Council of the European Union
General Secretariat

PUBLIC

Interinstitutional files:
2025/0360 (COD)

Brussels, 12 March 2026

WK 3735/2026 ADD 2

LIMITE

SIMPL
ANTICI
DATAPROTECT
CYBER
TELECOM
CODEC
PROCIV

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From:	General Secretariat of the Council
To:	Antici Group (Simplification)
Subject:	Omnibus VII (Digital Omnibus) - Drafting suggestions on the Commission proposal on Cyber and data issues (deadline 27.02 extension to 6.03.26) - additional comments from EE

Following the meeting of the AGS on 13 February 2026 on Digital Omnibus, delegations will find one document including the additional comments received today from EE Delegation.

This document is added to the MS tables for comments initially consolidated under: WK 3735 INIT (and ADD1).

PUBLIC

Guidelines to be followed

Please kindly provide your contributions in the table below.

Drafting suggestions: you may use '**track changes**'* or formatting (for example **bold-underline** for additions and ~~strike-through~~ for deletions, **where necessary, in a different colour**). *Track changes can only be connected once the cursor is placed in editable areas (Drafting or Comments columns).

To make it feasible to consolidate all contributions, the structure of the table must not be changed, so **no rows can be added or deleted.**

New provisions may only be added in any of the **'existing cells'.**

Name of document: please add the **two initials** of your delegation's country followed by a space (to the MS Word document name), followed by any optional text, for example, for Austria: **AT comments on … .docx**

Thank you for your cooperation!

Commission proposal	Drafting suggestions and Comments
General Comments	
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)	

Commission proposal	Drafting suggestions and Comments
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[1], 1 OJ C […], […], p. […].	
Having regard to the opinion of the European Central Bank[2], 2 OJ C […], […], p. […].	
Having regard to the opinion of the Committee of the Regions[3], 3 OJ C […], […], p. […].	
Acting in accordance with the ordinary legislative procedure,	
Whereas:	
(1) In its Communication on a simpler and faster Europe[4] , 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	

PUBLIC

Commission proposal	Drafting suggestions and Comments
proposal of immediate adjustments to legislation, including digital legislation, to address the competitiveness challenge of the Union. 4 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) 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-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.	EE_Comments (Drafting suggestions): (2) Union digital legislation sets high standard**s** in the Union and can be a powerful source of competitive advantage for businesses that abide by the**se** rules, showing a world-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**s** of consumer protection and safety, and ~~**for the protection**~~ **protecting** fundamental rights, not least privacy and data protection. EE_Comments (Comments): Just some small grammatical fixes with articles, parallel structure, and wording.
(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	

PUBLIC

Commission proposal	Drafting suggestions and Comments
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[5] and (EU) 2023/2854[6] 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 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) 6 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	

PUBLIC

Commission proposal	Drafting suggestions and Comments
of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act)	
(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 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[7] 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[8]. 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,	

PUBLIC

Commission proposal	Drafting suggestions and Comments
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[9] on guidance on the processing of personal data in the context of scientific research. 7 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). 8 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). 9 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).	
(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	

PUBLIC

Commission proposal	Drafting suggestions and Comments
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 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.	

PUBLIC

Commission proposal	Drafting suggestions and Comments
(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 [10], 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. 10 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).	
(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 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.	

PUBLIC

Commission proposal	Drafting suggestions and Comments
(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	

PUBLIC

Commission proposal	Drafting suggestions and Comments
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	

PUBLIC

Commission proposal	Drafting suggestions and Comments
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[11] 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. 11 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).	
(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	

PUBLIC

Commission proposal	Drafting suggestions and Comments
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 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.	

PUBLIC

Commission proposal	Drafting suggestions and Comments
(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[12] 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 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,	

PUBLIC

Commission proposal	Drafting suggestions and Comments
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. 12 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).	
(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.	

PUBLIC

Commission proposal	Drafting suggestions and Comments
(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	

PUBLIC

Commission proposal	Drafting suggestions and Comments
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[13] 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[14] 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. 13 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). 14 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).	

PUBLIC

Commission proposal	Drafting suggestions and Comments
(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.	
[…]	
(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.	

PUBLIC

Commission proposal	Drafting suggestions and Comments
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	

PUBLIC

Commission proposal	Drafting suggestions and Comments
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	

PUBLIC

Commission proposal	Drafting suggestions and Comments
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.	

PUBLIC

Commission proposal	Drafting suggestions and Comments
(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[15], 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]. 15 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).	
[…]	
(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.	
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:	

PUBLIC

Commission proposal	Drafting suggestions and Comments
(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);	

PUBLIC

Commission proposal	Drafting suggestions and Comments
(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:	

PUBLIC

Commission proposal	Drafting suggestions and Comments
'(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;	EE_Comments (Drafting suggestions): '(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; EE_Comments (Comments): "use **or** make available" includes also data recipients, i.e. everyone who can use the data but do not have the right or obligation to make it available. As the importance of a "data holder" is in making data available, the definition should concentrate on this aspect – the "right to use" the data is not relevant and can be removed.
(c) the following points (28a) and (28b) are inserted:	

PUBLIC

Commission proposal	Drafting suggestions and Comments
'(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:	

PUBLIC

Commission proposal	Drafting suggestions and Comments
‘(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 :	EE_Comments (Comments): The definition has been changed, but it is not clear what was the purpose. The deleted parts are: (a) services that obtain data from data holders and aggregate, enrich or transform the data for the purpose of adding substantial value to it and license the use of the resulting data to data users, without establishing a commercial relationship between data holders and data users; (c) services that are exclusively used by one data holder in order to enable the use of the data held by that data holder, or that are used by multiple legal persons in a closed group, including supplier or customer relationships or collaborations established by contract, in particular those that have as a main objective to ensure the functionalities of objects and devices connected to the Internet of Things.
(1) do not have as their main purpose the intermediation of copyright-protected content;	EE_Comments (Drafting suggestions): (1) do**es** not have as **its ~~their main~~** purpose **~~the intermediation of~~ to intermediate the content** protected by copyright or related rights. EE_Comments (Comments): This phrasing creates many questions: 1. What exactly qualifies as “main purpose”? 2. How should regulators determine when copyright intermediation becomes the primary activity? 3. Does the exclusion apply if copyright content intermediation is secondary or incidental?

Commission proposal	Drafting suggestions and Comments
	Therefore, we should avoid ambiguous thresholds like "main purpose". We also would like to see more clear phrasing on this matter. Thus, we proposed clearer phrasing that aligns with terminology used in EU copyright law.
(2) are not jointly procured by several legal persons for exclusive use among them;	EE_Comments (Comments): Important to add **(3): are not data sharing services offered by public sector bodies**; This is the part of the current definition as well, and there is no need to take it away. The data intermediation service regulation in this act should focus on the private sector bodies, not public. Otherwise it would create additional unneccessary burdens on MS.
(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;	

PUBLIC

Commission proposal	Drafting suggestions and Comments
(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	EE_Comments (Drafting suggestions): (a) any content whatever its medium (paper or electronic form or as a sound, visual or audiovisual recording); or EE_Comments (Comments): The definition of document excluding digital forms is not thought through as: • it opposes the common definition of document in archiving, information management, the Tromso convention etc • it creates a lot of confusion in parts that have been copy-paste'd from previous acts (f.ex Open Data Directive) and which do not make sense with the new definition (f.ex. a) the requirement to publish HVD **documents** in machine readable formats; b) definition of 'common specification' in the Data Act: ".. a **document**, other than a standard, containing technical solutions providing a means to comply with certain requirements and obligations established under this Regulation". As such all common specifications must be non-digital?)
(b) any part of such content;	

Commission proposal	Drafting suggestions and Comments
(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;	EE_Comments (Comments): What is meant by "documents in a digital form" if document is defined by being "non-digital"?
(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;	

PUBLIC

PUBLIC

Commission proposal	Drafting suggestions and Comments
(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;	EE_Comments (Comments): Both the terms "re-user" and "data recipient" exist in the omnibus. Please consider if both terms are indeed necessary and are not too overlapping.
(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;	

Commission proposal	Drafting suggestions and Comments
(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;	EE_Comments (Comments): If document is defined as "non-digital" then what is it's relevance in regard to the definition of "open format"?
(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	

Commission proposal	Drafting suggestions and Comments
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:	

PUBLIC

PUBLIC

Commission proposal	Drafting suggestions and Comments
'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	EE_Comments (Comments): Estonia supports amending the EU Data Act to allow public authorities to request data from the private sector in situations of public emergency, but stresses that such powers must be exercised with full respect for fundamental rights and on the basis of clear and harmonised criteria across Member States. Estonia's key concerns are the **primary use of non-personal data**, the **systematic consideration of privacy-enhancing technologies (including pseudonymisation) when personal data is necessary**, and avoiding divergent national interpretations of what constitutes 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	

PUBLIC

Commission proposal	Drafting suggestions and Comments
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.	EE_Comments (Drafting suggestions): 2. Where the data requested are necessary to respond to a public emergency, and the requesting body ~~**pursuant**~~ **referred** to **in** 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 **or with the use of equivalent privacy- enhancing technologies,** subject to appropriate technical and organisational measures to ensure their protection. EE_Comments (Comments): Requests should primarily concern non-personal data, and where personal data is necessary, privacy- enhancing technologies, including pseudonymisation, should be used. This should always be the case.
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.’;	EE_Comments (Drafting suggestions): Where the data requested are necessary to mitigate or support the recovery from a public emergency, a requesting body ~~**pursuant**~~ **referred** to **in** 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:	

Commission proposal	Drafting suggestions and Comments
'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:	

PUBLIC

Commission proposal	Drafting suggestions and Comments
'(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	

PUBLIC

Commission proposal	Drafting suggestions and Comments
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.	

PUBLIC

PUBLIC

Commission proposal	Drafting suggestions and Comments
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;	

Commission proposal	Drafting suggestions and Comments
(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	

PUBLIC

Commission proposal	Drafting suggestions and Comments
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.	

PUBLIC

Commission proposal	Drafting suggestions and Comments
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:	

PUBLIC

Commission proposal	Drafting suggestions and Comments
'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

Commission proposal	Drafting suggestions and Comments
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).	

PUBLIC

PUBLIC

Commission proposal	Drafting suggestions and Comments
(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;	EE_Comments (Drafting suggestions): ~~They~~ **it** do**es** not use the data for which it provides data intermediation services for purposes other **than to make them available to data users ~~put them at the disposal of data users~~**; EE_Comments (Comments): The amendments ensure grammatical consistency by aligning the subject and verb in the singular form (“it”) when referring to the data intermediation service provider. In addition, the wording “make them available to data users” is used instead of “put them at the disposal of” to reflect clearer and more commonly used terminology in EU legal drafting.
(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;	

Commission proposal	Drafting suggestions and Comments
(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;	EE_Comments (Drafting suggestions): (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, **the use of privacy-enhancing technologies, including** anonymisation and pseudonymisation, such tools and services shall be used only at the explicit request or approval of the data holder or data subject; EE_Comments (Comments): The provision should refer more broadly to privacy-enhancing technologies rather than limiting the wording to anonymisation and pseudonymisation. Privacy-enhancing technologies cover a wider range of technical measures that enable data sharing while ensuring a high level of protection of personal data and privacy. A broader reference ensures a more technologically neutral approach and future-proofs the provision, allowing the use of innovative privacy-preserving solutions beyond anonymisation and pseudonymisation.
(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;	

Commission proposal	Drafting suggestions and Comments
(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.	

PUBLIC

Commission proposal	Drafting suggestions and Comments
Article 32e	
Registration	EE_Comments (Drafting suggestions): *Registration in public Union register* EE_Comments (Comments): The title must be precise to ensure clear understanding.
(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.	EE_Comments (Comments): Estonia supports the proposal to remove the notification requirement for data intermediation services.
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.	

PUBLIC

Commission proposal	Drafting suggestions and Comments
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.	EE_Comments (Comments): If registration is made in the Union's registry, shouldn't a unified form be used? Since it is not a economic notification or authorisation scheme, it should not be the CA's obligation.
(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	EE_Comments (Comments):

PUBLIC

Commission proposal	Drafting suggestions and Comments
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.	Clarification is needed on what is meant by "registration in accordance with national law." In this context, registration could be understood as registration in the Union registry, which is established under the new Data Act, which is directly applicable. The Digiomnibus proposal removed the notification requirements for data intermediation services.
(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	EE_Comments (Comments):

Commission proposal	Drafting suggestions and Comments
data holder allows the processing. The recognised data altruism organisation shall not use misleading marketing practices to solicit the provision of data.	Please clarify what is meant by the general interest in this context. Is this connected to a legitimate interest?
(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.	

PUBLIC

Commission proposal	Drafting suggestions and Comments
(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	

PUBLIC

Commission proposal	Drafting suggestions and Comments
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.'	

PUBLIC

PUBLIC

Commission proposal	Drafting suggestions and Comments
Chapter VIIc	
Re-use of data and documents held by public sector bodies	EE_Comments (Comments): The digital omnibus proposed by the European Commission has not yet sufficiently harmonised the terminology used in the Data Governance Regulation, the Open Data Directive, and the Data Act. The most significant vocabulary inconsistency concerns the definition of the term "document." Under the current Open Data Directive, the concept of a document includes data on any type of medium, which is consistent with the definition used in the Council of Europe Convention on Access to Official Documents. However, the proposed digital package distinguishes between "data" (on digital media) and "documents" (on non-digital media). Despite this change, several provisions in the package that require the description and disclosure of public information continue to use the earlier wording "data or documents," as in the Open Data Directive and the Data Governance Regulation. As a result, under the new definition, the Data Act would effectively require the description and disclosure of all paper documents, either under open data or restricted data regimes. This requirement is considered unreasonable, unnecessary, and disproportionate. Please see also markings in specific provisions on the matter.
SECTION 1	
GENERAL PROVISIONS	
Article 32i	
Subject matter and scope	EE_Comments

Commission proposal	Drafting suggestions and Comments
	(Comments): Estonia considers it essential that the revised EU Data Act **clearly defines when personal data may be treated as open data.** Disclosure of personal data as open data should be allowed **only with the data subject's consent or where such disclosure is explicitly provided for by law**. The current uncertainty around the relationship between open data and personal data undermines legal clarity and trust, and that making personal data publicly available constitutes a serious interference with privacy, requiring a clear legal basis and a prior assessment of necessity and proportionality.
(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.	

Commission proposal	Drafting suggestions and Comments
(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;	EE_Comments (Comments): Clarification is needed on what is meant by “general interest”.
(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:	EE_Comments (Comments): Why have the provisions been reduced compared to the Open Data Directive in circumstances to which the provisions do not apply?

PUBLIC

Commission proposal	Drafting suggestions and Comments
(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);	

PUBLIC

Commission proposal	Drafting suggestions and Comments
(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.	EE_Comments (Comments): Note that “document” has been defined above as “non-digital”.
(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).	

PUBLIC

Commission proposal	Drafting suggestions and Comments
(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	

PUBLIC

Commission proposal	Drafting suggestions and Comments
(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	

PUBLIC

Commission proposal	Drafting suggestions and Comments
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	

PUBLIC

Commission proposal	Drafting suggestions and Comments
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.	

PUBLIC

Commission proposal	Drafting suggestions and Comments
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	

PUBLIC

Commission proposal	Drafting suggestions and Comments
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.	EE_Comments (Comments): Please note that as "document" has been defined as "non-digital", this point requires all responses of requests to be made available as "non-digital" which is not reasonable.
(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	

PUBLIC

Commission proposal	Drafting suggestions and Comments
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	

PUBLIC

Commission proposal	Drafting suggestions and Comments
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	

PUBLIC

Commission proposal	Drafting suggestions and Comments
(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-	

PUBLIC

Commission proposal	Drafting suggestions and Comments
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.	

PUBLIC

Commission proposal	Drafting suggestions and Comments
(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.	EE_Comments (Comments): The current setup of requiring the separate description and publication of open data (Article 32s) and certain categories of protected data (Article 32aa) is inefficient. At least these two articles should be joined into a single generic article which outlines the obligation of PSI holders to: • describe their datasets • publish these dataset descriptions on National Single Information Points • (for NSIPs to publish these descriptions onto the EU data portal)

PUBLIC

Commission proposal	Drafting suggestions and Comments
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	

PUBLIC

Commission proposal	Drafting suggestions and Comments
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.	

PUBLIC

Commission proposal	Drafting suggestions and Comments
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	

PUBLIC

Commission proposal	Drafting suggestions and Comments
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	

PUBLIC

Commission proposal	Drafting suggestions and Comments
(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;	

PUBLIC

Commission proposal	Drafting suggestions and Comments
(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.	

PUBLIC

Commission proposal	Drafting suggestions and Comments
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	

PUBLIC

Commission proposal	Drafting suggestions and Comments
(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.	

PUBLIC

Commission proposal	Drafting suggestions and Comments
(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.	

PUBLIC

Commission proposal	Drafting suggestions and Comments
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];	

PUBLIC

Commission proposal	Drafting suggestions and Comments
(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.	

PUBLIC

PUBLIC

Commission proposal	Drafting suggestions and Comments
(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	

Commission proposal	Drafting suggestions and Comments
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	EE_Comments (Comments): The current setup of requiring the separate description and publication of open data (Article 32s) and certain categories of protected data (Article 32aa) is inefficient. At least these two articles should be joined into a single generic article which outlines the obligation of PSI holders to: • describe their datasets • publish these dataset descriptions on National Single Information Points • (for NSIPs to publish these descriptions onto the EU data portal)
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.	

PUBLIC

Commission proposal	Drafting suggestions and Comments
(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	

PUBLIC

Commission proposal	Drafting suggestions and Comments
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.	

PUBLIC

Commission proposal	Drafting suggestions and Comments
(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	

PUBLIC

Commission proposal	Drafting suggestions and Comments
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:	

PUBLIC

Commission proposal	Drafting suggestions and Comments
(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:	

PUBLIC

Commission proposal	Drafting suggestions and Comments
'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.	

PUBLIC

Commission proposal	Drafting suggestions and Comments
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	

PUBLIC

Commission proposal	Drafting suggestions and Comments
In the table in Annex II to Regulation (EU) 2018/1724, the entry 'Starting, running and closing a business' is replaced by the following:	
[Table]	
[…]	
Article 6	
Amendments to Directive (EU) 2022/2555	EE_Comments (Comments): Since we can't add new lines and cells (see the feedback's guidelines at the top), we note the following: - We should also aim to harmonize the reporting timelines – especially since with this Omnibus, it is exepected that personal data breach notifications timeline in GDPR article 33 shall be extended up to 96h. The introduction of SEP and harmonized templates are one part of the equation in the matter of notifying incidents, personal data data breaches and other similar cases to the relevant competent authorities. There is the need to harmonize also the timelines of reporting. - This shouldn't be an issue, from the technical side – all of the EU acts, that are expected to use SEP, shall have a reference to relevant article of NIS2. Meaning that there is already a need to make amendments to the same EU acts. In doing so, the most tricky part is: (a) reaching a common ground whether there shall be multi-step notification (as it is foreseen with Article 23 (4) of the NIS2: early warning and incident notification) or one notification (as it is foreseen in Article 33 of the GDPR); (b) reaching a common ground on the timeline or timelines (depending on step a) across several EU acts. - If the timeline harmonization is not done, then the proposed SEP shall help with doing the notification to relevant authorities, but it also means that the entity is expected to use the SEP several times for notifying one incident.

PUBLIC

Commission proposal	Drafting suggestions and Comments
	- Since the Digital Omnibus's aim is to simplify doing the reporting of incidents, then it is essential that this matter is also solved an taken care of.
Directive (EU) 2022/2555 is amended as follows:	
1. The following Article 23a is added:	
'Article 23a	
Single-entry point for incident reporting	EE_Comments (Comments): Regarding SEP – the key question is which development model would be the most rational, cost-effective, and sustainable in the long term for the European Union as a whole. Estonia proposes that ENISA develop the central core solution of the SEP and release it under the MIT open-source licence. This approach would enable a substantial part of the software to be developed collectively, thereby avoiding a situation in which all 27 Member States effectively duplicate the same work independently. If ENISA were to limit its role to defining requirements and leave implementation entirely to the Member States, the practical outcome would be 27 separate procurement procedures, 27 distinct architectural designs, 27 security and compliance assessment cycles, and extensive duplication of analysis and development efforts. Each Member State would need to launch its own procurement process and reassess which technical solution to adopt and how to structure it, despite the existence of common technical standards. In practice, the same regulatory logic would give rise to 27 different technical implementations. Each country would also conduct its own security audits, testing, and certification

PUBLIC

Commission proposal	Drafting suggestions and Comments
	processes, even though the underlying regulatory and technical requirements are identical across the Union. Beyond direct financial efficiencies, a centrally developed core solution would significantly reduce administrative burden, accelerate implementation timelines, and limit architectural fragmentation across the Union. It would ensure interoperability by design and from the outset, while also facilitating cross-border cooperation and seamless data exchange. The MIT licence provides an appropriate legal and strategic framework for this model, as it guarantees maximum flexibility for Member States. A country may adopt the solution as-is, without additional development. Member States with similar legal frameworks and operational needs may collaborate to develop shared enhancements or modules, pooling expertise and sharing costs. At the same time, each Member State retains full freedom to adapt, extend, integrate, or further develop the solution, including the option to build additional modules or even a fully independent system. The MIT licence does not constrain sovereignty; rather, it establishes a shared technical foundation upon which national specificities can be built. In Estonia's assessment, when the regulatory framework is harmonised at EU level, it is both logical and prudent to consider joint development of the underlying technical base. Such an approach does not diminish national autonomy. Instead, it prevents unnecessary duplication of public expenditure and contributes to strengthening the European Union's collective digital resilience. Estonia therefore considers a centrally developed SEP core solution under the MIT licence to be a balanced, economically sound, and strategically justified model. One that effectively combines EU-level efficiency with Member State flexibility and sovereignty.

Commission proposal	Drafting suggestions and Comments
(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.	EE_Comments (Comments): We agree that ENISA shall develop and maintain SEP, but we propose that housing of SEP should be with eu-LISA – at its headquarter's infrastructure. eu-LISA already has substantial knowledge on these matters and this wouldn't be, from the practical view, a new task for said authority. Due to this proposition, there should be also similar requirements to eu-LISA as they are for ENISA regarding SEP (mainly, see this article's paragraphs 2 and 4).
(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	EE_Comments (Drafting suggestions):

PUBLIC

Commission proposal	Drafting suggestions and Comments
place and, provide technical protocols and tools that allow the entities and authorities to further process the receive information within their systems;	(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**d** information within their systems; EE_Comments (Comments): The end of the sentence refers that those technical arrangements also apply to entities doing the reporting. The same part also gives an impression that technical protocols and tools shall provided to the entities (and authorities) to further process the received information within their systems. Does this mean that in addition to relevant competent authorities that receive the reports/notifications, also the entities that are reporting, can be linked with the SEP (e.g. via an API or something else)?
(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;	EE_Comments (Comments): If our propositon of NIS2 Article 23 (3a) is taken into account (see below), then does this wording also cover said aspect? Or should there be amendments made to point (c)? Or should there be a new point *(ca): common EU taxonomies are taken into account*;? With point (ca), we did not reference only to the NIS2 Article 23 (3a), since other EU acts may also foresee taxonomies. Hence its wording is more neutral and flexible in this matter.
(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;	EE_Comments (Drafting suggestions): Deletion] EE_Comments (Comments):

Commission proposal	Drafting suggestions and Comments
	To our knowledge, the EBW is not meant to be mandatory for private sector (see Digital Package | Shaping Europe's digital future, section 5, third question "Will companies and public bodies be obliged to use them?" and its answer), but the wording of (d) hints that it is not the case. We are also not in favour of the EBW's as they are proposed in their own proposal for a regulation. Hence, we propose that in this document the reference to EBW is deleted.
(e) entities using the single-entry point can retrieve and supplement information that they have previously submitted via the single-entry point;	EE_Comments (Comments): See the comment on this paragraph's point b.
(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.	EE_Comments (Comments): This requirement is also one aspect on why there is a need to harmonize the notification timelines.
(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.	EE_Comments (Comments): This paragraph is only about those EU acts that are added to SEP via this proposal. But this paragraph does not give a clear understanding on what is the timeline for future EU Acts that need to use SEP in the future. Therefore, this aspect needs to be reviewed in this paragraph and in the next paragraphs also.
(6) The Commission shall, in cooperation with ENISA, assess the proper functioning, reliability, integrity and confidentiality of the single-entry point.	

Commission proposal	Drafting suggestions and Comments
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:	EE_Comments (Comments): In addition to the aforementioned, we propose following amendment to NIS2 Article 23 – a new paragraph 3a: *3a. In order to contribute to the provision of comparable information about incidents, ENISA shall, in cooperation with CSIRTs network and other relevant aurhorities, adopt incident classiciation taxonomy. Said taxonomy is mandatory for CSIRTs.* Explanation: there is a need to have a common ground on what cases are incidents in the meaning of NIS2. This means that there is a need to have a unified taxonomy on this matter and it needs to be mandatory. ENISA has already done such a taxonomy (see https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy), hence it is not a new task for ENISA. Since the last taxonomy resulted from collaboration initiatives such as the annual ENISA/EC3 Workshop which involved CSIRTs, LEAs, ENISA, and EC3, then the new paragraph includes "and other relevant authorities". Nevertheless, it is

PUBLIC

Commission proposal	Drafting suggestions and Comments
	essential, that this task is done with cooperation with CSIRTs network since the taxonomy is expected to be mandatory to CSIRTs. With this proposition, there might not be a need to amend Article 23 (9) second sentence of the NIS2 (*In order to contribute to the provision of comparable information, ENISA may adopt technical guidance on the parameters of the information to be included in the summary report.),* but this should be clarified during the process of discussions. With regarind Article 23 – see also the comment on harmonizing timelines for notifications at proposed Article 23a of the NIS2.
(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,	

Commission proposal	Drafting suggestions and Comments
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:	

PUBLIC

Commission proposal	Drafting suggestions and Comments
'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	EE_Comments (Comments): We propose an amendment to DORA Article 30 – a new paragraph 4a: *4a. Full contract may be prepared as part of a document provided by another legal instrument. ICT third-party service provider can prove compliance with requirements in paragraphs (1) and (2) with cybersecurity risk management measures that are documented due to requirements set in Article 21 of Directive (EU) 2022/2555 if said article applies to ICT third-party service provider.* Explanation: As a general rule, entities falling under the DORA are excempted from following NIS2, especially its risk management measures (Article 21 of NIS2). Then again, in practice there are ICT third-party service providers who also need to follow NIS2 requirements and DORA requirements. In DORA those entities are named as "ICT third-party service providers" and in NIS2 they are "managed service providers" and/or "managed security service providers". When ICT third-party service providers provide services to financial entities (see DORA Article 2 (1) (a)-(t)), then those ICT third-party service providers are part of financial entity's ecosystem and/or part of the services that the financial entity provides. Therefore there is an assumption that ICT third-party service providers need to follow requirements of DORA – then again, they also need to follow NIS2. DORA article 28 (5) first sentece sets how the

PUBLIC

Commission proposal	Drafting suggestions and Comments
	financial entity and ICT third-party service provider make the contractual agreement. Said agreement's content is regulated in DORA Article 30. At the same time, the same entity (in terms of DORA "ICT third-party service provider" and in terms of NIS2 the "managed service provider" and "managed security service provider") needs to follow the cybersecurity risk management measrues foreseen in Article 21 of NIS2, that are further specified in Commission Implementing Regulation (EU) 2024/2690. The same entities are also subject to supervision of the competent authorities of NIS2. In practice, DORA Article 30 has not made things easier to entities that need to follow NIS2 requirements. Said DORA Article has made it so that each financial entity requires from the ICT third-party service provider (that is also subject to NIS2) to duplicate and restructure their cybersecurity risk management measures that are in place, to the needs of each financial entity. This menas that there is the need to duplicate the same work for different financial entites – and that work does not enhance the level of cybersecurity, but it raises the administrative burden and costs of the ICT third-party service provider. Currently, the interplay between NIS2 and DORA means that the same ICT service provider needs to do tailor-made documentations for each financial entity and/or for competent authorities in NIS2 and DORA.
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:	

Commission proposal	Drafting suggestions and Comments
'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	

PUBLIC

PUBLIC

Commission proposal	Drafting suggestions and Comments
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	

PUBLIC

Commission proposal	Drafting suggestions and Comments
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.	EE_Comments (Comments): This timeline (18 and/or 24 months) needs to be reviewed at a later stage, when there is a better understanding on what SEP is and what is expected from Member States due to that. This is due to the fact that COM proposal only foresees provisions regarding SEP mainly to ENISA, but it does not address what needs to be done at the Member State level with the national part of SEP.
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*	
<u>Annex II</u>	

Commission proposal	Drafting suggestions and Comments
List of thematic categories of high-value datasets, as referred to in Article 32ab(1) of Regulation (EU) 2023/2854	EE_Comments (Comments): Estonia considers that datasets which could endanger internal or external security must not be made public and should not be included in the list of high- value datasets. For example, energy infrastructure data must be explicitly excluded from the list of high- value datasets, as its public disclosure would pose unacceptable risks to internal and external security. When establishing new categories of high- value datasets, the impact on smaller Member States must be carefully assessed. The decisions must be based on clear impact assessments that consider security risks, fundamental rights, and the competitiveness of businesses, alongside social and economic benefits.
1. Geospatial	
2. Earth observation and environment	
3. Meteorological	
4. Statistics	
5. Companies and company ownership	
6. Mobility	

PUBLIC