market to grow: For one, the regime for data intermediation services providers shall be turned into a voluntary regime. Second, the most critical obligation, the obligation to keep data intermediation services legally separate from any other service a company may want to offer, will be replaced by an obligation to

keep services functionally separate paired with an additional set of conditions. Finally, the list of obligations is drastically shortened. As concerns data altruism, reporting and transparency obligations for data altruism organisations are repealed as well as the idea to supplement the rules of Regulation (EU) 2022/868 (Data Governance Act) in a "data altruism Rulebook" with even more detailed rules.

It introduces a new Chapter VIIb under which the prohibition of localisation requirements for non-personal data withing the Union, formerly contained under the to be repealed Regulation (EU) 2018/1807 (Free Flow of Non-personal Data Regulation) is inserted into Regulation (EU) 2023/2854 (Data Act). The obligation to notify the Commission is maintained but abolishes the national online single information point where Member States should publish applicable data localisation requirements.

Paragraphs (4), (33) – (58) introduce the merged provisions on the re-use of data and documents held by public sector bodies under Chapter II of Regulation (EU) 2022/868 (Data Governance Act) and Directive (EU) 2019/1024 (Open Data Directive):

- Points (4) introduces definitions from the inserted provisions into Regulation (EU) 2023/2854 (Data Act), harmonising the definition of data and documents by providing a strict delineation between digital (data) and non-digital (document) content.
- It introduces the new Chapter VIIc on the re-use of data and documents held by public sector bodies.
- It introduces a new Section 1, introducing the general principles applicable to the newly inserted chapter.
- It introduces the subject matter and the scope of the merged Chapter, combining the common rules of Chapter II of Regulation (EU) 2022/868 (Data Governance Act) and Directive (EU) 2019/1024 (the Open Data Directive).
- It sets out the common principle of non-discrimination applicable to the sharing of open government data and certain categories of protected data.
- It sets out the prohibition of exclusive arrangements, common to the regime of open government data and certain categories of protected data.
- It sets out general principles relating to charging for the re-use of open government data or certain categories of protected data. As a new rule, public sector bodies will need to ensure that any charges can also be paid online through widely available cross-border payment services, without discrimination for the re-use of open government data. This represents an extension of this rule formerly only known for the re-use of certain categories of protected data under Chapter II of Regulation (EU) 2022/868 (Data Governance Act).
- It provides for the right of re-users of open government data and certain categories of protected data to be informed of available means of redress relating to decisions or practices affecting them.
- It inserts the section on the rules for the re-use of open government data, formerly the rules under Directive (EU) 2019/1024 (Open Data Directive).

- It determines the scope of the section, including the non-application to certain categories of protected data in scope of the general Chapter on the re-use of data and documents held by public sector bodies.
- It sets out the general principle for the re-use of open government data.
- It sets out the rules for processing requests for re-use of open government data, inserting the former provision of Directive (EU) 2019/1024 (Open Data Directive).
- It introduces the rules on available formats for the re-use of open government data, formerly included under Directive (EU) 2019/1024 (Open Data Directive).
- It introduces the rules governing the charging for open government data, formerly governed by Directive (EU) 2019/1024 (Open Data Directive). As a new rule, public sector bodies may charge higher charges for the re-use by very large enterprises. Such charges must be proportionate and their amount based on objective criteria.
- It introduces the rules on standard licences for re-use of open government data, formerly included in Directive (EU) 2019/1024 (Open Data Directive). As a new rule, public sector bodies may foresee special conditions for very large enterprises. Such conditions must be proportionate and must be based on objective criteria.
- It introduces the rules on practical arrangements formerly included in Directive (EU) 2019/1024 (Open Data Directive), to facilitate the search for data or documents available for re-use in Regulation (EU) 2023/2854 (Data Act).
- It introduces the rules on research data formerly included in Directive (EU) 2019/1024 (the Open Data Directive) in Regulation (EU) 2023/2854 (Data Act).
- It introduces the rules on high value datasets, formerly included in Directive (EU) 2019/1024 (Open Data Directive) in Regulation (EU) 20232854 (Data Act).
- It creates a new section for the re-use of certain categories of protected data to include the former rules under Chapter II of Regulation (EU) 2022/868 (Data Governance Act) into the Chapter. The point outlines the scope of application of this third section, which excludes from the scope the data and documents in scope of Section two, governing the regime of re-use of open government data. As a new rule, documents are included in the scope of this section.
- It sets out the general principle relating to the re-use of certain categories of protected data. This is the principle set out under Chapter II of Regulation (EU) 2022/868 (Data Governance Act), that the section does not create an obligation on public sector bodies to allow the re-use of protected data, but rather sets out minimum conditions where public sector bodies decide to make such data available for re-use.
- It introduces the rules on the conditions for re-use of certain categories of protected data, formerly included in Chapter II of Regulation (EU) 2022/868 (Data Governance Act) in a simplified and streamlined form. It includes a clarification which rules are applicable in cases where personal data have been anonymised. The requirements relating to transfers of non-personal data to third countries are kept but split into a new Article under point (54).
- It introduces the rules on charging fees, formerly part of Chapter II of Regulation (EU) 2022/868 (Data Governance Act) into Regulation (EU) 2023/2854 (Data Act). As a new rule, public sector bodies may foresee higher fees for the re-use by very

large enterprises. Such fees must be proportionate and based on objective criteria. The special consideration to incentivise re-use by SMEs is extended to SMCs.

- It introduces the rules on competent bodies, formerly part of Chapter II of Regulation (EU) 2022/868 /Data Governance Act into Regulation (EU) 2023/2854 (Data Act). Competent bodies are designed to help public sector bodies in responding to requests for re-use of data and documents covered in Section 3.
- It introduces the rules on the single information point, formerly part of Chapter II of Regulation (EU) 2022/868 (Data Governance Act) into Regulation (EU) 2023/2854 (Data Act)the Data Act. Single information points are designed to help re-users to find information on the re-use of certain categories of protected data in an easy manner.
- It introduces the rules on the procedure for requests for re-use of certain categories of protected data, formerly regulated under Chapter II of Regulation (EU) 2022/868 (Data Governance Act) under Regulation (EU) 2023/2854 (Data Act).

Paragraph (57) integrates the basic rules on the European Data Innovation Board (EDIB), a group advising the Commission on the consistent enforcement of the Data Act and serving as a coordination forum for policy-making in the domain of data economy policies. It will integrate the basis rules into the Data Act. The changes will allow the Commission to modify the relevant foundational documents of the EDIB (the Commission decision of 20 February 2023 – C(2023)1074 final) and expand the membership to representatives of national policy-making in addition to competent authorities.

Paragraphs (61) - (65) contain amendments to the provisions of Regulation (EU) 2023/2854 (Data Act) on Committee procedure and the power of delegation, and points (66) on Regulation (EU) 2022/868 (Data Governance Act) necessary to introduce the rules of Regulation (EU) 2022(868 (Data Governance Act) and Directive (EU) 2019/1024 (Open Data Directive) into Regulation (EU) 2023/2854 (Data Act).

Paragraph (68) extends the special focus for SMEs in the context of evaluation to SMCs and point (69) introduces the evaluation of the newly inserted rules into Regulation (EU) 2023/2854 (Data Act).

Article 2 introduces in Regulation (EU) 2018/174 the relevant references to data intermediation services and data altruism in the annex related to ‘starting, renewing and closing a business’.

Amendments to Regulation (EU) 2016/679, Regulation (EU) 2018/1725 and Directive 2002/58/EC

Article 3 of the proposal would introduce targeted amendments to Regulation (EU) 2016/679 (‘General Data Protection Regulation’).

In Article 3:

Paragraph 1 would clarify the definition of personal data under Article 4 of Regulation (EU) 2016/679 (General Data Protection Regulation) by stating that information is not to be considered personal data for a given entity when it does not have means reasonably likely to be used to identify the natural person to whom the information relates. As a result, such an entity would not, in principle, fall within the scope of application of that Regulation.

Paragraph 2 would provide for two additional exemptions to the processing of special categories of data: It would provide for an exemption from the general prohibition on the processing of biometric data, when it is necessary for confirming the identity of the data subject and when the data and means for such verification are under the sole control of that data subject. It would also provide for an exemption for the residual processing of special categories of personal data for development and operation of an AI system or an AI model, subject to certain conditions, including appropriate organisational and technical measures to avoid collecting special categories of personal data and removing such data.

Paragraph 3 would clarify the situation under Article 12 of Regulation (EU) 2016/679 (General Data Protection Regulation) where the right of access is abused by data subjects for purposes other than the protection of their personal data. As a result, the controller could refuse to comply with the request or charge a reasonable fee. Moreover, it would clarify the conditions to demonstrate that an access request was excessive.

Paragraph 4 would focus on the controller's obligation to inform the data subjects about the processing of their personal data under Article 13 of Regulation (EU) 2016/679 (General Data Protection Regulation) by removing this obligation in situations where there are reasonable grounds to assume that the data subject already has the information, unless the controller transmits the data to other recipients or categories of recipients, transfers the data to a third country, carries out automated decision-making or the processing is likely to cause a high risk to data subject's rights.

Paragraph 5 would clarify the requirements for automated individual decision-making under Article 22 of Regulation (EU) 2016/679 (General Data Protection Regulation), in the context of entering into, or performance of, a contract between the data subject and a data controller, in particular that the requirement of 'necessity' is regardless of whether the decision could be taken otherwise than by solely automated means.

Paragraph 6 would align the controller's obligation to notify data breaches to the competent supervisory authority under Article 33 of Regulation (EU) 2016/679 (General Data Protection Regulation) with its obligation to notify data subjects of such breaches by stipulating that the notification in only required if a data breach is likely to result in a high risk to the data subject's rights. It would also extend the notification deadline to 96 hours. It is also proposed that controllers use the single-entry point when they notify data breaches to the supervisory authority. In addition, the European Data Protection Board would be obliged to prepare and submit to the Commission a proposal for a common template for data breach notifications, which the Commission would be empowered to adopt by means of an implementing act, after reviewing it, as necessary.

Paragraph 7 would harmonise the lists of processing activities requiring and not requiring data protection impact assessment by providing that a single lists of processing operations which require and do not require a data protection impact assessment be provided at EU level, thereby contributing to the harmonisation of the notion of high risk. The European Data Protection Board would be obliged to prepare proposals for such lists. It would also be obliged to prepare a proposal for a common template and common methodology for conducting data protection impact assessments, which the Commission would be empowered to adopt by means of an implementing act, after reviewing them, as necessary.

Paragraph 8 establishes that the Commission can support, together with the European Data Protection Board, controllers in assessing whether data resulting from pseudonymisation does not constitute personal data by specifying means and criteria relevant for such an assessment, including the state of the art of available techniques and criteria to assess the risk of reidentification...

Paragraph 12 reforms the legal regime on processing of personal data on or from terminal equipment ('connected devices'), currently part of Directive 2002/58/EC (ePrivacy Directive). A new Article 88a is inserted in Regulation (EU) 2016/679 (General Data Protection Regulation), which lays down the consent requirement for the storing or accessing of personal data on the terminal equipment of natural persons and which brings the processing of personal data on and from terminal equipment within the rules of Regulation (EU) 2016/679 (General Data Protection Regulation). A new Article 88b Regulation (EU) 2016/679 (General Data Protection Regulation), for automated and machine-readable indications of individual choices and respect of those indications by website providers once standards are available.

In Article 4:

Article 4 of the proposal would introduce targeted amendments to Regulation (EU) 2018/1725, in order to align its text with the amendments to the Regulation (EU) 2016/679 introduced in Article 3.

In Article 5:

Article 5 provides for amendments to Directive 2002/58/EC, the Directive on privacy and electronic communications ('ePrivacy Directive'). Article 4 of that Directive is repealed. The addition to Article 5 paragraph 3 of that Directive permits to move to Regulation (EU) 2016/679 (General Data Protection Regulation) the rules on storing and accessing personal data from the terminal equipment of a natural person, by way of inserting a new Article 88a of Regulation (EU) 2016/679 (General Data Protection Regulation) as described above.

Single-Entry Point for Incident Reporting

In Article 6:

In Paragraphs (1) and (2), the single-entry point for incident reporting is established, by including specific requirements to ENISA. Further, it is established that incident reporting mandated under the NIS2 Directive should be done through the new single-entry point.

In Article 7: the single entry-point is mandated also for incident reporting under Regulation (EU) 910/2014 (eIDAS Regulation)

In Article 8: the single entry-point is mandated also for Regulation (EU) 2022/2554 (DORA)

In Article 9: the single entry point is mandated also for Directive (EU) 2022/2557 (CER)

In addition, in Article 3(6), the data breach incident reporting is mandated also for Regulation (EU) 2016/679 (General Data Protection Regulation) to be channelled through the single-entry point. In Article 5(1), the reporting requirements under Directive 2002/58/EC (ePrivacy Directive) are repealed, as they are obsolete in view of the provisions in Regulation (EU) 2016/679 (General Data Protection Regulation).

Repeals of Acts and Final provisions

In Article 10:

Paragraph 1 repeals Regulation (EU) 2019/1150 (the P2B Regulation), considered of residual relevance in view of recent rules that largely cover the same issues. By way of derogation, paragraph 2 addresses any cross-references to Regulation (EU) 2019/1150 (P2B Regulation)

in other legal instruments: these will remain in application until amended in their original acts, at the latest by 31 December 2032 in order to avoid any legal uncertainty.

Paragraph 3 repeals the legal texts absorbed into Regulation (EU) 2023/2854 (Data Act).

Article 11 sets the final provisions of the amending Regulation.

2025/0360 (COD)

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)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 and 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee[21],

Having regard to the opinion of the European Central Bank[22],

Having regard to the opinion of the Committee of the Regions[23],

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) In its Communication on a simpler and faster Europe[24] , the Commission announced its commitment to an ambitious programme to promote forward-looking, innovative policies that strengthen the Union's competitiveness and radically lighten the regulatory load for people, businesses and administrations, while maintaining the highest standard in promoting the Union's values. Consequently, the Commission prioritised the proposal of immediate adjustments to legislation, including digital legislation, to address the competitiveness challenge of the Union.

(2) Union digital legislation sets high standard in the Union and can be a powerful source of competitive advantage for businesses that abide by the rules, showing a world-

[21] OJ C […], […], p. […].

[22] OJ C […], […], p. […].

[23] OJ C […], […], p. […].

[24] 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

leading mark of quality, safety and trustworthiness. Digital regulations have framed the clear rules of the game in the Union for responsible businesses, ensuring fairness and transparency in business-to-business relations, stimulating innovative business models, setting high standard of consumer protection and safety, and for the protection fundamental rights, not least privacy and data protection.

(3) Union digital legislation has evolved incrementally over the past years, in response to the rapidly growing footprint of digital technologies in the Union's economy and societal dynamic, and in view of addressing emerging challenges and promoting business opportunities in the EU. Notwithstanding the Commission's commitment to a systematic 'stress test' of the digital rules, along with other Union rules, which might lead to further regulatory adjustments notably following the forthcoming Digital Fitness Check, as well as other targeted evaluations of digital rules, immediate regulatory changes are necessary. Consequently, this Regulation proposes a first set of amendments to the digital legislative framework, aimed at providing immediate regulatory clarifications that stimulate innovation in the Union market, and that cut administrative compliance costs in particular for businesses, while also streamlining supervisory and administrative costs for supervisory authorities and advisory bodies. The amendments also seek to provide clarity to individuals.

(4) Given the foundational role of data in driving value-creation in the digital economy, and pursuant to the objectives of the Communication for a European Data Union Strategy, the amendments presented in this Regulation to the legislative framework regarding data seek to build a coherent and cohesive regulatory framework for the availability and use of data, streamlining and consolidating the data regulatory framework into only two legal acts, namely Regulations (EU) 2016/679[25] and (EU) 2023/2854[26] of the European Parliament and of the Council, from currently five different applicable acts. The amendments seek to cut unnecessary administrative costs and stimulate the availability of data as a prerequisite for supporting competitive digital businesses in the Union, while maintaining the highest standard of protections for privacy, personal data protection, and fair business practices, and ensuring core regulatory objectives, including compliance with EU and national competition law.

(5) Acknowledging the iterative evolution of horizontal and sector-specific rules, it is indispensable to address also overlaps in specific provisions that result in unnecessary duplications of administrative burdens. This is the case in requirements across several rules for reporting following cybersecurity and related incidents, where digital solutions, as proposed in this Regulation, can bring an immediate relief to businesses across all concerned sectors.

(6) Similarly, with the iterative regulation of online platforms over the past years, more recent rules have established a clearer and more ambitious framework than some of the

---

[25] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[26] 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)

predating rules, rendering them obsolete. It is therefore necessary that the legal framework evolves, eliminating any unnecessary duplications that add legal complexity.

(7) Regulation (EU) 2022/868 of the European Parliament and of the Council[27] has established rules for intermediary functions in three different settings: (a) functions that support the re-use of protected data held by public sector bodies under controlled conditions; (b) data intermediation services that facilitate data sharing between data subjects, data holders and data users; and (c) data altruism organisations that support the use of data made available by data subjects and data holders on an altruistic or philanthropic basis. Functions supporting the re-use of protected data held by the public sector have a close link with rules of Directive (EU) 2019/1024 of the European Parliament and of the Council[28]. Their interplay has caused confusion namely among public sector bodies. It is thus necessary to merge the two sets of rules. The evaluation of the rules on data intermediation services has shown that the definition of data intermediation service providers has weaknesses and that the rules are overly stringent for service providers to find a sustainable financial model. It is thus also necessary to streamline the regime. With respect to data altruism, certain rules of Regulation (EU) 2022/868, notably the obligation on Member States to have national policies on data altruism in place, the establishment of a 'rulebook' and developing a European data altruism consent form appear unnecessary regulation, also in light of on-going work by the European Data Protection Board referred to in Article 68 of Regulation (EU) 2016/679 of the European Parliament and of the Council[29] on guidance on the processing of personal data in the context of scientific research.

(8) While the importance of data intermediation services is recognised in the context of many initiatives supporting data sharing and collaboration, the rules of Regulation (EU) 2022/868 on data intermediation service providers should be clarified. In particular, the definition of such providers should be made more precise. It should eliminate elements that served merely as illustrative examples, rather than exceptions. Moreover, it should address loopholes resulting from ambiguous formulations, notably as regards the notion of 'closed group'. Services should not be eligible to register as data intermediation services where they are exclusively used by a closed group of companies and where any extension of that group of companies can only be decided by that group and not the service provider. More importantly, making this emerging market subject to a compulsory regime has created unnecessary compliance costs. At this stage of market development, a voluntary regime, allowing neutral players to distinguish themselves from other players, appears sufficient. Also, in order to enable

---

27 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) (OJ L 152, 3.6.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/868/oj).

28 Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (OJ L 172, 26.6.2019, p. 56, ELI: http://data.europa.eu/eli/dir/2019/1024/oj).

29 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

sustainable business models, the regime should be made less strict by abolishing the requirement for a legal separation between data intermediation services and other value-added services that a service should be allowed to offer, replacing it with a functional separation while keeping certain safeguards. The administrative monitoring regime should be simplified. Instead of national and a Union public register for data intermediation services providers and data altruism organisations, there should only be Union public registers, namely one for data intermediation service providers and another for data altruism organisations. Competent authorities overseeing the award of the label and the compliance of the entities with the requirements for obtaining it should be independent in this task. This should be understood to mean that they are legally and functionally independent from a data intermediation service or data altruism organisation, including at the level of their top-management. It should be possible for government organisations to financially support data intermediation services or data altruism organisations, in particular given the emerging nature of these entities, provided that they are legally separate entities. In order to ensure that recognised entities are easily identifiable throughout the Union, the Commission established Implementing Regulation (EU) 2023/1622 on the design of common logos to identify data intermediation services providers and data altruism organisations recognised in the Union. on the design of common logos to identify data intermediation services providers and data altruism organisations recognised in the Union.

(9) Regulation (EU) 2023/2854 removes barriers to data access and use, unlocks data-driven innovation and competitiveness, and safeguards the incentives of those who invest in data technologies.

(10) Chapter II of Regulation (EU) 2023/2854 requires data holders to make data available, including data protected as trade secrets, to users and their selected third parties, provided confidentiality measures established by the data holder are maintained. This requirement of maintaining confidentiality complements Directive (EU) 2016/943 of the European Parliament and of the Council [30], which sets the standard for protecting trade secrets within the Union. However, disclosure of trade secrets to third-country entities may increase risks to their integrity and confidentiality where there is exposure to jurisdictions with inadequate protections or difficulties in their actual enforcement, potentially resulting in unauthorised use, economic damage and legal uncertainty.

(11) It is necessary to strengthen Regulation (EU) 2023/2854 by introducing an additional ground for data holders to refuse the disclosure of trade secrets, supplementing existing provisions which allow refusal based on the data holder's demonstration of a high likelihood of serious economic damage. Under the new provision, data holders may refuse to disclose trade secrets if they demonstrate a high risk of unlawful acquisition, use, or disclosure to entities subject to regimes with inadequate protection, non-equivalent, or weaker legal frameworks than the applicable Union rules. The new provision also covers instances where the third country legal framework, in theory, is

[30] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (OJ L 157, 15.6.2016, p. 1).

robust or exceeds such Union rules, but lacks appropriate enforcement in practice. Such risks highlight the possibility that trade secrets could be acquired, used, or disclosed in violation of Union law, threatening the integrity and confidentiality of trade secrets.

(12) The activation of the refusal mechanism should remain voluntary, and the demonstration done only upon its activation. Data holders should not be required to conduct a full-scale analysis or demonstration of the level of trade secret protection in third countries or by a third country entity as a precondition to be able to substantiate their refusal to sharing data or to disclose trade secrets. In their demonstration, data holders may take into consideration various factors, such as insufficient or inadequate legal standards, poor or arbitrary enforcement, historical infringements, foreign disclosure obligations conflicting with Union law, limited legal recourse or remedies for Union entities, the strategic misuse of procedural tactics to undermine competitors, or undue political influence. Given the diverse range of entities, third countries, and data sharing scenarios involved, data holders should focus their assessment and demonstration on pertinent risks and act accordingly, including by setting appropriate safeguards or activating the refusal mechanism. Refusals should be clear, proportionate, and tailored to the specific circumstances of each case, rather than being applied systematically or in a generalized manner across an entire third country.

(13) An insufficient protection of trade secrets and the challenges in enforcing them in third countries may cause irreparable harm to European businesses. The objective is therefore to strengthen the safeguards for trade secrets by preventing their leakage to natural or legal persons that are established in or subject to jurisdictions posing such risks. This includes Union-based entities controlled by third country entities, who may be acting in bad faith or as fronts for third country entities. Additionally, the objective is to avert direct exposure to third country entities operating within the Union, that are subject to such jurisdictions. Being subject to a third country jurisdiction means the natural or legal person is legally governed, controlled or otherwise bound by the laws or regulatory authority of a third country. Subsidiaries or affiliates of third country parent companies may exploit these jurisdictions to evade or circumvent Union laws. Direct or indirect control refers to the ability to exercise decisive or dominant influence over another entity's management or strategic decisions, whether through ownership of capital or voting rights, financial participation, contractual arrangements, or intermediary entities. Control may be exercised directly or through other means, even without majority ownership. Data holders should use best efforts to obtain the relevant information, which may include searches in public registers or requesting it from the user or third party directly, while ensuring it remains appropriately non-intrusive.

(14) Protecting trade secrets from those vulnerabilities is essential for European industries to sustain their market position and competitive advantage. While data holders may exercise discretion in protecting their trade secrets, refusals to share data should be limited to justified, exceptional circumstances, in order to preserve the objectives of Regulation (EU) 2023/2854 of fostering data-driven innovation and a thriving digital economy in the Union. Safeguards against misuse of the refusal mechanism should remain in place, including the data holder's obligation to demonstrate in a duly substantiated manner that disclosure poses a high risk and to notify competent authorities. This demonstration should be provided in writing without undue delay to the user or third party and proportionate to the case at hand. All parties involved should treat the decision and supporting demonstration as confidential in order to

uphold the confidential nature of the trade secrets concerned. Users and third parties, as the case may be, may challenge the data holder's decision with the competent authority, in court, or through dispute settlement bodies.

(15) To simplify the business-to-government data sharing framework under Regulation (EU) 2023/2854 and to clarify ambiguities that previously imposed broader obligations on businesses, it is necessary to narrow the scope of Chapter V of that Regulation from 'exceptional need' to 'public emergencies'. The concept of 'public emergencies', which is defined under Article 2(29) of Regulation (EU) 2023/2854, thus ensures that the obligations laid down in that Chapter are invoked only under well-defined, urgent situations, reducing the technical, administrative and legal challenges that business faced under the previous regime. This would ensure that data requests are relevant and proportionate to responding, mitigating, or supporting the recovery from public emergencies. Since the updated Union framework on European statistics under Regulation (EC) No 223/2009 of the European Parliament and of the Council[31] does not address public emergencies, it is essential to preserve the role of official statistics under Chapter V of Regulation (EU) 2023/2854 to ensure clarity and effectiveness in such situations. It is also necessary to clarify the compensation regime for situations where microenterprises and small enterprises are required to provide data to address a public emergency, in which case such enterprises are allowed to claim compensation.

(16) In order to mitigate legal uncertainties that could discourage innovative business models, it is necessary to address the substantial compliance ambiguities and burdens associated with the provisions on smart contracts executing data sharing agreements under Article 36 of Regulation (EU) 2023/2854. The absence of harmonised standards and clear definitions for key concepts such as 'robustness', 'access control', and 'consistency with contractual terms', combined with the requirement for a 'safe termination or interruption mechanism' potentially incompatible with decentralised or public blockchain architectures built on immutable ledgers, posed challenges to innovators from a cost and opportunity perspective. Additionally, the ambiguity surrounding the performance of the conformity assessment under Article 36(2) of that Regulation risks imposing disproportionate burdens. The elimination of Article 36 of Regulation (EU) 2023/2854 would therefore promote the development and market introduction of new business models, foster innovation, and reduce barriers for emerging technologies.

(17) Certain data processing services, which do not fall within the Infrastructure as a Service (IaaS) delivery model, are custom-made to the needs or ecosystem of a customer. The provision of such data processing services is based on time-intensive pre-contractual and contractual negotiations to determine the specific requirements of

---

[31] Regulation (EC) No 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation (EC, Euratom) No 1101/2008 of the European Parliament and of the Council on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities, Council Regulation (EC) No 322/97 on Community Statistics, and Council Decision 89/382/EEC, Euratom establishing a Committee on the Statistical Programmes of the European Communities (OJ L 87, 31.3.2009, p. 164, ELI: http://data.europa.eu/eli/reg/2009/223/oj).

the customer and subsequent technical efforts to customise the data processing service and to deliver a tailored solution. Those are services not provided off-the-shelf and are personalised to the needs of a customer to provide a tailored solution where the majority of features and functionalities of the data processing service has been adapted by the provider to the specific needs of the customer where the majority of features and functionalities would not be usable for a customer without prior adaptation by the provider. Those services differ from custom-built data processing services referred to in Article 31(1) of Regulation (EU) 2023/2854. Custom-built data processing services are services of which the majority of main features has been custom-built to accommodate the specific needs of an individual customer or where those data processing services are not offered at broad commercial scale via the service catalogue of the provider. To avoid additional costs and administrative burden connected to the need to reopen and renegotiate contracts concluded before or on 12 September 2025, it is necessary to clarify that, with the exception of the obligation to reduce and ultimately remove switching and egress charges, custom-made services provided according to contracts concluded before or on 12 September 2025 should not fall within scope of Chapter VI of Regulation (EU) 2023/2854.

(18) For reasons relating to financial planning and attracting investment, providers of data processing services, especially SMEs and SMCs, may prefer and offer contracts of a fixed duration. It is necessary to clarify that providers of data processing services may include provisions on proportionate early termination penalties in those contracts as long as they do not constitute an obstacle to switching. In addition, providers of data processing services that are SMEs or SMCs are particularly burdened by the need to align existing contracts for the provision of data processing services to Regulation (EU) 2023/2854. It is therefore necessary to establish a specific regime for those providers if they provide data processing services, other than IaaS, based on contracts concluded before or on 12 September 2025. Taking into account the aim of Regulation (EU) 2023/2854 to enable switching between data processing services and given that switching charges, including egress charges, constitute a serious obstacle to switching, the new lighter regimes for data processing services that are custom-made or are provided by SMEs or SMCs should not undermine the gradual withdrawal of those charges. Contractual provisions running contrary to that objective should be considered to never have existed, if they are included in contractual agreements on the provision of services falling within the scope of those two new specific regimes.

(19) Regulation (EU) 2018/1807 of the European Parliament and of the Council[32] introduced a key principle for supporting the data-driven economy within the Union, underpinning in concrete terms the freedom of establishment and freedom to provide a service. 'Free flow of data' in the Union, clarified through the prohibition to impose data localisation, remains a fundamental principle, providing legal certainty to businesses, and should be retained in Regulation (EU) 2023/2854. The provision does not affect the data processing in so far as it is carried out as part of an activity which

---

[32] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (OJ L 303, 28.11.2018, p. 59, ELI: http://data.europa.eu/eli/reg/2018/1807/oj).

falls outside the scope of Union law, in particular as regards national security, in accordance with Article 4 of the Treaty on European Union. At the same time, other provisions of Regulation (EU) 2018/1807 are superseded by more recent rules. Notably, Chapter VI of Regulation (EU) 2023/2854 introduced a modern horizontal legal framework addressing switching between data processing services and rendered Article 6 of Regulation (EU) 2018/1807 practically obsolete. The co-existence of those provisions has increased legal complexity for businesses. Therefore, Regulation (EU) 2018/1807 should be repealed.

(20) The concept of 'public security', within the meaning of Article 52 TFEU and as interpreted by the Court of Justice, covers both the internal and external security of a Member State, as well as issues of public safety, in order, in particular, to facilitate the investigation, detection and prosecution of criminal offences. It presupposes the existence of a genuine and sufficiently serious threat affecting one of the fundamental interests of society, such as a threat to the functioning of institutions and essential public services and the survival of the population, as well as the risk of a serious disturbance to foreign relations or the peaceful coexistence of nations, or a risk to military interests. In compliance with the principle of proportionality, data localisation requirements that are justified on grounds of public security should be suitable for attaining the objective pursued, and should not go beyond what is necessary to attain that objective.

(21) Both Directive (EU) 2019/1024 and Chapter II of Regulation (EU) 2022/868 regulate the re-use of public sector information for innovation purposes. The interplay of the two sets of rules has created legal uncertainty, mainly for public sector bodies. An alignment of the rules in one legal instrument is therefore necessary to bring further legal coherence and certainty.

(22) Since both Directive (EU) 2019/1024 and Regulation (EU) 2022/868 share the goal of enhancing the re-use of public sector information, and inn order to simplify rules from the perspective of both public sector bodies and of re-users of public sector information, it is rational to repeal Directive (EU) 2019/1024 and Regulation (EU) 2022/868 and align the two regimes and consolidate the rules in a single Chapter under this Regulation. This solution will increase harmonisation of those rules across the Union, reduce the administrative burden associated with interpreting and implementing national legislation and make it easier for businesses to develop cross-border services and products. When designating competent bodies, Member States should ensure that even where sector-specific competent bodies are designated, all relevant sectors are ultimately covered. The amendments in this Regulation should be understood not to alter the interpretation of the different definition and terms, unless clearly specified.

(23) Data and documents, which can be made publicly available for reuse, and data and documents, which are protected on the grounds of commercial confidentiality, including business, professional and company secrets, statistical confidentiality, the protection of intellectual property rights of third parties or the protection of personal data, are often held by the same public sector bodies. Therefore, it is necessary to align definitions and common principles applying to all public sector information and address questions regarding the interplay of the two sets of rules.

(24) The existing rules should be streamlined to enhance clarity and consistency. Nevertheless, the two reuse regimes should remain distinct and their respective scope of application should continue to depend on the characteristics of the data or

documents and the context of their reuse. Public sector bodies should apply the open data regime whenever possible. Only where they determine that data or a document contains information corresponding to certain categories of protected data should they limit its public availability and consider making it available for reuse as protected data.

(25) Start-ups, small enterprises and enterprises that qualify as medium-sized enterprises under Article 2 of the Annex to Commission Recommendation 2003/361/EC[33] and enterprises from sectors with less-developed digital capabilities struggle to re-use data and documents. At the same time a few very large entities have emerged with considerable economic power in the digital economy through the accumulation and aggregation of vast volumes of data and the technological infrastructure for monetising them. Those very large enterprises include undertakings that provide core platform services and are designated as gatekeepers under Regulation (EU) 2022/1925 of the European Parliament and of the Council[34] and subject to special obligations to address the imbalances. To address those imbalances and strengthen competition and innovation, public sector bodies should be able to introduce special conditions in licences pertaining to the re-use of data and documents by very large enterprises. Any such conditions should be proportionate, be based on objective criteria, taking into consideration the economic power, the entity's ability to acquire data or the designation as a gatekeeper under Regulation € 2022/1925, other such criteria, where appropriate. Such special conditions may, inter alia, pertain to the charges and fees or the purposes of re-use.

(26) 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. Very large enterprises, and in particular undertakings designated as gatekeepers under Regulation (EU) 2022/1925, hold significant power and influence over the internal market. To prevent such entities from leveraging their substantial means to the detriment of fair competition and innovation, public sector bodies should be able to set out higher charges and fees for the re-use of open government data and protected data. Such higher charges and fees should be proportionate and should be based on objective criteria, taking into consideration the economic power and the entity's ability to acquire data. This measure serves to safeguard opportunities for smaller businesses and new market entrants to innovate and compete in the digital economy.

(27) This Regulation proposes a series of targeted amendments to Regulation (EU) 2016/679 for clarification and simplification, whilst preserving the same level of data protection. Article 4 of Regulation (EU) 2016/679 provides that personal data is any information relating to an identified or identifiable natural person. In order to

---

33 Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36, ELI: http://data.europa.eu/eli/reco/2003/361/oj).

34 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) (OJ L 265, 12.10.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/1925/oj).

determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used to identify the natural person directly or indirectly. Taking into account the case-law of the Court of Justice of the European Union concerning the definition of personal data, it is necessary to provide further clarity on when a natural person should be considered to be identifiable. The existence of additional information enabling the data subject to be identified does not, in itself, mean that pseudonymised data must be regarded as constituting, in all cases and for every person or entity, personal data for the purposes of the application of Regulation (EU) 2016/679. In particular, it should be clarified that information is not to be considered personal data for a given entity where that entity does not have means reasonably likely to be used to identify the natural person to whom the information relates. A potential subsequent transmission of that information to third parties who have means reasonably allowing them to identify the natural person to whom the information relates, such as cross-checking with other data at their disposal, renders that information personal data only for those third parties who have such means at their disposal. 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. In this respect the Court of Justice of the European Union has held that a means of identifying the data subject is not reasonably likely to be used where the risk of identification appears in reality to be insignificant, in that the identification of that data subject is prohibited by law or impossible in practice, for example because it would involve a disproportionate effort in terms of time, cost and labour. An example of a prohibition against reidentification can be found in the obligations of health data users in Article 61(3) of Regulation (EU) 2025/327 of the European Parliament and of the Council[35]. The Commission, together with the European Data Protection Board, should support controllers in the application of this updated definition by stipulating technical criteria in an implementing act.

(28) In order to assess whether research meets the conditions of scientific research for the purpose of this Regulation, account can be taken of elements such as methodological and systematic approach applied while conducting the research in the specific area. Research and technology development should be conducted in academic, industry and other settings, including small and medium-sized undertakings, (Article 179(2) TFEU) and should be always of a of high quality and should adhere to the principles of principles of reliability, honesty, respect and accountability (verifiability).

(29) It should be reiterated that further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. In such cases it is not necessary to ascertain on the basis of Article 6(4) of this Regulation whether the purpose of the further processing is compatible with the purpose for which the personal data are initially collected.

---

[35] Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 (OJ L, 2025/327, 5.3.2025, ELI: http://data.europa.eu/eli/reg/2025/327/oj)

(30) Trustworthy AI is key in providing for economic growth and supporting innovation with socially beneficial outcomes. The development and use of AI systems and the underlying models such as large language models and generative video models rely on data, including personal data, in various phases in the AI lifecycle, such as the training, testing and validation phase and may in some instances be retained in the AI system or the AI model. The processing of personal data in this context may therefore be carried out for purposes of a legitimate interest within the meaning of Article 6 of Regulation (EU) 2016/679, where appropriate. This does not affect the obligation of the controller to ensure that the development or use (deployment) of AI in a specific context or for specific purposes complies with other Union or national law, or to ensure compliance where its use is explicitly prohibited by law. It also does not affect its obligation to ensure that all other conditions of Article 6(1)(f) of Regulation (EU) 2016/679 as well as all other requirements and principles of that Regulation are met.

(31) When the controller, in the light of the risk-based approach which informs the scalability of the obligations under this Regulation, is balancing the legitimate interest pursued by the controller or a third party and the interests, rights and freedoms of the data subject, consideration should be given to whether the interest pursued by the controller is beneficial for the data subject and society at large, which may for instance be the case where the processing of personal data is necessary for detecting and removing bias, thereby protecting data subjects from discrimination, or where the processing of personal data is aiming at ensuring accurate and safe outputs for a beneficial use, such as to improve accessibility to certain services. Consideration should also, among others, be given to reasonable expectations of the data subject based on their relationship with the controller, appropriate safeguards to minimise the impact on data subjects' rights such as providing enhanced transparency to data subjects, providing an unconditional right to object to the processing of their personal data, respecting technical indications embedded in a service limiting the use of data for AI development by third parties, the use of other state of the art privacy preserving techniques for AI training and appropriate technical measures to effectively minimise risks resulting, for example, from regurgitation, data leakage and other intended or foreseeable actions.

(32) The processing of personal data for scientific research purposes and the application of the GDPR's provisions on scientific research are conditional on the adoption of appropriate safeguards for the rights and freedoms of data subjects, pursuant to Article 89(1) GDPR. To that end, the GDPR balances the right to protection of personal data, pursuant to Article 8 CFREU, with the freedom of science, pursuant to Article 13 CFREU. The processing of personal data for the purpose of scientific research therefore pursues a legitimate interest within the meaning of Article 6(1)(f) of Regulation (EU) 2016/679, provided that such research is not contrary to Union or Member State law. This is without prejudice to the obligation of the controller to ensure that all other conditions of Article 6(1)(f) of Regulation (EU) 2016/679 as well as all other requirements and principles of that Regulation are met.

(33) The development of certain AI systems and AI models may involve the collection of large amounts of data, including personal data and special categories thereof. Special categories of personal data may residually exist in the training, testing or validation data sets or be retained in the AI system or the AI model, although the special categories of personal data are not necessary for the purpose of the processing. 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 personal data, derogating from the prohibition on processing special categories of personal data under Article 9(2) of Regulation (EU) 2016/679 should be allowed. The derogation should only apply where the controller has implemented appropriate technical and organisational measures in an effective manner to avoid the processing of those data, takes the appropriate measures during the entire lifecycle of an AI system or AI model and, once it identifies such data, effectively remove them. If removal would require disproportionate effort, notably where the removal of special categories of data memorised in the AI system or AI model would require re-engineering the AI system or AI model, the controller should effectively protect such data from being used to infer outputs, being disclosed or otherwise made available to third parties. This derogation should not apply where the processing of special categories of personal data is necessary for the purpose of the processing. In this case, the controller should rely on the derogations pursuant to Article 9(2)(a) – (j) of Regulation (EU) 2016/679.

(34) Biometric data, as defined in Article 4(14) of Regulation (EU) 2016/679, means processing of certain characteristics of a natural person through a specific technical means and which allows or confirms the unique identification of that person. The notion of biometric data includes two distinct functions, namely the identification of a natural person or the verification (also called authentication) of his or her claimed identity, both of which rely on different technical processes. The identification process is based on a 'one-to-many' search of the data subject's biometric data in a database, while the verification process is based on a 'one-to-one' comparison of biometric data provided by the data subject, who is thereby claiming his or her identity. Derogating from the prohibition to process biometric data under Article 9(1) of the Regulation should also be allowed where the verification of the claimed identity of the data subject is necessary for a purpose pursued by the controller, and suitable safeguards apply to enable the data subject to have sole control of the verification process. For example, where the biometric data are securely stored solely at the side of the data subject or are securely stored at the side of the controller in a state-of-the-art encrypted form and the encryption key or equivalent means is held solely by the data subject, that processing is not likely to create significant risks to his or her fundamental rights and freedoms. The controller does not gain knowledge of the biometric data or only for a very limited time during the verification process.

(35) Article 15 of Regulation (EU) 2016/679 provides data subjects with the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed and, where that is the case, access to the personal data and certain additional information. The right of access should allow the data subject to be aware of, and to verify, the lawfulness of the processing and enable him or her to exercise his or her other rights under Regulation (EU) 2016/679. By contrast, it should be clarified in Article 12 of the Regulation that the right of access, which is from the outset favourable to data subjects, should not be abused in the sense that the data subjects abuse them for purposes other than the protection of their data. For example, such an abuse of the right of access would arise where the data subject intends to cause the controller to refuse an access request, in order to subsequently demand the payment of compensation, potentially under the threat of bringing a claim for damages. Other examples of abuse include situations where data subjects make excessive use of the right of access with the only intent of causing damage or harm to the controller or when an individual makes a request, but at the same time offers to withdraw it in return for some form of benefit from the controller. Moreover, in order to keep their burden to a reasonable extent, controllers should bear a lower burden of

proof regarding the excessive character of a request than regarding the manifestly unfounded character of a request. The reason is that the manifestly unfounded character of a request depends on facts that lie principally within the controller's sphere of responsibility, whereas the excessive character of a request concerns the possibly abusive conduct of a data subject, which lies primarily outside the controller's sphere of influence, and therefore the controller may be able to prove such abuse only to a reasonable level. In any event, while requesting access under Article 15 of Regulation (EU) 2016/679 the data subject should be as specific as possible. Overly broad and undifferentiated requests should also be regarded as excessive.

(36) Article 13 of Regulation (EU) 2016/679 requires the data controller to provide the data subject with certain information on the processing of his or her personal data as well as certain further information necessary to ensure fair and transparent processing, as defined in paragraphs 1, 2 and 3 of that provision. According to paragraph 4 of Article 13 of Regulation (EU) 2016/679, that obligation does not apply where and insofar as the data subject already has the information. To further reduce the burden of data controllers, without undermining the possibilities of the data subject to exercise his or her rights under Chapter III of the Regulation, this derogation should be extended to situations where the processing is not likely to result in a high risk, within the meaning of Article 35 of the Regulation, and there are reasonable grounds to assume that the data subject already has the information referred to in points (a) and (c) of paragraph 1 in the light of the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller. These should be the situations where the context of the relationship between the controller and the data subject is very clear and circumscribed and the controller's activity is not data-intensive, such as the relationship between a craftsman and their clients, where the scope of processing is limited to the minimum data necessary to perform the service. The controller's activity is not data-intensive where it collects a low amount of personal data and its processing operations are not complex, which is not the case, for example, in the field of employment. In such circumstances, that is to say when the processing is non data-intensive, non-complex and where the controller collects a low amount of personal data, it should be reasonable to expect, for instance, that the data subject has the information on the identity and contact details of the controller as well as on the purpose of the processing when that processing is carried out for the performance of a contract to which a data subject is a party, or when the data subject has given his or her consent to that processing, in accordance with the requirements laid down in Regulation (EU) 2016/679. The same should apply to associations and sport clubs where the processing of personal data is confined to the management of membership, communication with members and the organisation of activities. Nevertheless, this derogation from the obligations of Article 13 is without prejudice to the independent obligations of the controller under Article 15 of that Regulation, which applies in case the data subject requests access based on the latter provision. Where the derogation from the obligations of Article 13 does not apply, in order to balance the need for completeness and easy understanding by the data subject, controllers may adopt a layered approach when providing the information required, notably by allowing users to navigate to further information.

(37) Where the processing takes place for the purpose of scientific research and the provision of information to the data subject proves to be impossible or would involve a disproportionate effort it should not be necessary to provide the information provided for under Article 13 of this Regulation. The controller should make reasonable efforts to acquire contact details if they are readily available and acquisition would not require

a disproportionate effort. The provision of the information would involve a disproportionate effort in particular where the controller at the time of collection of the personal data did not know or anticipate that it would process personal data for scientific research purposes at a later stage, in which case it may not have easily available contact details of the data subjects. In such situations the controller should inform data subjects indirectly, such as by making the information publicly available. The provision of such information should ensure that as many data subjects concerned as possible are reached. Relevant means to make the information publicly available should be determined depending on the context of the research project and the data subjects involved.

(38) Article 22 of Regulation (EU) 2016/679 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. In order to provide greater legal certainty, it should be clarified that decisions based solely on automated processing are allowed when specific conditions are met, as set out in Regulation (EU) 2016/679. It should also be clarified that when assessing whether a decision is necessary for entering into, or performance of, a contract between the data subject and a data controller, as set out in Article 22(2)(a) of Regulation (EU) 2016/679, it should not be required 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 When several equally effective automated processing solutions exist, the controller should use the less intrusive one.

(39) In order to reduce the burden on controllers while ensuring that supervisory authorities have access to the relevant information and can act on violations of the Regulation, the threshold for notification of a personal data breach to the supervisory authority under Article 33 of Regulation (EU) 2016/679 should be aligned with that of communication of a personal data breach to the data subject under Article 34 of that Regulation. 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 should not be required to notify the competent supervisory authority. The higher threshold for notifying a data breach to the supervisory authority does not affect the obligation of the controller to document the breach in accordance with paragraph 5 of Article 33 of Regulation (EU) 2016/679, or its obligation to be able to demonstrate its compliance with that Regulation, in accordance with Article 5(2) of that Regulation. In order to facilitate compliance by controllers and a harmonised approach in the Union, the Board should 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 Commission should take due account of the proposal prepared by the Board and review them, as necessary, prior to adoption. In order to take account of new information security threats, the common template and the list should be reviewed at least every three years and updated where necessary. The lack of 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 should not affect the obligations of controllers to notify those breaches.

(40) Article 35 of that Regulation (EU) 2016/679 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 natural persons. The supervisory authorities established pursuant to that Regulation are required to establish and make public a list

of the kind of processing operations which are subject to the requirement for a data protection impact assessment. In addition, the Regulation provides that supervisory authorities may establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. In order to effectively contribute to the aim of convergence of the economies and to effectively ensure free flow of personal data between Member States, increase legal certainty, facilitate compliance by controllers and ensure a harmonised interpretation of the notion of a high risk to the rights and freedoms of data subjects, a single list of processing operations should be provided at EU level, to replace the existing national lists. In addition, the publication of a list of the type of processing operations for which no data protection impact assessment is required, which is currently optional, should be made mandatory. The lists of processing operations should be prepared by the Board and adopted by the Commission as an implementing act. In order to facilitate compliance by controllers, the Board should also 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 Commission should take due account of the proposals prepared by the Board and review them, as necessary, prior to adoption. In order to take account of technological developments, the lists and the common template and methodology should be reviewed at least every three years and updated where necessary.

(41) Regulation (EU) 2018/1725 of the European Parliament and of the Council[36] applies to the processing of personal data by the Union institutions, bodies, offices and agencies. Directive (EU) 2016/680 of the European Parliament and of the Council[37] applies to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. Regulation (EU) 2018/1725 and Directive (EU) 2016/680 should be brough into alignment with the amendments to Regulation (EU) 2016/679 introduced by this Regulation.

(42) As clarified in recital 5 of Regulation (EU) 2018/1725, whenever the provisions of Regulation (EU) 2018/1725 follow the same principles as the provisions of Regulation (EU) 2016/679, those two sets of provisions should, under the case law of the Court of Justice of the European Union, be interpreted homogeneously. The scheme of Regulation (EU) 2018/1725 should be understood as equivalent to the scheme of Regulation (EU) 2016/679. Therefore, this Regulation also amends the provisions of Regulation (EU) 2018/1725 that are concerned by the amendments of Regulation (EU)

---

[36] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

[37] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj).

2016/679, insofar as the latter amendments are also relevant in the context of the processing of personal data by the Union institutions, bodies, offices and agencies.

(43) In order to provide a strong and coherent data protection framework in the Union, the necessary adaptations of Directive (EU) 2016/680 and any other Union legal act applicable to such processing of personal data should follow after the adoption of this regulation, in order to allow for their application as close as possible to the entry into application of the amendments to Regulation (EU) 2016/679 and Regulation (EU) 2018/1725.

(44) The storing of personal data, or the gaining of access to personal data already stored, in a terminal equipment and the subsequent processing of such data should be regulated under a single legal framework, namely Regulation (EU) 2016/679, where the subscriber of the electronic communications service or the user of the terminal equipment is a natural person. The amendments presented in this Regulation continue 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 amendments concern in particular storage of information in that equipment, accessing or otherwise collecting information from that equipment that entails the processing of personal data through cookies or similar technologies to gain information from the terminal equipment. The relevant rules should also apply regardless of whether the terminal equipment is owned by the natural person or by another legal or natural person.

The storing of personal data, or the gaining of access to personal data already stored, in a terminal equipment should continue to be allowed only on the basis of consent. Similar to the approach in Directive 2002/58/EC, this requirement should not preclude storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person, when that is based on Union or Member State law within the meaning of Article 6 of Regulation (EU) 2016/679 and if it fulfils all conditions of lawfulness laid down in that provision, and is done for the objectives laid down in Article 23(1) of Regulation (EU) 2016/679.

With a view to reducing the compliance burden and providing legal clarity to controllers, and given that certain purposes of processing pose a low risk to the rights and freedoms of data subjects or that such processing may be necessary to provide a service requested by the data subject, it is necessary to define a limitative list of purposes for which the processing should be permitted without consent. As regards storing of personal data, or the gaining of access to personal data already stored, in a terminal equipment, and subsequent processing that is necessary for those purposes, this Regulation should therefore provide that the processing is lawful. The controller, such as a media service provider, may mandate a processor, such as a market research company, to carry out the processing on its behalf.

For the subsequent processing of personal data for other purpose than those defined in the limitative list, Article 6 and, where relevant, Article 9 of Regulation (EU) 2016/679 should be applied. It is the responsibility of the controller in the light of the principle of accountability to choose the appropriate legal basis for the intended processing. In order to be able to rely on legitimate interest under Article 6(1), point f, of Regulation (EU) 2016/679 as a ground for the subsequent processing of personal data, the controller must show that it pursues the controller's or third parties' legitimate interest, the processing is necessary in order to achieve the purpose of that legitimate interest, and the interests or fundamental rights of the data subject do not

override the interests pursued by the controller. In this context, controllers should take outmost account of the following elements: whether the data subject is a child; the reasonable expectations of data subject; the impact on the individual either because of the scale of data processed or the sensitivity of the data processed; the scale of the processing at issue in the sense that the processing cannot be particularly extensive either because of their amount or the range of categories of data; the processing should be based on data limited to what is necessary and cannot be based on monitoring of large parts of the online activity of the data subjects; and other relevant factors as appropriate. The processing should not give rise to the continuous monitoring of the data subject's private life.

Where the controller cannot rely on legitimate interest as a legal ground for the subsequent processing, the processing should be based on another ground in Article 6(1), in particular on consent in accordance with Articles 6 and 7 of Regulation (EU) 2016/679, provided that all principles of Regulation (EU) 2016/679 are met.

(45) Data subjects that have refused a request for consent are often confronted with a new request to give consent each time they visit the same controller's online service again. This may have detrimental effects to the data subjects which may consent just in order to avoid repeating requests. The controller should therefore be obliged to respect the data subject's choices to refuse a request for consent for at least a certain period.

(46) Data subjects should have the possibility to rely on automated and machine-readable indications of their choice to consent or refuse a consent request or object to the processing of data. Such means should follow the state of the art. They can be implemented in the settings of a web browser or in the EU Digital Identity Wallet as set out by Regulation (EU) 914/2014, or any other adequate means. Rules set out in this Regulation should support the emergence of market-driven solutions with appropriate interfaces. The controller should be obliged to respect automated and machine-readable indications of data subject's choices once there are available standards. In light of the importance of independent journalism in a democratic society and in order not to undermine the economic basis for that, media service providers should not be obliged to respect the machine-readable indications of data subject's choices. The obligation for providers of web browsers to provide the technical means for data subjects to make choices with respect to the processing should not undermine the possibility for media service providers to request consent by data subjects.

(47) Directive 2002/58/EC on privacy and electronic communications 'ePrivacy Directive'), last revised in 2009, provides a framework for the protection of the right to privacy, including the confidentiality of communications. It also specifies Regulation (EU) 2016/679 in relation to processing of personal data in the context of electronic communication services. It protects the privacy and the integrity of user's or subscriber's terminal equipment used for such communications. The current provision of Article 5(3) of Directive 2002/58/EC should remain applicable insofar as the subscriber or user is not a natural person, and the information stored or accessed does not constitute or lead to the processing of personal data.

(48) Article 4 of Directive 2002/58/EC should be repealed. Article 4 of Directive 2002/58/EC sets requirements for providers of publicly available electronic communications services as regards safeguarding the security of their services and notification requirements. Subsequently, Directive (EU) 2022/2555 has set new requirements as regards cybersecurity risk-management measures and incident reporting for those providers. In order to reduce overlapping obligations for entities in

the electronic communications sector, Article 4 of Directive 2002/58/EC should be repealed. As regards the security of processing of personal data pursuant to Article 4(1) and (1a) of this directive and the notification of personal data breaches pursuant to Article 4(3) to (5) of Directive 2002/58/EC this directive, the Regulation (EU) 2016/679 already provide for comprehensive and up-to-date rules. These rules should therefore apply to providers of publicly available electronic communication services and providers of public communications networks, thereby ensuring that one regime applies to the controllers and processors.

(49) Several horizontal or sectorial Union legal acts require the notification of the same event to different authorities using different technical means and channels. The single-entry point for incident reporting should allow entities to fulfil reporting obligations under Directive (EU) 2022/2555, Regulation (EU) 2016/679, Regulation (EU) 2022/2554, Regulation (EU) No 910/2014 and Directive (EU) 2022/2557 by submitting notifications to a single interface. Furthermore, the single-entry point should give a possibility for entities to retrieve information that they have previously submitted using the single-entry point, thereby helping entities to keep track of their compliance with reporting obligations in connection with specific incidents.

(50) To ensure the security of the single-entry point, ENISA should take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of the single-entry point and the information submitted or disseminated via the single-entry point. When assessing the risk, and the appropriateness and proportionality of those measures, ENISA should take into account the sensitivity of information submitted or disseminated pursuant to the relevant Union legal acts. ENISA should consult competent authorities under the relevant Union legal acts when drafting the technical, operational and organisational measures necessary to establish, maintain and securely operate the single-entry point by making use of existing cooperation groups and networks of Member States established under these acts.

(51) Before enabling the notification of incidents, ENISA should pilot the functioning of the single-entry point which should include a thorough testing of the specificities and requirements for the notifications for the relevant Union legal acts. Based on the results of the piloting, the Commission should assess the proper functioning, reliability, integrity and confidentiality of the single-entry point. The Commission should consult the CSIRTs network and the competent authorities under the relevant Union legal acts, by making use of existing cooperation groups and networks of Member States established under these acts, when carrying out the assessment. Where the Commission finds that the single-entry point ensures the proper functioning, reliability, integrity and confidentiality, it should publish a notice to that effect in the Official Journal of the European Union. In case the Commission considers that the proper functioning, reliability, integrity and confidentiality is not ensured, ENISA should take all necessary corrective measures, followed by a reassessment by the Commission.

(52) To ensure the continuity and interoperability with existing national technical solutions that facilitate incident reporting, to the extent feasible, ENISA should take into account such national technical solutions when developing the specifications on the technical, operational and organisational measures necessary to establish, maintain and securely operate the single-entry point. Further, ENISA should consider technical protocols and tools such as application programming interfaces and machine-readable

standards that enable entities to integrate reporting obligations into business processes, and authorities to connect the single-entry point with their national reporting systems.

(53) To ensure that the single-entry point enables the relevant entities to submit the type of information and the format required under the relevant Union legal acts, ENISA should consult the Commission and the competent authorities under those acts. Where a Union legal act is not fully harmonized regarding the type of information and the format of notifications, Member States should inform ENISA about their national provisions.

(54) Based on Regulation (EU) 2022/2554, the financial sector has been at the forefront in implementing a harmonised, comprehensive and effective framework, including with regard to incident reporting. In order to simplify compliance, it is appropriate to align the incident reporting framework established under Regulation (EU) 2022/2554 with the single-entry point, while ensuring continuity and stability of the existing reporting framework, and considering that the single-entry point would be operational after it has been assessed that it ensures the proper functioning, reliability, integrity and confidentiality. Further, Regulation (EU) 2022/2554 has introduced standardised reporting templates streamlining the content of reports for major ICT-related incidents for the financial sector. The experience gained from the adoption of these templates provides valuable insights and best practices that should be taken into account when specifying the type of information, the format and the procedure of a notification for the purposes of reporting to the single-entry point under Directive (EU) 2022/2555, Directive (EU) 2022/2557 or Regulation (EU) 2016/679, where appropriate. For this purpose, the Commission should take due account of the regulatory technical standards adopted pursuant to Regulation (EU) 2022/2554, which specify the content of the initial notification, as well as the intermediate and final reports, concerning major ICT-related incidents. This approach aims to ensure consistency, promote synergies and reduce administrative burden on entities by minimizing the number of data fields that entities are required to complete, thereby facilitating more efficient and streamlined reporting processes.

(55) Under the relevant Union legal acts, certain incident-specific information is to be shared at a subsequent stage between competent authorities to facilitate effective oversight and coordination. Therefore, the single-entry point should be designed to accommodate and support the exchange of information at that level for each relevant Union legal act, ensuring that appropriate data flows between authorities are enabled in a secure, timely, and efficient manner, should the Member States decide to make use of this additional feature.

(56) To ensure that incident reporting is carried out via the single-entry point Directive (EU) 2022/2555, Regulation (EU) 2016/679, Regulation (EU) 2022/2554, Regulation (EU) 910/2014, and Directive (EU) 2022/2557 should therefore be amended accordingly. The single-entry point should start being used for the purpose of reporting under those acts within 18 months from the entry into force of this Regulation. When the Commission initiates the mechanisms of the notice delaying the date of application to 24 months from the entry into force of the Regulation, the corresponding provisions of Directive (EU) 2022/2555, Regulation (EU) 910/2014, Regulation (EU) 2022/2554 and Directive (EU) 2022/2557 should continue to apply for the purpose of meeting the reporting obligations laid down in the provisions.

(57) In the exceptional event that a technical impossibility prevents the submission of incident notifications using the single-entry point, entities should fulfil their reporting

obligations through alternative means. For that purpose, addressees of incident notifications under the relevant Union legal acts should ensure that they can receive such incident notifications through alternative means and should make information about that alternative means publicly available.

(58) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council[38], and delivered its opinion on [DATE]. The European Data Protection Board was consulted in accordance with Article 42(2) of Regulation (EU) 2018/1725 and delivered an opinion on [DATE].

(59) Regulation (EU) 2019/1150 establishes a targeted set of mandatory rules at Union level to ensure a fair, predictable, sustainable and trusted online business environment within the internal market. Regulation (EU) 2022/2065 and Regulation (EU) 2022/1925 provide a comprehensive regulatory framework for a safe, predictable and trusted online environments for all end-users of online services, and establish a level playing field for businesses in digital markets. In the interest of simplification of Union legislation in the field of online intermediation services and online platforms, and given that the objectives and material provisions of the Platform-to-Business Regulation are largely covered by the Digital Services Act and the Digital Markets Act, Regulation (EU) 2019/1050 should be repealed. Regulation (EU) 2022/2065 and Regulation (EU) 2022/1925 contribute to a fully harmonised regulatory framework for digital services and digital markets, by approximating national measures concerning the requirements for providers of intermediary services and the contestability and fairness of core platforms services provided by gatekeepers. For purposes of legal certainty, selected definitions in Article 2, the provisions on restrictions and suspensions in Article 4, as well as on the internal complaint-handling system in Article 11 of Regulation (EU) 2019/1150 that are cross-referenced by other legal acts, in particular Directive (EU) 2023/2831 on improving working conditions in platform work, and Article 15 ensuring enforcement, will temporarily remain in application until the original acts are amended.

(60) Given the technical nature of the amendments proposed in this Regulation and the urgency to deliver on a simplified legal framework, this Regulation should enter into force immediately after its publication in the Official Journal. As appropriate, transitional periods should be afforded for Member States and regulated entities to adjust to the rules.

---

[38] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

HAVE ADOPTED THIS REGULATION:

Article 1

Amendments to Regulation (EU) 2023/2854

Regulation (EU) 2023/2854 is amended as follows:

1. Article 1 is amended as follows:

(a) in paragraph 1, the following points are inserted:

‘(ea) voluntary registration of data intermediation services;

(eb) voluntary registration of entities which collect and process data made available for altruistic purposes;

(ec) the establishment of a European Data Innovation Board;

(ed) data localisation requirements and the availability of data to competent authorities;

(ee) the re-use of certain data and documents held by public sector bodies or by certain public undertakings, and of research data.’;

(b) in paragraph 2, the following points are added:

‘(g) Chapter VIIa applies to personal and non-personal data;

(h) Chapter VIIb applies to any non-personal data;

(i) Chapter VIIc applies to personal and non-personal data, namely the following:

(i) documents held by public sector bodies of Member States as referred

(1) to in Article 32i(1), point (a) or by public undertakings as referred

(2) to in Article 32i(1), point (b);

(ii) research data as referred to in Article 32i(1), point (c);

(iii) certain categories of protected data as referred to in Article 32i(1), point (a).’

(c) in paragraph 3, point (g) is replaced by the following:

‘(g) participants in data spaces.’;

(d) paragraph 7 is deleted.

(e) the following paragraphs 11, 12 and 13 are added:

‘11. Chapter VIIb of this Regulation is without prejudice to laws, regulations, and administrative provisions that relate to the internal organisation of Member States and that allocate, among public authorities and bodies governed by public law, powers and responsibilities for the processing of data without contractual remuneration of private parties, as well as to laws, regulations, and administrative provisions of Member States that provide for the implementation of such powers and responsibilities.

12. Where sector-specific Union or national law requires public sector bodies, data intermediation services providers or recognised data altruism organisations to comply with specific additional technical, administrative or organisational requirements that relate to Chapters VIIa and VIIb, including through an authorisation or certification regime, those provisions of that sector-specific Union or national law shall also apply. Any such specific additional requirements shall be non-discriminatory, proportionate and objectively justified.'

13. With regards to data and documents in scope of Section II of Chapter VIIc, Chapter VIIc of this Regulation does not affect the possibility for Member States to adopt more detailed or stricter rules, provided that those rules allow for more extensive re-use of data and documents.'

2. Article 2 is amended as follows:

(a) the following points (4a), (4b) and (4c) are inserted:

'(4a) 'consent' means consent as defined in Article 4, point (11), of Regulation (EU) 2016/679;

(4b) 'permission' means giving data users the right to the processing of non-personal data;

(4c) 'access' means data use, in accordance with specific technical, legal or organisational requirements, without necessarily implying the transmission or downloading of data;'

(b) point (13) is replaced by the following:

'(13) 'data holder' means a natural or legal person that has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation adopted in accordance with Union law, to use or make available data, including, where contractually agreed, product data or related service data, which it has retrieved or generated during the provision of a related service;

(c) the following points (28a) and (28b) are inserted:

'(28a) 'bodies governed by public law' means bodies that have all of the following characteristics:

(a) they are established for the specific purpose of meeting needs in the general interest, not having an industrial or commercial character;

(b) they have legal personality;

(c) they are financed, for the most part by the State, regional or local authorities, or by other bodies governed by public law; or are subject to management supervision by those authorities or bodies; or have an administrative, managerial or supervisory board, more than half of whose members are appointed by the State, regional or local authorities, or by other bodies governed by public law;

(28b) 'public undertaking' means any undertaking over which a public sector body may exercise directly or indirectly a dominant influence by virtue of their ownership of it, their financial participation therein, or the rules which govern it. A dominant

influence on the part of the public sector bodies shall be presumed in any of the following cases in which those bodies, directly or indirectly:

(a) hold the majority of the undertaking's subscribed capital;

(b) control the majority of the votes attaching to shares issued by the undertaking;

(c) can appoint more than half of the undertaking's administrative, management or supervisory body;';

(d) the following points (38a) and (38b) are inserted:

'(38a) 'data intermediation service' means a service which aims to establish relationships of an economic character for the purposes of data sharing between an undetermined number of data subjects or data holders and data users, through technical, legal or other means, including for the purpose of exercising the rights of data subjects in relation to personal data, and which :

(1) do not have as their main purpose the intermediation of copyright-protected content;

(2) are not jointly procured by several legal persons for exclusive use among them;

(38b) 'data altruism' means the voluntary sharing of data on the basis of the consent of data subjects to process personal data pertaining to them, or of permissions of data holders to allow the use of their non-personal data without seeking or receiving a reward that goes beyond compensation related to the costs that they incur where they make their data available for objectives of general interest as provided for in national law, where applicable, such as healthcare, combating climate change, improving mobility, facilitating the development, production and dissemination of official statistics, improving the provision of public services, public policy making or scientific research purposes in the general interest;'

(e) the following points (44) to (63) are added:

'(44) 'medium-sized enterprise' means a medium-sized enterprise as defined in Article 2 of Annex I to Recommendation 2003/361/EC;

(45) 'small mid-cap' or 'SMC' means a small mid-cap enterprise as defined in Article 2 of the Annex to Commission Recommendation (EU) 2025/1099;

(46) 'university' means a public sector body that provides post-secondary-school higher education leading to academic degrees;

(47) 'standard licence' means a set of predefined re-use conditions in a digital format, preferably compatible with standardised public licences available online;

(48) 'document' means:

(a) any content that is non-digital whatever its medium (paper or as a sound, visual or audiovisual recording); or

(b) any part of such content;

(50) ‘dynamic data’ means data and documents in a digital form, subject to frequent or real-time updates, in particular because of their volatility or rapid obsolescence; data generated by sensors are typically considered to be dynamic data;

(51) ‘research data’ means data , other than scientific publications, which are collected or produced in the course of scientific research activities and are used as evidence in the research process, or are commonly accepted in the research community as necessary to validate research findings and results;

(52) ‘re-use’ means the use by natural persons or legal entities of documents held by:

(a) public sector bodies, for commercial or non-commercial purposes other than the initial purpose within the public task for which the documents were produced, except for the exchange of documents between public sector bodies purely in pursuit of their public tasks; or

(b) public undertakings, under Chapter VIIc Section 2 for commercial or non-commercial purposes other than for the initial purpose of providing services in the general interest for which the documents were produced, except for the exchange of documents between public undertakings and public sector bodies purely in pursuit of the public tasks of public sector bodies;

(53) ‘high-value datasets’ means data and documents the re-use of which is associated with important benefits for society, the environment and the economy, in particular because of their suitability for the creation of value-added services, applications and new, high-quality and decent jobs, and because of the number of potential beneficiaries of the value-added services and applications based on those data and documents;

(54) ‘certain categories of protected data’ means data and documents held by public sector bodies which are protected on the grounds of

(a) commercial confidentiality, including business, professional and company secrets;

(b) statistical confidentiality;

(c) the protection of intellectual property rights of third parties; or

(d) the protection of personal data, insofar as such data fall outside the scope of Section 2 of Chapter VIIc;

(56) ‘secure processing environment’ means the physical or virtual environment and organisational means to ensure compliance with Union law in particular with regard to data subjects’ rights, intellectual property rights, and commercial and statistical confidentiality, integrity and accessibility, as well as with applicable national law, and to allow the entity providing the secure processing environment to determine and supervise all data processing actions, including the display, storage, download and export of data and the calculation of derivative data through computational algorithms;

(57) ‘re-user’ means a natural or legal person who was granted the right to re-use data or documents held by a public sector body or a public undertaking under Chapter VIIc or to research data or certain categories of protected data;

(58) ‘machine-readable format’ means a file format structured so that software applications can easily identify, recognise and extract specific data, including individual statements of fact, and their internal structure;

(59) ‘open format’ means a file format that is platform-independent and made available to the public without any restriction that impedes the re-use of documents;

(60) ‘formal open standard’ means a standard which has been laid down in written form, detailing specifications for the requirements on how to ensure software interoperability;

(61) ‘reasonable return on investment’ means a percentage of the overall charge, in addition to the amount needed to recover the eligible costs, not exceeding 5 percentage points above the fixed interest rate of the ECB;

(62) ‘data localisation requirement’ means any obligation, prohibition, condition, limit or other requirement provided for in the laws, regulations or administrative provisions of a Member State or resulting from general and consistent administrative practices in a Member State and in bodies governed by public law, including in the field of public procurement, without prejudice to Directive 2014/24/EU, which imposes the processing of data in the territory of a specific Member State or hinders the processing of data in any other Member State;

(63) ‘pseudonymisation’ means pseudonymisation as referred to under Article 4(5) of Regulation (EU) 2016/679.’

3. in Article 4, paragraph 8 is replaced by the following:

‘8. In exceptional circumstances, where the data holder who is a trade secret holder is able to demonstrate that, despite the technical and organisational measures taken by the user pursuant to paragraph 6 of this Article, it is highly likely to suffer serious economic damage from the disclosure of trade secrets or that the disclosure of trade secrets to the user poses a high risk of unlawful acquisition, use, or disclosure to third country entities, or entities established in the Union under the direct or indirect control of such entities, which are subject to jurisdictions offering weaker or non-equivalent protection compared to that under Union law, that data holder may refuse on a case-by-case basis a request for access to the specific data in question. That demonstration shall be duly substantiated on the basis of objective elements, such as the enforceability of trade secrets protection in third countries, the nature and level of confidentiality of the data requested, and the uniqueness and novelty of the connected product. It shall be provided in writing to the user without undue delay. Where the data holder refuses to share data pursuant to this paragraph, it shall notify the competent authority designated pursuant to Article 37.’;

4. in Article 5, paragraph 11 is replaced by the following:

‘11. In exceptional circumstances, where the data holder who is a trade secret holder is able to demonstrate that, despite the technical and organisational measures taken by the third party pursuant to paragraph 9 of this Article, it is highly likely to suffer serious economic damage from the disclosure of trade secrets or that the

disclosure of trade secrets to the third party poses a high risk of unlawful acquisition, use, or disclosure to third country entities, or entities established in the Union under the direct or indirect control of such entities, which are subject to jurisdictions offering weaker or non-equivalent protection compared to that under Union law, that data holder may refuse on a case-by-case basis a request for access to the specific data in question. That demonstration shall be duly substantiated on the basis of objective elements, such as the enforceability of trade secrets protection in third countries, the nature and level of confidentiality of the data requested, and the uniqueness and novelty of the connected product. It shall be provided in writing to the third party without undue delay. Where the data holder refuses to share data pursuant to this paragraph, it shall notify the competent authority designated pursuant to Article 37.';

5. the title of Chapter V is replaced by the following:

'MAKING DATA AVAILABLE TO PUBLIC SECTOR BODIES, THE COMMISSION, THE EUROPEAN CENTRAL BANK AND UNION BODIES ON THE BASIS OF A PUBLIC EMERGENCY';

6. Articles 14 and 15 are deleted;

7. the following Article 15a is inserted:

'Article 15a

Obligation for data holders to make data available on the basis of a public emergency

1. Where a public sector body, the Commission, the European Central Bank or a Union body demonstrates an exceptional need to use certain data to carry out its statutory duties in the public interest when responding to, mitigating, or supporting the recovery from a public emergency, it may request from data holders that are legal persons, other than public sectors bodies, to make available those data, including the metadata necessary to interpret and use those data. Upon such duly reasoned request, data holders shall make the data and metadata available to the requesting public sector body, the Commission, the European Central Bank or Union body. Such requests may also be made where the production of official statistics is required in relation to a public emergency.

2. Where the data requested are necessary to respond to a public emergency, and the requesting body pursuant to paragraph 1 is unable to obtain such data by other means in a timely and effective manner under equivalent conditions, the request shall concern non-personal data. Where the provision of non-personal data is insufficient to address the public emergency, personal data may also be requested and, where possible, made available in pseudonymized form, subject to appropriate technical and organisational measures to ensure their protection.

3. Where the data requested are necessary to mitigate or support the recovery from a public emergency, a requesting body pursuant to paragraph 1 acting on the basis of Union or national law, may request specific non-personal data, the lack of which prevent it from mitigating or supporting the recovery from a public emergency. Such requests shall not be made to microenterprises and small enterprises.';

8. in Article 16, paragraph 2 is replaced by the following:

‘2. This Chapter shall not apply to activities carried out by public sector bodies, the Commission, the European Central Bank or Union bodies relating to the prevention, investigation, detection or prosecution of criminal or administrative offences or the execution of criminal penalties, or to customs or taxation administration. This Chapter does not affect Union or national law governing such activities.’

9. Article 17 is amended as follows:

(a) paragraph 1 is amended as follows:

(i) the introductory wording is replaced by the following:

‘When requesting data pursuant to Article 15a, a public sector body, the Commission, the European Central Bank or a Union body shall:’;

(ii) points (b) and (c) are replaced by the following:

‘(b) demonstrate that the conditions to make a request under Article 15a are met;

(c) explain the purpose of the request, the intended use of the data requested, including, where applicable, by a third party in accordance with paragraph 4 of this Article, the duration of that use, and, where relevant, how the processing of personal data is to address the public emergency;’;

(b) paragraph 2 is amended as follows:

(i) point (c) is replaced by the following:

‘(c) be proportionate to the public emergency and duly justified, regarding the granularity and volume of the data requested and the frequency of access to the data requested;’;

(ii) point (e) is deleted.;

(c) paragraphs 5 and 6 are deleted;

10. Article 18 is amended as follows:

(a) in paragraph 2, the introductory wording is replaced by the following:

‘2. Without prejudice to specific needs regarding the availability of data defined in Union or national law, a data holder may decline or seek the modification of a request to make data available under this Chapter without undue delay and, in any event, no later than five working days after the receipt of a request pursuant to Article 15a(2) and without undue delay and, in any event, no later than 30 working days after the receipt of a request pursuant to Article 15a(3), on any of the following grounds:’;

(b) paragraph 5 is deleted;

11. Article 19 is amended as follows:

(a) in paragraph 1, the introductory wording is replaced by the following:

‘A public sector body, the Commission, the European Central Bank or a Union body receiving data pursuant to a request made under Article 15a shall:’;

(b) paragraph 3 is replaced by the following:

‘3. Disclosure of trade secrets to a public sector body, the Commission, the European Central Bank or a Union body shall be required only to the extent that it is strictly necessary to achieve the purpose of a request under Article 15a. In such a case, the data holder or, where they are not the same person, the trade secret holder shall identify the data which are protected as trade secrets, including in the relevant metadata. The public sector body, the Commission, the European Central Bank or the Union body shall, prior to the disclosure of trade secrets, take all necessary and appropriate technical and organisational measures to preserve the confidentiality of the trade secrets, including, as appropriate, the use of model contractual terms, technical standards and the application of codes of conduct.’;

12. Article 20 is replaced by the following:

‘Article 20

Compensation for making data available under Chapter V

1. Data holders shall make available data necessary to respond to a public emergency pursuant to Article 15a(2) free of charge. The public sector body, the Commission, the European Central Bank or the Union body that has received data shall provide public acknowledgement to the data holder if requested by the data holder.

2. The data holder shall be entitled to fair compensation for making data available in compliance with a request made pursuant to Article 15a(3). Such compensation shall cover the technical and organisational costs incurred to comply with the request including, where applicable, the costs of anonymisation, pseudonymisation, aggregation and of technical adaptation, and a reasonable margin. Upon request of the public sector body, the Commission, the European Central Bank or the Union body, the data holder shall provide information on the basis for the calculation of the costs and the reasonable margin.

3. By way of derogation from paragraph 1 of this Article, a data holder that is a microenterprise or small enterprise may claim compensation for making data available in response to a request under Article 15a(2), according to the conditions set in paragraph 2 of this Article.

4. Data holders shall not be entitled to compensation for making data available in compliance with a request made pursuant to Article 15a(3), where the specific task carried out in the public interest is the production of official statistics and where the purchase of data is not allowed by national law. Member States shall notify the Commission where the purchase of data for the production of official statistics is not allowed by national law.’;

13. Article 21 is amended as follows:

(a) the heading is replaced by the following:

‘**Sharing of data obtained in the context of a public emergency with research organisations or statistical bodies**’;

(b) paragraph 5 is replaced by the following:

‘5. Where a public sector body, the Commission, the European Central Bank or a Union body intends to transmit or make data available under paragraph 1, it shall without undue delay notify the data holder from whom the data was received, stating the following:

(a) the identity and contact details of the organisation or the individual receiving the data;

(b) the purpose of the transmission or making available of the data;

(c) the period for which the data is to be used and the technical protection;

(d) the organisational measures taken, including where personal data or trade secrets are involved.’;

14. The following Article 22a is inserted before Chapter VI:

‘Article 22a

Right to lodge a complaint

Where a dispute arises concerning a request for data under Article 15a, including its refusal, modification, the level of compensation, or the transmission or making available of data, the data holder, the public sector body, the Commission, the European Central Bank or the Union body may lodge a complaint with the competent authority, designated pursuant to Article 37, of the Member State where the data holder is established.’;

15. in Article 31, the following paragraphs 1a and 1b are inserted:

‘1a. The obligations laid down in Chapter VI, with the exception of Article 29, and in Article 34 shall not apply to data processing services other than those referred to in Article 30(1), where the majority of features and functionalities of the data processing service has been adapted by the provider to the specific needs of the customer, if the provision of such services is based on a contract concluded before or on 12 September 2025.

The provider of such data processing services shall not be required to renegotiate or amend a contract for the provision of those services before its expiry if that contract was concluded before or on 12 September 2025. Any contractual provision contained in that contract that is contrary to Article 29(1), (2), or (3) shall be considered null and void.

1b. A provider of a data processing service may include provisions on proportionate early termination penalties in a contract of fixed duration on the provision of data processing services other than those referred to in Article 30(1).

Where the provider of data processing service is a small and medium-sized enterprise or a small mid-cap, the obligations laid down in Chapter VI, with the exception of Article 29, and in Article 34 shall not apply to data processing services other than those referred to in Article 30(1), if the provision of such services is based on a contract concluded before or on 12 September 2025.

Where the provider of a data processing service is a small and medium-sized enterprise or a small mid-cap, the provider shall not be required to renegotiate or amend a contract for the provision of a data processing service other than

those referred to in Article 30(1) before its expiry 1 if that contract was concluded before or on 12 September 2025. Any contractual provision contained in that contract that is contrary to Article 29(1), (2), or (3) shall be considered null and void.';

16. Article 32 is amended as follows:

(a) paragraph 1 and 2 are replaced by the following:

'1. Providers of data processing services, the public sector body making available data or documents in accordance with Chapter VIIc Section 3, the natural or legal person to which the right to re-use data or documents in accordance with Chapter VIIc Section 3 was granted, a data intermediation services provider or a recognised data altruism organisation shall take all adequate technical, organisational and legal measures, including contracts, in order to prevent international and third-country governmental access and transfer of non-personal data held in the Union where such transfer or access would create a conflict with Union law or with the national law of the relevant Member State, without prejudice to paragraph 2 or 3.

2. Any decision or judgment of a third-country court or tribunal and any decision of a third-country administrative authority requiring a provider of data processing services, the public sector body making available data or documents in accordance with Chapter VIIc Section 3, the natural or legal person to which the right to re-use data or documents in accordance with Chapter VIIc Section 3 was granted, a data intermediation services provider or a recognised data altruism organisation to transfer or give access to non-personal data falling within the scope of this Regulation held in the Union shall be recognised or enforceable in any manner only if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union, or any such agreement between the requesting third country and a Member State.';

(b) in paragraph 3, first subparagraph, the introductory wording is replaced by the following:

'3. In the absence of an international agreement as referred to in paragraph 2, where a provider of data processing services, the public sector body making available data or documents in accordance with Chapter VIIc Section 3, the natural or legal person to which the right to re-use data or documents in accordance with Chapter VIIc Section 3 was granted, a data intermediation services provider or a recognised data altruism organisation is the addressee of a decision or judgment of a third-country court or tribunal or a decision of a third-country administrative authority to transfer or give access to non-personal data falling within the scope of this Regulation held in the Union and compliance with such a decision or judgement would risk putting the addressee in conflict with Union law or with the national law of the relevant Member State, transfer to or access to such data by that third-country authority shall take place only where:';

(c) paragraphs 4 and 5 are replaced by the following:

'4. If the conditions laid down in paragraph 2 or 3 are met, the provider of data processing services, the public sector body making available data or documents in accordance with Chapter VIIc Section 3, the natural or legal person to which

the right to re-use data or documents in accordance with Chapter VIIc Section 3 was granted, the data intermediation services provider or the recognised data altruism organisation shall provide the minimum amount of data permissible in response to a request, on the basis of the reasonable interpretation of that request by the provider or relevant national body or authority referred to in paragraph 3, second subparagraph.

5. The provider of data processing services, the public sector body making available data or documents in accordance with Chapter VIIc Section 3, the natural or legal person to which the right to re-use data or documents in accordance with Chapter VIIc Section 3 was granted, the data intermediation services provider or the recognised data altruism organisation shall inform the natural or legal person whose rights and interests might be affected about the existence of a request of a third-country authority to access its data before complying with that request, except where the request serves law enforcement purposes and for as long as this is necessary to preserve the effectiveness of the law enforcement activity.';

17. Article 36 is deleted.

18. the following Chapters VIIa, VIIb and VIIc are inserted:

'CHAPTER VIIa
DATA INTERMEDIATION SERVICES
AND DATA ALTRUISM ORGANISATIONS'

Article 32a

Public Union registers

(1) The Commission shall keep and regularly update public Union registers of:

(a) recognised data intermediation services providers and

(b) recognised data altruism organisations.

(2) Data intermediation services providers registered in the public Union register referred to in paragraph 1 point (a) may use the label 'data intermediation services provider recognised in the Union' in its written and spoken communication, as well as a common logo referred to in paragraph 4.

(3) Data altruism organisations registered in the public Union register referred to in paragraph 1 point (b) may use the label 'data altruism organisation recognised in the Union' in its written and spoken communication, as well as the common logo referred to in paragraph 4.

(4) In order to ensure that data intermediation services providers recognised in the Union are easily identifiable throughout the Union, the Commission is empowered to adopt implementing acts establishing a design for the common logo. Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 46(1a).

Article 32b

Competent authorities for the registration of data intermediation services providers and data altruism organisations

(1) Each Member State shall designate one or more competent authorities responsible for the application and enforcement of this Chapter in accordance with Article 37(1).

(2) The competent authorities shall be set up in a manner so that their independence from any recognised data intermediation services provider or recognised data altruism organisation is guaranteed.

Article 32c

General requirements for registration of recognised data intermediation services providers

In order to qualify for registration in the public Union register referred to in Article 32a paragraph 1 point (a), a data intermediation services provider shall meet all of the following requirements:

(a) they do not use the data for which it provides data intermediation services for purposes other than to put them at the disposal of data users;

(b) the data they collect with respect to any activity of a natural or legal person for the purpose of the provision of the data intermediation service, including the date, time and geolocation data, duration of activity and connections to other natural or legal persons established by the person who uses the data intermediation service, are used only for the development of that data intermediation service;

(c) where they offer additional tools and services to data holders or data subjects for the specific purpose of facilitating the exchange of data, such as temporary storage, curation, conversion, encryption, anonymisation and pseudonymisation, such tools and services are used only at the explicit request or approval of the data holder or data subject;

(d) where data intermediation service providers which are not micro and small sized enterprises offer value-added services to their clients other than the services referred to in point (c), they fulfil the following conditions:

    (i) the value-added services are explicitly requested by the user;

    (ii) the data are not used for other purposes than performing the value-added service;

    (iii) the value-added services are offered through a functionally separate entity;

    (iv) the undertaking seeking to offer the value-added services is not designated as a gatekeeper pursuant to Article 3 of Regulation (EU) 2022/1925;

    (v) the commercial terms, including pricing, for the provision of data intermediation services to a data holder or data user are not dependent upon whether the data holder or data user uses value-added services provided by the data intermediation services provider or by a related entity;

(e) the data intermediation services provider offering services to data subjects acts in the data subjects' best interest where it facilitates the exercise of their rights, in particular by informing and, where appropriate, advising data subjects in a concise, transparent, intelligible and easily accessible manner about intended data uses by data users and standard terms and conditions attached to such uses before data subjects give consent.

Article 32d

General requirements for registration of recognised data altruism organisations

In order to qualify for registration in the public Union register referred to in Art. 32a paragraph 1 point (b), a data altruism organisation shall meet all of the following requirements:

(a) they carry out data altruism activities;

(b) they are a legal person established pursuant to national law to meet objectives of general interest as provided for in national law, where applicable;

(c) they operate on a not-for-profit basis and are legally independent from any entity that operates on a for-profit basis;

(d) they carry out their data altruism activities through a structure that is functionally separate from their other activities.

Article 32e

Registration

(1) Data intermediation services provider which meets the requirements set out in Article 32c may submit an application for registration in the public Union register of recognised data intermediation services providers to the competent authority referred to in Article 32b in the Member State in which they have their main establishment.

Data altruism organisation which meets the requirements set out in Article 32d may submit an application for registration in the public Union register of recognised data altruism organisations to the competent authority referred to in Article 32b in the Member State in which they have their main establishment.

(2) Data intermediation services providers and data altruism organisations that have no main establishment in the Union shall designate a legal representative in one of the Member States. The legal representative shall be mandated to be addressed in addition to or instead of the data intermediation services provider or data altruism organisation by competent authorities or data subjects and data holders. The legal representative shall cooperate with and comprehensively demonstrate to the competent authority, upon request, the actions taken and provisions put in place by the data intermediation services provider or the data altruism organisation to ensure compliance with this Regulation.

The data intermediation services provider or data altruism organisation shall be deemed to be under the jurisdiction of the Member State in which the legal representative is located. The designation of a legal representative shall be without prejudice to any legal actions which could be initiated against the data intermediation services provider or data altruism organisation.

(3) Competent authorities shall establish the necessary application forms.

(4) Where a data intermediation services provider has submitted all necessary information pursuant to paragraph 3 of this Article, and complies with the requirements set out in Article 32c, the competent authority shall, within 12 weeks after the receipt of the application for registration, take a decision on whether the provider complies with the criteria set out in Article 32c. Where the provider complies with the criteria, the competent authority shall submit the relevant

information to the Commission which shall register the providers in the public Union register as a recognised data intermediation services provider.

The first subparagraph shall also apply where a data altruism organisation has submitted all necessary information pursuant to paragraph 2, and complies with the registration requirements set out in Article 32d.

The registration in the public Union register shall be valid in all Member States.

(5) The competent authority may charge fees for the registration in accordance with national law. Such fees shall be proportionate and objective and be based on the administrative costs related to the monitoring of compliance. In the case of small-mid caps, small and medium-sized enterprises, and start-ups, the competent authority may charge a discounted fee or waive the fee.

(6) Registered entities shall notify the competent authority of any subsequent changes to the information as provided during the application process or where they cease their data intermediation or data altruism activities in the Union.

(7) The competent authority shall without delay and by electronic means notify the Commission of any notification pursuant to paragraph 6. The Commission shall without undue delay update the public Union register.

Article 32f

Duties of recognised data altruism organisations

(1) Recognised data altruism organisations shall inform data subjects or data holders prior to any processing of their data in a clear and easily comprehensible manner of the following:

(a) the objectives of general interest and, if applicable, the specified, explicit and legitimate purpose for which personal data is to be processed, and for which it permits the processing of their data by a data user;

(b) the location of the processing and the objectives of general interest for which it permits any processing carried out in a third country, where the processing is carried out by the recognised data altruism organisation.

(2) Recognised data altruism organisations shall not use the data for other objectives than the objectives of general interest for which the data subject or data holder allows the processing. The recognised data altruism organisation shall not use misleading marketing practices to solicit the provision of data.

(3) Recognised data altruism organisations shall provide electronic means for obtaining consent from data subjects or permissions to process data made available by data holders as well as for their withdrawal.

(4) Recognised data altruism organisations shall, without delay, inform data holders in the event of any unauthorised transfer, access or use of the non-personal data that it has shared.

(5) Where recognised data altruism organisations facilitate data processing by third parties, including by providing tools for obtaining consent from data subjects or permissions to process data made available by data holders, they shall, where relevant, specify the third-country in which the data use is intended to take place.

Article 32g

Monitoring of compliance

(1) The competent authorities referred to in Article 32b shall, either on their own initiative or on a request by a natural or legal person, monitor and supervise whether recognised data intermediation services providers and recognised data altruism organisations comply with the requirements laid down in this Chapter, including whether they continue to comply with the requirements for registration laid down therein.

(2) The competent authorities shall have the power to request from recognised data intermediation services providers or recognised data altruism organisations, or their legal representative, all the information that is necessary to verify compliance with the requirements laid down in this Chapter. Any request for information shall be proportionate to the performance of the task and shall be reasoned.

(3) Where a competent authority finds that a recognised data intermediation services provider or a recognised data altruism organisation does not comply with one or more of the requirements laid down in this Chapter, it shall notify that entity, or its legal representative, of those findings and give it the opportunity to state its views, within 30 days of the receipt of the notification.

(4) The competent authority shall have the power to require the cessation of the non-compliance referred to in paragraph 3 either immediately or within a reasonable time limit and shall take appropriate and proportionate measures with the aim of ensuring compliance.

(5) If a recognised data intermediation services provider or a recognised data altruism organisation does not comply with one or more of the requirements laid down in this Chapter even after having been notified in accordance with paragraph 3, that entity shall:

(a) lose its right to use the label referred to in Article 32a in written and spoken communication;

(b) be removed from the public Union register referred to in Article 32a.

Any decision revoking the right to use the label as referred to in the first subparagraph, point (a), shall be made public by the competent authority.

‘CHAPTER VIIb

Free flow of non-personal data in the Union’

‘Article 32h

Prohibition of localisation requirements for non-personal data within the Union

(1) Data localisation requirements for non-personal data shall be prohibited, unless they are justified on grounds of public security in compliance with the principle of proportionality or laid down on the basis of Union law.

(2) Member States shall immediately communicate to the Commission any draft act which introduces a new data localisation requirement or makes changes to an existing data localisation requirement in accordance with the procedures set out in Articles 5, 6 and 7 of Directive (EU) 2015/1535 of the European Parliament and of the Council.’

Chapter VIIc

Re-use of data and documents held by public sector bodies

SECTION 1

GENERAL PROVISIONS

Article 32i

Subject matter and scope

(1) This Chapter establishes a set of rules governing the re-use and the practical arrangements for facilitating the re-use of the following:

(a) existing data and documents held by public sector bodies of the Member States, including certain categories of protected data;

(b) existing data and documents held by public undertakings that are:

(i) active in the areas referred to in Chapter II of Directive 2014/25/EU of the European Parliament and of the Council;

(ii) acting as public service operators pursuant to Article 2 of Regulation (EC) No 1370/2007 of the European Parliament and of the Council;

(iii) acting as air carriers fulfilling public service obligations pursuant to Article 16 of Regulation (EC) No 1008/2008 of the European Parliament and of the Council; or

(iv) acting as Community shipowners fulfilling public service obligations pursuant to Article 4 of Council Regulation (EEC) No 3577/92 ;

(c) research data pursuant to the conditions set out in Article 32t.

(2) This Chapter does not apply to the following:

(a) data and documents the supply of which is an activity falling outside the scope of the public task of the public sector bodies concerned as defined by law or by other binding rules in the Member State, or, in the absence of such rules, as defined in accordance with common administrative practice in the Member State in question, provided that the scope of the public tasks is transparent and subject to review;

(b) data and documents held by public undertakings and:

(i) produced outside the scope of the provision of services in the general interest as defined by law or other binding rules in the Member State;

(ii) related to activities directly exposed to competition and therefore, pursuant to Article 34 of Directive 2014/25/EU, not subject to procurement rules;

(c) data and documents, such as sensitive data, which are excluded from access by virtue of the access regimes in the Member State on grounds of the protection of national security (namely, State security), defence, or public security;

(d) data and documents held by public service broadcasters and their subsidiaries, and by other bodies or their subsidiaries for the fulfilment of a public service broadcasting remit.

(3) Section 2 of this Chapter does not apply to:

(a) data or documents, such as sensitive data or documents, which are excluded from access by virtue of the access regimes in the Member State, including on grounds of:

(i) statistical confidentiality;

(ii) commercial confidentiality (including business, professional or company secrets);

(b) data or documents access to which is restricted by virtue of the access regimes in the Member States,

(i) including cases whereby citizens or legal entities have to prove a particular interest to obtain access to documents;

(ii) on grounds of protection of personal data, and parts of data or documents accessible by virtue of those regimes which contain personal data the re-use of which has been defined by law as being incompatible with the law concerning the protection of individuals with regard to the processing of personal data or as undermining the protection of privacy and the integrity of the individual, in particular in accordance with Union or national law regarding the protection of personal data; logos, crests and insignia;

(c) data or documents for which third parties hold intellectual property rights;

(d) data or documents held by cultural establishments other than libraries, including university libraries, museums and archives;

(e) data or documents held by educational establishments of secondary level and below, and, in the case of all other educational establishments, data other than those referred to in paragraph 1, point (c);

(f) data or documents other than those referred to in paragraph 1, point (c), held by research performing organisations and research funding organisations, including organisations established for the transfer of research results;

(g) Data or documents access to which is excluded or restricted on grounds of critical entity or critical infrastructure protection related information as defined in points (1) and (4) of Article 2 of Directive (EU) 2022/2557.

(4) Section 3 of this Chapter does not apply to:

(a) data and documents that are not certain categories of protected data;

(b) data or documents held by public undertakings;

(c) data or documents held by cultural establishments and educational establishments;

(d) data and documents covered by Section 2 of this Chapter.

(5) This Chapter builds on, and is without prejudice to, Union and national access regimes, in particular with regard to the granting of access to and disclosure of official documents.

(6) The obligations imposed in accordance with this Chapter shall apply only insofar as they are compatible with the provisions of international agreements on the protection of intellectual property rights, in particular the Berne Convention for the Protection of Literary and Artistic Works (Berne Convention), the Agreement on Trade-related Aspects of Intellectual Property Rights (TRIPS Agreement and the World Intellectual Property Organization Copyright Treaty (WCT).

(7) The right for the maker of a database provided for in Article 7(1) of Directive 96/9/EC shall not be exercised by public sector bodies in order to prevent the re-use of data and documents or to restrict re-use beyond the limits set by this Chapter.

(8) This Chapter governs the re-use of existing data and documents held by public sector bodies and public undertakings of the Member States, including data and documents to which Directive 2007/2/EC of the European Parliament and of the Council applies.

(9) This Chapter is without prejudice to Union and national law and international agreements to which the Union or Member States are party on the protection of categories of data or documents referred to in Article 2(54).

Article 32j

Non-discrimination

(1) Any applicable conditions for the re-use of data or documents shall be non-discriminatory, transparent, proportionate and objectively justified with regard to the categories of data or documents and the purposes of re-use and the nature of the data or documents for which re-use is allowed. Those conditions shall not be used to restrict competition. This principle shall equally apply for comparable categories of re-use, including for cross-border re-use.

(2) If data or documents are re-used by a public sector body as input for its commercial activities which fall outside the scope of its public tasks, the same charges and other conditions shall apply to the supply of the data or documents for those activities as the ones that apply to other re-users.

Article 32k

Exclusive arrangements

(1) The re-use of data or documents shall be open to all potential actors in the market, even if one or more market actors already exploit added-value products based on those data or documents. Agreements or other arrangements or practices pertaining to the re-use of data or documents, which have as their objective or effect to grant exclusive rights or to restrict the availability of data or documents for re-use by entities other than the parties to such agreements, arrangements or practices, shall be prohibited.

(2) By way of derogation of paragraph 1, where an exclusive right is necessary for the provision of a service of general interest, such a right may be granted to the extent

necessary for the provision of the service or the supply of the product under the following conditions:

(a) the exclusive right is granted through an administrative act or contractual agreement in accordance with applicable Union and national law and in compliance with the principles of transparency, equal treatment and non-discrimination.

(b) the agreements granting the exclusive right, including the reasons as to why it is necessary to grant such a right, is transparent and made publicly available online, in a form that complies with relevant Union law on public procurement and national law.

(c) except for exclusive rights related to the digitisation of cultural resources, the validity of the reason for granting exclusive rights concerning data and documents within the scope of Section 2 shall be subject to regular review, and shall in any event, be reviewed every three years.

(d) exclusive arrangements established on or after 16 July 2019 shall be made publicly available online at least two months before they come into effect. The final terms of such arrangements shall be transparent and shall be made publicly available online.

(3) By way of derogation of paragraph 1, where an exclusive right relates to the digitisation of cultural resources, the period of exclusivity shall in general not exceed 10 years. Where that period exceeds 10 years, its duration shall be in accordance with applicable Union and national law subject to review during the 11th year and, if applicable, every seven years thereafter.

(4) In the case of an exclusive right referred to in paragraph 3, the public sector body concerned shall be provided free of charge with a copy of the digitised cultural resources as part of those arrangements. That copy shall be available for re-use at the end of the period of exclusivity.

(5) For certain categories of protected data, the duration of an exclusive right to re-use data shall not exceed 12 months. Where a contract is concluded, the duration of the contract shall be the same as the duration of the exclusive right.

(6) Agreements or other arrangements or practices that, without expressly granting an exclusive right, aim at, or could reasonably be expected to lead to, a restricted availability for the re-use of data and documents within the scope of Section 2 by entities other than parties to such arrangementsshall be made publicly available online at least two months before their coming into effect. The effect of such legal or practical arrangements on the availability of data for re-use shall be subject to regular reviews and shall, in any event, be reviewed every three years. The final terms of such arrangements shall be transparent and made publicly available online.

(7) For existing exclusive arrangements, the following shall apply:

(a) exclusive arrangements concerning data and documents within the scope of Section 2existing on 17 July 2013 that do not qualify for the exceptions set out in paragraphs 2 and 3 and that were entered into by public sector bodies shall be terminated at the end of the contract and in any event not later than 18 July 2043;

(b) exclusive arrangements concerning data and documents within the scope of Section 2 existing on 16 July 2019 that do not qualify for the exceptions set out

in paragraphs 2 and 3, and that were entered into by public undertakings, shall be terminated at the end of the contract and in any event not later than 17 July 2049;

Article 32l

General principles relating to charging

(1) Any charges set out under Section 2 or Section 3 shall be transparent, non-discriminatory, proportionate and objectively justified and shall not restrict competition.

(2) In the case of standard charges for the re-use of data or documents, any applicable conditions and the actual amount of those charges, including the calculation basis for such charges, shall be established in advance and published, through electronic means where possible and appropriate.

(3) In the case of charges for the re-use other than those referred to in paragraph 1, the factors that are taken into account in the calculation of those charges shall be indicated at the outset. Upon request, the holder of the data or documents in question shall also indicate the way in which such charges have been calculated in relation to a specific re-use request.

(4) Public sector bodies shall ensure that any charges can also be paid online through widely available cross-border payment services, without discrimination based on the place of establishment of the payment service provider, the place of issue of the payment instrument or the location of the payment account within the Union.

Article 32m

Information on means of redress

Public sector bodies shall ensure that applicants for re-use of data or documents are informed of available means of redress relating to decisions or practices affecting them.

SECTION 2

RE-USE OF OPEN GOVERNMENT DATA

Subsection 1 Scope and General Principles

Article 32n

General principle for re-use of open government data

(1) Data or documents in scope of this Section shall be re-usable for commercial or non-commercial purposes in accordance with Section 1 and Section 2 Subsection 3.

(2) For data or documents in which libraries, including university libraries, museums and archives hold intellectual property rights and for data or documents held by public undertakings, where the re-use of such data or documents is allowed, those data or documents shall be re-usable for commercial or non-commercial purposes in accordance with Section 1 and Section 2 Subsection 3.

Subsection 2

Requests for re-use

Article 32o

Processing requests for re-use

(1) Public sector bodies shall, through electronic means where possible and appropriate, process requests for re-use and shall make the document available for re-use to the applicant or, if a licence is needed, finalise the licence offer to the applicant within a reasonable time that is consistent with the time frames laid down for the processing of requests for access to data or documents.

(2) Where no time limits or other rules regulating the timely provision of data or documents have been established, public sector bodies shall process the request and shall deliver the data or documents for re-use to the applicant or, if a licence is needed, finalise the licence offer to the applicant as soon as possible, and in any event within 20 working days of receipt. That time frame may be extended by a further 20 working days in the case of extensive or complex requests. In such cases, the applicant shall be notified as soon as possible, and in any event within three weeks of the initial request, that more time is needed to process the request and the reasons why.

(3) In the event of a negative decision, the public sector bodies shall communicate the grounds for refusal to the applicant on the basis of the relevant provisions of the access regime in that Member State or the provisions of this Regulation, in particular points (a) to (c) of paragraph 2 of Article 32i and points (a) to (d) of paragraph 3 of Article 32i or Article 32n (general principle ODD Section). Where a negative decision is based on point (d) of paragraph 3 of Article 32i, the public sector body shall include a reference to the natural or legal person who is the rightsholder, where known, or alternatively to the licensor from which the public sector body has obtained the relevant material. Libraries, including university libraries, museums and archives, shall not be required to include such a reference.

(4) The means of redress shall include the possibility of review by an impartial review body with the appropriate expertise, such as the national competition authority, the relevant access to data or documents authority, the supervisory authority established in accordance with Regulation (EU) 2016/679 or a national judicial authority, whose decisions are binding upon the public sector body concerned.

(5) For the purposes of this Article, Member States shall establish practical arrangements to facilitate effective re-use of data or documents. Those arrangements may in particular include the means to supply adequate information on the rights provided for in this Regulation and to offer relevant assistance and guidance.

(6) This Article shall not apply to the following entities:

(a) public undertakings;

(b) educational establishments, research performing organisations and research funding organisations.

Subsection 3

Conditions for re-use

Article 32p

Available formats

(1) Without prejudice to Subsection 5, public sector bodies and public undertakings shall make their data or documents available in any pre-existing format or language and, where possible and appropriate, by electronic means, in formats that are open, machine-readable, accessible, findable and re-usable, together with their metadata. Both the format and the metadata shall, where possible, comply with formal open standards.

(2) Member States shall encourage public sector bodies and public undertakings to produce and make available data or documents falling within the scope of this Section in accordance with the principle of 'open by design and by default.

(3) Paragraph 1 shall not imply an obligation for public sector bodies to create or adapt data or documents or provide extracts in order to comply with that paragraph where this would involve disproportionate effort, going beyond a simple operation.

(4) Public sector bodies shall not be required to continue the production and storage of a certain type of document with a view to the re-use of such data or documents by a private or public sector organisation.

(5) Public sector bodies shall make dynamic data available for re-use immediately after collection, via suitable APIs and, where relevant, as a bulk download.

(6) Where making dynamic data available for re-use immediately after collection, as referred to in paragraph 5, would exceed the financial and technical capacities of the public sector body, thereby imposing a disproportionate effort, those dynamic data shall be made available for re-use within a time frame or with temporary technical restrictions that do not unduly impair the exploitation of their economic and social potential.

(7) Paragraphs 1 to 6 shall apply to existing data or documents held by public undertakings which are available for re-use.

(8) The high-value datasets, as listed in accordance with Article 32v(1) shall be made available for re-use in machine- readable format, via suitable APIs and, where relevant, as a bulk download.'

Article 32q

Principles governing charging for open government data

(1) The re-use of data or documents within the scope of this Section shall be free of charge. However, the recovery by the public sector body holding the data of the marginal costs incurred for the reproduction, provision and dissemination of such data or documents as well as for anonymisation of personal data and measures taken to protect commercially confidential information may be allowed.

(2) Paragraph 1 shall not apply to the following entities:

(a) public sector bodies that are required to generate revenue to cover a substantial part of their costs relating to the performance of their public tasks;

(b) libraries, including university libraries, museums and archives;

(c) public undertakings.

(3) Member States shall publish online a list of the public sector bodies referred to in paragraph 2, point (a).

(4) In the cases referred to in paragraph 2, points (a) and (c), the total charges shall be calculated in accordance with objective, transparent and verifiable criteria. Such

criteria shall be laid down by Member States. The total income from supplying and allowing the re-use of data or documents over the appropriate accounting period shall not exceed the cost of their collection, production, reproduction, dissemination and data storage, together with a reasonable return on investment, and where applicable, the anonymisation of personal data and measures taken to protect commercially confidential information. Charges shall be calculated in accordance with the applicable accounting principles.

(5) Where charges are made by the public sector bodies referred to in paragraph 2, point (b), the total income from supplying and allowing the re-use of data or documents over the appropriate accounting period shall not exceed the cost of collection, production, reproduction, dissemination, data storage, preservation and rights clearance and, where applicable, the anonymisation of personal data and measures taken to protect commercially confidential information, together with a reasonable return on investment. Charges shall be calculated in accordance with the accounting principles applicable to the public sector bodies involved.

(6) Public sector bodies may set out higher charges for the re-use of data and documents by very large enterprises than the charges provided for in paragraphs 1, 4 and 5. Any such charges shall be proportionate and based on objective criteria, taking into account the economic power, or the ability of the entity to acquire data, including in particular a designation as a gatekeeper under Regulation (EU) 2022/1925. In addition to the elements listed in paragraph 1 of this Article, such charges may cover the cost of collection, production, reproduction dissemination and data storage and where applicable the cost of anonymisation or measures to protect the confidentiality of the data or documents, together with a reasonable return on investment.

(7) The re-use of the following shall be free of charge for the user:

(a) subject to Article 32v paragraph (3), (4) and (5), the high-value datasets, as listed in accordance with paragraph 1 of that Article;

(b) research data referred to in point (c) of paragraph 1 of Article 32i.

Article 32r

Standard licences

(1) The re-use of data or documents shall not be subject to conditions, unless such conditions are objective, proportionate, non-discriminatory and justified on grounds of a public interest objective.

(2) When re-use is subject to conditions, those conditions shall not unnecessarily restrict possibilities for re-use and shall not be used to restrict competition.

(3) In Member States where licences are used, public sector bodies shall ensure that the standard licences for the re-use of public sector data or documents, which can be adapted to meet particular licence applications, are available in digital format and able to be processed electronically.

(4) Public sector bodies may establish special conditions for the re-use of data and documents by very large enterprises. Such conditions shall be proportionate and should be based on objective criteria. They shall be established taking into consideration the economic power, or the ability of the entity to acquire data, including in particular a designation as a gatekeeper under Regulation (EU) 2022/1925.

Article 32s

Practical arrangements

(1) Member States shall make practical arrangements facilitating the search for data or documents available for re-use, such as asset lists of main data or documents with relevant metadata, accessible where possible and appropriate online and in machine-readable format, and portal sites that are linked to the asset lists. Where possible, Member States shall facilitate the cross-linguistic search for data or documents, in particular by enabling metadata aggregation at Union level.

Member States shall also encourage public sector bodies to make practical arrangements facilitating the preservation of data or documents available for re-use.

(2) Member States shall, in cooperation with the Commission, continue efforts to simplify access to datasets, in particular by providing a single point of access and by progressively making available suitable datasets held by public sector bodies with regard to the data or documents to which this Section applies, as well as to data held by Union institutions, in formats that are accessible, readily findable and re-usable by electronic means.

Subsection 4

Research data

Article 32t

Research data

(1) Member States shall support the availability of research data by adopting national policies and relevant actions aiming at making publicly funded research data openly available (‘open access policies’), following the principle of ‘open by default’ and compatible with the FAIR principles. In that context, concerns relating to intellectual property rights, personal data protection and confidentiality, security and legitimate commercial interests, shall be taken into account in accordance with the principle of ‘as open as possible, as closed as necessary’. Those open access policies shall be addressed to research performing organisations and research funding organisations.

(2) Without prejudice to Article 32n, paragraph 3, point (d), research data shall be re-usable for commercial or non-commercial purposes in accordance with Section 1 and Section 2 Subsection 3, insofar as they are publicly funded and researchers, research performing organisations or research funding organisations have already made them publicly available through an institutional or subject-based repository. In that context, legitimate commercial interests, knowledge transfer activities and pre-existing intellectual property rights shall be taken into account.

Subsection 5

High-value datasets

Article 32u

Thematic categories of high-value datasets

(1) The thematic categories of high-value datasets shall be as set out in Annex I.

(2) The Commission is empowered to adopt delegated acts in accordance with Article 45(2a) in order to amend Annex I by adding new thematic categories of high-value datasets reflecting technological and market developments.

Article 32v

Specific high-value datasets and arrangements for publication and re-use

(1) The Commission shall adopt implementing acts laying down a list of specific high-value datasets belonging to the categories set out in Annex I and held by public sector bodies and public undertakings among the data or documents to which this Section applies.

Such specific high-value datasets shall be:

(a) available free of charge, subject to paragraphs 3, 4 and 5;

(b) machine readable;

(c) provided via APIs; and

(d) provided as a bulk download, where relevant.

Those implementing acts may specify the arrangements for the publication and re-use of high-value datasets. Such arrangements shall be compatible with open standard licences.

The arrangements may include terms applicable to re-use, formats of data and metadata and technical arrangements for dissemination. Investments made by the Member States in open data approaches, such as investments into the development and roll-out of certain standards, shall be taken into account and balanced against the potential benefits from inclusion in the list.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 46(2).

(2) The identification of specific high-value datasets pursuant to paragraph 1 shall be based on the assessment of their potential to:

(a) generate significant socioeconomic or environmental benefits and innovative services;

(b) benefit a high number of users, in particular SMEs and SMCs;

(c) assist in generating revenues; and

(d) be combined with other datasets.

For the purpose of identifying such specific high-value datasets, the Commission shall carry out appropriate consultations, including at expert level, conduct an impact assessment and ensure complementarity with existing legal acts, such as Directive 2010/40/EU of the European Parliament and of the Council, with respect to the re-use of data or documents. That impact assessment shall include a cost-benefit analysis and an analysis of whether providing high-value datasets free of charge by public sector bodies that are required to generate revenue to cover a substantial part of their costs relating to the performance of their public tasks would lead to a substantial impact on the budget of such bodies. With regard to high-value datasets held by public undertakings, the impact assessment shall give special consideration to the role of public undertakings in a competitive economic environment.

(3) By way of derogation from paragraph 1, second subparagraph, point (a), the implementing acts referred to in that paragraph shall provide that the availability of high-value datasets free of charge is not to apply to specific high-value datasets held

by public undertakings where that would lead to a distortion of competition in the relevant markets.

(4) The requirement to make high-value datasets available free of charge pursuant to point (a) of the second subparagraph of paragraph 1 shall not apply to libraries, including university libraries, museums and archives.

(5) Where making high-value datasets available free of charge by public sector bodies that are required to generate revenue to cover a substantial part of their costs relating to the performance of their public tasks would lead to a substantial impact on the budget of the bodies involved, Member States may exempt those bodies from the requirement to make those high-value datasets available free of charge for a period of no more than two years following the entry into force of the relevant implementing act adopted in accordance with paragraph 1.

Section 3

Re-use of certain categories of protected data held by public sector bodies

Article 32w

Conditions for re-use

(1) Public sector bodies which are competent under national law to grant or refuse access for the re-use of data or documents belonging to certain categories of protected data shall make publicly available the conditions for allowing such re-use and the procedure to request the re-use via the single information point referred to in Article 32aa. Where they grant or refuse access for re-use, they may be assisted by the competent bodies referred to in Article 32z (1).

Member States shall ensure that public sector bodies are equipped with the necessary resources to comply with this Article and Article 32x.

(2) Re-use of data or documents shall not affect the protected nature of those data or documents and shall only be allowed:

(a) in compliance with intellectual property rights.

(b) if data that is considered confidential in accordance with Union or national law on commercial or statistical confidentiality, is not disclosed, as a result of allowing re-use, unless such re-use is allowed based on the data subject's consent or the data holder's permission in accordance with paragraph 5.

(c) in compliance with Regulation (EU) 2016/679.

(3) To ensure the preservation of the protected nature as referred to in paragraph 2, public sector bodies may establish the following requirements:

(a) to grant access for the re-use of data or documents only where the public sector body or the competent body, following the request for re-use, has ensured that those data or documents have been:

(i) anonymised, in the case of personal data;

(ii) subject to other forms of preparation of personal data;

(iii) modified, aggregated or treated by any other method of disclosure control, in the case of commercially confidential information, including trade secrets or content protected by intellectual property rights;

(b) to access and re-use the data or documents remotely within a secure processing environment that is provided or controlled by the public sector body;

(c) to access and re-use the data or documents within the physical premises in which the secure processing environment is located in accordance with high security standards, provided that remote access cannot be allowed without jeopardising the rights and interests of third parties.

In the case of re-use allowed in accordance with the first subparagraph, point (a)(i), the re-use of data or documents shall be subject to the rules on open government data set out in Section 2. This is without prejudice to Article 32y, which prevails in case of conflict.

In the case of re-use allowed in accordance with the first subparagraph, points (b) and (c), the public sector bodies shall impose conditions that preserve the integrity of the functioning of the technical systems of the secure processing environment used.

(4) The public sector body shall reserve the right to verify the process, the means and any results of processing of data or documents undertaken by the re-user to preserve the integrity of the protection of the data or documents. It shall also reserve the right to prohibit the use of results that contain information jeopardising the rights and interests of third parties. The decision to prohibit the use of the results shall be comprehensible and transparent to the re-user.

Unless national law provides for specific safeguards on applicable confidentiality obligations relating to the re-use of certain categories of protected data, the public sector body shall make the re-use of data or documents provided in accordance with paragraph 3 conditional on the adherence by the re-user to a confidentiality obligation that prohibits the disclosure of any information that jeopardises the rights and interests of third parties and that the re-user may have acquired despite the safeguards put in place. In the event of the unauthorised re-use of non-personal data, the re-user shall be obliged, without delay, where appropriate with the assistance of the public sector body, to inform the natural or legal persons whose rights and interests may be affected.

(5) Where the re-use of data or documents cannot be allowed in accordance with paragraphs 3 and 4, re-use shall only be possible:

(a) where there is no legal basis other than consent for transmitting the data under Regulation (EU) 2016/679, with the consent of the data subjects;

(b) with the permission from the data holders whose rights and interests may be affected by such re-use.

The public sector body shall make best efforts, in accordance with Union and national law, to provide assistance to potential re-users in seeking consent of the data subjects or permission from the data holders whose rights and interests may be affected by such re-use, where this is feasible without a disproportionate burden on the public sector body.

Where it provides such assistance, the public sector body may be assisted by the competent bodies referred to in Article 32z.

Article 32x

Requirements for transfers of non-personal data to third countries by re-users

(1) Where a re-user intends to transfer certain categories of protected data that are non-personal to a third country, it shall inform the public sector body of its intention to transfer such data and the purpose of such transfer at the time of requesting the re-use of the data. In the case of re-use based on the data holder's permission the re-user shall, where appropriate with the assistance of the public sector body, inform the natural or legal person whose rights and interests may be affected of that intention, purpose and the appropriate safeguards. The public sector body shall not allow the re-use unless the natural or legal person gives permission for the transfer.

(2) Public sector bodies shall transmit non-personal confidential data or data protected by intellectual property rights to a re-user which intends to transfer those data to a third country other than a country designated in accordance with paragraph 7 only if the re-user contractually commits to:

(a) complying with the obligations imposed in accordance with intellectual property rights and Union or national law on commercial or statistical confidentiality even after the data is transferred to the third country;

(b) accepting the jurisdiction of the courts or tribunals of the Member State of the transmitting public sector body with regard to any dispute related to compliance with intellectual property rights and Union or national law on commercial or statistical confidentiality.

(3) The Commission may adopt implementing acts establishing model contractual clauses for complying with the obligations referred to in paragraph 2 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 46(2).

(4) Public sector bodies shall, where relevant and to the extent of their capabilities, provide guidance and assistance to re-users in complying with the obligations referred to in paragraph 2.

(5) Where justified because of the substantial number of requests across the Union concerning the re-use of non- personal data in specific third countries, the Commission may adopt implementing acts declaring that the legal, supervisory and enforcement arrangements of a third country:

(a) ensure protection of intellectual property and trade secrets in a way that is essentially equivalent to the protection ensured under Union law;

(b) are being effectively applied and enforced; and

(c) provide effective judicial redress.

(6) Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 46(2).

(7) Specific Union legislative acts may deem certain non-personal data categories held by public sector bodies to be highly sensitive for the purposes of this Article where their transfer to third countries may put at risk Union public policy objectives, such as safety and public health or may lead to the risk of re-identification of non-personal, anonymised data. Where such an act is adopted, the Commission shall adopt delegated acts in accordance with Article 45 supplementing this Regulation by laying down special conditions applicable to the transfers of such data to third countries.

If required by a specific Union legislative act referred to in the first subparagraph, such special conditions may include terms applicable for the transfer or technical arrangements in this regard, limitations with regard to the re-use of data in third countries or categories of persons entitled to transfer such data to third countries or, in exceptional cases, restrictions with regard to transfers to third countries.

The re-user to whom the right to re-use non-personal data was granted may transfer the data only to those third countries for which the requirements set out in paragraphs 2, 4 and 5 are met.

Article 32y

Fees

(1) Public sector bodies which allow re-use of certain categories of protected data may charge fees for allowing the re-use of such data.

(2) Where public sector bodies charge fees, they shall take measures to provide incentives for the re-use of certain categories of protected data for non-commercial purposes, such as scientific research purposes, and by start-ups, SMEs and SMCs in accordance with Union State aid rules. In that regard, public sector bodies may also make the data available at a discounted fee or free of charge, in particular to start-ups, SMEs and SMCs, civil society, research and educational establishments. To that end, public sector bodies may establish a list of categories of re-users to which data or documents for re-use is made available at a discounted fee or free of charge. That list, together with the criteria used to establish it, shall be made public.

(3) Any fees shall be derived from the costs related to conducting the procedure for requests for the re-use of certain categories of protected data and limited to the necessary costs in relation to:

(a) the reproduction, provision and dissemination of data;

(b) the clearance of rights;

(c) anonymisation or other forms of preparation of personal data and commercially confidential data as provided for in Article 32w(3)[conditions for re-use];

(d) the maintenance of the secure processing environment;

(e) the acquisition of the right to allow re-use in accordance with this Section by third parties outside the public sector; and assisting re-users in seeking consent from data subjects and permission from data holders whose rights and interests may be affected by such re-use.

(4) The criteria and methodology for calculating fees shall be laid down by the Member States and published. The public sector body shall publish a description of the main categories of costs and the rules used for the allocation of costs.

(5) Public sector bodies may charge higher fees than those allowed in accordance with paragraph 2 and 3 of this Article with respect to very large enterprises, based on objective criteria, taking into account the economic power, or the ability of the entity to acquire data, including in particular a designation as a gatekeeper under Regulation (EU) 2022/1925. Any such calculated fees shall be proportionate. In addition to the elements listed in paragraph 3 of this Article, they can cover the cost of collection and production of the data, together with a reasonable return on investment.

Article 32z

Competent bodies

(1) For the purpose of carrying out the tasks referred to in this Article, each Member State shall designate one or more competent bodies in accordance with Article 37(1), which may be competent for particular sectors, but that collectively need to cover all sectors, to assist the public sector bodies which grant or refuse access for the re-use of certain categories of protected data. Member States may either establish one or more new competent bodies or rely on existing public sector bodies or on internal services of public sector bodies that fulfil the conditions laid down in this Section.

(2) The competent bodies may be empowered to grant access for the re-use of certain categories of protected data pursuant to Union or national law which provides for such access to be granted. Where they grant or refuse access for re-use, those competent bodies shall be subject to Articles 32k, 32w, 32x, 32y and 32ab.

(3) The competent bodies shall have adequate legal, financial, technical and human resources to carry out the tasks assigned to them, including the necessary technical knowledge to be able to comply with relevant Union or national law concerning the access regimes for the categories of protected data referred to in in Article 2(54).

(4) The assistance referred to in paragraph 1 shall include, where necessary:

(a) providing technical support by making available a secure processing environment for providing access for the re-use of data or documents;

(b) providing guidance and technical support on how to best structure and store data to make that those data or documents easily accessible;

(c) providing technical support for anonymization, pseudonymisation and state-of-the-art privacy-preserving methods. not limited to personal data, but also to commercially confidential information, including trade secrets or content protected by intellectual property rights;

(d) assisting the public sector bodies, where relevant, to provide support to re-users in requesting consent for re-use from data subjects or permission from data holders in line with their specific decisions, including on the jurisdiction in which the data processing is intended to take place and assisting the public sector bodies in establishing technical mechanisms that allow the transmission of requests for consent or permission from re-users, where practically feasible;

(e) providing public sector bodies with assistance in assessing the adequacy of contractual commitments made by a re-user pursuant to Article 32x(2).

Article 32aa

Single information point

(1) Each Member State shall designate a single information point. That point shall make available easily accessible information concerning the application of Articles 32w, 32x and 32y.

(2) The single information point shall be competent to receive enquiries or requests for the re-use of the certain categories of protected data and shall transmit them, where possible and appropriate by automated means, to the competent public sector bodies, or the competent bodies referred to in Paragraph 1 of Article 32z, where relevant.

(3) The single information point may include a separate, simplified and well-documented information channel for SMEs, SMCs, start-ups and research establishments addressing their needs and capabilities in requesting the re-use of the categories of data referred to in Article 2(54).

(4) The single information point shall make available by electronic means a searchable asset list containing an overview of all available document_resources including, where relevant, those document resources that are available at sectoral, regional or local information points, with relevant information describing the available data or documents, including at least the data format and size and the conditions for their re-use.

(5) The Commission shall establish a European single access point offering a searchable electronic register of data or documents available in the national single information points and further information on how to request data or documents via those national single information points.

Article 32ab

Procedure for requests for re-use

(1) Unless shorter time limits have been established in accordance with national law, the competent public sector bodies or the competent bodies referred to in paragraph 1 of Article 32z shall adopt a decision on the request for the re-use of certain categories of protected data within two months of the date of receipt of the request.

(2) In the case of exceptionally extensive and complex requests for re-use, that two-month period may be extended by up to 30 days. In such cases the competent public sector bodies or the competent bodies referred to in paragraph 1 of Article 32z shall notify the applicant as soon as possible that more time is needed for conducting the procedure, together with the reasons for the delay.

(3) Any natural or legal person directly affected by a decision as referred to in paragraph 1 shall have an effective right of redress in the Member State where the relevant body is located. Such a right of redress shall be laid down in national law and shall include the possibility of review by an impartial body with the appropriate expertise, such as the national competition authority, the relevant access-to-documents authority, the supervisory authority established in accordance with Regulation (EU) 2016/679 or a national judicial authority, whose decisions are binding upon the public sector body or the competent body concerned.'

19. Article 38 is replaced by the following:

(1) 'Without prejudice to any other administrative or judicial remedy, natural and legal persons shall have the right to lodge a complaint, individually or, where relevant, collectively:

(a) with the relevant competent authority in the Member State of their habitual residence, place of work or establishment if they consider that their rights under this Regulation have been infringed;

(b) any matter falling within the scope of this Regulation specifically against a recognised data intermediation services provider or a recognised data altruism organisation, with the relevant competent authority for the registration of data

intermediation services or the relevant competent authority for the registration of data altruism organisations.

(2) The data coordinator shall, upon request, provide all the necessary information to natural and legal persons for the lodging of their complaints with the appropriate competent authority.

(3) The competent authority with which the complaint has been lodged shall inform the complainant, in accordance with national law, of:

(a) the progress of the proceedings, of the decision taken; and

(b) the judicial remedies provided for in Article 39.'

20. in Article 40, paragraph (6) is inserted:

'6. This Article shall not apply to Chapter VIIc.'

21. after Article 41, the following heading is inserted:

'CHAPTER IXa

European Data Innovation Board';

22. the following Article 41a is inserted:

'Article 41a

European Data Innovation Board

(1) The European Data Innovation Board is established as a means to advising and assisting the Commission in coordinating the enforcement of this Regulation and to serve as a forum of discussion for the development of a European data economy and data policies.

(2) It shall be composed at least of representatives of Member States competent for matters related to data, the competent authorities for enforcement of Chapters II, III, V, VIIa and VIIc of this Regulation, the European Data Protection Board, the European Data Protection Supervisor, ENISA, the EU SME Envoy or a representative appointed by the network of SME envoys. The Commission may decide to add additional categories of members. In its appointments of individual experts, the Commission shall aim to achieve gender and geographical balance among the members of the group.

(3) The Commission shall decide on the composition of the different configurations in which the Board will fulfil its tasks.

(4) The Commission shall chair the meetings of the European Data Innovation Board.'

23. Article 42 is replaced by the following:

'Article 42

Role of the EDIB

(1) The EDIB shall support the consistent application of this Regulation by:

(a) serving as a forum for strategic discussions on data policies, data governance, international data flows and cross-sectoral developments relevant to the European data economy;

(b) advising and assisting the Commission with regard to developing consistent practice of competent authorities in the enforcement of Chapters II, III, V, VII, VIIa and VIIc;

(c) facilitating cooperation between competent authorities through capacity-building and the exchange of information;

(d) fostering an exchange of experience and good practice between the Member States in the field of re-use of public sector information in collaboration with other relevant governance bodies.';

24. Article 45 is amended as follows:

(a) paragraph 2 is replaced by the following:

'2. The power to adopt delegated acts referred to in Article 29(7), Article 32u(2) and Article 33(2) shall be conferred on the Commission for an indeterminate period of time.'

(b) paragraph 3 is replaced by the following:

'3. The delegation of power referred to in Article 29(7), Article 32u(2) and Article 33(2) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.'

(c) paragraph 6 is replaced by the following:

'6. A delegated act adopted pursuant to Article 29(7), Article 32u(2) or Article 33(2) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of three months of notification of that act to the European Parliament and to the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by three months at the initiative of the European Parliament or of the Council.

25. Article 46 is amended as follows:

(a) in paragraph 1, the first sentence is replaced by the following:

'The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.'

(b) the following paragraph 1a is inserted:

'1a. Where reference is made to this paragraph, Article 4 of Regulation (EU) No 182/2011 shall apply.'

26. Article 49 is amended as follows:

(a) paragraph 1 is amended as follows:

(i) the introductory wording is replaced by the following:

'1. By 12 September 2028, the Commission shall carry out an evaluation of chapters II, III, IV, V, VI, VII, and VIII and submit a report on its main findings to the European Parliament and to the Council, and to the

European Economic and Social Committee. That evaluation shall assess, in particular:'

(ii) point (m) is replaced by the following:

'(m) the impact of this Regulation on SMEs and SMCs with regard to their capacity to innovate and to the availability of data processing services for users in the Union and the burden of complying with new obligations'

(b) the following paragraph 2a is inserted:

'2a. By [date = entry into force plus 5 years], the Commission shall carry out an evaluation of chapters VIIa, VIIb and VIIc of this Regulation and submit a report on its main findings to the European Parliament and to the Council as well as to the European Economic and Social Committee.

The report shall assess, in particular:

(a) the state of registrations of data intermediation services and the type of services they offer;

(b) the type of data altruism organisations registered and an overview of the objectives of general interests for which data are shared in view of establishing clear criteria in that respect.'

(c) the scope and social and economic impact of Chapter VIIc Section 2 including

(d) the extent of the increase in re-use of public sector documents to which Section 2 of Chapter VIIc applies, especially by SMEs and SMCs;

(e) the impact of the high-value datasets;

(f) the interaction between data protection rules and re-use possibilities;

(g) Member States shall provide the Commission with the Information necessary for the preparation of that report.'

(c) paragraph 5 is replaced by the following:

'5. On the basis of the reports referred to in paragraphs 1, and 2 and 2a, the Commission may, where appropriate, submit a legislative proposal to the European Parliament and to the Council to amend this Regulation.'

27. Annex I is added as set out in the Annex II to this Regulation.

Article 2

Amendments to Regulation (EU) 2018/1724

In the table in Annex II to Regulation (EU) 2018/1724, the entry 'Starting, running and closing a business' is replaced by the following:

Life events	Procedures	Expected output subject to an assessment of the application by the competent authority in

		accordance with national law, where relevant
Starting, running and closing a business	Notification of business activity, permission for exercising a business activity, changes of business activity and the termination of a business activity not involving insolvency or liquidation procedures, excluding the initial registration of a business activity with the business register and excluding procedures concerning the constitution of or any subsequent filing by companies or firms within the meaning of the second paragraph of Article 54 TFEU	Confirmation of the receipt of notification or change, or of the request for permission for business activity
	Registration of an employer (a natural person) with compulsory pension and insurance schemes	Confirmation of registration or social security registration number
	Registration of employees with compulsory pension and insurance schemes	Confirmation of registration or social security registration number
	Submitting a corporate tax declaration	Confirmation of the receipt of the declaration
	Notification to the social security schemes of the end of contract with an employee, excluding procedures for the collective termination of employee contracts	Confirmation of the receipt of the notification
	Payment of social contributions for employees	Receipt or other form of confirmation of payment of social contributions for employees
	Registration as a data intermediation services provider	Confirmation of the registration
	Registration as a data altruism organisation recognised in the Union	Confirmation of the registration

Article 3

Amendments to Regulation (EU) 2016/679 (GDPR)

Regulation (EU) 2016/679 is amended as follows:

1. Article 4 is amended as follows:

(a) in point 1, the following sentences are added:

‘Information relating to a natural person is not necessarily personal data for every other person or entity, merely because another entity can identify that

natural person. Information shall not be personal for a given entity where that entity cannot identify the natural person to whom the information relates, taking into account the means reasonably likely to be used by that entity. Such information does not become personal for that entity merely because a potential subsequent recipient has means reasonably likely to be used to identify the natural person to whom the information relates.'

(b) the following points are added:

'(32) 'terminal equipment' means terminal equipment as set out in Article 1(1) of Directive 2008/63/EC;

(33) for 'electronic communications networks' the definition of Article 2(1) of Directive (EU) 2018/1972 shall apply;

(34) 'web browser' means web browser as defined in Article 2(11) of Regulation (EU) 2022/1925;

(35) 'media service' means a media service as defined in Article 2(1) of Regulation (EU) 2024/1083;

(36) 'media service provider' means a media service provider as defined in Article 2(2) of Regulation (EU) 2024/1083;'

(37) 'online interface' means an online interface as defined in Article 3(m) of Regulation (EU) 2022/2065.'

(38) "scientific research" means any research which can also support innovation, such as technological development and demonstration. These actions shall contribute to existing scientific knowledge or apply existing knowledge in novel ways, be carried out with the aim of contributing to the growth of society´s general knowledge and wellbeing and adhere to ethical standards in the relevant research area. This does not exclude that the research may also aim to further a commercial interest.'

2. Article 5 (1)(b) is replaced by the following:

'collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), be considered to be compatible with the initial purposes, independent of the conditions of Article 6(4) of this Regulation, ('purpose limitation');'

3. Article 9 is amended as follows:

(a) in paragraph 2, the following points are added:

'(k) processing in the context of the development and operation of an AI system as defined in Article 3, point (1), of Regulation (EU) 2024/1689 or an AI model, subject to the conditions referred to in paragraph 5.

(l) processing of biometric data is necessary for the purpose of confirming the identity of a data subject (verification), where the biometric data or the means needed for the verification is under the sole control of the data subject.'

(b) the following paragraph is added:

‘5. For processing referred to in point (k) of paragraph 2, appropriate organisational and technical measures shall be implemented to avoid v the collection and otherwise processing of special categories of personal data. Where, despite the implementation of such measures, the controller identifies special categories of personal data in the datasets used for training, testing or validation or in the AI system or AI model, the controller shall remove such data. If removal of those data requires disproportionate effort, the controller shall in any event effectively protect without undue delay such data from being used to produce outputs, from being disclosed or otherwise made available to third parties.’

4. In Article 12, paragraph 5 is replaced by the following:

‘5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character or also, for requests under Article 15 because the data subject abuses the rights conferred by this regulation for purposes other than the protection of their data, the controller may either:

(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

(b) refuse to act on the request.

The controller shall bear the burden of demonstrating that the request is manifestly unfounded or that there are reasonable grounds to believe that it is excessive.’

5. In Article 13, paragraph 4 is replaced by the following:

‘4. Paragraphs 1, 2 and 3 shall not apply where the personal data have been collected in the context of a clear and circumscribed relationship between data subjects and a controller exercising an activity that is not data-intensive and there are reasonable grounds to assume that the data subject already has the information referred to in points (a) and (c) of paragraph 1, unless the controller transmits the data to other recipients or categories of recipients, transfers the data to a third country, carries out automated decision-making, including profiling, referred to in Article 22(1), or the processing is likely to result in a high risk to the rights and freedoms of data subjects within the meaning of Article 35.’

6. In Article 13, paragraph 5 is added:

‘5. When the processing takes place for scientific research purposes and the provision of information referred to under paragraphs 1, 2 and 3 proves impossible or would involve a disproportionate effort subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing, the controller does not need to provide the information referred to under paragraphs 1, 2 and 3. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available.’

7. In Article 22, paragraphs 1 and 2 are replaced by the following:

‘1. A decision which produces legal effects for a data subject or similarly significantly affects him or her may be based solely on automated processing, including profiling, only where that decision:

(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller regardless of whether the decision could be taken otherwise than by solely automated means;

(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

(c) is based on the data subject's explicit consent.’

8. Article 33 is amended as follows:

(a) paragraph 1 is replaced by the following:

‘1. In the case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall without undue delay and, where feasible, not later than 96 hours after having become aware of it, notify the personal data breach via the single-entry point established pursuant to Article 23a of Directive (EU) 2022/2555 to the supervisory authority competent in accordance with Article 55 and Article 56. Where the notification to the supervisory authority is not made within 96 hours, it shall be accompanied by reasons for the delay.’

(b) the following paragraph is added:

‘1a. Until the establishment of the single-entry point pursuant to Article 23a of Directive (EU) 2022/2555, controllers shall continue to notify personal data breaches directly to the competent supervisory authority in accordance with Article 55 and Article 56.’

(c) the following paragraphs are added:

‘6. The Board shall prepare and transmit to the Commission a proposal for a common template for notifying a personal data breach to the competent supervisory authority referred to in paragraph 1 as well as for a list of the 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 proposals shall be submitted to the Commission within [OP date = nine months of the entry into application of this Regulation]. The Commission after due consideration reviews it, as necessary, and is empowered to adopt it by way of an implementing act in accordance with the examination procedure set out in Article 93(2).

7. The template and the list referred to in paragraph 6 shall be reviewed at least every three years and updated where necessary. The Board shall submit its assessment and possible proposals for updates to the Commission in due time. The Commission after due consideration of the proposals reviews them and is empowered to adopt any updates following the procedure in paragraph 6.’

9. Article 35 is amended as follows:

(a) paragraphs 4, 5 and 6 are replaced by the following:

‘4. The Board shall prepare and transmit to the Commission a proposal for a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1.

5. The Board shall prepare and transmit to the Commission a proposal for a list of the kind of processing operations for which no data protection impact assessment is required.

6. The Board shall prepare and transmit to the Commission a proposal for a common template and a common methodology for conducting data protection impact assessments.’

(b) the following paragraphs are inserted:

‘6a. The proposals for the lists referred to in paragraphs 4 and 5 and for the template and methodology referred to in paragraph 6 shall be submitted to the Commission within [OP date = 9 months of the entry into application of this Regulation]. The Commission after due consideration reviews them, as necessary, and is empowered to adopt them by way of an implementing act in accordance with the examination procedure set out in Article 93(2).

6b. The lists and the template and methodology referred to in paragraph 6a- shall be reviewed at least every three years and updated where necessary. The Board shall submit its assessment and possible proposals for updates to the Commission in due time. The Commission after due consideration of the proposals reviews them and is empowered to adopt any updates following the procedure in paragraph 6a.

6c. Lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment and of the kind of processing operations for which no data protection impact assessment is required established and made public by supervisory authorities remain valid until the Commission adopts the implementing act referred to in paragraph 6a.’

10. The following article is added:

‘Article 41a

(1) The Commission may adopt implementing acts to specify means and criteria to determine whether data resulting from pseudonymisation no longer constitutes personal data for certain entities.

(2) For the purpose of paragraph 1 the Commission shall:

(a) assess the state of the art of available techniques;

(b) develop criteria and or categories for controllers and recipients to assess the risk of re-identification in relation to typical recipients of data.

(3) The implementation of the means and criteria outlined in an implementing act may be used as an element to demonstrate that data cannot lead to reidentification of the data subjects.

(4) The Commission shall closely involve the EDPB in the preparations of the implementing acts. The EPDB shall issue an opinion on the draft implementing acts within a deadline of 8 weeks as of the receipt of the draft from the Commission.

(5) The Implementing Acts shall be adopted in accordance with the examination procedure referred to in Article 93(3).’

11. In Article 57(1) is amended as follows:

(a) point (k) is deleted;

12. In Article 64(1), point (a) is deleted.

13. In Article 70(1), point (h) is deleted.

14. In Article 70(1), the following points are inserted:

'(ha) prepare and transmit to the Commission a proposal for a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment and for which no data protection impact assessment is required, pursuant to Article 35.

(hb) prepare and transmit to the Commission a proposal for a common template and a common methodology for conducting data protection impact assessments, pursuant to Article 35.

(hc) prepare and transmit to the Commission a proposal for a common template for notifying a personal data breach to the competent supervisory authority as well as for a list of the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person pursuant to Article 33'

15. After Article 88, the following articles are added:

'Article 88a

Processing of personal data in the terminal equipment of natural persons

(1) Storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person is only allowed when that person has given his or her consent, in accordance with this Regulation.

(2) Paragraph 1 does not preclude storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person, based on Union or Member State law within the meaning of, and subject to the conditions of Article 6, to safeguard the objectives referred to in Article 23(1).

(3) Storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person without consent, and subsequent processing, shall be lawful to the extent it is necessary for any of the following:

(a) carrying out the transmission of an electronic communication over an electronic communications network;

(b) providing a service explicitly requested by the data subject;

(c) creating aggregated information about the usage of an online service to measure the audience of such a service, where it is carried out by the controller of that online service solely for its own use;

(d) maintaining or restoring the security of a service provided by the controller and requested by the data subject or the terminal equipment used for the provision of such service.

(4) Where storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person is based on consent, the following shall apply:

(a) the data subject shall be able to refuse requests for consent in an easy and intelligible manner with a single-click button or equivalent means;

(b) if the data subject gives consent, the controller shall not make a new request for consent for the same purpose for the period during which the controller can lawfully rely on the consent of the data subject;

(c) if the data subject declines a request for consent, the controller shall not make a new request for consent for the same purpose for a period of at least six months.

This paragraph also applies to the subsequent processing of personal data based on consent.

(5) This Article shall apply from [OP: please insert the date = 6 months following the date of entry into force of this Regulation]

Article 88b

Automated and machine-readable indications of data subject's choices with respect to processing of personal data in the terminal equipment of natural persons

(1) Controllers shall ensure that their online interfaces allow data subjects to:

(a) Give consent through automated and machine-readable means, provided that the conditions for consent laid down in this Regulation are fulfilled;

(b) decline a request for consent and exercise the right to object pursuant to Article 21(2) through automated and machine-readable means.

(2) Controllers shall respect the choices made by data subjects in accordance with paragraph 1.

(3) Paragraphs 1 and 2 shall not apply to controllers that are media service providers when providing a media service.

(4) The Commission shall, in accordance with Article 10(1) of Regulation (EU) 1025/2012, request one or more European standardisation organisations to draft standards for the interpretation of machine-readable indications of data subjects' choices.

Online interfaces of controllers which are in conformity with harmonised standards or parts thereof the references of which have been published in the *Official Journal of the European Union* shall be presumed to be in conformity with the requirements covered by those standards or parts thereof, set out in paragraph 1.

(5) Paragraphs 1 and 2 shall apply from [OP: please insert the date = 24 months following the date of entry into force of this Regulation].

(6) Providers of web browsers, which are not SMEs, shall provide the technical means to allow data subjects to give their consent and to refuse a request for consent and exercise the right to object pursuant to Article 21(2) through the automated and machine-readable means referred to in paragraph 1 of this Article, as applied pursuant to paragraphs 2 to 5 of this Article.

(7) Paragraph 6 shall apply from [OP: please insert the date = 48 months following the date of entry into force of this Regulation].

Article 88c

Processing in the context of the development and operation of AI

Where the processing of personal data is necessary for the interests of the controller in the context of the development and operation of an AI system as defined in Article 3, point (1), of Regulation (EU) 2024/1689 or an AI model, such processing may be pursued for legitimate interests within the meaning of Article 6(1)(f) of Regulation (EU) 2016/679, where appropriate, except where other Union or national laws explicitly require consent, and where such interests are overridden by the interests, or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Any such processing shall be subject to appropriate organisational, technical measures and safeguards for the rights and freedoms of the data subject, such as to ensure respect of data minimisation during the stage of selection of sources and the training and testing of AI an system or AI model, to protect against non-disclosure of residually retained data in the AI system or AI model to ensure enhanced transparency to data subjects and providing data subjects with an unconditional right to object to the processing of their personal data.'

Article 4

Amendments to Regulation (EU) 2018/1725 (EUDPR)

Regulation (EU) 2018/1725 is amended as follows:

1. Article 3 is amended as follows:

(a) in point 1, the following sentences are added:

'Information relating to a natural person is not necessarily personal data for every other person or entity, merely because another entity can identify that natural person. Information shall not be personal for a given entity where that entity cannot identify the natural person to whom the information relates, taking into account the means reasonably likely to be used by that entity. Such information does not become personal for that entity merely because a potential subsequent recipient has means reasonably likely to be used to identify the natural person to whom the information relates.'

(b) point 25 is replaced by the following:

'(25) for 'electronic communications networks' the definition of Article 2(1) of Directive (EU) 2018/1972 shall apply;'

(c) the following points are added:

'(27) 'mobile application' means a mobile application as defined in Article 3(2) of Directive (EU) 2016/2102;

(28) 'online interface' means an online interface as defined in Article 3(m) of Regulation (EU) 2022/2065;

(29) "scientific research" means any research which can also support innovation, such as technological development and demonstration. These

actions shall contribute to existing scientific knowledge or apply existing knowledge in novel ways, be carried out with the aim of contributing to the growth of society´s general knowledge and wellbeing and adhere to ethical standards in the relevant research area. This does not exclude that the research may also aim to further a commercial interest.'

2. Article 4 (1)(b) is replaced by the following:

'(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 13, be considered to be compatible with the initial purposes, independent of the conditions of Article 6 of this Regulation, ('purpose limitation');'

3. Article 10 is amended as follows:

(a) in paragraph 2, the following points are added:

'(k) processing in the context of the development and operation of an AI system as defined in Article 3, point (1), of Regulation (EU) 2024/1689 or an AI model, subject to the conditions referred to in paragraph 4. ~~.~~

(l) processing of biometric data is necessary for the purpose of confirming the identity of a data subject (verification), where the biometric data or the means needed for the verification is under the sole control of the data subject.'

(b) the following paragraph 4 is added:

'4. For processing referred to in point (k) of paragraph 2, appropriate organisational and technical measures shall be implemented to avoid the collection and otherwise processing of special categories of personal data. Where, despite the implementation of such measures, the controller identifies special categories of personal data in the datasets used for training, testing or validation or in the AI system or AI model, the controller shall remove such data. If removal of those data requires disproportionate effort, the controller shall in any event effectively protect without undue delay such data from being used to produce outputs, from being disclosed or otherwise made available to third parties.'

4. in Article 14, paragraph 5 is replaced by the following:

'5. Information provided under Articles 15 and 16 and any communication and any actions taken under Articles 17 to 24 and 35 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character or also, for requests under Article 17 because the data subject abuses the rights conferred by this Regulation for purposes other than the protection of their data, the controller may refuse to act on the request. The controller shall bear the burden of demonstrating that the request is manifestly unfounded or that there are reasonable grounds to believe that it is excessive.'

5. in Article 15 the new paragraph 5 is added:

'5. When the processing takes place for scientific research purposes and the provision of information referred to under paragraphs 1, 2 and 3 proves

impossible or would involve a disproportionate effort subject to the conditions and safeguards referred to in Article 13 or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing, the controller does not need to provide the information referred to under paragraphs 1, 2 and 3. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available.'

6. in Article 24 paragraphs 1 and 2 are replaced by the following:

'1. A decision which produces legal effects for a data subject or similarly significantly affects him or her may be based solely on automated processing, including profiling, only where that decision:

(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller regardless of whether the decision could be taken otherwise than by solely automated means;

(b) is authorised by Union law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

(c) is based on the data subject's explicit consent.'

7. in Article 34, paragraph 1 is replaced by the following

'1. In the case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall without undue delay and, where feasible, not later than 96 hours after having become aware of it, notify the personal data breach to the European Data Protection Supervisor. Where the notification to the European Data Protection Supervisor is not made within 96 hours, it shall be accompanied by reasons for the delay.'

8. In Article 37 the following paragraphs are added:

'(2) Storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person is only allowed when that person has given his or her consent, in accordance with this Regulation.

(3) Paragraph 1 does not preclude storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person, based on Union law within the meaning of, and subject to the conditions of Article 5, to safeguard the objectives referred to in Article 25(1).

(4) Storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person without consent, and subsequent processing, shall be lawful to the extent it is necessary for any of the following:

(a) carrying out the transmission of an electronic communication over an electronic communications network;

(b) providing a service explicitly requested by the data subject;

(c) creating aggregated information about the usage of an online service to measure the audience of such a service, where it is carried out by the controller of that online service solely for its own use;

(d) maintaining or restoring the security of a service provided by the controller and requested by the data subject or the terminal equipment used for the provision of such service.

(5) Where storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person is based on consent, the following shall apply:

(a) the data subject shall be able to refuse requests for consent in an easy and intelligible manner with a single-click button or equivalent means;

(b) if the data subject gives consent, the controller shall not make a new request for consent for the same purpose for the period during which the controller can lawfully rely on the consent of the data subject;

(c) if the data subject declines a request for consent, the controller shall not make a new request for consent for the same purpose for a period of at least six months.

This paragraph also applies to the subsequent processing of personal data based on consent.

(6) This Article shall apply from [OP: please insert the date = 6 months following the date of entry into force of this Regulation]]

(7) Controllers shall ensure that their online interfaces allow data subjects to:

(a) give consent through automated and machine-readable means, provided that the conditions for consent laid down in this Regulation are fulfilled;

(b) decline a request for consent through automated and machine-readable means.

(8) Controllers shall respect the choices made by data subjects in accordance with paragraph 7.

(9) Online interfaces of controllers which are in conformity with harmonised standards or parts thereof referred to in paragraph 4 of Article 88b of Regulation (EC) 2016/679 shall be presumed to be in conformity with the requirements covered by those standards or parts thereof, set out in paragraph 7.

(10) Paragraphs 7 to 9 shall apply from [OP: please insert the date = 24 months following the date of entry into force of this Regulation].

(8) Article 39 is amended as follows:

(a) Paragraph 4 is replaced by the following:

‘4. The lists, the template and methodology adopted by the Commission and referred to in paragraph 6a of Article 35 of Regulation (EU) 2016/679 should apply to the processing of personal data under this Regulation.’

(b) Paragraphs 5 and 6 are deleted.

(9) the following article is added:

‘Article 45a

The common criteria adopted by the Commission and referred to in article 41a of the Regulation (EU) 2016/679 should apply to the processing of personal data under this Regulation.'

Article 5

Amendments to and Directive 2002/58/EC (ePrivacy Directive)

Directive 2002/58/EC is amended as follows:

1. Article 4 is deleted;

2. After Article 5(3), the following subparagraph is added:

   'This paragraph shall not apply if the subscriber or user is a natural person, and the information stored or accessed constitutes or leads to the processing of personal data.'

Article 6

Amendments to Directive (EU) 2022/2555

Directive (EU) 2022/2555 is amended as follows:

1. The following Article 23a is added:

'Article 23a

Single-entry point for incident reporting

(1) ENISA shall develop and maintain a single-entry point to support the obligation to report incidents and related events under the Union legal acts where those Union legal acts provide so ('single-entry point'). Without prejudice to Article 16 of Regulation (EU) 2024/2847 of the European Parliament and of the Council, ENISA may ensure that the single-entry point builds on the single reporting platform established under that Regulation.

(2) ENISA shall take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of the single-entry point and the information submitted or disseminated via the single-entry point. ENISA shall take into account the sensitivity of information submitted or disseminated pursuant to the Union legal acts referred to in paragraph (1) and ensure that competent authorities under those Union legal acts have access to and process the information as required under those Union legal acts.

(3) ENISA shall provide and implement the specifications on the technical, operational and organisational measures regarding the establishment, maintenance and secure operation of the single-entry point. ENISA shall develop the specifications in cooperation with the Commission, the CSIRTs network and the competent authorities under the Union legal acts referred to in paragraph (1). The specifications shall ensure that:

   (a) the necessary capability for interoperability with regard to other relevant reporting obligations referred to in paragraph (1) is ensured;

(b) technical arrangements for the relevant entities and authorities under the Union legal acts referred to in paragraph (1) to access, submit , retrieve, transmit or otherwise process information from the single-entry point, are in place and, provide technical protocols and tools that allow the entities and authorities to further process the receive information within their systems;

(c) the specificities of the incident reporting requirements set out under the Union legal acts referred to in paragraph (1) are duly taken into account;

(d) where relevant, the single-entry point is interoperable and compatible with European Business Wallets referred to in *[Proposal for a Regulation: Insert title of the proposal]* and that the European Business Wallets can be used at least to identify and authenticate entities using the single-entry point;

(e) entities using the single-entry point can retrieve and supplement information that they have previously submitted via the single-entry point;

(f) a single notification of information submitted by an entity via the single-entry point can be used to fulfil reporting obligations as set out under any of the other Union legal acts which provide for incident reporting to the single-entry point.

(4) Unless provided for in the Union legal acts referred to in paragraph (1) of this, ENISA shall not have access to the notifications submitted through the single-entry point.

(5) Within [18] months from the entry into force of this Regulation, ENISA shall pilot the functioning of the single-entry point for each added Union legal act, including testing that takes into account the specificities and requirements for the notifications set out by each respective Union legal act, and after consulting the Commission and the relevant competent authorities under the respective Union legal acts. ENISA shall enable the notification of incidents under each Union legal act referred to in paragraph (1) only after piloting the functioning and after the Commission published a notice pursuant to paragraph 6.

(6) The Commission shall, in cooperation with ENISA, assess the proper functioning, reliability, integrity and confidentiality of the single-entry point. When the Commission, after consultation of the CSIRTs network and the competent authorities under the Union legal acts referred to in paragraph 1, finds that the single-entry point ensures the proper functioning, reliability, integrity and confidentiality, it shall publish a notice to that effect in the Official Journal of the European Union.

(7) Where the Commission finds in its assessment that the single-entry point does not ensure the proper functioning, reliability, integrity or confidentiality, ENISA shall take, in cooperation with the Commission and without undue delay, all necessary corrective measures to ensure the proper functioning, reliability, integrity or confidentiality without delay and inform the Commission of the results. Thereafter, the Commission shall reassess the proper functioning, reliability, integrity or confidentiality of the single-entry point and shall publish a notice in accordance with paragraph 6.'

2. Article 23 is amended as follows:

(a) in paragraph 1, the first sentence is replaced by the following:

'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 this Article of any incident that has a significant impact on the provision of their services as referred to in paragraph 3 of this Article (significant incident) via the single-entry point established pursuant to Article 23a.'

(a) the following paragraph 12 is added:

'When a manufacturer notifies a severe incident pursuant to Article 14(3) of Regulation (EU) 2024/2847 and the incident reporting under that Article contains relevant information as required under paragraph 4 of this Article, the reporting of the manufacturer under Article 14(3) of Regulation (EU) 2024/2847 shall constitute reporting of information under paragraph 4 of this Article.';

3. in Article 30, paragraph 1 is replaced by the following:

'1. Member States shall ensure that, in addition to the notification obligation provided for in Article 23, notifications can be submitted to the CSIRTs or, where applicable, the competent authorities, on a voluntary basis via the single-entry point established pursuant to Article 23a, by:

(a) essential and important entities with regard to incidents, cyber threats and near misses;

(b) entities other than those referred to in point (a), regardless of whether they fall within the scope of this Directive, with regard to significant incidents, cyber threats and near misses.'

Article 7

Amendment of Regulation (EU) 910/2014

Regulation (EU) 910/2014 is amended as follows:

1. in Article 19a, the following paragraph 1a is inserted:

'1a. Notifications pursuant to paragraph 1, point (b) of this Article to the supervisory body and, where applicable, to other relevant competent authorities, shall be made through the single-entry point pursuant to Article 23a of Directive (EU) 2022/2555.';

2. in Article 24, the following paragraph 2a is inserted:

'2a. Notifications pursuant to in paragraph 2, point (fb), of this Article to the supervisory body and, where applicable, to other relevant competent bodies, shall be made through the single-entry point pursuant to Article 23a of Directive (EU) 2022/2555.';

3. in Article 45a the following paragraph 3a is inserted:

'3a. Notifications pursuant to in paragraph 3 to the Commission and to the competent supervisory body, shall be made through the single-entry point pursuant to Article 23a of Directive (EU) 2022/2555.'

Article 8

Amendments to Regulation (EU) 2022/2554

Article 19 of Regulation (EU) 2022/2554 is amended as follows:

1. in paragraph 1, the first subparagraph is replaced by the following:

   ‘Financial entities shall report major ICT-related incidents to the relevant competent authority as referred to in Article 46 via the single-entry point established pursuant to Article 23a of Directive (EU) 2022/2555 in accordance with paragraph 4 of this Article.’

2. in paragraph 2, the first subparagraph is replaced by the following:

   ‘Financial entities may, on a voluntary basis, notify via the single-entry point established pursuant to Article 23a of Directive (EU) 2022/2555 significant cyber threats to the relevant competent authority when they deem the threat to be of relevance to the financial system, service users or clients. The relevant competent authority may provide such information to other relevant authorities referred to in paragraph 6.’

Article 9

Amendments to Directive (EU) 2022/2557

Article 15 of Directive (EU) 2022/2557 is amended as follows:

1. in paragraph 1, the first sentence is replaced as follows:

   ‘Member States shall ensure that critical entities notify via the single-entry point established pursuant to Article 23a of Directive (EU) 2022/2555 the competent authority, without undue delay, of incidents that significantly disrupt or have the potential to significantly disrupt the provision of essential services.’;

2. in paragraph 2, the following sub-paragraph is added:

   ‘The Commission may adopt implementing acts further specifying the type and format of information notified pursuant to Article 15(1). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 24(2).’

Article 10

Repeals and transitory clauses

1. Regulation 2019/1150/EU is repealed with effect from [date = entry into application of this Regulation].

2. By way of derogation from paragraph 1, the following provisions shall continue to apply until 31 December 2032:

   (a) Article 2, point (1);

   (b) Article 2, point (2);

   (c) Article 2, point (5);

   (d) Article 4;

(e) Article 11;

(f) Article 15.

3. The following acts are repealed, with effect from [Date, aligned with the entry into application of the amendments]:

a) Regulation (EU) 2022/868;

b) Regulation (EU) 2018/1807;

c) Directive 2019/1024.

4. References to Regulation (EU) 2022/868, Regulation (EU) 2018/1807 and Directive 2019/1024 shall be read in accordance with the correlation table set out in Annex I of this Regulation.

Article 11

Final provisions

This Regulation shall enter into force on the third day following that of its publication in the *Official Journal of the European Union*.

Deviating from paragraph 3, Article 5(2) shall enter into application 6 months after the publication in the Official Journal of the European Union.

Article 3(8), points (a) to (c), Articles 6 (2) and (3) and 7 to 9, shall enter into application 18 months from the entry into force of this Regulation. Deviating from the first sentence, where the Commission finds in its assessment pursuant to Article 23a (7) of Directive (EU) 2022/2555 that the single-entry point does not ensure the proper functioning, reliability, integrity or confidentiality, the obligations to report via the single-entry point set out in Article 23(4) of Directive (EU) 2022/2555, Article 19a (1a), Article 24 (2a) and Article 45a (3a) of Regulation (EU) 910/2014, Article 33 (1) of Regulation (EU) 2016/679, Article 19 (1) and (2) of Regulation (EU) 2022/2554, and Article 15(1) of Directive (EU) 2022/2557 shall enter into application 24 months from the entry into force of this Regulation.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

For the European Parliament	*For the Council*
The President	*The President*

LEGISLATIVE FINANCIAL AND DIGITAL STATEMENT

1.FRAMEWORK OF THE PROPOSAL/INITIATIVE 3
1.1.Title of the proposal/initiative 3
1.2.Policy area(s) concerned 3
1.3.Objective(s) 3
1.3.1.General objective(s) 3
1.3.2.Specific objective(s) 3
1.3.3.Expected result(s) and impact 3
1.3.4.Indicators of performance 3
1.4.The proposal/initiative relates to: 4
1.5.Grounds for the proposal/initiative 4
1.5.1.Requirement(s) to be met in the short or long term including a detailed timeline for roll-out of the imple
1.5.2.Added value of EU involvement (it may result from different factors, e.g. coordination gains, legal certa
created by Member States alone..... 4
1.5.3.Lessons learned from similar experiences in the past 4
1.5.4.Compatibility with the multiannual financial framework and possible synergies with other appropriate i
1.5.5.Assessment of the different available financing options, including scope for redeployment 5
1.6.Duration of the proposal/initiative and of its financial impact..... 6
1.7.Method(s) of budget implementation planned 6
2.MANAGEMENT MEASURES..... 8
2.1.Monitoring and reporting rules 8
2.2.Management and control system(s)..... 8
2.2.1.Justification of the budget implementation method(s), the funding implementation mechanism(s), the pa
2.2.2.Information concerning the risks identified and the internal control system(s) set up to mitigate them
2.2.3.Estimation and justification of the cost-effectiveness of the controls (ratio between the control costs and
2.3.Measures to prevent fraud and irregularities..... 9
3.ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE..... 10
3.1.Heading(s) of the multiannual financial framework and expenditure budget line(s) affected 10
3.2.Estimated financial impact of the proposal on appropriations..... 12
3.2.1.Summary of estimated impact on operational appropriations..... 12
3.2.1.1.Appropriations from voted budget 12
3.2.1.2.Appropriations from external assigned revenues 17
3.2.2.Estimated output funded from operational appropriations..... 22
3.2.3. Summary of estimated impact on administrative appropriations 24
3.2.3.1. Appropriations from voted budget 24

3.2.3.2.Appropriations from external assigned revenues 24
3.2.3.3.Total appropriations 24
3.2.4.Estimated requirements of human resources 25
3.2.4.1. Financed from voted budget 25
3.2.4.2.Financed from external assigned revenues 26
3.2.4.3.Total requirements of human resources 26
3.2.5.Overview of estimated impact on digital technology-related investments 28
3.2.6.Compatibility with the current multiannual financial framework 28
3.2.7.Third-party contributions 28
3.3.Estimated impact on revenue 29
4.DIGITAL DIMENSIONS 29
4.1.Requirements of digital relevance 30
4.2.Data 30
4.3.Digital solutions 31
4.4.Interoperability assessment 31
4.5.Measures to support digital implementation 32

1. FRAMEWORK OF THE PROPOSAL/INITIATIVE

1.1. Title of the proposal/initiative

Proposal for a Regulation of the European Parliament and of the Council on the simplification of the digital acquis, amending Regulation (EU) 2023/2854, Regulation (EU) 2016/679, Regulation (EU) 2024/1689 and Directive 2002/58/EC and Directive (EU) 2022/2555 and repealing Regulation (EU) 2022/868, Regulation EU 2018/1807, Regulation (EU) 2019/1150 and Directive (EU) 2019/1024 (Digital Omnibus for the digital acquis)

1.2. Policy area(s) concerned

Communications Networks, Content and Technology;

Internal Market, Industry, Entrepreneurship and SMEs

1.3. Objective(s)

1.3.1. General objective(s)

Simplification of the application of the Digital Acquis and cost saving for businesses

1.3.2. Specific objective(s)

<u>Specific objective No 1</u>

To enhance governance and effective enforcement of the Digital Acquis by reducing the complexity of rules, the administrative costs for businesses and admnistrations and repealing of Acts

<u>Specific objective No 2</u>

Providing a single-entry point for incident reporting across several legal frameworks

1.3.3. Expected result(s) and impact

Specify the effects which the proposal/initiative should have on the beneficiaries/groups targeted.

Reduced costs for businesses as a result of reducing complexity of legislation and by streamlined reporting

1.3.4. Indicators of performance

Specify the indicators for monitoring progress and achievements.

Indicator 1

Calculated cost reductions for businesses

Indicator 2

Cost savings for incident reporting by businesses

Indicator 3

1.4. The proposal/initiative relates to:

☐ a new action

☐ a new action following a pilot project / preparatory action[39]

☒ the extension of an existing action

☐ a merger or redirection of one or more actions towards another/a new action

1.5. Grounds for the proposal/initiative

1.5.1. Requirement(s) to be met in the short or long term including a detailed timeline for roll-out of the implementation of the initiative

The entry into force is expected within 3 days from the publication in the Official Journal. The entry into application should be immediate, with notable exceptions for rules that require a transitional period. For Chapter III on incident reporting and platform related rules a sufficient period for the implementation is required which is adapted to the needs of businesses, Member States and EU bodies.

1.5.2. Added value of EU involvement (it may result from different factors, e.g. coordination gains, legal certainty, greater effectiveness or complementarities). For the purposes of this section 'added value of EU involvement' is the value resulting from EU action, that is additional to the value that would have been otherwise created by Member States alone.

Reasons for action at EU level result from the fact that the modifications concern existing EU legislation and reduce the complexity of EU law (ex-ante) Expected generated EU added value (ex-post) consist in the streamlining of EU law, reduced administrative burden and costs for businesses. For the establishment of the single-entry point for incident reporting, the particular added value stems from providing a Union-level solution that caters for national requirements. Costs for businesses are optimised by providing one single-point, irrespective of where the reporting entity is located in the Union and what authorities are mandated to receive the reports.

1.5.3. Lessons learned from similar experiences in the past

The amendments to the respective regulations are informed by the practical experience in the implementation of the rules, as detailed in the accompanying Staff Working Document. They build on extensive stakeholder consultation, focusing primarily on the day-to-day application of the rules.

1.5.4. Compatibility with the multiannual financial framework and possible synergies with other appropriate instruments

The amendments are compatible with the multiannual financial framework since there is no additional expenditure forseen..

[39] As referred to in Article 58(2), point (a) or (b) of the Financial Regulation.

1.5.5. Assessment of the different available financing options, including scope for redeployment

N.A.

1.6. Duration of the proposal/initiative and of its financial impact

5. ☐ limited duration

☐ in effect from [DD/MM]YYYY to [DD/MM]YYYY

☐ financial impact from YYYY to YYYY for commitment appropriations and from YYYY to YYYY for payment appropriations.

6. ☒ unlimited duration

Implementation with a start-up period from YYYY to YYYY,

followed by full-scale operation.

1.7. Method(s) of budget implementation planned[40]

7. ☒ **Direct management** by the Commission

☒ by its departments, including by its staff in the Union delegations;

☐ by the executive agencies

8. ☐ **Shared management** with the Member States

9. ☐ **Indirect management** by entrusting budget implementation tasks to:

☐ third countries or the bodies they have designated

☐ international organisations and their agencies (to be specified)

☐ the European Investment Bank and the European Investment Fund

☐ bodies referred to in Articles 70 and 71 of the Financial Regulation

☐ public law bodies

☐ bodies governed by private law with a public service mission to the extent that they are provided with adequate financial guarantees

☐ bodies governed by the private law of a Member State that are entrusted with the implementation of a public-private partnership and that are provided with adequate financial guarantees

☐ bodies or persons entrusted with the implementation of specific actions in the common foreign and security policy pursuant to Title V of the Treaty on European Union, and identified in the relevant basic act

☐ bodies established in a Member State, governed by the private law of a Member State or Union law and eligible to be entrusted, in accordance with sector-specific rules, with the implementation of Union funds or budgetary guarantees, to the extent that such bodies are controlled by public law bodies or by bodies governed by private law with a public service mission, and are provided with adequate financial guarantees in the form of joint and several liability by the controlling

[40] Details of budget implementation methods and references to the Financial Regulation may be found on the BUDGpedia site: https://myintracomm.ec.europa.eu/corp/budget/financial-rules/budget-implementation/Pages/implementation-methods.aspx.

bodies or equivalent financial guarantees and which may be, for each action, limited to the maximum amount of the Union support.

I

2. MANAGEMENT MEASURES

2.1. Monitoring and reporting rules

10. The amendments will be monitored as part of the legistion that is modified,

2.2. Management and control system(s)

2.2.1. Justification of the budget implementation method(s), the funding implementation mechanism(s), the payment modalities and the control strategy proposed

11. The management and control systems that apply for the existing legislation ensures an effective control also for the amendments

2.2.2. Information concerning the risks identified and the internal control system(s) set up to mitigate them

12. No additional risks identified

2.2.3. Estimation and justification of the cost-effectiveness of the controls (ratio between the control costs and the value of the related funds managed), and assessment of the expected levels of risk of error (at payment & at closure)

13. The cost of control will not differ from the previous cost

2.3. Measures to prevent fraud and irregularities

14. The same preventive measures continue to apply for the amendments

3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

3.1. Heading(s) of the multiannual financial framework and expenditure budget line(s) affected

Existing budget lines

15. In order of multiannual financial framework headings and budget lines.

Heading of multiannual financial framework	Budget line	Type of expenditure	Contribution			
	Number	Diff./Non-diff.[41]	from EFTA countries [42]	from candidate countries and potential candidates [43]	From other third countries	other assigned revenue
	20 02 06 Administrative expenditure	Non-diff.	NO	NO	NO	NO

New budget lines requested

16. In order of multiannual financial framework headings and budget lines.

Heading of multiannual financial framework	Budget line	Type of expenditure	Contribution			
	Number	Diff./Non-diff.	from EFTA countries	from candidate countries and potential candidates	from other third countries	other assigned revenue

[41] Diff. = Differentiated appropriations / Non-diff. = Non-differentiated appropriations.
[42] EFTA: European Free Trade Association.
[43] Candidate countries and, where applicable, potential candidates from the Western Balkans.

3.2. Estimated financial impact of the proposal on appropriations

3.2.1. Summary of estimated impact on operational appropriations

☒The proposal/initiative does not require the use of operational appropriations

☐ The proposal/initiative requires the use of operational appropriations, as explained below

3.2.1.1. Appropriations from voted budget

EUR million (to three decimal places)

Heading of multiannual financial framework	Number	

DG: <…….>			Year	Year	Year	Year	**TOTAL MFF 2021-2027**
			2024	**2025**	**2026**	**2027**	
Operational appropriations							
Budget line	Commitments	(1a)					**0.000**
	Payments	(2a)					**0.000**
Budget line	Commitments	(1b)					**0.000**
	Payments	(2b)					**0.000**
Appropriations of an administrative nature financed from the envelope of specific programmes[44]							
Budget line		(3)					**0.000**
TOTAL appropriations for DG <…….>	Commitments	=1a+1b+3	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**
	Payments	=2a+2b+3	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**

[44] Technical and/or administrative assistance and expenditure in support of the implementation of EU programmes and/or actions (former 'BA' lines), indirect research, direct research.

==========

This section should be filled in using the 'budget data of an administrative nature' to be firstly inserted in the Annex to the Legislative Financial and Digital Statement (Annex 5[45] to the Commission Decision on the internal rules for the implementation of the Commission section of the general budget of the European Union), which is uploaded to DECIDE for interservice consultation purposes.

DG: <…….>		Year **2024**	Year **2025**	Year **2026**	Year **2027**	**TOTAL MFF 2021-2027**
• Human resources		0.000	0.000	0.000	0.000	**0.000**
• Other administrative expenditure		0.000	0.000	0.000	0.000	**0.000**
TOTAL DG <…….>	Appropriations	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**

DG: <…….>		Year **2024**	Year **2025**	Year **2026**	Year **2027**	**TOTAL MFF 2021-2027**
• Human resources		0.000	0.000	0.000	0.000	**0.000**
• Other administrative expenditure		0.000	0.000	0.000	0.000	**0.000**
TOTAL DG <…….>	Appropriations	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**

TOTAL appropriations under HEADING 7 of the multiannual financial framework	(Total commitments = Total payments)	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**

EUR million (to three decimal places)

	Year	Year	Year	Year	**TOTAL MFF**

[45] If you report the use of appropriations under Heading 7, completing Annex 5 is a compulsory requirement.

		2024	2025	2026	2027	2021-2027
TOTAL appropriations under HEADINGS 1 to 7	Commitments	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**
of the multiannual financial framework	Payments	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**

3.2.1.2. Appropriations from external assigned revenues

EUR million (to three decimal places)

Heading of multiannual financial framework	Number	

DG: <…….>			Year 2024	Year 2025	Year 2026	Year 2027	**TOTAL MFF 2021-2027**
Operational appropriations							
Budget line	Commitments	(1a)					**0.000**
	Payments	(2a)					**0.000**
Budget line	Commitments	(1b)					**0.000**
	Payments	(2b)					**0.000**
Appropriations of an administrative nature financed from the envelope of specific programmes[46]							
Budget line		(3)					**0.000**
TOTAL appropriations for DG <…….>	Commitments	=1a+1b+3	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**
	Payments	=2a+2b+3	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**

[46] Technical and/or administrative assistance and expenditure in support of the implementation of EU programmes and/or actions (former 'BA' lines), indirect research, direct research.

Heading of multiannual financial framework	**7**	'Administrative expenditure'[47]

EUR million (to three decimal places)

DG: <…….>		Year **2024**	Year **2025**	Year **2026**	Year **2027**	**TOTAL MFF 2021-2027**
• Human resources		0.000	0.000	0.000	0.000	**0.000**
• Other administrative expenditure		0.000	0.000	0.000	0.000	**0.000**
TOTAL DG <…….>	Appropriations	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**

DG: <…….>		Year **2024**	Year **2025**	Year **2026**	Year **2027**	**TOTAL MFF 2021-2027**
• Human resources		0.000	0.000	0.000	0.000	**0.000**
• Other administrative expenditure		0.000	0.000	0.000	0.000	**0.000**
TOTAL DG <…….>	Appropriations	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**

TOTAL appropriations under HEADING 7 of the multiannual financial framework	(Total commitments = Total payments)	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**

EUR million (to three decimal places)

	Year **2024**	Year **2025**	Year **2026**	Year **2027**	**TOTAL MFF 2021-2027**

[47] The necessary appropriations should be determined using the annual average cost figures available on the appropriate BUDGpedia webpage.

TOTAL appropriations under HEADINGS 1 to 7	Commitments	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**
of the multiannual financial framework	Payments	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**

3.2.2. Estimated output funded from operational appropriations (not to be completed for decentralised agencies)

Commitment appropriations in EUR million (to three decimal places)

Indicate objectives and outputs ⇩			Year **2024**		Year **2025**		Year **2026**		Year **2027**		Enter as many years as necessary to show the duration of the impact (see Section1.6)						**TOTAL**	
	OUTPUTS																	
	Type [48]	Average cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	Total No	Total cost
SPECIFIC OBJECTIVE No 1[49]…																		
- Output																		
- Output																		
- Output																		
Subtotal for specific objective No 1																		
SPECIFIC OBJECTIVE No 2 ...																		
- Output																		

[48] Outputs are products and services to be supplied (e.g. number of student exchanges financed, number of km of roads built, etc.).
[49] As described in Section 1.3.2. 'Specific objective(s)'

Subtotal for specific objective No 2																
TOTALS																

3.2.3. Summary of estimated impact on administrative appropriations

☒The proposal/initiative does not require the use of appropriations of an administrative nature

☐ The proposal/initiative requires the use of appropriations of an administrative nature, as explained below

3.2.3.1. Appropriations from voted budget

VOTED APPROPRIATIONS	Year 2024	Year 2025	Year 2026	Year 2027	TOTAL 2021 - 2027
HEADING 7					
Human resources	0.000	0.000	0.000	0.000	**0.000**
Other administrative expenditure	0.000	0.000	0.000	0.000	**0.000**
Subtotal HEADING 7	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**
Outside HEADING 7					
Human resources	0.000	0.000	0.000	0.000	**0.000**
Other expenditure of an administrative nature	0.000	0.000	0.000	0.000	**0.000**
Subtotal outside HEADING 7	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**
TOTAL	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**

The appropriations required for human resources and other expenditure of an administrative nature will be met by appropriations from the DG that are already assigned to management of the action and/or have been redeployed within the DG, together, if necessary, with any additional allocation which may be granted to the managing DG under the annual allocation procedure and in the light of budgetary constraints.

3.2.4. Estimated requirements of human resources

☒The proposal/initiative does not require the use of human resources

☐ The proposal/initiative requires the use of human resources, as explained below

3.2.4.1. Financed from voted budget

Estimate to be expressed in full-time equivalent units (FTEs)[50]

17.

VOTED APPROPRIATIONS	Year 2024	Year 2025	Year 2026	Year 2027
• Establishment plan posts (officials and temporary staff)				
20 01 02 01 (Headquarters and Commission's Representation Offices)	0	0	0	0
20 01 02 03 (EU Delegations)	0	0	0	0
01 01 01 01 (Indirect research)	0	0	0	0

[50] Please specify below the table how many FTEs within the number indicated are already assigned to the management of the action and/or can be redeployed within your DG and what are your net needs.

01 01 01 11 (Direct research)		0	0	0	0
Other budget lines (specify)		0	0	0	0
• **External staff (inFTEs)**					
20 02 01 (AC, END from the 'global envelope')		0	0	0	0
20 02 03 (AC, AL, END and JPD in the EU Delegations)		0	0	0	0
Admin. Support line [XX.01.YY.YY]	- at Headquarters	0	0	0	0
	- in EU Delegations	0	0	0	0
01 01 01 02 (AC, END - Indirect research)		0	0	0	0
01 01 01 12 (AC, END - Direct research)		0	0	0	0
Other budget lines (specify) - Heading 7		0	0	0	0
Other budget lines (specify) - Outside Heading 7		0	0	0	0
TOTAL		**0**	**0**	**0**	**0**

3.2.5. Overview of estimated impact on digital technology-related investments

18. Compulsory: the best estimate of the digital technology-related investments entailed by the proposal/initiative should be included in the table below.

19. Exceptionally, when required for the implementation of the proposal/initiative, the appropriations under Heading 7 should be presented in the designated line.

20. The appropriations under Headings 1-6 should be reflected as "Policy IT expenditure on operational programmes". This expenditure refers to the operational budget to be used to re-use/ buy/ develop IT platforms/ tools directly linked to the implementation of the initiative and their associated investments (e.g. licences, studies, data storage etc). The information provided in this table should be consistent with details presented under Section 4 "Digital dimensions".

TOTAL Digital and IT appropriations	Year **2024**	Year **2025**	Year **2026**	Year **2027**	**TOTAL MFF 2021 - 2027**
HEADING 7					
IT expenditure (corporate)	0.000	0.000	0.000	0.000	**0.000**
Subtotal HEADING 7	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**
Outside HEADING 7					
Policy IT expenditure on operational programmes	0.000	0.000	0.000	0.000	**0.000**
Subtotal outside HEADING 7	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**
TOTAL	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**

3.2.6. Compatibility with the current multiannual financial framework

21. The proposal/initiative:

☒can be fully financed through redeployment within the relevant heading of the multiannual financial framework (MFF)

☐ requires use of the unallocated margin under the relevant heading of the MFF and/or use of the special instruments as defined in the MFF Regulation

☐ requires a revision of the MFF

3.2.7. Third-party contributions

22. The proposal/initiative:

☒does not provide for co-financing by third parties

☐ provides for the co-financing by third parties estimated below:

Appropriations in EUR million (to three decimal places)

	Year **2024**	Year **2025**	Year **2026**	Year **2027**	Total
Specify the co-financing body					
TOTAL appropriations co-financed					

3.3. Estimated impact on revenue

☒The proposal/initiative has no financial impact on revenue.

– ☐ The proposal/initiative has the following financial impact:

– ☐ on own resources

– ☐ on other revenue

– ☐ please indicate, if the revenue is assigned to expenditure lines

EUR million (to three decimal places)

Budget revenue line:	Appropriations available for the current financial year	Impact of the proposal/initiative[51]			
		Year **2024**	Year **2025**	Year **2026**	Year **2027**
Article …….					

23. For assigned revenue, specify the budget expenditure line(s) affected.

24. […]

25. Other remarks (e.g. method/formula used for calculating the impact on revenue or any other information).

[51] As regards traditional own resources (customs duties, sugar levies), the amounts indicated must be net amounts, i.e. gross amounts after deduction of 20% for collection costs.

26. […]

27. 4. DIGITAL DIMENSIONS

4.1. Requirements of digital relevance

High-level description of the requirements of digital relevance and related categories (data, process digitalisation & automation, digital solutions and/or digital public services)

Reference to the requirement	**Requirement description**	**Actors affected or concerned by the requirement**	**High-level Processes**	**Categories**
Article 1	Amendment to Article 1(1) of the Data Act, widening its scope of application to the establishment of the following: • a framework for registration of data intermediation services; • a framework for voluntary registration of entities which collect, and process data made available for altruistic purposes; • a framework for the establishment of a European Data Innovation Board.	European Commission Data intermediation services Data collection and processing entities	Extension of the scope of application of the Data Act	Digital Public Service
Article 1	Amendment to Articles 4(8) and 5(11) of the Data Act. Data holders refusing to share data pursuant to the trade secrets exception shall provide adequate notification of such decision.	Data holders (trade secret holders) Access request originators	Notification	Data

Article 1	Insertion of Article 15a into the Data Act. Obligation to make data available on the basis of a public emergency.	Public sector body European Commission European Central Bank Union body Data holders	Making data available	Data
Article 1	Amendment to Article 21(5) of the Data Act. Requirements regarding the sharing of data obtained in the context of a public emergency with research organisations or statistical bodies. Insertion of Article 22a into the Data Act, allowing for complaints as relates to Chapter V (‘*Making data available to public sector bodies, the Commission, the European Central Bank and Union Bodies on the basis of an exceptional need’*).	Public sector body European Commission European Central Bank Union body Data holder National competent authority	Data sharing Complaints	Data
Article 1	Amendments to Article 32(1-5) of the Data Act on third-country access to non-personal data.	Providers of data processing services Data intermediation services providers Data altruism organisations National bodies or authorities	International governmental data access and transfer	Data Digital Public Service

Article 1	Amendment to Article 35(5) of the Data Act, allowing the Commission to adopt common specifications as relates to the interoperability of data processing services.	Providers of data processing services European Commission	Adoption of common specifications	Digital Public Service
Article 1	Amendments to Article 32a-32e of the Data Act to introduce Chapter VIIa on the regulatory framework for a European label for data intermediation services including notification, creation of a public register, conditions for service provision, designation of competent authorities, and monitoring of compliance Amendments to Article 32h of the Data Act to introduce Chapter VIIb on the free flows of data within the Union including prohibition of data localisation requirements, notification obligations to the Commission, and publication of a consolidated list.	Data intermediation services providers Data subjects, Data holders, Data users Member States Competent authorities European Commission	Establishment of the European label for data intermediation services Establishment of the free movement of data within the European Union	Data Digital Solution Process Digitalisation Digital Public Service

Article 1	Amendments to Article 32h of the Data Act to introduce Chapter VIIb on the free flows of data within the Union including prohibition of data localisation requirements, notification obligations to the Commission, and publication of a consolidated list.	Member States European Commission	Establishment of the free movement of data within the European Union	Data Process digitalisation Digital Public Service
Article 1	Insertion of Article 32i into the Data Act, defining the scope of Chapter VIIc. This establishes a set of minimum rules governing the re-use and the practical arrangements for facilitating the re-use of data. Insertion of Article 32j into the Data Act; provision on non-discrimination as regards the re-use of data and documents.	Member States Data holders Data users	Defining subject matter and scope Non-discrimination	Digital Public Service
Article 1	Insertion of Article 32k into the Data Act. Rules regarding exclusive arrangements for data reuse. Includes obligation to make the final terms of arrangements publicly	Potential actors in the market Public sector bodies		Digital Public Service Data

	available.	Parties to such agreements		
Article 1	Amendments to the Data Act: • (41): Inserting Article 32n on general principle for the re-use of open government data. • (42): Inserting Article 32o on the processing of requests for data re-use • (43): Inserting Article 32p on formats for data reuse • (46): Inserting Article 32s on practical arrangements facilitating the search for data or documents available for re-use	Data holders Data users Member States (Public sector bodies) European Commission	Data re-use rules	Digital Public Service Data Process digitalisation
Article 1	Insertion of Article 32t into the Data Act; requirement to support the availability of research data.	Member States Research organisations Data users	Data re-use rules	Digital Public Service Data
Article 1	Insertion of Article 32u into the Data Act. Laying down arrangements for the publication and re-use of specific high-value datasets.	European Commission Public sector bodies, Public undertakings	Data re-use rules	Digital Public Service Data
Article 1	Insertion of Article 32w into the Data Act. Laying down conditions for the re-use of certain categories of data. The procedures for requesting and the conditions for	Public sector bodies Data users	Data re-use rules	Digital Public Service Data

	allowing such re-use shall be made publicly available via the single information point.			
Article 1	Insertion of Article 32x into the Data Act; requirements for the transfers of non-personal data to third countries by re-users.	Re-users of data Public sector bodies Natural/legal persons whose rights may be affected	Transfer of data to third countries	Digital Public Service Data
Article 1	Amendments to the Data Act: • (55): Inserting Article 32z; organisational measures pertaining to competent bodies. • (57): Inserting Article 32ab on procedures for requests for re-use of data. • (58): Replacing Article 38(1-2) on the right to lodge a complaint.	Competent bodies Member States Public sector bodies	Establishment of competent bodies Request procedures Complaints	Digital Public Service Data
Article 1	Inserting Article 32aa into the Data Act. Mandating the use of a Single Information Point to facilitate data reuse.	Member States Data holders Data users European Commission.	Establishment of a single access point	Digital solutions Digital Public Service Process digitalisation Data

Article 1	Amendments to Articles 41a, 42, 45, 46, 48a, 49, 49a of the Data Act to introduce Chapter IXa establishing the European Data Innovation Board (EDIB) as an expert group to coordinate enforcement and facilitate development of a European data economy, including composition requirements, role, facilitating cooperation between competent authorities, and supporting consistent application of legal requirements.	European Commission, European Data Innovation Board (EDIB) Member States representatives competent for data economy policy Competent authorities for enforcement of Chapters II, III and V Competent authorities for re-use of public sector information (Open Data Directive) Competent authorities for data intermediation services Competent authorities for registration of data altruism organisations European Data Protection Board (EDPB), European Data Protection Supervisor (EDPS) ENISA (European Union Agency for Cybersecurity)	Establishment of the European Data Innovation Board (EDIB)	Digital Public Service Data

		EU SME Envoy or representative from the network of SME envoys Other representatives of relevant bodies in specific sectors Bodies with specific expertise Standardisation organisations European Parliament, Council of the European Union, European Economic and Social Committee Data intermediation services providers Recognised data altruism organisations		
Article 3	Amendment of Article 33, Regulation (EU) 2016/679 (GDPR), as pertains to personal data breach notifications. Inter alia, mandates the use of the single-entry point established pursuant to Article 23a of Directive (EU) 2022/2555, and foresees the use of notification templates.	Data subjects Data controllers Supervisory authorities European Data Protection Board European Commission	Notification	Data

Article 3	Amendment of Article 35 and 70(1), Regulation (EU) 2016/679 (GDPR). Requirement for the European Data Protection Board to transmit to the Commission proposals to further operationalise certain aspects of the data protection impact assessment. These include a common template for such assessments.	European Data Protection Board European Commission	Board proposals transmitted to Commission	Data
Article 3	Insertion of Article 88b into Regulation (EU) 2016/679 (GDPR); data subjects shall be able to provide consent / exercise the right to object through automated and machine-readable means. Standards are foreseen to be drafted by one or more European standardisation organisations.	Data subjects Data controllers European standardisation organisations European Commission	Automated and machine-readable indications of data subject's choices	Digital solutions Process automation
Article 6	Amendment of Directive (EU) 2022/2555 (NIS2): • (1): Inserting Article 23a on the development and maintenance of a single-entry point for incident reporting; • (3): Amending Article 23(4) to mandate the use of the single-entry point for notifications of severe incidents; • (4): Inserting Article 23(12), which ensures that severe incidents are reported only once (either under	Notifiers (essential and important entities) CSIRTs/competent authorities (as applicable) European Commission ENISA	Notification	Data Digital solutions Digital Public Service

	NIS2, or under the Cyber Resilience Act); • (5): Amending Article 30(1) ensuring that the single-entry point can be used, on a voluntary basis, for notifications by different entities.			
Article 7	Amendment of Regulation (EU) 910/2014 (EUDIW) requiring the use of the single-entry point, pursuant to Article 23a of Directive (EU) 2022/2555, for: • Article 19a(1a): Notifications referred to in paragraph (1), point (b). • Article 24(2a): Notifications referred to in paragraph (2), point (fb). Article 45a(3a): Notifications referred to in paragraph (3).	Notifiers (non-qualified trust service providers; qualified trust service providers; providers of a web-browser) Supervisory bodies Other relevant competent bodies/authorities European Commission	Notification	Data

Article 8	Amendment of Regulation (EU) 2022/2554 (DORA) requiring the use of the single-entry point, pursuant to Article 23a of Directive (EU) 2022/2555, for: • Article 19(1): Major ICT-related incidents • Article 19(2): voluntary notifications of significant cyber threats.	Notifiers (financial entities) Supervisory bodies Other relevant competent bodies/authorities European Commission ENISA	Notification	Data
Article 9	Amendment of Directive (EU) 2022/2557 (CER) requiring the use of the single-entry point, pursuant to Article 23a of Directive (EU) 2022/2555, for: • Article 15(1): Incidents that significantly disrupt or have the potential to significantly disrupt the provision of essential services.	Notifiers (critical entities) Supervisory bodies Other relevant competent bodies/authorities European Commission ENISA	Notification	Data

4.2. Data

High-level description of the data in scope

Type of data	**Reference to the requirement(s)**	**Standard and/or specification (if applicable)**
Refusal of a request for access to data on the basis of the trade secret exception (*and notification of such to the competent authority*)	Article 1	To be duly substantiated on the basis of objective elements.
Data to be made available in the context of a public emergency	Article 1	Including the metadata necessary to interpret and use the data. In the case of personal data, pseudonymized where possible.
Notification of intent to make data available in the context of a public emergency	Article 1	Stating the identity and contact details of the organisation or the individual receiving the data, the purpose of the transmission or making available of the data, the period for which the data is to be used, and the technical protection and organisational measures taken.
Complaints under Chapter V ('*Making data available to public sector bodies, the Commission, the European Central Bank and Union Bodies on the basis of an exceptional need*')	Article 1	//
Non-personal data held in the European Union	Article 1	//
Data to be provided in response to a data re-use request	Article 1	To provide the minimum amount of data permissible

Notification of data-reuse request about to be granted	Article 1	//
Data for which intermediation services are provided (European label for data intermediation services and data altruism organisations)	Article 1	Format received from data subject/holder, Conversions only to enhance interoperability or comply with international/European data standards
Information about data uses and terms (European label for data intermediation services and data altruism organisations)	Article 1	Must be provided in a concise, transparent, intelligible, and easily accessible manner
Applications for registration in the public Union register and changes to notified information (European label for data intermediation services and data altruism organisations)	Article 1	Competent authorities shall establish the necessary application forms.
Accepted applications for registration to be added to the public Union register (European label for data intermediation services and data altruism organisations)	Article 1	//
Notification of subsequent changes to the information provided during the application process (European label for data intermediation services and data altruism organisations)	Article 1	//
Receipt of notification of subsequent changes (European label for data intermediation services and data altruism organisations)	Article 1	//
Information provided to data subjects/holders prior to processing (European label for data	Article 1	//

intermediation services and data altruism organisations)		
Consent (or withdrawal of consent) for data processing by a recognised data altruism organisation (European label for data intermediation services and data altruism organisations)	Article 1	To be obtained via electronic means
Information on third-country jurisdiction in which data use is intended to take place	Article 1	//
Notification of unauthorised transfers, access, or use of non-personal data (European label for data intermediation services and data altruism organisations)	Article 1	//
Information for compliance monitoring (European label for data intermediation services and data altruism organisations)	Article 1	Requests must be proportionate and reasoned
Notification of non-compliance (European label for data intermediation services and data altruism organisations)	Article 1	//
Decision to revoke the right to use the label (European label for data intermediation services and data altruism organisations)	Article 1	//
Draft acts on data localisation requirements	Article 1	//

The final terms of exclusive arrangements	Article 1	//
Data (and/or notifications) pertaining to a request for re-use	Article 1	In any pre-existing format or language and, where possible and appropriate, by electronic means, in formats that are open, machine-readable, accessible, findable, and re-usable, together with their metadata.
Publicly funded research data	Article 1	Openly available, following the principle of 'open by default' and compatible with the FAIR principles.
Specific high-value datasets	Article 1	Available free of charge; machine readable; provided via APIs and as a bulk download (where relevant). Implementing acts to follow; these may include formats of data and metadata.
Conditions for allowing the re-use of data or documents referred to in Article 2 (54)	Article 1	Publicly available.
Notification of unauthorised re-use of non-personal data	Article 1	//
Notification of intention to transfer non-personal data to a third country and the purpose of such transfer (*to the public sector body*)	Article 1	//
Notification of intention to transfer non-personal data to a third country, the purpose of this transfer, and the appropriate safeguards (*to the natural or legal person whose rights and interests may be affected*)	Article 1	//

All relevant information concerning the application of Articles 32z [conditions for re-use], 32aa [third countries] and 32ab [Fees] of the Data Act.	Article 1	Available and easily accessible through a single information point.
Complaint lodged by natural/legal persons if their rights under the Data Act have been infringed or as regards other relevant matters	Article 1	//
Information on progress of proceedings / judicial remedies in connection to a complaint lodged under the Data Act	Article 1	//
Experience and good practice data (EDIB)	Article 1	//
Evaluation of chapters II, III, IV, V, VI, VII, and VIII of the Data Act Evaluation of chapters VIIa, VIIb and VIIc of the Data Act	Article 1 Article 1	Minimum content requirements for reports are provided.
Notifications of personal data breaches	Article 3	Via (and thus respecting the specifications of) the single-entry point established pursuant to Article 23a of Directive (EU) 2022/2555. The European Data Protection Board shall prepare a proposal for a common template (*see following entry*).
EDPB proposal for a common data breach notification template	Article 3	//

EDPB proposals regarding the data protection impact assessment	Article 3	//
Reports on significant incidents pursuant to the NIS2 Directive	Article 6	Via (and thus respecting the specifications of) the single-entry point established pursuant to Article 23a of Directive (EU) 2022/2555.
Notifications of personal data breaches	Article 3	Via (and thus respecting the specifications of) the single-entry point established pursuant to Article 23a of Directive (EU) 2022/2555
Notifications of major ICT-related incidents pursuant to DORA; voluntary notifications of significant cyber threats pursuant to DORA	Article 8	Via (and thus respecting the specifications of) the single-entry point established pursuant to Article 23a of Directive (EU) 2022/2555
Notifications of incidents that significantly disrupt or have the potential to significantly disrupt the provision of essential services, pursuant to the CER Directive	Article 9	Via (and thus respecting the specifications of) the single-entry point established pursuant to Article 23a of Directive (EU) 2022/2555

Alignment with the European Data Strategy

Explanation of how the requirement(s) are aligned with the European Data Strategy

These amendments to the Data Act introduce the EDIB (Chapter IXa), which coordinates the application of rules and develops guidelines for sectoral common European data spaces; the European labels for data intermediation services and data altruism organisations (Chapter VIIa) that create a trustworthy ecosystem for data sharing with and rights protection in place; Chapter VIIb implements the free flow of non-personal data by prohibiting unjustified data localisation requirements; Chapter VIIc streamlines rules on the re-use of public sector data, merging the provisions under the Open Data Directive and Data Governance Act; the rules on international data transfers strengthen European digital sovereignty by protecting data from unauthorised access by third countries; finally, exemptions for SMEs and the presence of the EU SME Envoy in the EDIB ensure that the data economy is better accessible to small businesses as well.

Alignment with the once-only principle

Explanation of how the once-only principle has been considered and how the possibility to reuse existing data has been explored

These amendments support the once-only principle by creating infrastructure for efficient data reuse: the EDIB develops interoperability standards across common European data spaces to reduce duplicate data provision; data intermediation services act as trusted intermediaries enabling secure sharing of existing data, eliminating redundant collection; data altruism organisations facilitate voluntary data sharing for public benefit, making available data reusable for research and public services; free flow provisions prevent barriers requiring duplicate storage across locations; and international transfer safeguards ensure cross-border data accessibility while maintaining protection, collectively enabling individuals and businesses to provide their data once with subsequent needs met through secure, rights-respecting sharing mechanisms. Meanwhile, the provisions under the single-entry point further enable the once-only principle when it comes to incident reporting.

Explanation of how newly created data is findable, accessible, interoperable, and reusable, and meets high-quality standards

These amendments ensure newly created data meets FAIR principles and quality standards through coordinated mechanisms: the EDIB develops common technical specification and accessible interoperability protocols across sectoral data spaces; free flow provisions prevent fragmentation that undermines data quality; the EDIB's coordination role may enable harmonised implementation of metadata standards, technical requirements, and quality benchmarks across Member States.

Data flows

High-level description of the data flows

NB: Most of the data flows detailed below are preexisting flows that are being moved from one Regulation to another. Namely, provisions from the Data Governance Act are transferred to the Data Act.

Type of data	**Reference(s) to the requirement(s)**	**Actors who provide the data**	**Actors who receive the data**	**Trigger for the data exchange**	**Frequency (if applicable)**
Refusal of a request for access to data on the basis of the trade secret exception (*and notification*	Article 1 *Amending Articles 4(8) and 5(11) of the*	Data holder	Data user (making the request); Competent	Refusal of a request to access data based on the trade secret	Ad hoc

of such to the competent authority)	*Data Act*		authority designated pursuant to Article 37	exception	
Data to be made available in the context of a public emergency	Article 1 *Inserting Article 15a into the Data Act*	Data holder	Public sector body; European Commission; European Central Bank; Union body	Public emergency + Request for access to data meeting the necessary conditions	Ad hoc
Notification of intent to make data available in the context of a public emergency	Article 1 *Amending Article 21(5) of the Data Act*	Public sector body; European Commission; European Central Bank; Union body	Data holder from whom the data was received	Public emergency + Intention to transmit or made data available	Ad hoc
Complaints under Chapter V ('Making data available to public sector bodies, the Commission, the European Central Bank and Union Bodies on the basis of an exceptional need')	Article 1 *Inserting Article 22a into the Data Act*	Data holder; public sector body; European Commission; European Central Bank; Union body	Competent authority of the Member State where the data holder is established	Where a dispute arises concerning a request for data under Article 15a of the Data Act	Ad hoc
Non-personal data held in the European Union	Article 1 *Amending the following Articles of the Data Act:* *Article 32(1), Article 32(3), Article 32(4)*	Data processing services providers, Data intermediation services providers, Data altruism organisations	Third-country courts/tribunals, Third-country administrative authorities, Customers (data holders/subjects)	Third-country request based on international agreement, Third-country request meeting conditions of Article 32(3), Customer request for access to their own	Ad hoc

				data	
Data to be provided in response to a data re-use request	Article 1 *Amending Article 32(4-5) of the Data Act*	Data intermediation services provider or the recognised data altruism organisation	The originator of the data re-use request (third country authority)	Date re-use request granted	Ad hoc
Notification of data-reuse request about to be granted	Article 1 *Amending Article 32(4-5) of the Data Act*	Data intermediation services provider or the recognised data altruism organisation	Customer	Date re-use request of third country authority granted (*except where the request serves law enforcement purposes*)	Ad hoc
Information to be published in public registers (European label for data intermediation services and data altruism organisations)	Article 1 *Inserting Article 32a into the Data Act*	European Commission	Public	Information on recognised data intermediation services or data altruism organisations becomes available or in need of change	Ongoing (register regularly updated)
Data for which intermediation services are provided (European label for data intermediation services and data altruism organisations)	Article 1 *Inserting Article 32c into the Data Act*	Data subjects Data holders	Data users (via data intermediation services provider)	Data subject consent Data holder permission Data user request	As per agreement/contract between parties

Information about data uses and terms (European label for data intermediation services and data altruism organisations)	Article 1 *Inserting Article 32c into the Data Act*	Data intermediation services provider	Data subjects	Before data subject gives consent for data use	Each time before consent is requested
Applications for registration in the public Union register and changes to notified information (European label for data intermediation services and data altruism organisations)	Article 1 *Inserting Article 32e into the Data Act*	Data intermediation services providers Data altruism organisations	Competent authority in the Member State of main establishment	Application	Ad hoc
Accepted applications for registration to be added to the public Union register (European label for data intermediation services and data altruism organisations)	Article 1 *Inserting Article 32e into the Data Act*	Competent authority	European Commission	Application approved	Ad hoc (within 12 weeks after the receipt of an application, provided that the decision is positive)
Notification of subsequent changes to the information provided during the application process (European label for data intermediation services and data altruism organisations)	Article 1 *Inserting Article 32e into the Data Act*	Registered entities	Competent authority	Changes to the information provided or where entities cease their activities in the Union	Ad hoc

Receipt of notification of subsequent changes (European label for data intermediation services and data altruism organisations)	Article 1 *Inserting Article 32e into the Data Act*	Competent authority	European Commission	Registered entities notify change (see entry above)	Ad hoc, without delay
Information provided to data subjects/holders prior to processing (European label for data intermediation services and data altruism organisations)	Article 1 *Inserting Article 32f into the Data Act*	Recognised data altruism organisation	Data subjects Data holders	Prior to any processing of their data	Before each processing activity (must be clear and easily comprehensible)
Consent (or withdrawal of consent) for data processing by a recognised data altruism organisation (European label for data intermediation services and data altruism organisations)	Article 1 *Inserting Article 32f into the Data Act*	Data subjects Data holders (if non-personal data)	Data altruism organisation	Data subject consent / Data holder permission needed for processing activities	As per consent/permission granted, with possibility of withdrawal at any time
Information on third-country jurisdiction in which data use is intended to take place	Article 1 *Inserting Article 32f into the Data Act*	Data altruism organisation	Data holders	Where data altruism organisation facilitates data processing by third parties	Ad hoc
Notification of unauthorised transfers, access, or use of non-personal data (European label for data intermediation services and data altruism organisations)	Article 1 *Inserting Article 32f into the Data Act*	Data altruism organisation	Data holders	Unauthorised action	Ad hoc, without delay
Information for compliance	Article 1	Data	Competent	Request from	Ad hoc (upon

monitoring (European label for data intermediation services and data altruism organisations)	*Inserting Article 32g into the Data Act*	intermediation services providers Data altruism organisations	authorities	competent authority Request from natural or legal person	request, which must be proportionate and reasoned)
Notification of non-compliance (European label for data intermediation services and data altruism organisations)	Article 1 *Inserting Article 32g into the Data Act*	Competent authority	Entity who is found non-compliant	Competent authority finds that a recognised data intermediation services provider or a recognised data altruism organisation is non-compliant	Ad hoc (followed by opportunity for entity to state its views within 30 days)
Decision to revoke the right to use the label (European label for data intermediation services and data altruism organisations)	Article 1 *Inserting Article 32g into the Data Act*	Competent authority	Public	Following decision of label revocation	Ad hoc
Draft acts on data localisation requirements	Article 1	Member States	European Commission	Creation of draft act which introduces a new data localisation requirement or makes changes to an existing data localisation requirement	Ad hoc, immediately
The final terms of exclusive arrangements	Article 1	Parties to the arrangement	Public	Exclusive arrangements	Ad hoc, at least two months before

				established on or after 16 July 2019	an arrangement comes into effect
Data (and/or notifications) pertaining to a request for re-use	Article 1 *Inserting Article 32p into the Data Act*	Public sector bodies	Originators of data re-use requests	If documents any of the following are to be provided: requested data/documents; licence offer; notifications of delays; notification of a negative decision.	Ad hoc
The final terms of exclusive arrangements	Article 1 *Inserting Article 32k into the Data Act*	Parties to an exclusive arrangement	General public	Final terms of an exclusive arrangement being reached	Ad hoc
Conditions for allowing the re-use of data or documents referred to in Article 2 (54)	Article 1 *Inserting Article 32z into the Data Act*	Public sector bodies (competent to grant or refuse access requests)	General public	When they grant re-use of data or documents	Ad hoc
Notification of unauthorised re-use of non-personal data	Article 1 *Inserting Article 32z into the Data Act*	Re-user (potentially with the assistance of the public sector body)	Natural or legal persons whose rights and interests may be affected	Unauthorised reuse made	Ad hoc
Notification of intention to transfer non-personal data to a third country and the purpose of	Article 1 *Inserting Article 32aa*	Re-user	Public sector body	Intention to transfer data to a third country	Ad hoc

such transfer (to the public sector body)	*into the Data Act*				
Notification of intention to transfer non-personal data to a third country, the purpose of this transfer, and the appropriate safeguards (to the natural or legal person whose rights and interests may be affected)	Article 1 *Inserting Article 32aa into the Data Act*	Re-user (potentially with the assistance of the public sector body)	Natural or legal person whose rights and interests may be affected	Intention to transfer data to a third country	Ad hoc
All relevant information concerning the application of Articles 32z [conditions for re-use], 32aa [third countries] and 32ab [Fees] of the Data Act.	Article 1 *Inserting Article 32ad into the Data Act*	Member States	Available to users of the single information point	Relevant information needs to be provided	Ad hoc
Complaint lodged by natural/legal persons if their rights under the Data Act have been infringed or as regards other relevant matters	Article 1 *Amending Article 38(1-2) of the Data Act*	Natural or legal persons	Relevant competent authority in the pertinent Member State	Complaint to be made	Ad hoc
Information on progress of proceedings / judicial remedies in connection to a complaint lodged under the Data Act	Article 1 *Amending Article 38(1-2) of the Data Act*	Relevant competent authority	Natural or legal persons who originated the complaint	Complaint lodged	Ad hoc
Experience and good practice data (EDIB)	Article 1 *Inserting Chapter IXa into the Data Act*	European Data Innovation Board	Commission; Competent authorities	Input to be provided	Ad hoc

Evaluation of chapters II, III, IV, V, VI, VII, and VIII of the Data Act Evaluation of chapters VIIa, VIIb and VIIc of the Data Act	Article 1 *Amending Article 49(1) of the Data Act* Article 1 *Amending Article 49(2) of the Data Act*	European Commission	European Parliament; Council; European Economic and Social Committee	Evaluation on Data Act conducted	By 12 September 2028 By [entry into force plus 5 years]
Notifications of personal data breaches	Article 3 *Amending Article 33(1) of the GDPR*	Data controller	Supervisory authority	Data breach occurring	Ad hoc
EDPB proposal for a common data breach notification template	Article 3 *Amending Article 33(1) of the GDPR*	European Data Protection Board	Commission	Proposal to be submitted	Within [months] of the entry into application of this Regulation Every three years
EDPB proposals regarding the data protection impact assessment	Article 3 *Amending Article 70(1) of the GDPR*	European Data Protection Board	Commission	Proposal to be submitted	Ad hoc
Reports on significant incidents pursuant to the NIS2 Directive	Article 6 *Inserting Articles 23a and 23b, amending Articles 23 and 30(1) of NIS2*	Essential and important entities	CSIRTs/competent authorities (as applicable)	Circumstances described in Article 23(3) of the NIS2 Directive	Ad hoc

Notifications of personal data breaches	Article 3 *Amending Article 33 of GDPR*	Data controllers	Supervisory authority	Personal data breach	Ad hoc
Notifications of major ICT-related incidents pursuant to DORA; voluntary notifications of significant cyber threats pursuant to DORA	Article 8 *Amending Article 19 of DORA*	Financial entities	Relevant competent authority	Major ICT-related incidents; significant cyber threats	Ad hoc
Notifications of incidents that significantly disrupt or have the potential to significantly disrupt the provision of essential services pursuant to CER Directive	Article 9 *Amending Article 15 of CER Directive*	Critical entities	Competent authority	Incidents that significantly disrupt or have the potential to significantly disrupt the provision of essential services	Ad hoc

4.3. Digital solutions

High-level description of digital solutions

NB: All of the digital solutions detailed below are preexisting solutions whose legal basis is being moved from one Regulation to another. Namely, provisions from the Data Governance Act are transferred to the Data Act.

Digital solution	Reference(s) to the requirement(s)	Main mandated functionalities	Responsible body	How is accessibility catered for?	How is reusability considered?	Use of AI technologies (if applicable)
Public Union register of data intermediation services and data altruism organisations	*Inserting Article 32a into the Data Act*	Storage and publication of mandatory information	European Commission	//	//	N/A
Single Information Point (under the Data Act)	Article 1 *Inserting Article 32ad into the Data Act*	Information to be made available and accessible Competent to receive enquiries or requests for the re-use of the categories of protected data Transmit requests, where possible and appropriate by automated means, to the competent public	European Commission	Single access point offering a searchable electronic register of data available in the national single information points and further information on how to request data via those national single	Availability by electronic means a searchable asset list containing an overview of all available data resources […] and the conditions for their re-use.	N/A

		sector bodies Make available by electronic means a searchable asset list containing an overview of all available document resources		information points		
Single-entry point for incident notifications	Article 6 *Inserting Article 23a into NIS2*	Enable reporting of incidents pursuant to relevant Union level acts Ensure interoperability and compatibility with European Business Wallets	European Commission; ENISA	Interoperability & compatibility with European Business Wallets and their own accessibility means	Possibility to cater for the reporting of incidents under different legal acts; possibility to onboard further legal bases into the single-entry point solution in the future	N/A

For each digital solution, explanation of how the digital solution complies with applicable digital policies and legislative enactments

Public Union register of data intermediation services and data altruism organisations

Digital and/or sectorial policy (when these are applicable)	**Explanation on how it aligns**

AI Act	N/A
EU Cybersecurity framework	N/A
eIDAS	N/A
Single Digital Gateway and IMI	Amendment to Regulation (EU) 2018/1724 to add 'Registration as a data intermediation services provider' and 'Registration as a data altruism organisation recognised in the Union' under Annex II.
Others	N/A

Single Information Point (under the Data Act)

Digital and/or sectorial policy (when these are applicable)	**Explanation on how it aligns**
AI Act	N/A
EU Cybersecurity framework	Public sector bodies may provide for a requirement to access and re-use the data or documents remotely within a secure processing environment that is provided or controlled by the public sector body. In such cases, the public sector bodies shall impose conditions that preserve the integrity of the functioning of the technical systems of the secure processing environment used.
eIDAS	N/A
Single Digital Gateway and IMI	N/A
Others	The Single Information Point shall be in compliance with Regulation (EU) 2016/679 (GDPR). Public sector bodies may provide requirements to grant access for the re-use of data or documents only where these have been anonymised, and/or subject to other form of pertinent preparation. Moreover,

	in the event of the unauthorised re-use of non-personal data, the re-user shall be obliged to inform the natural persons whose rights and interests may be affected.

Single-entry point for incident notifications

Digital and/or sectorial policy (when these are applicable)	**Explanation on how it aligns**
AI Act	N/A
EU Cybersecurity framework	As an amendment to NIS2, there is an inherent focus on cybersecurity. More broadly, the single-entry point aims to serve as a gateway, channelling all cybersecurity-related incident reports to respective competent authorities, under several Union legal acts.
eIDAS	The single entry-point is mandated also for incident reporting under Regulation (EU) 910/2014 (eIDAS Regulation). ENISA shall ensure that the single-entry point is interoperable and compatible with the European Business Wallets and that the European Business Wallets can be used at least to identify and authenticate entities using the single-entry point. The European Business Wallet policy initiative will build on the eIDAS framework.
Single Digital Gateway and IMI	N/A
Others	The proposal took into account the entire digital acquis, including policies pertaining to data, cybersecurity, and telecommunications.

4.4. Interoperability assessment

High-level description of the digital public service(s) affected by the requirements

Digital public service or category of digital public services	**Description**	**Reference(s) to the requirement(s)**	**Interoperable Europe Solution(s)** **(NOT APPLICABLE)**	**Other interoperability solution(s)**
European data governance and transparency infrastructure	Digital public service allowing for data governance and transparency infrastructure and leveraging, inter alia, an EU public register of data intermediation services and data altruism organisations, and a single information point helping re-users find information on the re-use of certain categories of protected data. Category of digital public services according to COFOG 04.9.0 - Economic affairs n.e.c. (CS)	Article 1	//	//
Incident Reporting	Digital public service allowing for incident reporting via the single-entry point. Category of digital public services according to COFOG 03.6.0 Public order and safety n.e.c.	Article 6	//	European Business Wallets

Impact of the requirement(s) as per digital public service on cross-border interoperability

NB: In the analysis that follows, the Article numbers provided throughout the 'Measure(s)' section are in reference to the Act(s) being amended. The mapping to the requirements of the Omnibus is done once, at the top of every cell.

Digital public service #1 - European data governance and transparency infrastructure

Assessment	**Measure(s)**	**Potential remaining barriers (if applicable)**
Alignment with existing digital and sectorial policies **Please list the applicable digital and sectorial policies identified**	Article 1 Alignment with existing digital and sectorial policies is reflected in the Recitals to the Data Governance Act: Single Digital Gateway (Regulation (EU) 2018/1724) (Recital 56): The notification procedures for data intermediation services and registration procedures for data altruism organisations must be made available through the Single Digital Gateway, ensuring cross-border online access. European Interoperability Framework (Recital 54): The digital infrastructure must adhere to European Interoperability Framework principles to ensure cross-border and cross-sector data use. CEF Building Blocks (Connecting Europe Facility Digital Service Infrastructures) (Recital 54): References "the Core Vocabularies and the CEF Building Blocks". The digital service should leverage CEF Building Blocks (such as eDelivery, eID, eSignature) for technical implementation. Accessibility Requirements (Directives (EU) 2016/2102 and (EU) 2019/882) (Recital 62). Directive (EU) 2016/2102 (Web Accessibility Directive): Public registers and digital services must be accessible to persons with disabilities; Directive (EU) 2019/882 (European Accessibility Act): Digital services must comply with accessibility requirements. GDPR (Regulation (EU) 2016/679) (Recital 4 and 35): All digital services handling personal data must comply with GDPR requirements for data protection, privacy, and	

	security. Regulation (EU) 2018/1725 (Recital 4): Where EU institutions process data through these registers, they must comply with this regulation. Open Data Directive (Directive (EU) 2019/1024) (Recital 6 and 10): "Directive (EU) 2019/1024 and sector-specific Union law ensure that the public sector bodies make more of the data they produce easily available for use and re-use": The digital service complements the Open Data Directive by addressing categories of protected data that fall outside its scope, while ensuring public sector bodies follow "open by design and by default" principles where applicable. Sectorial policies on European data spaces and sectorial data, including European Health Data Space, European Mobility Data Space, European Green Deal / Climate and Energy Data, Manufacturing and Industrial Data, Financial Services Data, Agricultural Data, Public Administration Data Space, and Skills Data Space.	

Organisational measures for a smooth cross-border digital public services delivery **Please list the governance measures foreseen**	Article 1 **Competent authority designation and coordination** - Article 32b: Each Member State shall designate one or more competent authorities responsible for the registration of data intermediation services providers and data altruism organisations. These competent authorities shall maintain their independence from any recognised data intermediation services provider or recognised data altruism organisation. Article 32ac: Each Member State shall designate one or more competent bodies to assist the public sector bodies which grant or refuse access for the re-use of categories of protected data. Article 32g: The competent authorities shall monitor and supervise compliance of recognised data intermediation services providers and recognised data altruism organisations with the provisions of the Data Act. **Cross-border jurisdiction mechanism** Articles 32e: Data intermediation services fall under the purview of the competent authority in the Member State of main establishment. Same principle applies to data altruism organisations. **Mutual recognition and single registration** Article 32e: Registration as a data intermediation service/data altruism organisation shall be valid in all Member States. Article 32a: Use of a common logo design **Centralized EU-level registries for data collection and transparency** Article 32(a): Public Union registers of all recognised data intermediation services providers and data altruism organisations. Article 32(e): Competent authorities notify the Commission electronically without delay	

	of new registrations, changes, and removals and the Commission updates EU registers accordingly **Monitoring and enforcement coordination** National competent authorities European Data Innovation Board **Third-country data transfer governance** Article 32aa: Requirements for transfers of non-personal data to third countries by re-users. **Exclusive Arrangements** Article 32k: Defines permissibility of exclusive arrangements pertaining to the re-use of data or documents held by public sector bodies. Demands transparency of final terms.	
Measures taken to ensure a shared understanding of the data **Please list such measures**	Article 1 **Common standards and interoperable frameworks** - EDIB advises the European Commission on standardisation activities to be undertaken in relation to cross-sector aspects of data sharing, including in relation to the emergence of common European data spaces, considering sector-specific standardisation activities. o Article 42: EDIB assists in adopting "adoption of guidelines establishing interoperable frameworks and common practices for the functioning of common European data spaces". - Common logo for the identification of data intermediation services and data altruism organisations.	

	- Article 32q: Public sector bodies and public undertakings shall make their data or documents available, where possible and appropriate, by electronic means, in formats that are open, machine-readable, accessible, findable, and re-usable, together with their metadata. Both the format and the metadata shall, where possible, comply with formal open standards. **Other Relevant Measures:** - Article 32t: Member States shall, in cooperation with the Commission, shall continue efforts to simplify access to datasets, making available suitable datasets in formats that are accessible, readily findable, and re-usable by electronic means. - Article 32u: Member States shall support the availability of research data in a way that is compatible with the FAIR principles.	
Use of commonly agreed open technical specifications and standards **Please list such measures**	Article 1 **Machine-Readable Data Measures:** - Article 32a: Machine-readable European Union register of data intermediation services providers. - Article 32a: Machine-readable European Union register of data altruism organisations. - Article 32q: Public sector bodies will make their data/documents available, where possible, in formats that are open, machine-readable, accessible, findable, and re-usable, together with their metadata. Both the format and the metadata shall, where possible, comply with formal open standards. - Article 32q: The high-value datasets shall be made available for re-use in machine-readable format, via suitable APIs and, where relevant, as a bulk download. - Article 32t: Member States shall make practical arrangements facilitating the search for data or documents available for re-use, such as asset lists of main data or documents with relevant metadata, accessible where possible and appropriate	

	online and in machine- readable format, and portal sites that are linked to the asset lists. Where possible, Member States shall facilitate the cross-linguistic search for data or documents. - Article 32w: Specific high-value datasets hall be machine readable. Implementing acts may specify arrangements relating to formats of data and metadata and technical arrangements for dissemination. **Machine-to-Machine Interaction Measures:** - Article 32ad: Mandating the use of the Single Information Point. The single information point shall be competent to receive enquiries or requests and shall transmit them, where possible and appropriate by automated means, to the competent public sector bodies, or the competent bodies. **Other Relevant Measures:** - Article 48a: Amending Annex II to Regulation (EU) 2018/1724 (Single Digital Gateway). Synergies explored. - Recital 52of the Omnibus: To the extent feasible, ENISA should take into account existing national technical solutions that facilitate incident reporting, such as national platforms, when developing the specifications on the technical, operational and organisational measures regarding the establishment, maintenance and secure operation of the single-entry point. Further, ENISA should consider technical protocols and tools such as application programming interfaces and machine-readable standards that enable entities to facilitate the integration of reporting obligations into business processes, and for authorities to connect the single-entry point with their national reporting systems.	

Digital public service #2 - Incident Reporting

Assessment	Measure(s)	Potential remaining barriers (if applicable)
Alignment with existing digital and sectorial policies **Please list the applicable digital and sectorial policies identified**	Article 6 General alignment with existing digital and sectorial policies is provided via Directive (EU) 2022/2555 (NIS2), which the Digital Omnibus is now amending. Additionally, the Omnibus provides for synergies with the European Business Wallet , and Regulation (EU) 2024/2847 (Cyber Resilience Act). In particular: • Article 23(4) mandates the use of the single-entry point for NIS2 notification. • Article 23(1) establishes that a notification of severe incident pursuant to Article 14(3) of Regulation (EU) 2024/2847 (Cyber Resilience Act) shall also constitute reporting of information under Directive (EU) 2022/2555 (NIS2). This is in line with the once-only principle. • Article 23a(3)(d) provides for the link with the European Business Wallets.	
Organisational measures for a smooth cross-border digital public services delivery **Please list the governance measures foreseen**	Article 6 Article 23a defines roles and responsibilities. Namely, ENISA shall: • Develop and maintain a single-entry point to support the obligation to report incidents and related events under the Union legal acts. • Take technical, operational, and organisational measures to manage the risks posed to the security of the single-entry point and the information submitted or disseminated. In doing so, it shall consult the Commission, the CSIRTs network, and relevant competent authorities.	
Measures taken to ensure a shared	Article 6	

understanding of the data **Please list such measures**	Article 23a charges ENISA with preparing specifications that shall ensure the necessary capability for interoperability with regard to other relevant reporting obligations. *NB: Content requirements for incident reporting are further laid out in the relevant Union legal acts, including Directive (EU) 2022/2555 (NIS2). Article 23a(3)(c) of the Omnibus clarifies that ENISA shall ensure that these are duly taken into account.*	

Use of commonly agreed open technical specifications and standards
 	
Please list such measures
	Article 6
	
	Article 23a calls for specifications to be developed:
	• ENISA shall provide and implement the specifications on the technical measures regarding the establishment, maintenance, and secure operation of the single-entry point. These specifications shall include, inter alia:
	  ○ the necessary capability for interoperability with regard to other relevant reporting obligations.
	  ○ technical arrangements for the relevant entities and authorities to access, submit, retrieve, transmit or otherwise process information from the single-entry point, as well as technical protocols and tools that allow the entities and authorities to further process the receive information within their systems.
	• Where available, the single-entry point shall be interoperable and compatible with European Business Wallets.	

4.5. Measures to support digital implementation

High-level description of measures supporting digital implementation

Description of the measure	Reference(s) to the	Commission role	Actors to be	Expected

	requirement(s)	(if applicable)	**involved** (if applicable)	**timeline** (if applicable)
Implementing act: Common logo design for data intermediation services providers	Article 1	Lay down the characteristics of the common logo, including its design and use modalities.	Examination procedure committee	//
Implementing act: Common logo design for recognised data altruism	Article 1	Lay down the characteristics of the common logo, including its design and use modalities.	Examination procedure committee	//
Monitoring and compliance: Competent authorities may monitor compliance either on its own initiative or based on a request from natural or legal persons	Article 1	//	Competent authorities, data intermediation services, data altruism organisations	//
Implementing act: Specific high-value datasets	Article 1	Laying down a list of specific high-value datasets. May specify the arrangements for the publication and re-use of high-value datasets.	Examination procedure committee	//

Guidelines: • EDIB to advise on guidelines for common European data spaces • EDIB to adopt guidelines on interoperable frameworks	Article 1	Support from the EDIB	EDIB	//
Implementing act: Common template for notifying a personal data breach	Article 3	Adopt a common template based on EDPB's proposal.	Examination procedure committee	//
Delegated act: Automated and machine-readable indications of data subject's choices	Article 3	Set out obligation for web browsers and providers of terminal equipment	Examination procedure committee	//
Implementing act: CER incident notifications	Article 9	Further specifying the type and format of information notified pursuant to Article 15(1) of Directive (EU) 2022/2557 (CER).	//	//