Council of the European Union
General Secretariat

Interinstitutional files:
2025/0360 (COD)

Brussels, 11 March 2026

WK 3735/2026 INIT

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)

Following the meeting of the AGS on 13 February 2026 on Digital Omnibus, delegations will find comments as received from 14 Member States:

BE, DE, DK, EL, ES, FI, FR, IT, LU, LV, NL, PL, RO, SE, SI and SK .

Omnibus VII (Digital omnibus) - Cyber and data issues - Consultation on Commission proposal Deadline: ***27 February 2026***
From: BE, DE, DK, EL, ES, FI, FR, IT, LU, LV, NL, PL, RO, SE, SI, SK **Updated: 10/03/2026 14:58**

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	DE (Comments): DE must submit a scrutiny reservation. Our review and assessment has not been concluded. All drafting suggestions and comments are preliminary in nature. In collaboration with France, Italy and the Netherlands, we have developed this draft and share a unified position on the Commission's proposal concerning the single-entry point for incident reporting. The minor differences in our drafts are a result of our internal consoldiation processes. None of these minor differences should be regarded as non-negotiable. We remain open to discussing this further and aligning our drafts. FI (Comments):

Commission proposal	Drafting suggestions and Comments
	Finland is in progress of analysing the proposals and forming our position. Below are our preliminary comments. We thus reserve the possibility to further specify our comments and suggestions in due course. FI: We kindly ask the Presidency to take into account the joint opinion of the EDPB and EDPS from 11 February 2026. FI: We kindly ask the Presidency to take into account the DK proposal for simplification of Chapter VI of the Data Act regarding cloud switching. FR (Comments): On the Single-entry point (cyber part), in collaboration with Germany, Italy and the Netherlands, we have developed this draft and share a unified position on the Commission's proposal concerning the single-entry point for incident reporting. The minor differences in our drafts are a result of our internal consoldiation processes. None of these minor differences should be regarded as non-negotiable.We remain open to discussing this further and aligning our drafts. Moreover, this draft proposal aligns with the published non-paper supported by the Netherlands, Italy, Germany, Spain, Sweden and France regarding the Single-entry point. This non-paper underlines that a single-entry point is an unadequate solution to adress the issue of heterogeneity in the incident reporting framework at EU-level and suggest to adopt another approach regarding to simplification based on developping an information point for entities and harmonising the incident notification framework. As we believe that this second approach should be adopted in the digital omnibus, this draft proposes modifications in line with it. IT (Comments):

Commission proposal	Drafting suggestions and Comments
	In collaboration with France, Germany and the Netherlands, we have developed this draft and share a unified position on the Commission's proposal concerning the single-entry point for incident reporting. The minor differences in our drafts are a result of our internal consolidation processes. None of these minor differences should be regarded as non-negotiable. LU (Drafting suggestions): General Comments LU welcomes the proposal to establish a European Single Entry Point (SEP) for incident reporting. Luxembourg supports the objective of simplifying and harmonising reporting obligations across the Union, under the condition that the SEP can be fully integrated with existing national tools and that no changes will occur in the way incident notifications are submitted, treated and followed up by national competent authorities. Luxembourg recalls that the **ILR** (Institut Luxembourgeois de Régulation, competent authority for NIS2 sectors – except the financial and banking sectors, NCCS competent authority, and AI-market surveillance authority NIS 2 national authority) and the **CSSF** (Commission de Surveillance du Secteur Financier, NIS 2 authority for the financial sector and DORA authority for most financial entities) — have already developed dedicated reporting tools, namely: SERIMA (Security Risk Management), an open source platform, capable of hosting multi-sectors, multi-regulators and multi-regulations incident notifications. which once NIS2 has been transposed, will be used for for incident notifications under NIS2, CER and GDPR. Currently SERIMA is used for NIS1 and EECC notifications. and

Commission proposal	Drafting suggestions and Comments
	the CSSF's ICT incident reporting tool for the financial sector. It is therefore essential that the SEP architecture allows seamless integration with these national systems and preserves the operational responsibilities of national authorities. **ILR General comments** For the SEP to be beneficial for operators and to foster collaboration among Member States, we believe that clarifications and specifications are still needed, both legally and practically. - The SEP is supposed to work for NIS2, GDPR, CER, e-IDAS, DORA, NCCS and aviation. However, incident notification is also part of the AI-ACT, which is currently not foreseen to be integrated in the SEP, we suggest also including the AI-ACT to guarantee EU-wide harmonisaiton. - The regulation foresees that ENISA is responsible for the security of the platform. We are not sure that this is completely realistic and does not seem to follow a risk-based approach due to the interconnection and data transfer towards national platforms. Therefore, we suggest further detailing the mode of operation of the platform, carrying out risk assessment and define roles and responsibilities depending on the workflow and interconnectivity with national solutions. - Having experience with SERIMA, we would like to highlight to ENISA the importance of foreseeing a workflow and risk assessment for situations in which the wrong authority has been notified (whether due to wrongful information of an entity or due to a misconfiguration).

Commission proposal	Drafting suggestions and Comments
	CSSF general comments CSSF welcomes the the proposal for a European Single Entry Point (SEP) for incident reporting, the condition of its understanding that the SEP can be fully integrated with national tools and that there will be no changes to the way incident notifications are submitted, processed, and followed up for all supervised entities. In fact, the CSSF has had in place, for almost two years, a tool through which supervised entities notify ICT major incident reporting (as well as significant cyber threats). The CSSF understanding is that the following aspects can be ensured (non-exhaustive list): - The entry point will be different in the background, but financial entities will always have the possibility to connect to the CSSF tool and be redirected to the presentation layer of the SEP tool, before being redirected back. - The follow-up of the incident will continue to be carried out by the CSSF - ENISA will not access data from entities, except for the identification data and will not have access to Luxembourg entities - The CSSF will be able to continue to maintain the local data base, back-up etc. Please also note that what is still not clear, if the data remains in Luxembourg is the following: - How will the ESAs have access to the incident notifications if there is only a local database in Luxembourg? Will it still be the CSSF that automatically sent the data (as now)? Does ENISA plan to retrieve the data from Luxembourg? If so, ENISA will always have a database also containing Luxembourg data.

Commission proposal	Drafting suggestions and Comments
	- How will other countries have access to the incident notifications where the cross-border criterion is selected? Will ENISA retrieve the Luxembourg data? How? General comments on the Data Act and discussion note discussed in AGS on 13 february 2026 **Question 3:** Do Member States support the consolidation of the DGA, the ODD and the key principle of the FFDR into the DA? Luxembourg supports the consolidation of these texts in one single regulation. A clear and concise legal framework as well as a more streamlined, coherent and efficient governance should be of paramount importance to **facilitate compliance and reduce legal uncertainty**. However, the consolidation of the aforementioned legal texts may risk, due to the changes to the rules and principles of the DGA, changing the rationale of those regimes. Although seeking legal certainty, those changes therefore risk undermining the rules established over the years. Anyway, it should be ensured that the objective of administrative simplification does not entail the addition of new concepts or conditions compared to Chapter II DGA, which could have the opposite effect wished for. **Question 4:** Do Member States support the merging of rules on the re-use of public sector information under Chapter II DGA and the ODD and turning the ODD into a Regulation?

Commission proposal	Drafting suggestions and Comments
	One solution to achieve the objectives of simplification and clarification could be to merge the rules of the ODD with those of Chapter II of the DGA, including them in a chapiter *IIbis* within the DGA. This consolidation could aim to harmonise, clarify, and simplify rules for more easily accessible and reusable data, without affecting the principles and requirements of the DGA and without undermining its current national implementation. Question 8: Luxembourg would like to stress that this question is still under discussion at national level. Under the DGA the definition of a 'data intermediation service' is altered and the requirement for a separate legal person are removed. Instead, an obligation to keep value-added services functionally separate is introduced, except for micro or small entities. We recommend including clear criteria for functional separation. The fulfilment of such criteria should be verifiable for the supervisory/competent authority and might include requirements to have technical and organisational segregation of data as well as separate management, financing and staff. Further, such functional separation within the same legal person should be required on the one hand between the provision of the data intermediation service, and on the other hand all other activities of the data intermediation services provider (not only with regard to value-added services) in order to enhance neutrality and legal clarity. Concerning the alignment of the different access regimes in sections 2 and 3 of new Chapter VIIc of the Data Act, as well as of the DGA and the Open Data Directive: if the intend is to align the different access regimes, we recommend to not add unnecessary rules, principles and layers of exceptions applicable in various situations. The provisions currently foreseen by Chapter VII of the proposal and the different definitions (e.g.

Commission proposal	Drafting suggestions and Comments
	proposed article 2 (54)) are very complex, have different scopes and profit from exemptions or exceptions, the case may be. This could adversely affect legal certainty and render impossible the correct application of the proposed provisions in practice. Therefore it is suggested to not touch the balance established by Chapter II of the DGA and to align of other provisions, in particular of the Open Data Directive, with this framework. This would allow to streamline said frameworks without adding further complexity or administrative burden for undertakings and public sector administrations alike. LV (Comments): LV: I Overall consolidation approach The consolidation of the Data Governance Act, the Open Data Directive and Regulation 2018/1807 into Regulation (EU) 2023/2854 enhances legal coherence. However, merging heterogeneous regimes (B2B data access, B2G access, data intermediation, public sector information reuse and free flow of non-personal data) into a single instrument significantly increases structural and interpretative complexity. Clear guidance will be necessary to avoid divergent national implementation. II Interaction with Statistical Confidentiality 1. Chapter VIIc (Section 3) introduces mechanisms for reuse of protected data, including statistical confidentiality. It is essential to ensure that: • Nothing in the Regulation undermines statistical confidentiality as protected under Regulation (EC) No 223/2009;

Commission proposal	Drafting suggestions and Comments
	• Secure processing environments remain under full control of the competent statistical authority. 2. Interaction with High-Value Dataset Mechanism The relationship between high-value datasets (originating from Directive 2019/1024) and protected data regimes (originating from Regulation 2022/868) requires careful clarification to ensure that datasets subject to statistical confidentiality are not indirectly subjected to open access obligations. 3. Advanced anonymisation and disclosure control requirements Although anonymisation and disclosure control existed under Regulation 2022/868, the broader integration into a harmonised Data Act framework may increase demand for complex access scenarios (e.g. remote processing, third-country transfer assessments). For statistical authorities, anonymisation is not a one-time technical operation but a continuous risk-based process involving: • Statistical disclosure control methodologies; • Re-identification risk assessment; • Monitoring of cumulative disclosure across datasets; • Supervision of outputs from secure processing environments. • These methodological requirements are intrinsic to the statistical system under Regulation (EC) No 223/2009 and must remain fully safeguarded. Proposal for amandment: Therfore a recital explicitly safeguarding statistical confidentiality would enhance legal clarity (similarly to recital 3 in REGULATION (EU) 2022/868.)
2025/0360 (COD)	
Proposal for a	

Commission proposal	Drafting suggestions and Comments
REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL	LU (Drafting suggestions): Preliminary written suggestions are set out below under Article 6 — Amendments to Directive (EU) 2022/2555
amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus)	
THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,	
Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 and 114 thereof,	
Having regard to the proposal from the European Commission,	
After transmission of the draft legislative act to the national parliaments,	
Having regard to the opinion of the European Economic and Social Committee[1], 1 OJ C […], […], p. […].	
Having regard to the opinion of the European Central Bank[2], 2 OJ C […], […], p. […].	

Commission proposal	Drafting suggestions and Comments
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 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.	

Commission proposal	Drafting suggestions and Comments
(3) Union digital legislation has evolved incrementally over the past years, in response to the rapidly growing footprint of digital technologies in the Union's economy and societal dynamic, and in view of addressing emerging challenges and promoting business opportunities in the EU. Notwithstanding the Commission's commitment to a systematic 'stress test' of the digital rules, along with other Union rules, which might lead to further regulatory adjustments notably following the forthcoming Digital Fitness Check, as well as other targeted evaluations of digital rules, immediate regulatory changes are necessary. Consequently, this Regulation proposes a first set of amendments to the digital legislative framework, aimed at providing immediate regulatory clarifications that stimulate innovation in the Union market, and that cut administrative compliance costs in particular for businesses, while also streamlining supervisory and administrative costs for supervisory authorities and advisory bodies. The amendments also seek to provide clarity to individuals.	
(4) Given the foundational role of data in driving value-creation in the digital economy, and pursuant to the objectives of the Communication for a European Data Union Strategy, the amendments presented in this Regulation to the legislative framework regarding data seek to build a coherent and cohesive regulatory framework for the availability and use of data, streamlining and consolidating the data regulatory framework into only two legal acts, namely Regulations (EU) 2016/679[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.	IT (Comments): To reduce risks creating **regulatory blind spots** (reducing five legal acts into two) the consolidation of multiple data-related legal acts must ensure **continuity of sector-specific oversight mechanisms**.

Commission proposal	Drafting suggestions and Comments
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 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.	IT (Drafting suggestions): **Adding at the end:** In order to ensure effective implementation, Member States shall be continuously and structurally involved in the design, development and maintenance of the Single Entry Point (SEP), through a formal joint governance mechanism. The SEP shall interoperate with national reporting systems without replacing them, and its technical architecture shall rely on open standards and, where feasible, open source components to ensure auditability, verifiability and security. Clear rules on data access, classification and confidentiality shall guarantee full national control over sensitive information. The transitional period shall be risk based and flexible, including a voluntary pilot phase and possible extensions where security audits or interoperability tests identify residual risks . In additiona **periodic technical and procedural audits** of interoperability between national systems and the Single Entry Point (SEP) should be foreseen. IT (Comments):

Commission proposal	Drafting suggestions and Comments
	Ensures structured Member State involvement, preserves national autonomy in incident reporting, and aligns the SEP with open, auditable and secure technical principles. Guarantees operational sovereignty of Member States and prevents unintended centralisation
(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, 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	IT (Drafting suggestions): Regulation (EU) 2022/868 of the European Parliament and of the Council7 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. **Such consolidation shall not weaken existing safeguards, legal certainty or fundamental rights protections. The principle of free flow of non personal data shall remain clearly guaranteed as a horizontal principle within the Data Act**. 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 Council8. 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.

Commission proposal	Drafting suggestions and Comments
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).	With respect to data altruism, certain rules of Regulation (EU) 2022/868, notably the obligation on Member States to have national policies on data altruism in place, the establishment of a 'rulebook' and developing a European data altruism consent form appear unnecessary regulation, also in light of on-going work by the European Data Protection Board referred to in Article 68 of Regulation (EU) 2016/679 of the European Parliament and of the Council9 on guidance on the processing of personal data in the context of scientific research. IT (Comments): Preserves the core guarantees of DGA, ODD and FFDR while supporting consolidation. Prevents regulatory overreach and maintains proportionality: it should be explicitly clarified that the consolidated definition of **data intermediation service providers must not unintentionally cover infrastructure level services** (such as cloud compute, storage, or database-as-a-service offerings). This clarification is necessary to avoid imposing disproportionate obligations on actors that are not engaged in economic intermediation between data holders and data users.
(8) While the importance of data intermediation services is recognised in the context of many initiatives supporting data sharing and collaboration, the rules of Regulation (EU) 2022/868 on data intermediation service providers should be clarified. In particular, the definition of such providers should be made more precise. It should eliminate elements that served merely as illustrative examples, rather than exceptions. Moreover, it should address loopholes resulting from ambiguous formulations, notably as regards the notion of 'closed group'. Services should not be eligible to register as data intermediation services where they are exclusively used by a closed group of companies and where any extension of that group of companies can only be decided by that group and not the service provider. More importantly, making	

Commission proposal	Drafting suggestions and Comments
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.	

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.	FR (Drafting suggestions): 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 a request to access to the data** ~~to disclose trade secrets~~ if they demonstrate a high risk of unlawful acquisition, use, or disclosure to entities subject to regimes with inadequate protection **of trade secrets**, 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

Commission proposal	Drafting suggestions and Comments
	possibility that trade secrets could be acquired, used, or disclosed in violation of Union law, threatening the integrity and confidentiality of trade secrets. FR (Comments): France fully supports the necessity to strenghthen the preservation of trade secrets, which have a strategic value, especially for industry and in B2B relations. We kindly remind the provisions of article 8 in chapter III of Regulation (EU) 2023/2854 , and especially 8.6, which states "*unless otherwise provided for in Union Law; including Article 4(6) and Article 5(9) of this Régulation or by national legislation adopted in accotdance with Union Law, an obligation to make data available to data recipient shall not oblige the disclosure of trade secrets*". In coherence with the strenghthening objectives of the Data Act, France considers that the refusal process should not create supplementary administrative or technical burden for trade secret holders. Please see our propositions for Data Act articles 4 and 5. IT (Drafting suggestions): This strengthening should include clearer criteria for identifying third countries with non equivalent protection, allowing data holders to refuse access in high risk situations, supported by proportionate and case by case procedural guarantees. IT (Comments):

Commission proposal	Drafting suggestions and Comments
	Aligns with the need for stronger but proportionate protection of trade secrets.
(12) The activation of the refusal mechanism should remain voluntary, and the demonstration done only upon its activation. Data holders should not be required to conduct a full-scale analysis or demonstration of the level of trade secret protection in third countries or by a third country entity as a precondition to be able to substantiate their refusal to sharing data or to disclose trade secrets. In their demonstration, data holders may take into consideration various factors, such as insufficient or inadequate legal standards, poor or arbitrary enforcement, historical infringements, foreign disclosure obligations conflicting with Union law, limited legal recourse or remedies for Union entities, the strategic misuse of procedural tactics to undermine competitors, or undue political influence. Given the diverse range of entities, third countries, and data sharing scenarios involved, data holders should focus their assessment and demonstration on pertinent risks and act accordingly, including by setting appropriate safeguards or activating the refusal mechanism. Refusals should be clear, proportionate, and tailored to the specific circumstances of each case, rather than being applied systematically or in a generalized manner across an entire third country.	FR (Drafting suggestions): (12) The activation of the refusal mechanism should remain voluntary, and the demonstration done only upon its activation. **In line with the principle that trade secrets shall be preserved and should not, by design, be disclosed,** 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~~ **may** 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.~~ FR (Comments): France fully supports the necessity to strenghthen the preservation of trade secrets, which have a strategic value, especially for industry and in B2B relations.

Commission proposal	Drafting suggestions and Comments
	In coherence with the strenghthening objectives of the Data Act, France considers that the refusal process should not create supplementary administrative or technical burden for trade secret holders. In coherence with the spirit of recital (12), we propose to replace "should" by "may"and to delete the last sentence which creates an administrative and technical burden which is not compatible with day-to-day data sharing practices, especially in B2B relations. Please also see our propositions for Data Act articles 4 and 5. IT (Comments): The competent authorities should develop **non-binding but harmonised EU-wide guidance** listing key indicators for assessing third-country risk
(13) An insufficient protection of trade secrets and the challenges in enforcing them in third countries may cause irreparable harm to European businesses. The objective is therefore to strengthen the safeguards for trade secrets by preventing their leakage to natural or legal persons that are established in or subject to jurisdictions posing such risks. This includes Union-based entities controlled by third country entities, who may be acting in bad faith or as fronts for third country entities. Additionally, the objective is to avert direct exposure to third country entities operating within the Union, that are subject to such jurisdictions. Being subject to a third country jurisdiction means the natural or legal person is legally governed, controlled or otherwise bound by the laws or regulatory authority of a third country. Subsidiaries or affiliates of third country parent companies may exploit these jurisdictions to evade or circumvent Union laws. Direct or indirect control refers to the ability to exercise decisive or dominant influence over another entity's management or strategic decisions, whether through ownership of capital or voting rights, financial participation, contractual arrangements, or intermediary entities. Control may be exercised directly or through other	

Commission proposal	Drafting suggestions and Comments
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.	DK (Drafting suggestions): (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. **The Commission shall issue guidance, in consultation with the European Data Innovation Board (EDIB), on the assessment of serious economic damage, the evaluation of risks relating to third-country jurisdictions, and the proportionality of refusal decisions. Such guidance should facilitate uniform interpretation while preserving the objectives of this Regulation.** DK

Commission proposal	Drafting suggestions and Comments
	(Comments): DK suggests to include text in the preamble on issuing guidance in line with our suggestion for an addition to Article 5. FR (Drafting suggestions): ~~(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.~~ FR (Comments): This recital brings confusion.
(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	FR (Drafting suggestions): (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

Commission proposal	Drafting suggestions and Comments
Regulation (EU) 2023/2854, thus ensures that the obligations laid down in that Chapter are invoked only under well-defined, urgent situations, reducing the technical, administrative and legal challenges that business faced under the previous regime. This would ensure that data requests are relevant and proportionate to responding, mitigating, or supporting the recovery from public emergencies. Since the updated Union framework on European statistics under Regulation (EC) No 223/2009 of the European Parliament and of the Council[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).	scope of Chapter V of that Regulation from 'exceptional need' to 'public emergencies'. The concept of 'public emergencies', which is defined under Article 2(29) of Regulation (EU) 2023/2854, thus ensures that the obligations laid down in that Chapter are invoked only under well-defined, urgent situations, reducing the technical, administrative and legal challenges that business faced under the previous regime. This would ensure that data requests are relevant and proportionate to responding, mitigating, or supporting the recovery from public emergencies. Since the updated Union framework on European statistics under Regulation (EC) No 223/2009 of the European Parliament and of the Council11 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). FR (Comments): French authorities express serious concerns about the amendments proposed by the Commission to Chapter V of the Data Act.

Commission proposal	Drafting suggestions and Comments
	The consequences of these multiple amendments, which appear to be semantic, raise serious questions related to the rights of State Member authorities to determine the terms and conditions for triggering "public emergencies". Please see our comments in chapter V. IT (Drafting suggestions): To simplify the business-to-government data sharing framework under Regulation (EU) 2023/2854 and to clarify ambiguities that previously imposed broader obligations on businesses, it is necessary to narrow the scope of Chapter V of that Regulation from 'exceptional need' to 'public emergencies'. The concept of 'public emergencies', which is defined under Article 2(29) of Regulation (EU) 2023/2854, thus ensures that the obligations laid down in that Chapter are invoked only under well-defined, urgent situations, reducing the technical, administrative and legal challenges that business faced under the previous regime. **Mandatory B2G access should be limited to clearly defined situations such as national security, public order, public health emergencies, disasters, crime prevention and public emergencies, excluding general administrative requests. Obligations on SMEs shall be proportionate**. 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 Council11 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

Commission proposal	Drafting suggestions and Comments
	a public emergency, in which case such enterprises are allowed to claim compensation. IT (Comments): Ensures targeted and justified B2G access. Specify that "public emergencies" should **not include strictly local or regional events** lacking cross border or systemic relevance. PL (Comments): Limiting public sector access to data held by private entities (B2G) only to "public emergency" situations **would significantly reduce the situations in which the public sector can effectively use private sector data**, thereby restricting its availability and potential for public tasks. Simplifying the provisions of Chapter V should not come at the expense of restricting public sector access to privately held data, especially given that such access is already significantly limited. Chapter V reflects a legislative compromise agreed upon by all Member States, and Poland has consistently emphasized the need to increase, rather than limit, access to private data for the purposes of the public interest.
(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	

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.	DK (Drafting suggestions): (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 **main** 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 **main** 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.

Commission proposal	Drafting suggestions and Comments
	The Commission shall issue guidelines, in consultation with the European Data Innovation Board (EDIB), to illustrate indicators of custom-built services, provide practical examples, and clarify assessment methods. These guidelines shall be updated as necessary to reflect technological developments, new service models, or emerging industry practices, without altering the fundamental definition of custom-built services. DK (Comments): DK suggests replacing the recital to correspond with our proposal for Article 31 1 a. (See below for 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	IT (Drafting suggestions): At the end: Exemptions for specific actors, such as micro enterprises or very small public bodies, may be considered where renegotiation would be technically impracticable or manifestly disproportionate IT (Comments): Ensures proportionality without undermining portability goals. Require an **annual proportionality review** of exemptions for micro enterprises and very small public entities, ensuring that growth over time does not distort competition.

Commission proposal	Drafting suggestions and Comments
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, 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).	IT (Comments): It is recommended to emphasise the importance of systematically monitoring Member State deviations, ensuring that new data localisation requirements do not re emerge through procurement practices or sector specific regulation.
(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	

Commission proposal	Drafting suggestions and Comments
threat to the functioning of institutions and essential public services and the survival of the population, as well as the risk of a serious disturbance to foreign relations or the peaceful coexistence of nations, or a risk to military interests. In compliance with the principle of proportionality, data localisation requirements that are justified on grounds of public security should be suitable for attaining the objective pursued, and should not go beyond what is necessary to attain that objective.	
(21) Both Directive (EU) 2019/1024 and Chapter II of Regulation (EU) 2022/868 regulate the re-use of public sector information for innovation purposes. The interplay of the two sets of rules has created legal uncertainty, mainly for public sector bodies. An alignment of the rules in one legal instrument is therefore necessary to bring further legal coherence and certainty.	
(22) Since both Directive (EU) 2019/1024 and Regulation (EU) 2022/868 share the goal of enhancing the re-use of public sector information, and inn order to simplify rules from the perspective of both public sector bodies and of re-users of public sector information, it is rational to repeal Directive (EU) 2019/1024 and Regulation (EU) 2022/868 and align the two regimes and consolidate the rules in a single Chapter under this Regulation. This solution will increase harmonisation of those rules across the Union, reduce the administrative burden associated with interpreting and implementing national legislation and make it easier for businesses to develop cross-border services and products. When designating competent bodies, Member States should ensure that even where sector-specific competent bodies are designated, all relevant sectors are ultimately covered. The amendments in this Regulation should be understood not to alter the interpretation of the different definition and terms, unless clearly specified.	IT (Drafting suggestions): (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. **Regulation shall respect national organisational specificities and cost recovery models, and ensure flexibility for regional and local administrations. Interactions with sectoral access regimes shall be carefully mapped to avoid unintended overlaps**. 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

Commission proposal	Drafting suggestions and Comments
	alter the interpretation of the different definition and terms, unless clearly specified. IT (Comments): Preserves national administrative structures and avoids "one size fits all" issues.
(23) Data and documents, which can be made publicly available for reuse, and data and documents, which are protected on the grounds of commercial confidentiality, including business, professional and company secrets, statistical confidentiality, the protection of intellectual property rights of third parties or the protection of personal data, are often held by the same public sector bodies. Therefore, it is necessary to align definitions and common principles applying to all public sector information and address questions regarding the interplay of the two sets of rules.	
(24) The existing rules should be streamlined to enhance clarity and consistency. Nevertheless, the two reuse regimes should remain distinct and their respective scope of application should continue to depend on the characteristics of the data or documents and the context of their reuse. Public sector bodies should apply the open data regime whenever possible. Only where they determine that data or a document contains information corresponding to certain categories of protected data should they limit its public availability and consider making it available for reuse as protected data.	BE (Drafting suggestions): **New (25)** This Regulation should be without prejudice to Regulations (EU) 2016/679 ([21]) and (EU) 2018/1725 ([22]) of the European Parliament and of the Council and to Directives 2002/58/EC ([23]) and (EU) 2016/680 ([24]) of the European Parliament and of the Council and the corresponding provisions of national law, including where personal and non-personal data in a data set are inextricably linked. In particular, this Regulation should not be read as creating a new legal basis for the processing of personal data for any of the regulated activities, or as amending the information requirements laid down in Regulation (EU) 2016/679. In general, insofar as personal data are concerned, the processing of personal data should be based upon one or more of the legal bases for processing provided in Articles 6 and 9 of Regulation (EU) 2016/679. In the event of a conflict between this Regulation and Union law on the protection of personal data or national law adopted in accordance

Commission proposal	Drafting suggestions and Comments
	with such Union law, the relevant Union or national law on the protection of personal data should prevail. It should be possible to consider data protection authorities to be competent authorities under this Regulation. Where other authorities function as competent authorities under this Regulation, they should do so without prejudice to the supervisory powers and competences of data protection authorities under Regulation (EU) 2016/679. (**New 26**) This Regulation/Chapter VIIc should not create an obligation to allow the re-use of protected data held by public sector bodies. In particular, each Member State should therefore be able to decide whether data is made accessible for re-use, also in terms of the purposes and scope of such access. This Regulation/Chapter VIIc should complement and be without prejudice to more specific obligations on public sector bodies to allow re-use of data laid down in sector-specific Union or national law. Public access to official documents may be considered to be in the public interest. Taking into account the role of public access to official documents and transparency in a democratic society, this Regulation/Chapter VIIc should also be without prejudice to Union or national law on granting access to and disclosing official documents. Access to official documents may in particular be granted in accordance with national law without imposing specific conditions or by imposing specific conditions that are not provided by this Regulation. BE (Comments): The newly proposed rectiles (25) and (26) consist of an integration of relevant parts of recitals 4, 7 and 11 of the current text of the DGA and are related to the proposed insertion of a a new article 32i (10) and (11). Similar to the arguments for proposing the new article 32i (10) and (11) the reasoning for inserting two new recitals (25) and (26) flows directly from the EDPB-EDPS JOINT OPINION 2/2026, p. 43/48 : For the new 32i (10) "*151.*

Commission proposal	Drafting suggestions and Comments
	As a general comment, applicable to all provisions of the new Chapter VIIc of the Data Act, the EDPB and the EDPS note that Article 1(2) DGA, which provides that the DGA 'does not create any obligation on public sector bodies to allow the re-use of data, nor does it release public sector bodies from their confidentiality obligations under Union or national law', is not retained in the Proposal. ***The specification under the current rules that there is no legal duty for public sector bodies to give access to personal data is important from a data protection viewpoint. For this reason, the EDPB and the EDPS recommend reinstating Article 1(2) DGA167.*** *".* (For the new article 32i (11), its motivation equally flows directly from the EDPB-EDPS JOINT OPINION 2/2026 p. 43/48 : "*152. The EDPB and the EDPS also note the Proposal would delete the provisions in Article 1(3) DGA, which clarify that 'the Regulation does not create a legal basis for the processing of personal data, nor does it affect any of the rights and obligation set out in Regulations (EU) 2016/679'.* ***For clarity, the EDPB and the EDPS recommend inserting an equivalent provision in the Proposal in relation to access granted by public bodies for re-use, governed by proposed Chapter VIIc, and in relation to activities of data intermediation services and data altruism organisations, governed by Chapter VIIa****.".* In any way these two sentences aspects form an important part of the DGA and should, for clarity reasons, thus be integrated into the new chapter VIIc. Indirect inferral does not constitute legal clarity. Omitting the integration of the extisting articles 1(2) and 1(3) DGA leads to questions and unnecessary unclarity regarding the voluntary nature for allowing public sector bodies the re-use of protected data, the continued obligations for public sector in terms of confidentiality and create confusion regarding the fact that the provisions do not provide for a new legal basis for the processing of personal data, or the full application of all rights and obligations set out in Regulation (EU) 2016/679. The Commission has not provided any reasons for not integration

Commission proposal	Drafting suggestions and Comments
	the extisting articles 1(2) and 1(3) DGA into the nex text, perhaps this was simply forgetfulness? We propose therefore to also include the relevant parts of recitals 4, 7 and 11 of the current text of the DGA related to the by Belgium's proposed insertion of a a new 32i (10) and (11).
(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).	BE (Drafting suggestions): ~~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.~~ BE

Formatted: Strikethrough

Formatted: English (Ireland)

Commission proposal	Drafting suggestions and Comments
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).	(Comments): Despite supporting the objective pursued by this proposed provision, to promote fair competition and innovation amongst small & medium sized businesses, Belgium has some concerns regarding the exception for very large enterprises set out in the proposed Articles 32q(6), 32r(4) and 32y(5). These provisions raise several difficulties: • Leaving the definition of the term 'very large enterprise' to the national authorities as well as the possibility to impose additional conditions may lead to fragmentation and additional administrative burdens. • The practical application of these provisions by public authorities may prove particularly complex and burdensome from an administrative point of view. Furthermore, questions may be raised about the ability of public authorities to identify these enterprises. • Finally, it should be noted that Article 32y.2 allows for a limitation of the costs borne by SMEs/SMCs, which therefore amounts to a de facto heavier financial burden for larger enterprises. • Therefore, we consider that this provision raises concerns regarding its effectiveness and practicability and would impose an additional administrative burden on public authorities. Even if the application is optional, the proposed articles 32q(6), 32r(4) and 32y(5) lead to additional complexity, including a multitude of administrative and legislative tasks for MS, for determining objective criteria and/or special or stricter conditions an/of higher fees and for its application and follow-up, and could in turn also create more fragmentation between MS. Finally, the regime is highly likley to be circumvented by VLE, who could eaisily set up 'strawman' like structures and who have the means use other alternative ways to avoid stricter conditions and higher fees.
(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	BE (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
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.	~~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.~~ BE (Comments): Despite supporting the objective pursued by this proposed provision, to promote fair competition and innovation amongst small & medium sized businesses, Belgium has some concerns regarding the exception for very large enterprises set out in the proposed Articles 32q(6), 32r(4) and 32y(5). These provisions raise several difficulties: • Leaving the definition of the term 'very large enterprise' to the national authorities as well as the possibility to impose additional conditions may lead to fragmentation and additional administrative burdens. • The practical application of these provisions by public authorities may prove particularly complex and burdensome from an administrative point of view. Furthermore, questions may be raised about the ability of public authorities to identify these enterprises.

Formatted: Strikethrough

Commission proposal	Drafting suggestions and Comments
	• Finally, it should be noted that Article 32y.2 allows for a limitation of the costs borne by SMEs/SMCs, which therefore amounts to a de facto heavier financial burden for larger enterprises. • Therefore, we consider that this provision raises concerns regarding its effectiveness and practicability and would impose an additional administrative burden on public authorities. Even if the application is optional, the proposed articles 32q(6), 32r(4) and 32y(5) lead to additional complexity, including a multitude of administrative and legislative tasks for MS, for determining objective criteria and/or special or stricter conditions an/of higher fees and for its application and follow-up, and could in turn also create more fragmentation between MS. Finally, the regime is highly likley to be circumvented by VLE, who could eaisily set up 'strawman' like structures and who have the means use other alternative ways to avoid stricter conditions and higher fees.
[…]	
(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.	BE (Drafting suggestions): 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**f**ulfil 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. **The single-**

Commission proposal	Drafting suggestions and Comments
	entry point shall operate exclusively as a secure transmission conduit and shall not entail centralised storage of incident data at Union level. Incident data shall remain under the control of the competent national authorities and shall not be transferred to or processed on infrastructure located outside their control. BE (Comments): Incident notifications submitted under the relevant Union legal acts may contain sensitive information related to national security. Belgium therefore considers that such data should at no point be transferred to or processed on infrastructure located outside the control of the member state involved. Clear guarantees should ensure that reporting data remains at any time during and after submission within secure infrastructure under the control of the competent national authorities. DE (Drafting suggestions): (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-**information**-~~entry~~-point for incident reporting should **support** ~~allow~~ entities to **gather the information needed for** fulfil**ling** reporting obligations under Directive (EU) 2022/2555, Regulation (EU) 2016/679, Regulation (EU) 2022/2554, Regulation (EU) No 910/2014 and Directive (EU) 2022/255~~7 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.~~ ES (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
	DELETE recital (49). REPLACE WITH: (49) Several horizontal or sectorial Union legal acts require the notification of the same event to different competent authorities, using different technical means and channels. With a view to supporting entities in identifying the appropriate national reporting channels, ENISA should develop and maintain a publicly accessible Single Information Point (SIP) consisting of a website providing information on incident reporting obligations, competent authorities and national entry points across all relevant Union legal acts, without collecting, processing or storing any incident notification data. This measure falls within ENISA's existing mandate under Regulation (EU) 2019/881. ES (Comments): ES: Recitals (49) to (57) exclusively support the SEP architecture. One new recital is sufficient to justify the Single Information Point. See proposed new Art 23a. FR (Drafting suggestions): (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 **information** ~~entry~~ point for incident reporting should **support** ~~allow~~ entities to **gather the information needed for** fulfil**ling** reporting obligations under Directive (EU) 2022/2555, Regulation (EU) 2016/679, Regulation (EU) 2022/2554, Regulation (EU) No 910/2014 and Directive (EU) 2022/255~~7 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.~~ IT

Commission proposal	Drafting suggestions and Comments
	(Drafting suggestions): (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 **information** ~~entry~~ point for incident reporting should **support** ~~allow~~ entities to **gather the information needed for** fulfil**ling** 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.~~ IT (Comments): To be read in conjunction with Art. 23(a). IT (Comments): The Single Information Point should provide a regulatory change alert system notifying entities of updates to thresholds, deadlines or formats across Union acts to ensures operators stay aligned with rapidly evolving notification standards. NL (Drafting suggestions): (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 **information** ~~entry~~ point for incident reporting should **support** ~~allow~~ entities to **gather the information needed**

Commission proposal	Drafting suggestions and Comments
	for fulfil**ling** 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.~~ RO (Comments): While Romania fully supports the Commission's objective to reduce the administrative burden on European businesses ("reporting fatigue"), we cannot support the creation of a centralized Single Reporting Point (SEP) managed by ENISA, as currently proposed. We believe this mechanism fundamentally misaligns with the operational realities of cyber incident response and the principle of subsidiarity. Our primary reservation is not merely one of national security — though that remains a competence of Member States under Article 4(2) TEU — but of operational sovereignty and effectiveness. Cybersecurity incidents are, in their vast majority, purely internal events. A ransomware attack on a national public institution, a regional hospital or a municipal water utility is a crisis that must be managed locally, by local authorities who speak the language, understand the infrastructure, and have established trust channels with the victim. By mandating a direct reporting line to a supranational agency, the proposal effectively bypasses the "first responders" (National CSIRTs). Only national competent authorities possess the contextual knowledge to determine which incidents are significant enough to warrant escalation to the European level, and can decide what data can be shared regarding an incident.
(50) To ensure the security of the single-entry point, ENISA should take appropriate and proportionate technical, operational and organisational	BE

Commission proposal	Drafting suggestions and Comments
measures to manage the risks posed to the security of the single-entry point and the information submitted or disseminated via the single-entry point. When assessing the risk, and the appropriateness and proportionality of those measures, ENISA should take into account the sensitivity of information submitted or disseminated pursuant to the relevant Union legal acts. ENISA should consult competent authorities under the relevant Union legal acts when drafting the technical, operational and organisational measures necessary to establish, maintain and securely operate the single-entry point by making use of existing cooperation groups and networks of Member States established under these acts.	(Drafting suggestions): To ensure the **highest level of** security of the single-entry point, ENISA should take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of the single-entry point and the information submitted or disseminated via the single-entry point. When assessing the risk, and the appropriateness and proportionality of those measures, ENISA should take into account the sensitivity for **national security** of **the** information submitted or disseminated pursuant to the relevant Union legal acts. **The single-entry point should be designed in a manner that prevents any unauthorised access, alteration, retention or centralised storage of incident data at Union level and shouldensure that incident notifications are transmitted automatically and without delay to the competent national authorities concerned.** ENISA should consult competent authorities under the relevant Union legal acts when drafting **and updating** 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. **Prior to becoming operational, the single-entry point should undergo independent security testing, including penetration testing and vulnerability assessments and shall be subject to a protocol agreement with each competent authority involved.** BE (Comments): Belgium considers that the Single Entry Point (SEP) should function strictly as a secure transmission conduit and not as a centralised EU-level database. Incident data must remain under the control of the competent national authorities, be transmitted immediately and automatically to all authorities concerned, and not be subject to central storage or reporting delays. Given the sensitive and potentially national security-related nature of such data, the SEP should only become operational once its security, resilience and

Commission proposal	Drafting suggestions and Comments
	reliability have been clearly defined and demonstrably ensured, including through independent security testing. DE (Drafting suggestions): ~~(50) To ensure the security of the single-entry point, ENISA should take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of the single-entry point and the information submitted or disseminated via the single-entry point. When assessing the risk, and the appropriateness and proportionality of those measures, ENISA should take into account the sensitivity of information submitted or disseminated pursuant to the relevant Union legal acts. ENISA should consult competent authorities under the relevant Union legal acts when drafting the technical, operational and organisational measures necessary to establish, maintain and securely operate the single-entry point by making use of existing cooperation groups and networks of Member States established under these acts.~~ **The EU single-information point should consist of a publicly accessible website developed and managed by ENISA. The single-information Point will reduce administrative burden for entities by providing information on reporting and assistance structures and a clear overview of information on incident reporting of the respective legislation. The single-information point will give a clear and centralised overview on when, where and how entities must report security incidents to the recipients defined in respective legislation. This overview may include the redirecting of Website-visitors to the respective Member States' national entry points and/or reporting forms.** ES (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
	DELETE recital (50). This recital exclusively supports the Single Entry Point architecture. ES (Comments): ES: Delete. Exists solely to justify the SEP operational architecture. FR (Drafting suggestions): ~~To ensure the security of the single-entry point, ENISA should take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of the single-entry point and the information submitted or disseminated via the single-entry point. When assessing the risk, and the appropriateness and proportionality of those measures, ENISA should take into account the sensitivity of information submitted or disseminated pursuant to the relevant Union legal acts. ENISA should consult competent authorities under the relevant Union legal acts when drafting the technical, operational and organisational measures necessary to establish, maintain and securely operate the single-entry point by making use of existing cooperation groups and networks of Member States established under these acts.~~ **The EU Single Information Point should consist of a publicly accessible website developed and managed by ENISA. The Single Information Point will reduce administrative burden for entities by providing information on reporting and assistance structures and a clear overview of information on incident reporting of the respective legislation. The Single Information Point will give a clear and centralised overview on when, where and how entities must report security incidents to the recipients defined in respective legislation. This overview may include the redirecting of Website-visitors to the respective Member States' national entry points and/or reporting forms.**

Commission proposal	Drafting suggestions and Comments
	IT (Drafting suggestions): ~~(50) To ensure the security of the single entry point, ENISA should take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of the single-entry point and the information submitted or disseminated via the single entry point. When assessing the risk, and the appropriateness and proportionality of those measures, ENISA should take into account the sensitivity of information submitted or disseminated pursuant to the relevant Union legal acts. ENISA should consult competent authorities under the relevant Union legal acts when drafting the technical, operational and organisational measures necessary to establish, maintain and securely operate the single entry point by making use of existing cooperation groups and networks of Member States established under these acts.~~ **The EU Single Information Point should consist of a publicly accessible website developed and managed by ENISA. The Single Information Point will reduce administrative burden for entities by providing information on reporting and assistance structures and a clear overview of information on incident reporting of the respective legislation. The Single Information Point will give a clear and centralised overview on when, where and how entities must report security incidents to the recipients defined in respective legislation. This overview may include the redirecting of Website-visitors to the respective Member States' national entry points and/or reporting forms.** IT (Comments): Further specifying Art. 23(a)(1a). NL

Commission proposal	Drafting suggestions and Comments
	(Drafting suggestions): ~~(50) To ensure the security of the single-entry point, ENISA should take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of the single-entry point and the information submitted or disseminated via the single-entry point. When assessing the risk, and the appropriateness and proportionality of those measures, ENISA should take into account the sensitivity of information submitted or disseminated pursuant to the relevant Union legal acts. ENISA should consult competent authorities under the relevant Union legal acts when drafting the technical, operational and organisational measures necessary to establish, maintain and securely operate the single-entry point by making use of existing cooperation groups and networks of Member States established under these acts.~~ **The EU Single Information Point should consist of a publicly accessible website developed and managed by ENISA. The Single Information Point will reduce administrative burden for entities by providing information on reporting and assistance structures and a clear overview of information on incident reporting of the respective legislation. The Single Information Point will give a clear and centralised overview on when, where and how entities must report security incidents to the recipients defined in respective legislation. This overview may include the redirecting of Website-visitors to the respective Member States' national entry points and/or reporting forms.**
(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	DE (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
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.	(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.~~ **Streamlining incident reporting requires building on the experiences and lessons learned at national level in the implementation of relevant Union law. On this basis, Member States may decide to establish one or more national entry points for reporting incidents to the national competent authorities. In addition, national experience could inform EU- level recommendations to be adopted by ENISA. Such recommendations should ensure that the establishment, maintenance, and operation of national entry points are as closely aligned as possible, by setting out the relevant technical, operational, and organisational measures to be applied at national level.** **Moreover, ENISA plays a key role in facilitating cross- border notifications to multiple national reporting structures. It should therefore leverage its expertise, as well as the available tools and platforms - such as the Cybersecurity Incident Reporting and Analysis System (CIRAS) - to support the alignment of incident notifications**

Commission proposal	Drafting suggestions and Comments
	submitted via national entry points. Such alignment should not prevent Member States from assessing possible cross- border impact of incidents. ES (Drafting suggestions): DELETE recital (51). This recital exclusively supports the Single Entry Point architecture. ES (Comments): ES: Delete. Exists solely to justify the SEP operational architecture. FR (Drafting suggestions): (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.~~

Commission proposal	Drafting suggestions and Comments
	Streamlining incident reporting requires building on the experiences and lessons learned at national level in the implementation of relevant Union law and should therefore take into account existing national arrangements. In addition, national experience could inform EU- level guidelines to be adopted by ENISA. Such guidelines should ensure that the establishment, maintenance, and operation of national entry points are as closely aligned as possible, by setting out the relevant technical, operational, and organisational measures to be applied at national level. **Moreover, ENISA plays a key role in facilitating cross- border notifications to multiple national reporting structures. It should therefore leverage its expertise, as well as the available tools and platforms - such as the Cybersecurity Incident Reporting and Analysis System (CIRAS) - to support the alignment of incident notifications submitted via national entry points. Such alignment should not prevent Member States from assessing possible cross- border impact of incidents.** IT (Drafting suggestions): (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~~

Commission proposal	Drafting suggestions and Comments
	~~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.~~ **Streamlining incident reporting requires building on the experiences and lessons learned at national level in the implementation of relevant Union law. On this basis, Member States may decide to establish one or more national entry points for reporting incidents to the national competent authorities. In addition, national experience could inform EU- level guidelines to be adopted by ENISA. Such guidelines should ensure that the establishment, maintenance, and operation of national entry points are as closely aligned as possible, by setting out the relevant technical, operational, and organisational measures to be applied at national level.** **Moreover, ENISA plays a key role in facilitating cross- border notifications to multiple national reporting structures. It should therefore leverage its expertise, as well as the available tools and platforms - such as the Cybersecurity Incident Reporting and Analysis System (CIRAS) - to support the alignment of incident notifications submitted via national entry points. Such alignment should not prevent Member States from assessing possible cross- border impact of incidents.** IT (Comments): To be read in conjunction with Art. 23(b) and (d). IT (Comments):

Commission proposal	Drafting suggestions and Comments
	In addition, to protect public investments and ensures stable transition, a requirement **for 24 month backward compatibility** with national systems to prevent forced redesigns of already deployed infrastructures, should be included NL (Drafting suggestions): (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.~~ **Streamlining incident reporting requires building on the experiences and lessons learned at national level in the implementation of relevant Union law. On this basis, Member States may decide to establish one or more national entry points for reporting incidents to the national competent authorities. In addition, national experience could inform EU-level**

Commission proposal	Drafting suggestions and Comments
	guidelines to be adopted by ENISA. Such guidelines should ensure that the establishment, maintenance, and operation of national entry points are as closely aligned as possible, by setting out the relevant technical, operational, and organisational measures to be applied at national level. **Moreover, ENISA plays a key role in facilitating cross-border notifications to multiple national reporting structures. It should therefore leverage its expertise, as well as the available tools and platforms - such as the Cybersecurity Incident Reporting and Analysis System (CIRAS) - to support the alignment of incident notifications submitted via national entry points. Such alignment should not prevent Member States from assessing possible cross-border impact of incidents.**
(52) To ensure the continuity and interoperability with existing national technical solutions that facilitate incident reporting, to the extent feasible, ENISA should take into account such national technical solutions when developing the specifications on the technical, operational and organisational measures necessary to establish, maintain and securely operate the single-entry point. Further, ENISA should consider technical protocols and tools such as application programming interfaces and machine-readable standards that enable entities to integrate reporting obligations into business processes, and authorities to connect the single-entry point with their national reporting systems.	DE (Drafting suggestions): (52)~~To ensure the continuity and interoperability with existing national technical solutions that facilitate incident reporting, to the extent feasible, ENISA should take into account such national technical solutions when developing the specifications on the technical, operational and organisational measures necessary to establish, maintain and securely operate the single-entry point. Further, ENISA should consider technical protocols and tools such as application programming interfaces and machine-readable standards that enable entities to integrate reporting obligations into business processes, and authorities to connect the single-entry point with their national reporting systems.~~ ES (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
	DELETE recital (52). This recital exclusively supports the Single Entry Point architecture. ES (Comments): ES: Delete. Exists solely to justify the SEP operational architecture FR (Drafting suggestions): (52)~~To ensure the continuity and interoperability with existing national technical solutions that facilitate incident reporting, to the extent feasible, ENISA should take into account such national technical solutions when developing the specifications on the technical, operational and organisational measures necessary to establish, maintain and securely operate the single-entry point. Further, ENISA should consider technical protocols and tools such as application programming interfaces and machine-readable standards that enable entities to integrate reporting obligations into business processes, and authorities to connect the single-entry point with their national reporting systems.~~ IT (Drafting suggestions): (52)~~To ensure the continuity and interoperability with existing national technical solutions that facilitate incident reporting, to the extent feasible, ENISA should take into account such national technical solutions when developing the specifications on the technical, operational and organisational measures necessary to establish, maintain and securely operate the single-entry point. Further, ENISA should consider technical protocols and tools such as application programming interfaces and machine-readable standards that enable entities to integrate reporting obligations into business processes,~~

Commission proposal	Drafting suggestions and Comments
	~~and authorities to connect the single-entry point with their national reporting systems.~~ IT (Comments): To facilitate automation and comparability, ENISA should define a **unified metadata format** to describe national-specific requirements not harmonised at EU level. NL (Drafting suggestions): (52)To ensure the continuity and interoperability with existing national technical solutions that facilitate incident reporting, to the extent feasible, ENISA should take into account such national technical solutions when developing the specifications on the technical, operational and organisational measures necessary to establish, maintain and securely operate the single-entry point. Further, ENISA should consider technical protocols and tools such as application programming interfaces and machine-readable standards that enable entities to integrate reporting obligations into business processes, and authorities to connect the single-entry point with their national reporting systems.
(53) To ensure that the single-entry point enables the relevant entities to submit the type of information and the format required under the relevant Union legal acts, ENISA should consult the Commission and the competent authorities under those acts. Where a Union legal act is not fully harmonized regarding the type of information and the format of notifications, Member States should inform ENISA about their national provisions.	BE (Drafting suggestions): (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. **ENISA should, in close cooperation with the Commission and the competent authorities, develop common reporting templates applicable for the relevant horizontal or sectorial Union legal acts.** Where a Union legal act is not fully harmonized regarding the type of

Commission proposal	Drafting suggestions and Comments
	information and the format of notifications, Member States should inform ENISA about their national provisions. BE (Comments): The Single Entry Point (SEP) should rely on harmonised and clear common reporting templates across the relevant Union legal acts. The objective should be to avoid duplicate reporting requirements and to enable entities to fulfil multiple obligations through a single, coherent submission. DE (Drafting suggestions): To ensure that the single-**information** ~~entry~~ point enables the relevant entities to **be informed about**~~ 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 . ES (Drafting suggestions): DELETE recital (53). This recital exclusively supports the Single Entry Point architecture. ES (Comments): ES: Delete. Exists solely to justify the SEP operational architecture. FR (Drafting suggestions): (53) To ensure that the single **information** ~~entry~~ point enables the relevant entities to **be informed about**~~ submit~~ the type of information and the format

Commission proposal	Drafting suggestions and Comments
	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 . IT (Drafting suggestions): (52)-To ensure that the single **information** ~~-entry~~ point enables the relevant entities to **be informed about** ~~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. NL (Drafting suggestions): (53) To ensure that the single **information** -entry point enables the relevant entities to **be informed about** 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	DE (Drafting suggestions): (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~~

Commission proposal	Drafting suggestions and Comments
been assessed that it ensures the proper functioning, reliability, integrity and confidentiality. Further, Regulation (EU) 2022/2554 has introduced standardised reporting templates streamlining the content of reports for major ICT-related incidents for the financial sector. The experience gained from the adoption of these templates provides valuable insights and best practices that should be taken into account when specifying the type of information, the format and the procedure of a notification for the purposes of reporting to the single-entry point under Directive (EU) 2022/2555, Directive (EU) 2022/2557 or Regulation (EU) 2016/679, where appropriate. For this purpose, the Commission should take due account of the regulatory technical standards adopted pursuant to Regulation (EU) 2022/2554, which specify the content of the initial notification, as well as the intermediate and final reports, concerning major ICT-related incidents. This approach aims to ensure consistency, promote synergies and reduce administrative burden on entities by minimizing the number of data fields that entities are required to complete, thereby facilitating more efficient and streamlined reporting processes.	~~established under Regulation (EU) 2022/2554 with the single-entry point, while ensuring continuity and stability of the existing reporting framework, and considering that the single-entry point would be operational after it has been assessed that it ensures the proper functioning, reliability, integrity and confidentiality. Further, Regulation (EU) 2022/2554 has introduced standardised reporting templates streamlining the content of reports for major ICT-related incidents for the financial sector. The experience gained from the adoption of these templates provides valuable insights and best practices that should be taken into account when specifying the type of information, the format and the procedure of a notification for the purposes of reporting to the single-entry point under Directive (EU) 2022/2555, Directive (EU) 2022/2557 or Regulation (EU) 2016/679, where appropriate. For this purpose, the Commission should take due account of the regulatory technical standards adopted pursuant to Regulation (EU) 2022/2554, which specify the content of the initial notification, as well as the intermediate and final reports, concerning major ICT-related incidents. This approach aims to ensure consistency, promote synergies and reduce administrative burden on entities by minimizing the number of data fields that entities are required to complete, thereby facilitating more efficient and streamlined reporting processes.~~ **Simplifying compliance and reducing the administative burden for entities falling within the scope of relevant Union legal acts requires aligning similar concepts provided in the different legal acts. This includes definitions, thresholds, deadlines, formats and procedures. For instance, a first key step should consist in aglining the definition of incident or breach under Article 3(8) of Regulation (EU) 2022/2554, Article 2(3) of Directive (EU) 2022/2557, Article 4(12) of Regulation (EU) 2016/679 and Article 6(6) of Directive (EU) 2022/2555.**

Commission proposal	Drafting suggestions and Comments
	Within [6 months after the entry into force of this Regulation] the Commission should submit a report to the European Parliament and to the Council outlining common definitions, thresholds, deadlines, formats and procedures applying to Article 23 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. **The report should in particular envisage concrete steps and a credible timeline for introducing the proposed unified approach to incident reporting under the Union legal acts.** **When developing the report, the Commission should consult existing groups and cooperation fora gathering national competent authorities under the relevant Union legal acts. Notably, the Cooperation Group established by article 14 of Directive (EU) 2022/2555, the European Data Protection Board established by Article 68 of Regulation (EU) 2016/679 and the Critical Entities Resilience Group established by Article 19 of Directive (EU) 2022/2557. Moreover, it should involve relevant European insitutions, bodies and agencies, including ENISA, EDPS an the European Supervisory Authorities for the financial sector.** ES (Drafting suggestions): DELETE recital (54). This recital exclusively supports the Single Entry Point architecture. ES (Comments): ES: Delete. Exists solely to justify the SEP operational architecture.

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

Commission proposal	Drafting suggestions and Comments
	instance, a first key step should consist in aglining the definition of incident or breach under Article 3(8) of Regulation (EU) 2022/2554, Article 2(3) of Directive (EU) 2022/2557, Article 4(12) of Regulation (EU) 2016/679 and Article 6(6) of Directive (EU) 2022/2555. **Within [6 months after the entry into force of this Regulation] the Commission should submit a report to the European Parliament and to the Council outlining common definitions, thresholds, deadlines, formats and procedures** **applying to Article 23 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.** **The report should in particular envisage concrete steps and a credible timeline for introducing the proposed unified approach to incident reporting under the Union legal acts.** **When developing the report, the Commission should extensively consult existing groups and cooperation fora gathering national competent authorities under the relevant Union legal acts. Notably, the Cooperation Group established by article 14 of Directive (EU) 2022/2555, the European Data Protection Board established by Article 68 of Regulation (EU) 2016/679 and the Critical Entities Resilience Group established by Article 19 of Directive (EU) 2022/2557. Moreover, it should involve relevant European insitutions, bodies and agencies, including ENISA, EDPS an the European Supervisory Authorities for the financial sector.** IT (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
	~~(54) Based on Regulation (EU) 2022/2554, the financial sector has been at the forefront in implementing a harmonised, comprehensive and effective framework, including with regard to incident reporting. In order to simplify compliance, it is appropriate to align the incident reporting framework established under Regulation (EU) 2022/2554 with the single-entry point, while ensuring continuity and stability of the existing reporting framework, and considering that the single-entry point would be operational after it has been assessed that it ensures the proper functioning, reliability, integrity and confidentiality. Further, Regulation (EU) 2022/2554 has introduced standardised reporting templates streamlining the content of reports for major ICT-related incidents for the financial sector. The experience gained from the adoption of these templates provides valuable insights and best practices that should be taken into account when specifying the type of information, the format and the procedure of a notification for the purposes of reporting to the single-entry point under Directive (EU) 2022/2555, Directive (EU) 2022/2557 or Regulation (EU) 2016/679, where appropriate. For this purpose, the Commission should take due account of the regulatory technical standards adopted pursuant to Regulation (EU) 2022/2554, which specify the content of the initial notification, as well as the intermediate and final reports, concerning major ICT-related incidents. This approach aims to ensure consistency, promote synergies and reduce administrative burden on entities by minimizing the number of data fields that entities are required to complete, thereby facilitating more efficient and streamlined reporting processes.~~ **Simplifying compliance and reducing the administative burden for entities falling within the scope of relevant Union legal acts requires aligning similar concepts provided in the different legal acts. This includes definitions, thresholds, deadlines, formats and procedures. For instance, a first key step should consist in aglining the definition of incident or breach under Article 3(8) of Regulation (EU) 2022/2554,**

Commission proposal	Drafting suggestions and Comments
	Article 2(3) of Directive (EU) 2022/2557, Article 4(12) of Regulation (EU) 2016/679 and Article 6(6) of Directive (EU) 2022/2555. **Within [6 months after the entry into force of this Regulation] the Commission should submit a report to the European Parliament and to the Council outlining common definitions, thresholds, deadlines, formats and procedures** **applying to Article 23 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.** **The report should in particular envisage concrete steps and a credible timeline for introducing the proposed unified approach to incident reporting under the Union legal acts.** **When developing the report, the Commission should extensively consult existing groups and cooperation *fora* gathering national competent authorities under the relevant Union legal acts. Notably, the Cooperation Group established by article 14 of Directive (EU) 2022/2555, the European Data Protection Board established by Article 68 of Regulation (EU) 2016/679 and the Critical Entities Resilience Group established by Article 19 of Directive (EU) 2022/2557. Moreover, it should involve relevant European insitutions, bodies and agencies, including ENISA, EDPS an the European Supervisory Authorities for the financial sector.** IT (Comments): To be read in conjuction with Art. 23(c). NL

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

Commission proposal	Drafting suggestions and Comments
	Simplifying compliance and reducing the administative burden for entities falling within the scope of relevant Union legal acts requires aligning similar concepts provided in the different legal acts. This includes definitions, thresholds, deadlines, formats and procedures. For instance, a first key step should consist in aglining the definition of incident or breach under Article 3(8) of Regulation (EU) 2022/2554, Article 2(3) of Directive (EU) 2022/2557, Article 4(12) of Regulation (EU) 2016/679 and Article 6(6) of Directive (EU) 2022/2555. **Within [6 months after the entry into force of this Regulation] the Commission should submit a report to the European Parliament and to the Council outlining common definitions, thresholds, deadlines, formats and procedures** **applying to Article 23 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.** **The report should in particular envisage concrete steps and a credible timeline for introducing the proposed unified approach to incident reporting under the Union legal acts.** **When developing the report, the Commission should extensively consult existing groups and cooperation fora gathering national competent authorities under the relevant Union legal acts. Notably, the Cooperation Group established by article 14 of Directive (EU) 2022/2555, the European Data Protection Board established by Article 68 of Regulation**

Commission proposal	Drafting suggestions and Comments
	(EU) 2016/679 and the Critical Entities Resilience Group established by Article 19 of Directive (EU) 2022/2557. Moreover, it should involve relevant European insitutions, bodies and agencies, including ENISA, EDPS an the European Supervisory Authorities for the financial sector.
(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.	DE (Drafting suggestions): ~~(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.~~ ES (Drafting suggestions): DELETE recital (55). This recital exclusively supports the Single Entry Point architecture. ES (Comments): ES: Delete. Exists solely to justify the SEP operational architecture. FR (Drafting suggestions): ~~(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,~~

Commission proposal	Drafting suggestions and Comments
	~~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.~~ IT (Drafting suggestions): ~~(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.~~ IT (Comments): Data minimisation and accountability should be ensured for example requiring strict application of the "need to know" principle and mandatory logging of all data access operations. NL (Drafting suggestions): ~~(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~~

Commission proposal	Drafting suggestions and Comments
	~~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.	BE (Drafting suggestions): To ensure that incident reporting **may be ~~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 **become operational ~~start being used~~** for the purpose of reporting under those acts within 18 months from the entry into force of this Regulation**, without prejudice to the possibility for entities to report directly to the competent national authorities where such national reporting mechanisms exist**. 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. DE (Drafting suggestions): ~~(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)~~

Commission proposal	Drafting suggestions and Comments
	~~2022/2554 and Directive (EU) 2022/2557 should continue to apply for the purpose of meeting the reporting obligations laid down in the provisions.~~ ES (Drafting suggestions): DELETE recital (56). This recital exclusively supports the Single Entry Point architecture. ES (Comments): ES: Delete. Exists solely to justify the SEP operational architecture. FR (Drafting suggestions): ~~(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.~~ IT (Drafting suggestions): ~~(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~~

Commission proposal	Drafting suggestions and Comments
	~~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.~~ IT (Comments): The transition should validate the cross border performance before enforcement. NL (Drafting suggestions): (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	BE (Drafting suggestions): 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**, including national reporting mechanisms, where available**. For that purpose,

Commission proposal	Drafting suggestions and Comments
alternative means and should make information about that alternative means publicly available.	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. DE (Drafting suggestions): ~~(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.~~ ES (Drafting suggestions): DELETE recital (57). This recital exclusively supports the Single Entry Point architecture. ES (Comments): ES: Delete. Exists solely to justify the SEP operational architecture. FR (Drafting suggestions): ~~(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.~~

Commission proposal	Drafting suggestions and Comments
	IT (Drafting suggestions): ~~(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.~~ NL (Drafting suggestions): ~~(57) In the exceptional event that a technical impossibility prevents the submission of incident notifications using the single entry point, entities should fulfil their reporting obligations through alternative means. For that purpose, addressees of incident notifications under the relevant Union legal acts should ensure that they can receive such incident notifications through alternative means and should make information about that alternative means publicly available.~~
(58) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council[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	

Commission proposal	Drafting suggestions and Comments
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.	IT (Comments): Accompany the rapid entry into force with **interpretative guidelines within three months** to support consistent implementation. LV (Comments): Taking into account the differing objectives and legal bases of the instruments currently in force. The implementation of the requirements set out in the proposal would require a period of at least two years.

Commission proposal	Drafting suggestions and Comments
HAVE ADOPTED THIS REGULATION:	
Article 1	

Amendments to Regulation (EU) 2023/2854	SI (Comments): SI raise the following key concerns regarding the proposed transformation of the Open Data Directive (ODD) into a Regulation: - Open data must remain a distinct policy objective. The re-use of open public data, that are free of charge, and accessible to all, must remain a specific policy objective supported by a dedicated, clear, and coherent legal framework, including within any Digital Omnibus initiative - Different regulatory logics must remain clearly separated. The regulatory foundations for re-use of open public sector data differ fundamentally from those governing payable data held by public bodies and conditional transmission/access arrangements. This distinction must be unequivocally reflected in the Digital Omnibus and in any Data Act provisions. SI is therefore not in favour of proposed changes affecting open data and considers that this aspect should be excluded from the Digital Omnibus. - A Directive framework enables necessary national flexibility. The current Open data Directive is designed to establish minimum common standards and principles while preserving Member States' flexibility to implement these rules in national legislation. An uncritical conversion of Open data Directive provisions into a Regulation within the Digital Omnibus Data Act framework risks creating legal inconsistencies and could undermine or lower standards already achieved in national open data regimes. - There is risk of diluting open data principles and obligations. Incorporating Open data Directive principles (free-of-charge, open-by-default) into a Regulation primarily addressing payable, protected, and conditional access to sensitive data risks blurring legal obligations and weakening political commitment to genuine open data. SI therefore call for greater

Commission proposal	Drafting suggestions and Comments
	clarity in further discussions on how the current Open data Directive provisions are and could be transformed and reflected in the Data Act.
Regulation (EU) 2023/2854 is amended as follows:	SI (Comments): SI considers that the proposed definitions in the Digital Omnibus raise significant concerns. In our view, they have been amended in an inappropriate manner and may create regulatory ambiguity: - Regarding the existing level of regulatory protection for "legally protected data", SI does not agree with the proposed amendments to the definitions currently laid down in the DGA. (SI already explicitly opposed the proposed modification of the definition of personal data in the GDPR-related part of the Omnibus). SI therefore calls for further clarification and, where necessary, revision of the proposed set of definitions.
1. Article 1 is amended as follows:	DE (Comments): **DE**: In principle, and with the exception of Chapter V, the Data Act should exclusively regulate data usage, while data protection should remain within data protection law. As a consequence, only the definition of the scope of application in Article 1(5) and the further explanations in Recital 7 of the Data Act would remain. As stated in the aforementioned rules, in cases of collision the data protection law should take precedence.

Commission proposal	Drafting suggestions and Comments
	Furthermore the opportunity should be taken to clarify the current Article 1 paragraph 5, especially taking into consideration that now several Regulations are combined. NL (Drafting suggestions): *Extra*: c) is deleted : ~~c) the making available of data by data holders to public sector bodies, the Commission, the European Central Bank and Union bodies, where there an exceptional need for those data for the performance of a specific task carried out in the public interest;~~ NL (Comments): In line with our suggestions for Chapter V; The Netherlands would support further simplification by removing the rules on requesting data in public emergencies and where there's an exceptional need, given the continuing uncertainty surrounding the application of these rules.
(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;	NL (Drafting suggestions): (ed) data localisation requirements~~ and the availability of data to competent authorities;~~ NL

Commission proposal	Drafting suggestions and Comments
	(Comments): Text deleted because the subject from art. 5 FFoD is also deleted.
(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;	NL (Drafting suggestions): '(g) Chapter VIIa applies to ~~personal and non-personal~~ data; NL (Comments): In line with current art. 1(2) DA 'data' instead of 'personal and non-personal data'. This is already made clear in the first paragraph of art. 1(2) DA.
(h) Chapter VIIb applies to any non-personal data;	
(i) Chapter VIIc applies to personal and non-personal data, namely the following:	NL (Drafting suggestions): (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);	

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.';	FI (Comments): FI: We suggest that Article 1(3)(e) in current Data Act is adjusted to correspond more clearly to the phrasing used in the new Article 15a(1). "Current Data Act 1(3)(e): public sector bodies, the Commission, the European Central Bank and Union bodies that request data holders to make data available where there is an exceptional need to use certain for those data for the performance of a specific task carried out to carry out their statutory duties in the public interest and to the data holders that provide those data in response to such request;" NL (Drafting suggestions): (g) participants in data spaces;- **In paragraph 3 the following points are added:** **(h) data intermediation servies;** NL (Comments): There are actors missing from the DGA
(d) paragraph 7 is deleted.	NL (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
	Extra: **Paragraph 5 is amendend. At the end a sentence is added : "<u>This Regulation does not create a legal basis for the processing of personal data.</u>"** NL (Comments): This sentence from art. 1(3) DGA was missing in art. 1(5) DA. Paragraphs following par. 7 must be renumberd.
(e) the following paragraphs 11, 12 and 13 are added:	NL (Drafting suggestions): (e) the following paragraphs ~~11, 12 and 13~~ **<u>10, 11 and 12</u>** are added: NL (Comments): Paragraphs following par. 7 must be renumberd.
'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.'	

Commission proposal	Drafting suggestions and Comments
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.'	FI (Drafting suggestions): FI: 13. With regards to data and documents in scope of Section **2** of Chapter VIIc, Chapter VIIc of this Regulation **establishes a set of minimum rules governing the re-use and the practical arrangements for facilitating the re-use of data and documents and** 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. FI (Comments): FI: In order to remove any ambiguity from the nature of Section 2, also considering its origin as a Directive, and the potential pitfalls of it not being clearly identified as minimum rules, we want to see language from Article 1(1) of the Open Data Directive introduced into this paragraph. This is particularly pertinent since the recitals of the ODD are not carried over into the Data Act (e.g. recitals 17 through 19 of the ODD), and this language has been used since the original PSI Directive. For instance, the FI implementation of the ODD does not create exceptions for fees for certain cultural bodies; it is up for interpretation whether such a solution is within the scope of "more detailed or stricter" rules. Also a small technical revision; sections use Arabic numerals.
2. Article 2 is amended as follows:	DE (Comments): **DE**: Please consider clarifying the relationship between the right of access under Article 3 and 4. What is the scope of Article 4, if data access is granted by design? In which cases is it likely to expect that access by design in accordance with Article 3 cannot be granted?

Commission proposal	Drafting suggestions and Comments
	FR (Comments): Réserve d'examen sur l'ensemble des définitions. PL (Comments): Definitions should rely on terms already established in applicable legal acts to avoid multiple definitions of the same concepts within the legal system. The Omnibus proposal introduces several new concepts into the re-use legal framework, some of which (including key terms) are not defined. Examples include definitions of "open government data", "open public data", or "very large enterprise". We therefore suggest: (1) verifying whether all new concepts (not previously used in the ODD or DGA) are necessary; (2) where possible, replacing them with concepts already used in existing legislation, and finally (3) retaining new key concepts only if they are clearly defined. Regarding "open data", this term is particularly relevant for re-use and is already defined in the recitals of the ODD. Although not legally binding, this definition is widely used and accepted. We therefore propose defining "open data" in line with the ODD definition.
(a) the following points (4a), (4b) and (4c) are inserted:	
'(4a) 'consent' means consent as defined in Article 4, point (11), of Regulation (EU) 2016/679;	
(4b) 'permission' means giving data users the right to the processing of non-personal data;	

Commission proposal	Drafting suggestions and Comments
(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;	DE (Comments): **DE**: This amendment changes "use and make available data" to "use or make available data". Clarification is needed whether this changes the scope of application of the term "data holder". **DE**: We deem the amendment to the definition as minor without impact on the interpretation. The grammatical problems of the term are not addressed. The term is used in different contexts and should therefore be drafted carefully in order to neatly work for different chapters of the proposed consolidated Data Act. With regard to chapter II, the petitio principii – i.e. the legal qualification cannot be part of the definition - could be resolved, in accordance with the telos, by limiting the definition to a description of the de facto access to the readily available data.
(c) the following points (28a) and (28b) are inserted:	
'(28a) 'bodies governed by public law' means bodies that have all of the following characteristics:	
(a) they are established for the specific purpose of meeting needs in the general interest, not having an industrial or commercial character;	

Commission proposal	Drafting suggestions and Comments
(b) they have legal personality;	
(c) they are financed, for the most part by the State, regional or local authorities, or by other bodies governed by public law; or are subject to management supervision by those authorities or bodies; or have an administrative, managerial or supervisory board, more than half of whose members are appointed by the State, regional or local authorities, or by other bodies governed by public law;	
(28b) 'public undertaking' means any undertaking over which a public sector body may exercise directly or indirectly a dominant influence by virtue of their ownership of it, their financial participation therein, or the rules which govern it. A dominant influence on the part of the public sector bodies shall be presumed in any of the following cases in which those bodies, directly or indirectly:	
(a) hold the majority of the undertaking's subscribed capital;	
(b) control the majority of the votes attaching to shares issued by the undertaking;	
(c) can appoint more than half of the undertaking's administrative, management or supervisory body;';	
(d) the following points (38a) and (38b) are inserted:	
'(38a) 'data intermediation service' means a service which aims to establish relationships of an economic character for the purposes of data sharing between an undetermined number of data subjects or data holders and data users, through technical, legal or other means, including for the purpose of exercising the rights of data subjects in relation to personal data, and which :	DE (Comments): **DE**: Prima vista the changes appear to be simplifications without material impact. ES

Commission proposal	Drafting suggestions and Comments
	(Comments): Check consistency with definition (10). This concepts is defined twice
(1) do not have as their main purpose the intermediation of copyright-protected content;	
(2) are not jointly procured by several legal persons for exclusive use among them;	
(38b) 'data altruism' means the voluntary sharing of data on the basis of the consent of data subjects to process personal data pertaining to them, or of permissions of data holders to allow the use of their non-personal data without seeking or receiving a reward that goes beyond compensation related to the costs that they incur where they make their data available for objectives of general interest as provided for in national law, where applicable, such as healthcare, combating climate change, improving mobility, facilitating the development, production and dissemination of official statistics, improving the provision of public services, public policy making or scientific research purposes in the general interest;'	DE (Drafting suggestions): Article 2 […] ~~(39) 'smart contract' means a computer program used for the automated execution of an agreement or part thereof, using a sequence of electronic data records and ensuring their integrity and the accuracy of their chronological ordering;~~ DE (Comments): **DE**: follows deletion of Article 36 Data Act NL (Drafting suggestions): ~~(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~~

Commission proposal	Drafting suggestions and Comments
	~~official statistics, improving the provision of public services, public policy making or scientific research purposes in the general interest;'~~ NL (Comments): In line with our comments on chapter VIIa, the definition for data altruism can be deleted.
(e) the following points (44) to (63) are added:	NL (Drafting suggestions): **(e) Point 39 is deleted.** **(f) the following points (44) to (70) are added:** **(64) 'data user' means a natural or legal person who has lawful access to certain personal or non-personal data and has the right, including under Regulation (EU) 2016/679 in the case of personal data, to use that data for commercial or non-commercial purposes;** **(65) 'data sharing' means the provision of data by a data subject or a data holder to a data user for the purpose of the joint or individual use of such data, based on voluntary agreements or Union or national law, directly or through an intermediary, for example under open or commercial licences subject to a fee or free of charge;** **(66) 'processing' means processing as defined in Article 4, point (2), of Regulation (EU) 2016/679 with regard to personal data or Article 3, point (2), of Regulation (EU) 2018/1807 with regard to non-personal data;** **(67) 'access' means data use, in accordance with specific technical, legal or organisational requirements, without necessarily implying the transmission or downloading of data;** **(68) 'services of data cooperatives' means data intermediation services offered by an organisational structure constituted by data subjects, one-person undertakings or SMEs who are members of that structure,**

Commission proposal	Drafting suggestions and Comments
	having as its main objectives to support its members in the exercise of their rights with respect to certain data, including with regard to making informed choices before they consent to data processing, to exchange views on data processing purposes and conditions that would best represent the interests of its members in relation to their data, and to negotiate terms and conditions for data processing on behalf of its members before giving permission to the processing of non-personal data or before they consent to the processing of personal data; **(69) 'legal representative' means a natural or legal person established in the Union explicitly designated to act on behalf of a data intermediation services provider ~~or an entity that collects data for objectives of general interest made available by natural or legal persons on the basis of data altruism not established in the Union~~, which may be addressed by the competent authorities for data intermediation ~~services and the competent authorities for the registration of data altruism organisations~~ in addition to or instead of the data intermediation services provider or entity with regard to the obligations under this Regulation, including with regard to initiating enforcement proceedings against a non-compliant data intermediation services provider or entity not established in the Union;** **(70) 'draft act' means a text drafted for the purpose of being enacted as a law, regulation or administrative provision of a general nature, the text being at the stage of preparation at which substantive amendments can still be made** NL (Comments): Art. 36 about smart contracts is deleted so the definition is no longer needed. Points 55 is missing, so the numebering is incorrect.

Commission proposal	Drafting suggestions and Comments
	Defitions from DGA (art. 2 points (9), (10), (12), (13), (15), (21)) en FFoD (art. 3(3) are missing.
'(44) 'medium-sized enterprise' means a medium-sized enterprise as defined in Article 2 of Annex I to Recommendation 2003/361/EC;	
(45) 'small mid-cap' or 'SMC' means a small mid-cap enterprise as defined in Article 2 of the Annex to Commission Recommendation (EU) 2025/1099;	
(46) 'university' means a public sector body that provides post-secondary-school higher education leading to academic degrees;	
(47) 'standard licence' means a set of predefined re-use conditions in a digital format, preferably compatible with standardised public licences available online;	
(48) 'document' means:	DE (Comments): **DE**: Some of the proposed definitions do not match. Therefore, we doubt that the targeted consistency can be reached through the proposed changes. We want to express our point at a specific example: According to Article 2 para. 6 ODD "document" means any content, independent from its medium. According to Article 2 para. 1 Data Act "data" means any digital content. According to Article 1 Number 2 sec. 48 of the Digital Omnibus "document" means any content, or any part of it, that is non-digital (the existing definition for "data" from the Data Act remains the same). According to Article 1 Number 2 sec. 50 "dynamic data" means data and documents in a digital form. According to the definition of "document" in the Digital Omnibus, there can't be a document in a digital form (it would define as "data" and not "document").

Commission proposal	Drafting suggestions and Comments
	We highly recommend to check on those questions regarding consistency formality aspects. PL (Comments): **Definition of "document" is unclear:** the document means any content that is non-digital whatever its medium (paper or as a sound, visual or audiovisual recording). How the definition of "non-digital" should be understood? Does this mean that the sound, visual or audiovisual recording referred to in the definition should be analog (e.g. VHS recordings or audio cassette)? **Definitions of "document" and "data**": "document" is meant to cover all non-digital content, while "data" refers to any digital representations of acts, facts or information, as well as their compilations. It is not clear whether such a strict distinction between digital content (data) and non-digital content (documents) is really necessary, or what the practical consequences of this approach would be. This kind of division leads to interpretative and practical difficulties in other definitions that refer to concepts of „data" and „documents".
(a) any content that is non-digital whatever its medium (paper or as a sound, visual or audiovisual recording); or	
(b) any part of such content;	
(50) 'dynamic data' means data and documents in a digital form, subject to frequent or real-time updates, in particular because of their volatility or rapid obsolescence; data generated by sensors are typically considered to be dynamic data;	ES (Comments): Review numbering. Point 49 is missing FI (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
	FI: ~~(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;~~ FI (Comments): FI: Our proposal is to remove the obligations specific to dynamic data; see Article 32p. Later definitions need to be re-numbered accordingly PL (Comments): **Definition of "dynamic data"**: it covers both data and documents in digital form. But this directly conflicts with the definition of a "document," which explicitly excludes digital content. On top of that, based on the definition itself, it seems obvious that non-digital content simply cannot be considered "dynamic data."
(51) 'research data' means data , other than scientific publications, which are collected or produced in the course of scientific research activities and are used as evidence in the research process, or are commonly accepted in the research community as necessary to validate research findings and results;	PL (Drafting suggestions): (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~~ **or** results;
(52) 're-use' means the use by natural persons or legal entities of documents held by:	DE (Comments): **DE**: 52 (re-use) largely corresponds to the definition in Art. 2(11) of the ODD, with a restriction to non-digital media resulting from the amendment in 48 – linguistically, it could make sense to refer to natural and legal persons

Commission proposal	Drafting suggestions and Comments
	instead of "persons or legal entities," as seems to be customary in the digital acquis. In that regard it should also be stated (e.g. in the Recitals) which concept of natural and legal persons is used, since the conceptual understanding deviates even in primary law (e.g. in Article 54 TFEU as referenced in e.g. Regulation 910/2014/EU). PL (Comments): **Definition of "re-use"** –does not include data. It covers only documents, which, when read literally, means that only non-digital content is subject to re-use. This is contrary to the whole concept of re-use of public sector information
(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;	PL (Comments): **Definition of "high-value dataset":** according to the definition, a "high-value dataset" includes both data and documents, with documents being non-digital content. Under the new Article 32p(3) of the amended Data Act, public sector bodies are not obliged to create or adapt data or documents in order to make

Commission proposal	Drafting suggestions and Comments
	data or documents available in any pre-existing format where this would involve disproportionate effort, going beyond a simple operation. In other words, they are not required to convert non-digital documents into the digital form needed for a high-value dataset. High-value datasets must, among other things, be machine-readable and accessible via APIs, which contradicts the concept of a "document" as a non-digital content.
(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;	NL (Drafting suggestions): (55) ~~(56)~~… NL (Comments): Numbering is incorrect, nr. 55 is missing.
(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;	

Commission proposal	Drafting suggestions and Comments
(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;	PL (Drafting suggestions): (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; PL (Comments): It is not possible to distinguish between "easy" and "not easy" identification, recognition, or extraction of specific data by applications.
(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;	PL (Comments): **Definition of "open format**" - this definition does not include data.
(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;	

Commission proposal	Drafting suggestions and Comments
(63) 'pseudonymisation' means pseudonymisation as referred to under Article 4(5) of Regulation (EU) 2016/679.'	DE (Drafting suggestions): Article 3 2. Before concluding a contract for the purchase, rent or lease of a connected product, the seller, rentor or lessor, which may be the manufacturer, shall provide at least the following information to the user, in a clear and comprehensible manner: […] ~~(c) whether the connected product is capable of storing data on device or on a remote server, including, where applicable, the intended duration of retention;~~ (d) how the user may access, retrieve or, where relevant, erase the data~~,~~ ~~including the technical means to do so, as well as their terms of use and quality of service~~. 3. Before concluding a contract for the provision of a related service, the provider of such related service shall provide at least the following information to the user, in a clear and comprehensible manner: […] ~~(c) whether the prospective data holder expects to use readily available data itself and the purposes for which those data are to be used, and whether it intends to allow one or more third parties to use the data for purposes agreed upon with the user;~~ […] ~~(e) the means of communication which make it possible to contact the prospective data holder quickly and communicate with that data holder efficiently;~~ […]

Commission proposal	Drafting suggestions and Comments
	~~(g) the user's right to lodge a complaint alleging an infringement of any of the provisions of this Chapter with the competent authority designated pursuant to Article 37;~~ **4. Paragraph 2 is applicable to the purchase, rent or lease of a pre-owned connected device if the product is placed on the market after 12 September 2025 and the information has been provided to the seller, rentor or lessor by the manufacturer of the connected product.** DE (Comments): **DE**: Reduce information obligations under Art. 3 para. 2 and para.3. Specific • remove Art. 3 para. 2 lit. c, • reduce the obligation in Art. 3 para. 2 lit. d to "how the user may access or retrieve or, where relevant, erase the data", • remove Art. 3 para 3 lit. c, lit. e, lit. g

Commission proposal	Drafting suggestions and Comments
	DE: proposal to clarify information obligations with regard to pre-owned connected devices FI (Drafting suggestions): FI: Suggestions for new points 64 and 65: **(64)** ‘(NEW) **‘machine-readable structured portability’ means the right of the customer to obtain exportable data and digital assets in a structured, commonly used and machine-readable format, including the full logical and relational structure necessary to reconstitute the data**

Commission proposal	Drafting suggestions and Comments
	and digital assets in another environment without material loss of functionality, integrity, or semantic coherence.' **(65) '**(NEW) '**AI model assets' are "digital assets" including artificial intelligence models developed, trained or fine-tuned by or on behalf of a customer in the context of a data processing service, including model parameters, weights, fine-tuning results, embeddings, inference configurations and training environment configurations that are not protected as trade secrets of the provider and that are necessary for the redeployment of the model by the customer.'** FI (Comments): FI: We propose adding new clarifying definitions to Article 2 corresponding to the additional wording suggested for Article 30(2) in the current Data Act. Recital 82 already includes metadata within "exportable data," and Recital 83 refers to metadata related to configuration, security and access management as part of digital assets. However, neither the definitions nor the recitals clarify that portability must include the full logical structure and semantic relationships necessary to reconstruct the dataset or service functionality in another environment. Metadata alone does not guarantee reconstructability. Likewise, while definition of "digital assets" is broad, it does not explicitly clarify that customer-developed AI models and their technical artefacts are included. Given the scale of AI development in cloud environments, explicit recognition of AI model assets under digital assets is necessary to avoid interpretative gaps and to prevent model-level lock-in.
3. in Article 4, paragraph 8 is replaced by the following:	DE (Drafting suggestions): Article 4 […]

Commission proposal	Drafting suggestions and Comments
	2. Users and data holders may contractually restrict or prohibit accessing, using or further sharing data, if such processing could undermine security requirements of the connected product, as laid down by Union or national law, resulting in a serious adverse effect on the health, safety or security of natural persons. Sectoral authorities may provide users and data holders with technical expertise in that context. ~~Where the data holder refuses to share data pursuant to this Article, it shall notify the competent authority designated pursuant to Article 37.~~ […] 7. Where there is no agreement on the necessary measures referred to in paragraph 6, or if the user fails to implement the measures agreed pursuant to paragraph 6 or undermines the confidentiality of the trade secrets, the data holder may withhold or, as the case may be, suspend the sharing of data identified as trade secrets. The decision of the data holder shall be duly substantiated and provided in writing to the user without undue delay. ~~In such cases, the data holder shall notify the competent authority designated pursuant to Article 37 that it has withheld or suspended data sharing and identify which measures have not been agreed or implemented and, where relevant, which trade secrets have had their confidentiality undermined.~~ DE (Comments): **DE**: Remove notification obligations for data holders under Art. 4 para. 2 sentence 3, para. 7 sentence 3.
'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	DE (Drafting suggestions): 8. In exceptional circumstances, where the data holder who is a trade secret holder is able to demonstrate that, despite the technical and organisational

Commission proposal	Drafting suggestions and Comments
acquisition, use, or disclosure to third country entities, or entities established in the Union under the direct or indirect control of such entities, which are subject to jurisdictions offering weaker or non-equivalent protection compared to that under Union law, that data holder may refuse on a case-by-case basis a request for access to the specific data in question. That demonstration shall be duly substantiated on the basis of objective elements, such as the enforceability of trade secrets protection in third countries, the nature and level of confidentiality of the data requested, and the uniqueness and novelty of the connected product. It shall be provided in writing to the user without undue delay. Where the data holder refuses to share data pursuant to this paragraph, it shall notify the competent authority designated pursuant to Article 37.’;	measures taken by the user pursuant to paragraph 6 of this Article, it is highly likely to suffer serious economic damage from the disclosure of trade secrets or that the disclosure of trade secrets to the user poses a high risk of unlawful acquisition, use, or disclosure to third country entities, or entities established in the Union under the direct or indirect control of such entities, which are subject to jurisdictions offering weaker or non-equivalent protection compared to that under Union law, that data holder may refuse on a case-by-case basis a request for access to the specific data in question. That demonstration shall be duly substantiated on the basis of objective elements, such as the enforceability of trade secrets protection in third countries, the nature and level of confidentiality of the data requested, and the uniqueness and novelty of the connected product. It shall be provided in writing to the user without undue delay. ~~Where the data holder refuses to share data pursuant to this paragraph, it shall notify the competent authority designated pursuant to Article 37~~. […] ~~12. Where the user is not the data subject whose personal data is requested, any personal data generated by the use of a connected product or related service shall be made available by the data holder to the user only where there is a valid legal basis for processing under Article 6 of Regulation (EU) 2016/679 and, where relevant, the conditions of Article 9 of that Regulation and of Article 5(3) of Directive 2002/58/EC are fulfilled.~~ 13. A data holder shall only use any readily available data that is non-personal data on the basis of a contract with the user. A data holder shall not use such data to derive insights about the economic situation, assets and

Commission proposal	Drafting suggestions and Comments
	production methods of, or the use by, the user in any other manner that could undermine the commercial position of that user on the markets in which the user is active. 14. Data holders shall not make available non-personal product data to third parties for commercial or non-commercial purposes other than the fulfilment of their contract with the user. Where relevant, data holders shall contractually bind third parties not to further share data received from them. DE (Comments): **DE**: Remove notification obligations for data holders under Art. 4 para. 8 sentence 4.

Commission proposal	Drafting suggestions and Comments
	DE: clear delineation of material scopes of Data Act and Data Protection law, also see remarks to Article 1 paragraph 5 above.

Commission proposal	Drafting suggestions and Comments
	DE: Evaluation of the necessity of contractual requirements in the Data Act for the use and sharing of non-personal data with third parties, including the obligation to define purposes in advance (Art. 4(13) Sentence 1, (14)). FI (Drafting suggestions): '8. In exceptional circumstances, where the data holder who is a trade secret holder is able to demonstrate that, despite the technical and organisational measures taken by the user pursuant to paragraph 6 of this Article, it is ~~highly~~ likely to suffer serious economic damage from the disclosure of trade secrets or that the disclosure of trade secrets to the user poses a high risk of unlawful acquisition, use, or disclosure to third country entities, or entities established in the Union under the direct or indirect control of such entities, which are subject to jurisdictions offering weaker or non-equivalent protection compared to that under Union law, that data holder may refuse on a case-by-case basis a request for access to the specific data in question… FI (Comments): FI: We propose deleting the term *'highly'* to ensure a more proportionate burden of proof. FR (Drafting suggestions): '8. ~~In exceptional circumstances, w~~ **W**here 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

Commission proposal	Drafting suggestions and Comments
	disclosure of trade secrets or that the disclosure of trade secrets to the user poses a high risk of unlawful acquisition, use, or disclosure to third country entities, or entities established in the Union under the direct or indirect control of such entities, which are subject to jurisdictions offering weaker or non-equivalent protection compared to that under Union law, that data holder may refuse ~~on a case-by-case basis~~ a request for access to the specific data in question. That demonstration **may** ~~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.'; FR (Comments): In line with the principle that trade secrets shall be preserved and should not, by design, be disclosed, we propose the deletion of the wording "in exceptional circumstances". In coherence with the strenghthening objectives of the Data Act, France considers that the refusal process should not create supplementary administrative or technical burden for trade secret holders. We propose to replace "should" by "may", in so far as the current wording creates unnecessary administrative and technical burden which is absolutely not compatible with day-to-day data sharing practices, especially in B2B relations. Moreover, since the refusal cannot exceed the scope of the request, the wording "on a case by cas basis" is redondant and should be deleted.

Commission proposal	Drafting suggestions and Comments
	LU (Comments): The Data Act provides users with a right to access data related to their use of a connected product and associated services, as well as the right to request that such data be transmitted to a data recipient. The data holder may refuse access by invoking trade secret protection. This safeguard is commonly referred to as the "trade secret hand brake." The Data Omnibus strengthens this mechanism by adding further provisions allowing the hand brake to be invoked, in particular when the requested data transfer would be made to an entity established in a jurisdiction whose level of data or trade secret protection is weaker or not equivalent to that of the EU. The objective is to prevent international transfers from undermining the confidentiality of sensitive information. Luxembourg welcomes this proposal, which reinforces the protection of trade secrets. SI (Comments): Regarding trade secrets mechanism, SI generally supports the introduction of clearer and well-defined safeguards. However, we express reservations where provisions are insufficiently precise or could, in practice, weaken the protection of confidential data.
4. in Article 5, paragraph 11 is replaced by the following:	DE (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
	Article 5 […] 10. Where there is no agreement on the necessary measures referred to in paragraph 9 of this Article or if the third party fails to implement the measures agreed pursuant to paragraph 9 of this Article or undermines the confidentiality of the trade secrets, the data holder may withhold or, as the case may be, suspend the sharing of data identified as trade secrets. The decision of the data holder shall be duly substantiated and provided in writing to the third party without undue delay. ~~In such cases, the data holder shall notify the competent authority designated pursuant to Article 37 that it has withheld or suspended data sharing and identify which measures have not been agreed or implemented and, where relevant, which trade secrets have had their confidentiality undermined.~~ DE (Comments): **DE**: Remove notification obligations for data holders under Art. 5 para. 10 sentence 3.
'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	DE (Drafting suggestions): 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,

Commission proposal	Drafting suggestions and Comments
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.’;	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.~~ DE (Comments): **DE**: Remove notification obligations for data holders under Art. 5 para. 11 sentence 4. DK (Drafting suggestions): ‘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.’

Commission proposal	Drafting suggestions and Comments
	The Commission shall issue guidance, in consultation with the European Data Innovation Board (EDIB), on the application of this paragraph, including on the assessment of serious economic damage, the evaluation of risks relating to third-country jurisdictions, and the proportionality of refusal decisions. DK (Comments): We would welcome further guidance from the Commission on what constitutes 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. Guidance could serve to assist both data holders and authorities on when a data holder can legally refuse a request for data access. EL (Comments): We welcome the strengthening of trade secret protection against third-country risks. However, the standard of "weaker or non-equivalent protection" may not provide sufficient legal certainty for uniform application across Member States. In the absence of a common benchmark, national competent authorities risk diverging in their assessment of refusal notifications, while data recipients, particularly SMEs, may face unjustified restrictions on access. We would therefore welcome the timely adoption of Commission guidance clarifying the burden of proof incumbent on data holders and the procedural role of competent authorities in reviewing refusals. Aggregated reporting on the use of this provision would further enable the Commission to monitor whether it is applied proportionately and does not become a

Commission proposal	Drafting suggestions and Comments
	means of circumventing the data access rights established by the Regulation. FR (Drafting suggestions): 11. ~~In exceptional circumstances, w~~ **W**here 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 **may** ~~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.'; FR (Comments): In line with the principle that trade secrets shall be preserved and should not, by design, be disclosed, we propose the deletion of the wording "in exceptional circumstances".

Commission proposal	Drafting suggestions and Comments
	In coherence with the strenghthening objectives of the Data Act, France considers that the refusal process should not create supplementary administrative or technical burden for trade secret holders. We propose to replace "should" by "may", in so far as the current wording creates unnecessary administrative and technical burden which is absolutely not compatible with day-to-day data sharing practices, especially in B2B relations. Moreover, since the refusal cannot exceed the scope of the request, the wording "on a case by cas basis" is redondant and should be deleted.
5. the title of Chapter V is replaced by the following:	DE (Comments): **DE**: Evaluation of the necessity of contractual requirements in the Data Act for the use and sharing of non-personal data with third parties, including the obligation to define purposes in advance (Art. 6(1), (2)(c)).
'MAKING DATA AVAILABLE TO PUBLIC SECTOR BODIES, THE COMMISSION, THE EUROPEAN CENTRAL BANK AND UNION BODIES ON THE BASIS OF A PUBLIC EMERGENCY';	DE (Drafting suggestions): Article 11 1. A data holder may apply appropriate technical protection measures, including ~~smart contracts and~~ encryption, to prevent unauthorised access to data, including metadata, and to ensure compliance with Articles 4, 5, 6, 8 and 9, as well as with the agreed contractual terms for making data available. Such technical protection measures shall not discriminate between data recipients or hinder a user's right to obtain a copy of, retrieve, use or access data, to provide data to third parties pursuant to Article 5 or any right of a third party under Union law or national legislation adopted in accordance

Commission proposal	Drafting suggestions and Comments
	with Union law. ~~Users, third parties and data recipients shall not alter or remove such technical protection measures unless agreed by the data holder.~~ […] DE (Comments): **DE**: Removal in Art. 11 para. 1 Sentence 1 Data Act follows the removal of smart contracts form the scope of Data Act (see Art. 36 Data Act). Removal of Art. 11 para. 1 Sentence 3 Data Act to avoid double regulation with the so-called hacker clause under the Council of Europe's Cybercrime Convention and to prevent undue restrictions on legitimate interests of security researchers. FI (Comments): FI: We draw the Presidency's attention to the recommendations of the EDPB and EDPS in their joint opinion (section 12 of the opinion) with regards to Chapter V. NL (Drafting suggestions): ~~**'MAKING DATA AVAILABLE TO PUBLIC SECTOR BODIES, THE COMMISSION, THE EUROPEAN CENTRAL BANK AND UNION BODIES ON THE BASIS OF A PUBLIC EMERGENCY';**~~ PL (Drafting suggestions): **Comment to the whole Chapter V: We would like to revert to the original wording – to keep the broader scope of "exceptional need" instead of limiting to "public emergency"**

Commission proposal	Drafting suggestions and Comments
	PL (Comments): Limiting public sector access to data held by private entities (B2G) only to "public emergency" situations would significantly reduce the situations in which the public sector can effectively use private sector data, thereby restricting its availability and potential for public tasks. Simplifying the provisions of Chapter V should not come at the expense of restricting public sector access to privately held data, especially given that such access is already significantly limited. Chapter V reflects a legislative compromise agreed upon by all Member States, and Poland has consistently emphasized the need to increase, rather than limit, access to private sector data for the purposes of the public interest. SI (Comments): Regarding Business to Government data sharing (Chapter V) SI considers that the distinction between "response to a public emergency" and "mitigation of or recovery from a public emergency" remains insufficiently clear and requires further clarification. Greater precision would also help delineate the circumstances in which a competent authority may request access to personal data. In our view, access to personal data for the purposes of "mitigation of or recovery from a public emergency" should, as a general rule, not be permitted.
6. Articles 14 and 15 are deleted;	DE (Comments):

Commission proposal	Drafting suggestions and Comments
	DE: Articles 14 and 15 are to be deleted in accordance with paragraphs 6 and 7 of the draft regulation and merged into a new Article 15a. From a regulatory perspective, this raises the question of whether/why there should be Articles 14/15 with new content in the future. There is no reason apparent to us for this. Hence, after Art. 13 it should continue with Article 14, instaed of 15a. **DE**: Article 13: Content control pursuant to Article 13(1) Data Act only applies to a section of the contract, namely to "contract clauses relating to data access and data use" and "liability and remedies in the event of a breach or termination of data-related obligations." According to the wording of the provision, this applies regardless of whether data is the main subject matter of the contract (as in contracts governed by Article 4 et seq. Data Act) or not. Contracts for the purpose of Article 4 et seq. Data Act. As a fully harmonizing legal act, this provision supersedes national law in this respect. Clauses within the material scope of Article 13 Data Act must therefore be reviewed solely on the basis of this provision. On the other hand, those parts of a contract that do not fall under Art. 13 Data Act can be reviewed on the basis of national regimes, which may lead to a division of the review regimes. **DE**: Article 13(6) the reference to "unilaterally imposed" should be adapted to the the Unfair Terms Directive; it is doubtful to create a legislative incentive to negotiate clauses; this likely amounts to favoring powerful market participants and disadvantaging weak negotiators: A clause is "unilaterally imposed" according to Art. 13(6) sentence 1 Data Act if (1) an attempt at negotiation has been made and nevertheless (2) no possibility of influencing the clause by the contractual partner can be affirmed. Recital 59

Commission proposal	Drafting suggestions and Comments
	Data Act clarifies that "contractual clauses that are merely introduced by one party and accepted by the other undertaking, or clauses that are negotiated between the contracting parties and subsequently agreed in amended form, [...] are not considered to be unilaterally imposed." The deviation from the Unfair Terms Directive – under which provisions that have "not been individually negotiated" can be reviewed – is striking. The Unfair Terms Directive also stipulates that only provisions that "were drafted in advance and which the consumer was therefore unable to influence, in particular in the context of a pre-formulated standard contract" can be reviewed. However, the characteristic of influence is more fluid and does not require the formal act of an attempt at negotiation. Apart from the fact that the different standards for distinguishing between general terms and conditions and individual agreements are detrimental to the coherence of European contract law, this restriction—which was already criticized during the legislative process—is also not convincing in all constellations. The idea that the other party must attempt to negotiate in order to benefit from clause control is questionable in view of the protective purpose of standard terms and conditions law, since, for example, information asymmetries can also lead to unfair terms in business-to-business transactions. The restriction is taken to absurdity in the case of online contracts, where the contract is concluded by clicking a "button." In this case, the other party has effectively been given no opportunity to negotiate the terms and conditions and, according to the wording of the provision, is nevertheless not entitled to benefit from content control. This is questionable from a legal policy perspective, even if one considers the aim of the regulation, which is to enable companies to conclude standard contracts in mass transactions. At the very least, Article 13 Data Act must therefore apply analogously if no negotiation is possible (or if very high barriers to such negotiation are

Commission proposal	Drafting suggestions and Comments
	erected), since such a scenario can also be classified as a "take-it-or-leave-it scenario."
7. the following Article 15a is inserted:	LU (Comments): Luxembourg favours a scope for the Business-to-Government data-sharing provisions in Chapter V of the Data Act, that reduce administrative burden and preserve greater autonomy for Member States when organising such mechanisms. Chapter V of the Data Act could be an opportunity to build an ecosystem for Business-to-Government data sharing in case of "exceptional need" That being said, the practical relevance of Article 15(1)(i) in its current form makes it difficult to identify whether situations are covered in practice by the notion of 'exceptional need'. It also observes that the practical relevance of Article 15(1)(i) insofar as it refers to "*fulfilling a specific task carried out in the public interest, that has been explicitly provided for by law*" is unclear, as it is difficult to identify concrete situations that would realistically fall within its scope. NL (Drafting suggestions): ~~7. the following Article 15a is inserted:~~
'Article 15a	EL (Comments): We appreciate the simplification of the B2G data-sharing framework and note that the revised Statistics Regulation may address the needs of the statistical community. However, the elimination of the non-emergency exceptional need ground also removes the legal basis for compulsory access to privately-held digital datasets for other public-interest tasks, such as environmental protection, evidence-based policymaking,

Commission proposal	Drafting suggestions and Comments
	and public health, for which no alternative compulsory horizontal instrument exists. We would therefore suggest retaining the non-emergency ground for non-personal data, with its existing safeguards intact, for public-interest tasks beyond official statistics. NL (Drafting suggestions): ~~'Article 15a~~
Obligation for data holders to make data available on the basis of a public emergency	DE (Comments): **DE**: The limitation to public emergencies is to be strongly supported. We have rather technical comments without questioning the goal of the amendment. Generally, we see the practical relevance for Chapter V to be rather limited. Due to the effective limitation to public emergencies, it could be considered whether the detailed substantiation requirements and waiting periods are neccesssary. These requirements seem to counteract the practical application of the B2G access under the Data Act in cases of – urgent – public emergencies with high impact on important fundamental rights. Currently we do not see any practical application that cannot, more effectively be covered by national, domain specific access rights. NL (Drafting suggestions): ~~*Obligation for data holders to make data available on the basis of a public emergency*~~
1. Where a public sector body, the Commission, the European Central Bank or a Union body demonstrates an exceptional need to use certain data to carry out its statutory duties in the public interest when responding to,	DE (Comments):

Commission proposal	Drafting suggestions and Comments
mitigating, or supporting the recovery from a public emergency, it may request from data holders that are legal persons, other than public sectors bodies, to make available those data, including the metadata necessary to interpret and use those data. Upon such duly reasoned request, data holders shall make the data and metadata available to the requesting public sector body, the Commission, the European Central Bank or Union body. Such requests may also be made where the production of official statistics is required in relation to a public emergency.	**DE**: Paragraph 1 as the basis for the access request could be formulated more clearly, inparticular: • define authorized body; • exceptional need: could be defined (should be assessed from an ex ante perspective based on available information; instead of "demonstrate," which is already covered by Art. 17 and concerns the formal requirements of the request, not its substantive conditions); • covered purposes (respond, mitigate, or support recovery); • the scope could be limited by defining what is meant by data; currently it is extremely broad, unclear what could be covered; • statistics should be treated separately FR (Drafting suggestions): 1. Where a public sector body, the Commission, the European Central Bank or a Union body demonstrates an exceptional need to use certain data to carry out its statutory duties in the public interest when responding to, mitigating, or supporting the recovery from a public emergency, it may request from data holders that are legal persons, other than public sectors bodies, to make available those data, including the metadata necessary to interpret and use those data. Upon such duly reasoned request, data holders shall make the data and metadata available to the requesting public sector body, the Commission, the European Central Bank or Union body. Such requests may also be made where the production of official statistics is required in relation to a public emergency. FR (Comments): On the whole chapter V :

Commission proposal	Drafting suggestions and Comments
	French authorities express serious concerns about the amendments proposed by the Commission to Chapter V of the Data Act. The consequences of these multiple amendments - which appear to be semantic, raise serious questions related to the rights of State Member authorities to determine the terms and conditions for deciding "public emergencies". France expresses concerns on the conditions and legal frameworks under which the article could allow European Union bodies and institutions to request data, including personal data, from private companies in Member States without the latter's consent and when no state of emergency has been declared by the Member State. France would oppose any transfer of this power to a Union institution or body outside the existing frameworks, as it is up to Member States to determine when an emergency situation exists and to declare it in accordance with their national law. For reasons related to defense and national security, France would oppose the application of this article, particularly when the request concerns an operator whose status and monitoring constitute, under the law of the Member States, classified information protected by national defense secrecy. This is particularly the case for operators concerned by the application of the provisions of Directive (EU) 2022/2557 NL (Drafting suggestions): ~~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,~~

Commission proposal	Drafting suggestions and Comments
	~~mitigating, or supporting the recovery from a public emergency, it may request from data holders that are legal persons, other than public sectors bodies, to make available those data, including the metadata necessary to interpret and use those data. Upon such duly reasoned request, data holders shall make the data and metadata available to the requesting public sector body, the Commission, the European Central Bank or Union body. Such requests may also be made where the production of official statistics is required in relation to a public emergency.~~
2. Where the data requested are necessary to respond to a public emergency, and the requesting body pursuant to paragraph 1 is unable to obtain such data by other means in a timely and effective manner under equivalent conditions, the request shall concern non-personal data. Where the provision of non-personal data is insufficient to address the public emergency, personal data may also be requested and, where possible, made available in pseudonymized form, subject to appropriate technical and organisational measures to ensure their protection.	DE (Comments): **DE**: Regarding collectively paragraphs 2 and 3: • First, it is unclear what the difference is between exceptional need and 'necessary' • Examination of whether the definition in Article 2, point 29 Data Act of public emergency should be tightened up, as very different cases are mentioned here; e.g., the substantial and immediate deterioration of economic goods. FI (Comments): FI: Contrary to what is suggested in the EDPB/EDPS opinion (section 123 and 124), we would retain the current wording as where possible' ensures that the competent authority can appropriately account for special circumstances when carrying out its supervisory functions. It is important that the interpretation of 'where possible' remains very narrow but we would rather clarify what 'where possible' means or to whom it applies than remove it completely. IT

Commission proposal	Drafting suggestions and Comments
	(Drafting suggestions): 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. IT (Comments): In line wiht the principle of data minimisation pusuant to art. 5 GDPR, data should only be provided in pseudonymised form to requesting bodies, and only when non-personal data is demonstrated to be insufficient to respond to the exceptional need to use the data (see Article 17(2)(e) of the current Data Act). This would also align with Article 18(4) current Data Act, which provides that where the data requested includes personal data, the data holder shall anonymise the data, unless the compliance with the request to make data available to a requesting body requires the disclosure of personal data. In such cases, the data holder shall pseudonymise the data We would recommend clarifying the difference between 'responding to a public emergency' and 'mitigating or supporting the recovery from [a public emergency' so as to ensure clarity about the circumstances in which access to personal data in pseudonymised form can be requested by the requesting body, as access to pseudonymised personal data would not be possible in case of 'mitigation or supporting the recovery from a public emergency NL (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
	~~2. Where the data requested are necessary to respond to a public emergency, and the requesting body pursuant to paragraph 1 is unable to obtain such data by other means in a timely and effective manner under equivalent conditions, the request shall concern non-personal data. Where the provision of non-personal data is insufficient to address the public emergency, personal data may also be requested and, where possible, made available in pseudonymized form, subject to appropriate technical and organisational measures to ensure their protection.~~
3. Where the data requested are necessary to mitigate or support the recovery from a public emergency, a requesting body pursuant to paragraph 1 acting on the basis of Union or national law, may request specific non-personal data, the lack of which prevent it from mitigating or supporting the recovery from a public emergency. Such requests shall not be made to microenterprises and small enterprises.'; 	NL (Drafting suggestions): ~~3. Where the data requested are necessary to mitigate or support the recovery from a public emergency, a requesting body pursuant to paragraph 1 acting on the basis of Union or national law, may request specific non-personal data, the lack of which prevent it from mitigating or supporting the recovery from a public emergency. Such requests shall not be made to microenterprises and small enterprises.';~~
8. in Article 16, paragraph 2 is replaced by the following: 	NL (Drafting suggestions): **Article 16 is deleted**
'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.'	NL (Drafting suggestions): ~~'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:	NL

Commission proposal	Drafting suggestions and Comments
	(Drafting suggestions): **Article 17 is deleted**
(a) paragraph 1 is amended as follows:	NL (Drafting suggestions): ~~(a) paragraph 1 is amended as follows:~~
(i) the introductory wording is replaced by the following:	NL (Drafting suggestions): ~~(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:';	NL (Drafting suggestions): ~~'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:	NL (Drafting suggestions): ~~(ii) points (b) and (c) are replaced by the following:~~
'(b) demonstrate that the conditions to make a request under Article 15a are met;	DE (Drafting suggestions): (b) demonstrate that the conditions ~~to make a~~ **for the** request under Article 15a are met; DE (Comments): **DE**: should be edited to read "[for] the request" instead of "[...] to make a request," as the request should not always be unlawful if the conditions were incorrectly assumed; NL

Commission proposal	Drafting suggestions and Comments
	(Drafting suggestions): ~~'(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;';	NL (Drafting suggestions): ~~(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:	NL (Drafting suggestions): ~~(b) paragraph 2 is amended as follows:~~
(i) point (c) is replaced by the following:	NL (Drafting suggestions): ~~(i) point (c) is replaced by the following:~~
'(c) be proportionate to the public emergency and duly justified, regarding the granularity and volume of the data requested and the frequency of access to the data requested;';	NL (Drafting suggestions): ~~'(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.;	IT (Drafting suggestions): **(iii) point (i) is repalced by the following:** **where personal data are requested, be notified without undue delay to the supervisory authority responsible for monitoring the application of Regulation (EU) 2016/679 in the Member State where the public sector**

Commission proposal	Drafting suggestions and Comments
	body is established or to the EDPS where the request is made by the Commission, the European Central Bank or a Union body IT (Comments): Article 17(2)(i) of the current Data Act provides that where personal data are requested, public sector bodies must inform the supervisory authority of the Member State in which the public sector body is established, whereas the ECB and Union bodies must inform the Commission of their requests. To promote coherence and to ensure that the EDPS can effectively exercise its responsibilities as responsible authority pursuant to Article 37(3) of the current Data Act, we recommend amending this Article so that it provides that the Commission, the ECB and Union Bodies must also notify the EDPS – as the European counterpart for national supervisory authorities – of their requests for data NL (Drafting suggestions): ~~(ii) point (e) is deleted.;~~
(c) paragraphs 5 and 6 are deleted;	NL (Drafting suggestions): ~~(c) paragraphs 5 and 6 are deleted;~~
10. Article 18 is amended as follows:	NL (Drafting suggestions): **10. Article 18 is deleted**
(a) in paragraph 2, the introductory wording is replaced by the following:	IT (Drafting suggestions): **(aa) paragraph 1 is replaced as follows:** **A data holder receiving a request to make data available under this Chapter shall make the data available to the requesting public sector**

Commission proposal	Drafting suggestions and Comments
	body, the Commission, the European Central Bank or a Union body without undue delay, implementing the necessary technical, organisational and legal measures IT (Comments): We recommend specifying that data holders must implement the necessary technical, organisational and legal measures referred to Article 18(1) of the current Data Act, rather than simply 'taking them into account'. This also would correspond with their duty to anonymise or pseudonymise data upon request by public sector bodies concerning personal data pursuant to Article 18(4) of the current Data Act NL (Drafting suggestions): ~~(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:';	NL (Drafting suggestions): ~~'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;	NL (Drafting suggestions): ~~(b) paragraph 5 is deleted;~~
11. Article 19 is amended as follows:	NL

Commission proposal	Drafting suggestions and Comments
	(Drafting suggestions): **11. Article 19 is deleted**
(a) in paragraph 1, the introductory wording is replaced by the following:	NL (Drafting suggestions): ~~(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:';	NL (Drafting suggestions): ~~'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:	NL (Drafting suggestions): ~~(b) paragraph 3 is replaced by the following~~:
'3. Disclosure of trade secrets to a public sector body, the Commission, the European Central Bank or a Union body shall be required only to the extent that it is strictly necessary to achieve the purpose of a request under Article 15a. In such a case, the data holder or, where they are not the same person, the trade secret holder shall identify the data which are protected as trade secrets, including in the relevant metadata. The public sector body, the Commission, the European Central Bank or the Union body shall, prior to the disclosure of trade secrets, take all necessary and appropriate technical and organisational measures to preserve the confidentiality of the trade secrets, including, as appropriate, the use of model contractual terms, technical standards and the application of codes of conduct.';	FR (Comments): France expresses concerns on the preservation of trade secrets. NL (Drafting suggestions): ~~'3. Disclosure of trade secrets to a public sector body, the Commission, the European Central Bank or a Union body shall be required only to the extent that it is strictly necessary to achieve the purpose of a request under Article 15a. In such a case, the data holder or, where they are not the same person, the trade secret holder shall identify the data which are protected as trade secrets, including in the relevant metadata. The public sector body, the Commission, the European Central Bank or the Union body shall, prior to the disclosure of trade secrets, take all necessary and appropriate technical and organisational measures to preserve the confidentiality of the trade secrets,~~

Commission proposal	Drafting suggestions and Comments
	~~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:	NL (Drafting suggestions): **12. Article 20 is deleted**
'Article 20	NL (Drafting suggestions): ~~'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.	NL (Drafting suggestions): ~~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.	NL (Drafting suggestions): ~~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.~~

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.	NL (Drafting suggestions): ~~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.'; 	NL (Drafting suggestions): ~~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:	NL (Drafting suggestions): **13. Article 21 and 22 is deleted**
(a) the heading is replaced by the following:	NL (Drafting suggestions): ~~(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**';	NL (Drafting suggestions): ~~'**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:	NL (Drafting suggestions): ~~(b) paragraph 5 is replaced by the following:~~

Commission proposal	Drafting suggestions and Comments
'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:	NL (Drafting suggestions): ~~'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;	NL (Drafting suggestions): ~~(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;	NL (Drafting suggestions): ~~(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;	NL (Drafting suggestions): ~~(c) the period for which the data is to be used and the technical protection;~~
(d) the organisational measures taken, including where personal data or trade secrets are involved.';	NL (Drafting suggestions): ~~(d) the organisational measures taken, including where personal data or trade secrets are involved.';~~ PL (Drafting suggestions): to reinstate, after the par. (5), par. (6): **6. The Commission shall develop a model template for requests pursuant to this Article.**

Commission proposal	Drafting suggestions and Comments
	PL (Comments): The model template for requests for data is the key element of the B2G data exchange system and can help streamline this process for both the public and private sectors. It is also important in the context of the primary objective of Data Act Regulation which is the harmonisation of the data market, including reducing its fragmentation and ensuring fair access to data for market participants. Failing to develop the model template may lead to additional barriers in the area of B2G data exchange.
14. The following Article 22a is inserted before Chapter VI:	NL (Drafting suggestions): ~~14. The following Article 22a is inserted before Chapter VI:~~
'Article 22a	NL (Drafting suggestions): ~~'Article 22a~~
Right to lodge a complaint	IT (Comments): The inclusion of this provision outside of the horizontal Chapter IX Data Act raises questions on the applicability of the new Art. 38(2)–(3) Data Act. Therefore, we recommend clarifying the relationship between this provision and the new Art. 38 Data Act, or merging the new Art. 22a and the new Art. 38 Data Act to ensure legal certainty. NL (Drafting suggestions): ~~*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	DE (Comments):

Commission proposal	Drafting suggestions and Comments
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.’;	**DE**: It should be the exclusive legislative authority of the member states to determine the competent authority for request according to Article 15a, in particular to designate authorities other than those pursuant to Article 37. NL (Drafting suggestions): ~~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.’;~~ PL (Drafting suggestions): Where a dispute arises concerning ~~a request for data under Article 15a~~ **any issue under Chapter V** ~~, 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.’; PL (Comments): We suggest to extend the right to lodge a complaint on all articles from Chapter V, and not only article 15a.
15. in Article 31, the following paragraphs 1a and 1b are inserted:	DE (Drafting suggestions): ~~Article 28~~

Commission proposal	Drafting suggestions and Comments
	~~1. Providers of data processing services shall make the following information available on their websites, and keep that information up to date:~~ ~~(a) the jurisdiction to which the ICT infrastructure deployed for data processing of their individual services is subject;~~ ~~(b) a general description of the technical, organisational and contractual measures adopted by the provider of data processing services in order to prevent international governmental access to or transfer of non-personal data held in the Union where such access or transfer would create a conflict with Union law or the national law of the relevant Member State.~~ ~~2. The websites referred to in paragraph 1 shall be listed in contracts for all data processing services offered by providers of data processing services.~~ Article 29 […] 5. Where relevant, providers of data processing services shall provide information to a customer on **circumstances that hinder the switching of** data processing services ~~that involve highly complex or costly switching or for which it is impossible to switch without significant interference in the data, digital assets or service architecture.~~ ~~6. Where applicable, providers of data processing services shall make the information referred to in paragraphs 4 and 5 publicly available to customers via a dedicated section of their website or in any other easily accessible way.~~ DE (Comments): **DE**: Remove information obligations for data processing services under Art. 28.

Commission proposal	Drafting suggestions and Comments
	DE: Simplify information obligations of providers of data processing services under Art. 29 para. 5 and 6 to the extent that providers should be generally required to inform about circumstances that hinder switching. DK (Drafting suggestions): Chapter VI SWITCHING BETWEEN DATA PROCESSING SERVICES Article 23 Removing obstacles to effective switching Providers of data processing services shall take the measures provided for in Articles 25, 26, 27, 29 and 30 to enable customers to switch to alternative data

Commission proposal	Drafting suggestions and Comments
	processing services of the same service type (as defined in article 2), or to on-premises ICT infrastructure, or to use multiple providers in parallel. Providers shall not impose or maintain undue pre-contractual, commercial, technical, organisational barriers to such switching. In particular, providers shall not inhibit customers from: (a) terminating the existing service contract after the maximum notice period and successful completion of the switching process; (b) entering a new contract for the same service type with a different provider; (c) porting the customer's exportable data and digital assets, to a different provider or to an on-premises ICT infrastructure, including any data obtained under a free-tier offering; (d) Achieving functional equivalence of service capabilities in the new environment of a different provider in accordance with Article 24; and (e) Where technically feasible, unbundling the services being switched as referred to in Article 30(1) from any other co-hosted services by the source provider. Article 24 Scope of the technical obligations The obligations of in Articles 23, 25, 29, 30 and 34 shall apply only to the source provider of the data processing services including the provider from whom the customer is switching. No other party - including the destination provider(s) - shall be subject to these specific obligations except where explicitly stated. Article 25 Contractual terms concerning switching 1. The rights and obligations of the customer and the provider relating to service switching including to on-premises are clearly specified in the contract. The contract must be in writing and made available to the customer in a way that allows the customer to store and reproduce the contract prior to signing.

Commission proposal	Drafting suggestions and Comments
	2. Without prejudice to Directive (EU) 2019/770, the contract referred to in paragraph 1 of this Article shall include at least the following: (a) Switching rights and assistance. Clauses allowing the customer, upon request, the right to switch to a different provider or to port all exportable data and digital assets to an on-premises ICT infrastructure, without undue delay and in any event not after the mandatory maximum transitional period of 30 calendar days, to be initiated after the maximum notice period referred to in point (d), During the notice and transitional periods, the source provider shall: (i) provide reasonable assistance to the customer and third parties authorised by the customer in the switching process. (ii) act with due care to maintain business continuity, and continue all contracted functions and services; (iii) inform the customer of any known risks to continuity in the provision of the functions or services on the part of the source provider of data processing services; (iv) ensure a high level of security is maintained throughout the switching process, in particular the security of the data during their transfer and the continued security of the data during the retrieval period specified in point (g), in accordance with applicable Union or national law; (b) Exit support. An obligation of the provider to support the customer's exit strategy relevant to the contracted services, including by providing all relevant information; (c) Termination and switching. A clause specifying that the contract shall be considered terminated, and the customer shall be notified of the termination, in either of the following cases: (i) Upon the successful completion of the switching process; or (ii) at the end of the maximum notice period, where the customer does not wish to switch but to erase its exportable data and digital assets;

Commission proposal	Drafting suggestions and Comments
	(d) Notice period. A clause specifying that the maximum notice period for initiating the switching process, which shall not exceed two months. (e) Data specification. an exhaustive specification of all categories of data and digital assets that can be ported during the switching process, including, at a minimum, all "exportable data" as defined in Article 2(38).; (f) Portability exemptions. An exhaustive list of any categories of data specific to the provider's internal functioning that are exempt on the grounds of protecting trade secrets. Any such exemptions must be strictly necessary and must not delay or prevent the switching process. ; (g) Retrieval period. A clause guaranteeing a minimum period for data retrieval of at least 30 calendar days, commencing after the agreed transitional period. During this period the customer can continue to access and download its data from the old service environment.; (h) Data deletion. A clause guaranteeing full erasure of all exportable data and digital assets generated by or relating to the customer, after the retrieval period has expired (or any later agreed date), provided that the switching process has been successfully completed. This ensures the customer's data is deleted (including from backups) once it is no longer needed; (i) Switching charges. A clear statement of any charges for the switching process that may be imposed by provider, which must comply with Article 29. 3. The contract shall include clauses allowing the customer to notify the provider, upon expiry of the notice period of its intended action. Specifically, the customer may indicate whether it will: (a) switch to a different provider, in which case the customer shall provide the necessary details of that provider; (b) switch to an on-premises ICT infrastructure; (c) erase its exportable data and digital assets.

Commission proposal	Drafting suggestions and Comments
	4. If the mandatory maximum transitional period as provided for in paragraph 2, point (a) is technically unfeasible, the provider shall notify the customer within 14 working days of the switching request, and shall duly justify the technical unfeasibility and indicate an alternative transitional period, which shall not exceed seven months. In accordance with paragraph 1, service continuity shall be ensured throughout the alternative transitional period. 5. Without prejudice to paragraph 4, the customer may extend the transitional period once, for an additional period that the customer deems necessary for its own purposes. Article 26 Information obligation of providers of data processing services The provider of data processing services shall provide the customer with easily accessible information on available procedures for switching and porting data. Specifically, providers shall ensure that the information under points (a) and (b) is presented in a clear and concise manner, using plain language: (a) This includes descriptions of all available procedures for switching and porting methods, including information on available switching and porting methods and formats as well as any known technical limitations or constraints on portability. ; (b) a reference to an up-to-date online register hosted by the provider of data processing services, with details of all the data structures and data formats as well as the relevant standards and open interoperability specifications, in which the exportable data referred to in Article 25(2), point (e), are available. Article 27 Obligation of good faith All parties involved in a switching process, including the source and destination providers, and the customer shall cooperate in good faith to make the switching process effective. Each party shall act to enable the timely transfer of data and maintenance of the continuity of the data processing service during the transition.

Commission proposal	Drafting suggestions and Comments
	Article 28 Contractual transparency obligations on international access and transfer 1. Providers of data processing services shall make the following information available on their websites, and keep that information up to date: (a) the jurisdiction(s) governing the ICT infrastructure used for data processing of each individual service: ; (b) a general description of the technical, organisational, and contractual measures adopted by the providers in order to prevent international governmental access to or transfer of non-personal data held in the Union where such access or transfer would create a conflict with Union law or the national law of the relevant Member State. 2. The websites referred to in paragraph 1 shall be listed in contracts for all data processing services offered by providers. Article 29 Gradual withdrawal of switching charges 1. From 12 January 2027, providers of data processing services shall not impose any switching charges on the customer for the switching process. 2. From 11 January 2024 to 12 January 2027, providers of data processing services may impose reduced switching charges on the customer for the switching process. 3. The reduced switching charges referred to in paragraph 2 shall not exceed the costs incurred by the provider of data processing services that are directly linked to the switching process concerned. 4. Before entering into a contract with a customer, providers of data processing services shall provide the prospective customer with clear information on the standard service fees and early termination penalties that might be imposed, as

Commission proposal	Drafting suggestions and Comments
	well as on the reduced switching charges that might be imposed during the timeframe referred to in paragraph 2. 5. Where relevant, providers of data processing services shall provide information to a customer on data processing services that involve highly complex or costly switching or for which it is impossible to switch without significant interference in the data, digital assets or service architecture. 6. Where applicable, providers of data processing services shall make the information referred to in paragraphs 4 and 5 publicly available to customers via a dedicated section of their website or in any other easily accessible way. 7. The Commission is empowered to adopt delegated acts in accordance with Article 45 to supplement this Regulation by establishing a monitoring mechanism for the Commission to monitor switching charges, imposed by providers of data processing services on the market to ensure that the withdrawal and reduction of switching charges, pursuant to paragraphs 1 and 2 of this Article are to be attained in accordance with the deadlines laid down in those paragraphs. Article 30 Technical aspects of switching 1. Providers of data processing services that concern scalable and elastic computing resources limited to infrastructural elements such as servers, networks and the virtual resources necessary for operating the infrastructure, but that do not provide access to the operating services, software and applications that are stored, otherwise processed, or deployed on those infrastructural elements, shall, in accordance with Article 27, take all reasonable measures in their power to facilitate that the customer, after switching to a service covering the same service type, achieves functional equivalence in the use of the destination data processing service. The source provider of data processing services shall facilitate the switching process by providing capabilities, adequate information, documentation, technical support and, where appropriate, the necessary tools.

Commission proposal	Drafting suggestions and Comments
	2. Providers of data processing services, other than those referred to in paragraph 1, shall make open interfaces available to an equal extent to all their customers and the concerned destination providers of data processing services free of charge to facilitate the switching process. Those interfaces shall include sufficient information on the service concerned to enable the development of software to communicate with the services, for the purposes of data portability and interoperability. 3. For data processing services other than those referred to in paragraph 1 of this Article, providers of data processing services shall ensure compatibility with common specifications based on open interoperability specifications or harmonised standards for interoperability at least 12 months after the references to those common specifications or harmonised standards for interoperability of data processing services were published in the central Union standards repository for the interoperability of data processing services following the publication of the underlying implementing acts in the Official Journal of the European Union in accordance with Article 35(8). 4. Providers of data processing services other than those referred to in paragraph 1 of this Article shall update the online register referred to in Article 26, point (b) in accordance with their obligations under paragraph 3 of this Article. 5. In the case of switching between services of the same service type, for which common specifications or the harmonised standards for interoperability referred to in paragraph 3 of this Article have not been published in the central Union standards repository for the interoperability of data processing services in accordance with Article 35(8), the provider of data processing services shall, at the request of the customer, export all exportable data in a structured, commonly used and machine-readable format. 6. Providers of data processing services shall not be required to develop new technologies or services, or disclose or transfer digital assets that are protected by

Commission proposal	Drafting suggestions and Comments
	intellectual property rights or that constitute a trade secret, to a customer or to a different provider of data processing services or compromise the customer's or provider's security and integrity of service. Article 31 Specific regime for certain data processing services 1. The obligations laid down in Article 23, point (d), Article 29 and Article 30(1) and (3) shall not apply to data processing services of which the majority of main features has been custom-built to accommodate the specific needs of an individual customer or where all components have been developed for the purposes of an individual customer, and where those data processing services are not offered at broad commercial scale via the service catalogue of the provider of data processing services. 2. The obligations laid down in this Chapter shall not apply to data processing services provided as a non-production version for testing and evaluation purposes and for a limited period of time. 3. Prior to the conclusion of a contract on the provision of the data processing services referred to in this Article, the provider of data processing services shall inform the prospective customer of the obligations of this Chapter that do not apply. DK (Comments): Apart from below suggestions to changes of the Commission's proposed article 31(1a), DK proposes to reformulate the original Chapter VI of the Data Act with the sole objective to make it more approachable and understandable.

Commission proposal	Drafting suggestions and Comments
	We have inserted the proposed text for Chapter VI here, as there are no additional rows provided for proposed additions. NL (Drafting suggestions): 15. in Article 31, the following paragraphs ~~1a,~~ ~~and~~ 1b, **1c and 1d** are inserted: SI (Comments): SI supports the proposal in Article 31(1a) and (1b) to exempt legacy custom-made solutions from the obligation to renegotiate contracts. This approach strikes an appropriate balance between consumer protection and market stability. Applying new and complex interoperability and switching obligations retroactively to bespoke contracts concluded years ago could create a disproportionate administrative burden and, for specialised providers, may be technically impracticable. SI therefore welcomes the distinction in the text: it ensures that financial lock-in, in particular switching fees, is removed immediately for all users, while the technical and contractual obligations apply prospectively, thereby preserving legal certainty for established contractual relationships.
‘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.	DK (Drafting suggestions): ‘‘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 **main** features ~~and functionalities of the data processing service~~ has been **custom-built to accommodate the specific needs of an individual** ~~adapted by the provider to the specific needs of~~ the customer, ~~**and where those data processing services are not offered at broad commercial scale via the service**~~

Commission proposal	Drafting suggestions and Comments
	~~**catalogue of the provider of data processing services**~~**,** if the provision of such services is based on a contract concluded before or on 12 September 2025. **The Commission shall issue guidelines, in consultation with the European Data Innovation Board (EDIB), to illustrate indicators for custom-built services, provide practical examples, and clarify assessment methods. These guidelines shall be updated as necessary to reflect technological developments, new service models, or emerging industry practices.** DK (Comments): The Data Act already has a description of a custom-built solution in Article 31, paragraph 1, which is the cause of legal uncertainty with regards to what constitutes a custom-made solution. Adding yet another and broader definition of a custom-built solution in the suggested Article 31 paragraph 1a could serve to create more legal uncertainty for both authorities and businesses. Hence, we note that it would be more prudent to utilise the existing description of a custom-built data processing service from Article 31 paragraph 1. We take note that Article 31 paragraph 1a with the corresponding recital 17 introduces a "majority of features adapted" test to define custom-made services, though without introducing objective parameters which bears risks of legal uncertainty. We suggest that the Commission issues guidelines to further clarify what constitutes a custom-built service. For further legal clarity, it would be prudent to add it in the listed definitions in Article 2, while further clarifying what constitutes a custom-built solution in the recitals.

Commission proposal	Drafting suggestions and Comments
	Finally, we believe that it may be an error that custom-made solutions are expressly not exempted from the rules regarding switching charges in Article 29 in the suggested paragraph 1a. Because in the original text, custom-made solutions are actually explicitly exempted from Article 29. It does not seem intentional that companies are supposed to gradually remove switching fees for existing contracts, while they are not obliged to gradually phase out switching fees in any new contracts. FR (Drafting suggestions): ~~'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.~~ FR (Comments): le règlement vise à garantir que les clients puissent changer de fournisseur de services de traitement de données dans des conditions effectives, sans interruption du service, ni obstacles injustifiés ou coûts de transfert excessifs, afin d'éviter des situations de dépendance durable vis-à-vis d'un prestataire. Cette exigence constitue un élément central de l'équilibre du texte, en vue de préserver une concurrence effective et de renforcer la protection des utilisateurs (y compris publics). Exclure les services autres que ceux visés à l'article 30 (1) irait donc à l'encontre de cette logique – d'autant que ces segments de marché présentent un risque structurel de verrouillage contractuel, les utilisateurs pouvant rencontrer des difficultés à changer de solution une fois intégrés dans un écosystème donné. Le cadre du règlement vise précisément à préserver des

Commission proposal	Drafting suggestions and Comments
	marges de manœuvre effectives pour les clients, afin d'éviter que les acteurs déjà établis ne bénéficient d'un avantage structurel susceptible de limiter l'accès au marché de solutions nouvelles, y compris potentiellement plus innovantes, et de fausser les conditions de concurrence. NL (Drafting suggestions): ~~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.~~ NL (Comments): The Netherlands does not see the merits of the proposed exemption for custom-made solutions. Due to the nature of the cloud market, a large share of offered services would fall under the exemption, thus leading to increased barriers to switching compared to the original Data Act text. This would hamper our efforts to boost portability and interoperability of data. Therefore, we would propose to delete this article.
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.	FR (Drafting suggestions): ~~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.~~ FR

Commission proposal	Drafting suggestions and Comments
	(Comments): Idem – d'autant que les fournisseurs de services ont eu un temps d'adaptation pour se mettre en conformité. NL (Drafting suggestions): ~~The provider of such data processing services shall not be required to renegotiate or amend a contract for the provision of those services before its expiry if that contract was concluded before or on 12 September 2025. Any contractual provision contained in that contract that is contrary to Article 29(1), (2), or (3) shall be considered null and void.~~
1b. A provider of a data processing service may include provisions on proportionate early termination penalties in a contract of fixed duration on the provision of data processing services other than those referred to in Article 30(1).	DE (Comments): **DE**: The possibility is provided for introducing an appropriate contractual penalty for early termination of fixed-term contracts for higher-value data processing services – this provision is to be welcomed as it extends freedom of contract; DK (Drafting suggestions): 1b. A provider of a data processing service may include provisions on proportionate early termination penalties in a contract of fixed duration on the provision of data processing services other than those referred to in Article 30(1). DK (Comments): Suggest to split up the first part of paragraph 1b and the second part in two separate paragraphs, as this first part covers one set of data hosting services (data processing services other than those referred to in Article 30(1), wheras the following part covers data processing services that are SMCs and SMEs.

Commission proposal	Drafting suggestions and Comments
	It seems confusing to include two different kinds of exceptions for two different kinds of services in the same paragraph FR (Drafting suggestions): ~~1b. A provider of a data processing service may include provisions on proportionate early termination penalties in a contract of fixed duration on the provision of data processing services other than those referred to in Article 30(1).~~ FR (Comments): le règlement vise à garantir que les clients puissent changer de fournisseur de services de traitement de données dans des conditions effectives, sans interruption du service, ni obstacles injustifiés ou coûts de transfert excessifs, afin d'éviter des situations de dépendance durable vis-à-vis d'un prestataire. Cette exigence constitue un élément central de l'équilibre du texte, en vue de préserver une concurrence effective et de renforcer la protection des utilisateurs (y compris publics). Exclure les services autres que ceux visés à l'article 30 (1) irait donc à l'encontre de cette logique – d'autant que ces segments de marché présentent un risque structurel de verrouillage contractuel, les utilisateurs pouvant rencontrer des difficultés à changer de solution une fois intégrés dans un écosystème donné. Le cadre du règlement vise précisément à préserver des marges de manœuvre effectives pour les clients, afin d'éviter que les acteurs déjà établis ne bénéficient d'un avantage structurel susceptible de limiter l'accès au marché de solutions nouvelles, y compris potentiellement plus innovantes, et de fausser les conditions de concurrence.
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	DK (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
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.	**1c.** 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. DK (Comments): See comment above. This section should be given its own "paragraph". FR (Drafting suggestions): ~~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.~~ FR (Comments): le règlement vise à garantir que les clients puissent changer de fournisseur de services de traitement de données dans des conditions effectives, sans interruption du service, ni obstacles injustifiés ou coûts de transfert excessifs, afin d'éviter des situations de dépendance durable vis-à-vis d'un prestataire. Cette exigence constitue un élément central de l'équilibre du texte, en vue de préserver une concurrence effective et de renforcer la protection des utilisateurs (y compris publics). Exclure les services autres que ceux visés à l'article 30 (1), quand bien même TPE/PME, irait donc à l'encontre de cette logique – d'autant que ces segments de marché présentent un risque structurel de verrouillage

Commission proposal	Drafting suggestions and Comments
	contractuel, les utilisateurs pouvant rencontrer des difficultés à changer de solution une fois intégrés dans un écosystème donné. Le cadre du règlement vise précisément à préserver des marges de manœuvre effectives pour les clients, afin d'éviter que les acteurs déjà établis ne bénéficient d'un avantage structurel susceptible de limiter l'accès au marché de solutions nouvelles, y compris potentiellement plus innovantes, et de fausser les conditions de concurrence. NL (Drafting suggestions): **1c.** NL (Comments): Seperate paragraph, as it introduces a new point
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.'; Article 24 The responsibilities of providers of data processing services laid down in Articles 23, 25, 29, 30 and 34 shall apply only to the services, contracts or commercial practices provided by the source provider of data processing services. **Within six months after [Digital Omnibus Regulation] has entered into force the Commission shall adopt guidelines on the scope of the technical obligations concerning switching between data processing services, taking into account the advice of the European Data Innovation Board (EDIB) referred to in Article 42, inter alia on the definition and classification of data processing services. The guidelines shall be updated at least annually.**	DE (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
	DE (Comments): **DE**: German Position Paper on the European Commission's Digital Omnibus, p. 1 ("[legal acts] should be formulated in a clear and precise manner ensuring legal clarity and certainty"), p. 2 ("ensure uniform implementation and harmonization"). Guidelines should be developed on specific topics and updated annually. The role of the EDIB in the creation of all guidelines should be laid down in the Data Act. **DE**: Proposal to address the needs of SaaS- and PaaS-data processing services and to provide legal certainty with regard to existing contracts concluded beforre 12 September 2025. DK (Drafting suggestions): **[1c. continued]** 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

Commission proposal	Drafting suggestions and Comments
	contractual provision contained in that contract that is contrary to Article 29(1), (2), or (3) shall be considered null and void.'; DK (Comments): See comment above. FR (Drafting suggestions): ~~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.'~~ FR (Comments): Idem - d'autant que les fournisseurs de services ont eu un temps d'adaptation pour se mettre en conformité. NL (Drafting suggestions): **1d.** NL (Comments): Separate paragraph, as it introduces a new point
16. Article 32 is amended as follows:	DE (Comments):

Commission proposal	Drafting suggestions and Comments
	DE: COM is called upon to examine Chapter VII Data Act according to the European Data Union Strategy (third priority area – international data flows) The rules in Chapter VII of the Data Act are fraught with legal uncertainties and shift responsibility to the companies concerned. From the perspective of "EU data sovereignty," legal regulations are nevertheless necessary in the interest of sovereignty (limiting data access from third countries) while taking into account economic interests (free data flow, legal certainty). FR (Comments): France has a review reservation regarding the whole amendments made to Article 32 of the Data Act. Further analysis is required before we can express our observations and proposals.
(a) paragraph 1 and 2 are replaced by the following:	
'1. Providers of data processing services, the public sector body making available data or documents in accordance with Chapter VIIc Section 3, the natural or legal person to which the right to re-use data or documents in accordance with Chapter VIIc Section 3 was granted, a data intermediation services provider or a recognised data altruism organisation shall take all adequate technical, organisational and legal measures, including contracts, in order to prevent international and third-country governmental access and transfer of non-personal data held in the Union where such transfer or access would create a conflict with Union law or with the national law of the relevant Member State, without prejudice to paragraph 2 or 3.	
2. Any decision or judgment of a third-country court or tribunal and any decision of a third-country administrative authority requiring a provider of data processing services, the public sector body making available data or documents in accordance with Chapter VIIc Section 3, the natural or legal	

Commission proposal	Drafting suggestions and Comments
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:';	DE (Drafting suggestions): 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: (a) the third-country system requires the reasons and proportionality of such a decision or judgment to be set out and requires such a decision or judgment

Commission proposal	Drafting suggestions and Comments
	to be specific in character, for instance by establishing a sufficient link to certain suspected persons or infringements; (b) the reasoned objection of the addressee is subject to a review by a competent third-country court or tribunal; and (c) the competent third-country court or tribunal issuing the decision or judgment or reviewing the decision of an administrative authority is empowered under the law of that third country to take duly into account the relevant legal interests of the provider of the data protected by Union law or by the national law of the relevant Member State. **Within six months after [Digital Omnibus Regulation] has entered into force the Commission shall adopt guidelines [for international data flows] on the assessment of whether the conditions laid down in the first subparagraph of this paragraph are met. The guidelines shall be updated at least annually.** […] DE (Comments): **DE**: German Position Paper on the European Commission‘s Digital Omnibus, p. 1 (“[legal acts] should be formulated in a clear and precise manner ensuring legal clarity and certainty”), p. 2 (“ensure uniform implementation and harmonization”). Guidelines should be developed on specific topics and updated annually. The role of the EDIB in the creation of all guidelines should be laid down in the Data Act.
(c) paragraphs 4 and 5 are replaced by the following:	

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.';	DE (Drafting suggestions): ~~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.~~ DE (Comments): **DE: Remove information obligations** in Chapter VII.
17. Article 36 is deleted.	NL (Drafting suggestions): ~~17.~~ **18. Article 36 is deleted.** NL

Commission proposal	Drafting suggestions and Comments
	(Comments): Numbering is incorrect. Article 36 should be after new artikels 32a etc. PL (Comments): PL agrees with the deletion of art. 36
18. the following Chapters VIIa, VIIb and VIIc are inserted:	NL (Drafting suggestions): ~~18.~~ 17. the following Chapters VIIa, VIIb and VIIc are inserted: NL (Comments): Numbering is incorrect. Article 36 should be after new artikels 32a etc.
‘**CHAPTER VIIa** **DATA INTERMEDIATION SERVICES**	DK (Comments): DK finds that the more flexible requirements for data intermediation services providers introduced in Chapter VIIa seems sensible. In Denmark no companies were genuinely interested in becoming a registered data intermediary service, and their feedback was that it was due to the strict requirements in the DGA, for instance with regards to composition and restrictions on what other acitivites could be carried out by the provider. LV (Comments): **Overall, the direction towards more flexible regulation of data intermediation service providers is supported**, including by making the registration and use of the label a voluntary mechanism. At the same time, it would be important to ensure that such services provide added value to data

Commission proposal	Drafting suggestions and Comments
	holders and data users, including by preparing or transforming data in line with the needs of data recipients.
AND DATA ALTRUISM ORGANISATIONS'	NL (Drafting suggestions): ~~**AND DATA ALTRUISM ORGANISATIONS**~~' NL (Comments): NL supports the deletion of articles on data altruism, as a contribution to simplification and legal clarity. In pratice, the effects of these measures have been limited
	IT (Drafting suggestions): **Article 32 aa** **This Chapter does not create a legal basis for the processing of personal data for data intermediation services and data altruism, nor does it affect any of the rights and obligations set out in Regulation (EU) 2016/679** IT (Comments): To ensure legal certainty, we recommend inserting an equivalent provision to Article 1(3) of the current DGA, so as to clarify that this Chapter does not create a legal basis for the processing of personal data for data intermediation services and data altruism, nor does it affect any of the rights and obligations set out in the GDPR. This clarification will ensure a consistent and coherent application of this Chapter and the GDPR
Article 32a	
Public Union registers	

Commission proposal	Drafting suggestions and Comments
(1) The Commission shall keep and regularly update public Union registers of:	
(a) recognised data intermediation services providers and	
(b) recognised data altruism organisations.	NL (Drafting suggestions): ~~(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.	NL (Drafting suggestions): ~~(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	NL (Drafting suggestions): ~~Article 32b~~
Competent authorities for the registration of data intermediation services providers and data altruism organisations	IT

Commission proposal	Drafting suggestions and Comments
	(Comments): In light of art. 37(1) of the current Data Act on the the designation of competent authorities, it is unclear why specific provisions defining the tasks of the competent authorities are also included in this Chapter, rather than in the overarching Chapter IX on enforcement. To ensure legal certainty, we recommend clarifying the relationship between the relevant provisions of this Chapter and Chapter IX NL (Drafting suggestions): ~~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).	NL (Drafting suggestions): ~~(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).~~ NL (Comments): Doubles with article 37.
(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.	NL (Drafting suggestions): ~~(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~~ NL (Comments):

Commission proposal	Drafting suggestions and Comments
	Move it to art. 37 paragraph 8a new so all rules about competent authorities are at one place. Check articles in Chapter VIIa : change references to the competent authorty in art. 32b to art. 37.
Article 32c	NL (Comments): Renumber if art. 32b is deleted.
General requirements for registration of recognised data intermediation services providers	FI (Comments): FI: It may be appropriate to retain certain existing regulatory requirements so that registration and supervision continue to carry weight and maintain trust. For this reason, FI proposes maintaining following requirements to Article 32c: • Re-insert current Art. 12 f) DGA (Fair, transparent and non-discriminatory access) • Re-insert current Art. 12 k) DGA (Information obligation in case of data leaks regarding non-personal data) including a clear threshold for when the duty to provide information applies –. • Re-insert requirements for security measures previously included in Article 31 l) DGA taking into account recent Union law such as NIS2 • Re-insert current Art. 12 o) DGA (Log record of the data intermediation activity) to support transparency and traceability of how data is accessed, used and shared, so that the data subject or data holder can effectively control their data. FR (Comments):

Commission proposal	Drafting suggestions and Comments
	We regret the conversion of the mandatory regime into an optional regime, as well as the removal of obligations relating to data security and the disappearance of FRAND conditions for access to services. IT (Comments): To foster transparency, we would recommend maintaining some of the requirements of the current DGA that the Proposal removes and in particular:
In order to qualify for registration in the public Union register referred to in Article 32a paragraph 1 point (a), a data intermediation services provider shall meet all of the following requirements:	
(a) they do not use the data for which it provides data intermediation services for purposes other than to put them at the disposal of data users;	
(b) the data they collect with respect to any activity of a natural or legal person for the purpose of the provision of the data intermediation service, including the date, time and geolocation data, duration of activity and connections to other natural or legal persons established by the person who uses the data intermediation service, are used only for the development of that data intermediation service;	FR (Drafting suggestions): (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, which may entail the use of data for the detection of fraud or cybersecurity, and shall be made available to the data holders upon request.** FR (Comments):

Commission proposal	Drafting suggestions and Comments
	We suggest to maitain the initial list in article 12 a) to o) of the Data Governanec Act IT (Drafting suggestions): (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 **which may entail the use of data for the detection of fraud or cybersecurity**, IT (Comments): the possibility to use the details collected about activity on the data intermediation service for security and detection of abusive or fraudulent acces (see Article 12(c) of the current DGA)
(c) where they offer additional tools and services to data holders or data subjects for the specific purpose of facilitating the exchange of data, such as temporary storage, curation, conversion, encryption, anonymisation and pseudonymisation, such tools and services are used only at the explicit request or approval of the data holder or data subject;	
(d) where data intermediation service providers which are not micro and small sized enterprises offer value-added services to their clients other than the services referred to in point (c), they fulfil the following conditions:	FI (Drafting suggestions): 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

Commission proposal	Drafting suggestions and Comments
	FI (Comments): FI: The proposed derogation in point (d) is too wide since it would currently apply to most data intermediary service providers. We propose that an exception for small and micro enterprises is added as a separate point e (the current point e) becoming point f)). **e) In derogation from point d) above micro and small sized enterprises may offer value-added services provided that they fulfill conditions laid down in point (d) (iii, iv, and iv).** IT (Drafting suggestions): (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: IT (Comments): We recommend deleting the derogation for micro and small sized enterprises since ensuring neutrality by managing conflicting interests would appear relevant, regardless of enterprise size. LU (Comments): To ensure that the label retains its full significance within the future European data governance framework, it is essential to preserve the safeguards that give it operational substance, credibility, and regulatory value. In view of the forthcoming Omnibus Data Act, which is expected to integrate the current

Commission proposal	Drafting suggestions and Comments
	DGA provisions in the Data Act, maintaining a robust and coherent set of requirements is vital to prevent any loss of clarity, transparency, or supervisory effectiveness. In this context, the reintroduction of several existing DGA based provisions, including Article 12(f) (fair, transparent and nondiscriminatory access), Article 12(k) (information duties in case of incidents affecting nonpersonal data, with a clearly defined applicability threshold), Article 12(o) (purpose of logging), Article 31(l) (security measures, with adjusted wording), and Article 11(12)–(13) (notification obligations for DISPs) remains essential. These elements support three key objectives: 1. **Transparency:** ensuring adequate and reliable information for all stakeholders. 2. **Preserving the value of the label:** keeping the label meaningful and trusted by retaining strong, clear and futureproof requirements, even as the legislative framework evolves. 3. **Effective oversight:** enabling authorities to maintain a complete, accurate and uptodate list of providers, which is indispensable for consistent supervision across the EU. Maintaining these safeguards is therefore crucial to ensure continuity, regulatory coherence, and a smooth transition from the DGA framework to the consolidated Omnibus Data Act
(i) the value-added services are explicitly requested by the user;	DE (Drafting suggestions): **(ii) The usage of the data for the value added-service is covered by consent/permission from the respective data subject/data holder;** DE (Comments): **DE**: wrong transposition of DGA rules into the Data Act

Commission proposal	Drafting suggestions and Comments
	- Complete exemption (d) for micro and small enterprises only makes sense for (vi), (v) and (vi). Otherwise, this would be a contradiction to Art. 32c lit a. - Furthermore, the services should only be provided at the explicit request of the user and be covered by consent/permission from the respective data subject/data holder to ensure data sovereignty and trust in order to incentivise voluntary data sharing. PL (Drafting suggestions): (i) the value-added services are explicitly requested by the ~~user~~ **data holder or data subject**; PL (Comments): This makes sure the user here is not confused with the user of connected products from Chapter III
(ii) the data are not used for other purposes than performing the value-added service;	DE (Drafting suggestions): (**iii**) 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;	DE (Drafting suggestions): (**iv**) the value-added services are offered through a functionally separate entity; IT (Drafting suggestions): iii) the **data intermediation services** are offered through a functionally separate entity **from the ones offering other services**

Commission proposal	Drafting suggestions and Comments
	IT (Comments): Functional separation within the same legal person should be required on the one hand between the provision of the data intermediation service, and on the other hand all other activities of the data intermediation services provider (not only with regard to value added services). Such an adjustment serves the interest of neutrality, as well as legal certainty, given the lack of criteria or definition to determine which other activities are value added services. Moreover, to ensure effectively the neutrality of data intermediation services, we recommend including clear criteria for functional separation (suc as requirements to have technical and organisational segregation of data as well as separate management, financing and staff)
(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;	DE (Drafting suggestions): (**v**) the undertaking seeking to offer the value-added services is not designated as a gatekeeper pursuant to Article 3 of Regulation (EU) 2022/1925; FI (Comments): FI: Further guidance may be necessary to clarify whether this also includes undertakings which belong to the same group of undertakings as a gatekeeper.
(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;	DE (Drafting suggestions): (**vi**) the commercial terms, including pricing, for the provision of data intermediation services to a data holder or data user are not dependent upon

Commission proposal	Drafting suggestions and Comments
	whether the data holder or data user uses value-added services provided by the data intermediation services provider or by a related entity; **Micro and small sized enterprises may offer value-added services without being bound by the conditions of (iv), (v) and (vi).**
(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.	DE (Drafting suggestions): **[…]** **(f) they ensure that the procedure for access to its service is fair, transparent and non-discriminatory for both data subjects and data holders, as well as for data users, including with regard to prices and terms of service;** **(g) they inform without delay data holders in the event of an unauthorised transfer, access or use of the non-personal data that it has shared, where such incident is likely to undermine trust in the data intermediation service, impair the neutral and reliable provision of data intermediation services or otherwise materially affect the data holder's ability to share or make available data through that service;;** **(h) they take necessary technical or organizational measures to ensure an appropriate level of security for the storage, processing and transmission of non-personal data;** **(i) they maintain a log record of the data intermediation activity for the purpose of ensuring transparency and traceability of the data access, use and sharing to enable the data subject or data holder to effectively control over their data.** DE

Commission proposal	Drafting suggestions and Comments
	(Comments): **DE**: Reduce requirements for DISP - but reasonably to not endanger trust in DISP: Reintroduce provisions of Article 12 lit f, k, l and o DGA with little modification. In order to give the label actual meaning in terms of trust, it is important to keep certain requirements in particular, as they can significantly improve trust in the service. The standards currently being developed under Art. 33 Data Act regarding data spaces will most likely help with the logging activity. FI (Drafting suggestions): **e) In derogation from point d) above micro and small sized enterprises may offer value-added services provided that they fulfill conditions laid down in point (d) (iii, iv, and iv).** ~~(e)~~ **(f)** 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. FI (Comments): FI: See justification in section 32(c)(d) above. IT (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
	(f) the data intermediation services provider shall have procedures in place to prevent fraudulent or abusive practices in relation to parties seeking access through its data intermediation services; **(g) the data intermediation services provider shall, in the event of its insolvency, ensure a reasonable continuity of the provision of its data intermediation services and, where such data intermediation services ensure the storage of data, shall have mechanisms in place to allow data holders and data users to obtain access to, to transfer or to retrieve their data and, where such data intermediation services are provided between data subjects and data users, to allow data subjects to exercise their rights;** **(h) the data intermediation services provider shall maintain a log record of the data intermediation activity ;** **(i) where a data intermediation services provider provides tools for obtaining consent from data subjects or permissions to process data made available by data holders, it shall, where relevant, specify the third-country jurisdiction in which the data use is intended to take place and provide data subjects with tools to both give and withdraw consent and data holders with tools to both give and withdraw permissions to process data** IT (Comments): To foster transparency, we would also recommend maintaining the following requirements of the current DGA that the Proposal removes:

Commission proposal	Drafting suggestions and Comments
	-a requirement to put procedures in place – corresponding to the risks involved – to prevent fraudulent or abusive practices by service users (see Article 12(g) of the current DGA) -a requirement for providers to arrange that, in the event of insolvency, data subjects have an opportunity to exercise their rights (see Article 12(h) of the current DGA) - a requirement to keep a log record of the data intermediation activity, corresponding to with the risks involved (see Article 12(o) of the current DGA) But above all, we recommend retaining the current provision on the use of tools for obtaining consent from data subjects by recognised data intermediation services providers (see Article 12(n) of the current DGA)
Article 32d	NL (Drafting suggestions): ~~Article 32d~~

Commission proposal	Drafting suggestions and Comments
General requirements for registration of recognised data altruism organisations	NL (Drafting suggestions): ~~*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:	NL (Drafting suggestions): ~~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;	NL (Drafting suggestions): ~~(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;	NL (Drafting suggestions): ~~(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;	NL (Drafting suggestions): ~~(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.	NL (Drafting suggestions): ~~(d) they carry out their data altruism activities through a structure that is functionally separate from their other activities~~
Article 32e	

Commission proposal	Drafting suggestions and Comments
Registration	SI (Comments): SI does not support removing obligations for data intermediation service providers; SI also does not support making registration and the use of the label voluntary. We consider it essential to retain key requirements such as notification, record-keeping, and reporting and we express reservations regarding any excessive liberalisation in this area. Accordingly, SI proposes that the Digital Omnibus should also include a requirement for prior notification, at least for those providers of data intermediation services whose envisaged intermediation involves the processing of personal data that is likely to result in a high risk to the rights and freedoms of natural persons.
(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.	FR (Drafting suggestions): (1) Data intermediation services provider which meets the requirements set out in Article 32c ~~may~~ **shall** 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. IT (Comments): Since transparency and effective oversight foster trust in data intermediation services for data subjects, data users and data sources, we recommend maintaining a prior registration requirement for data intermediation services providers, or at least maintaining this requirement when the intended data intermediation services involve processing of personal data that is likely to result in a high risk to the rights and freedoms of natural persons. The latter case would correspond with circumstances in which when the processing

Commission proposal	Drafting suggestions and Comments
	activities of the data intermediation service provider, taking into account the nature, scope, context and purposes of the processing, are likely to result in a high risk to the rights and freedoms of natural persons (see Article 35 GDPR) NL (Drafting suggestions): (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~~. NL (Comments): What the competent authority is, is already made clear in art. 37(10).
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.	NL (Drafting suggestions): ~~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	NL (Drafting suggestions): ~~(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~~

Commission proposal	Drafting suggestions and Comments
provider or the data altruism organisation to ensure compliance with this Regulation.	~~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.~~ NL (Comments): Better to merge with comparable rules in art. 37 (11)(12)(13). Renumber the remaining paragraphs.
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.	NL (Drafting suggestions): 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.	FI (Comments): FI: The content of the application forms should be harmonised similarly to the current DGA notifications (Art 11(6) ja 19(4)). IT (Comments): Given the role that registration plays in enabling competent authorities to exercise oversight over recognised data intermediation services providers and data altruism organisations, the lack of harmonisation of the application forms throughout the EU will likely lead to fragmentation. Therefore, we recommend harmonising the application form across the EU, for instance

Commission proposal	Drafting suggestions and Comments
	through an implementing act, to ensure consistency. Such an implementing act could set out the required description of the intended nature of data intermediation or data altruism processing activities, such as types of data, including categories of personal data and intended value-added services. The application form should ensure that competent authorities receive sufficient and reliable information to be aware of and enable supervision of the data intermediation and data altruism activities being pursued. PL (Comments): PL: The application forms should be established at the EU level rather than on national level – for the sake of better harmonisation.
(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.	NL (Drafting suggestions): ~~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.	

Commission proposal	Drafting suggestions and Comments
(5) The competent authority may charge fees for the registration in accordance with national law. Such fees shall be proportionate and objective and be based on the administrative costs related to the monitoring of compliance. In the case of small-mid caps, small and medium-sized enterprises, and start-ups, the competent authority may charge a discounted fee or waive the fee.	
(6) Registered entities shall notify the competent authority of any subsequent changes to the information as provided during the application process or where they cease their data intermediation or data altruism activities in the Union.	FI (Comments): FI: We propose adding notification deadlines, following an approach similar to Article 11(12)–(13) of the DGA. NL (Drafting suggestions): (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	NL (Drafting suggestions): ~~Article 32f~~
Duties of recognised data altruism organisations	NL (Drafting suggestions): ~~*Duties of recognised data altruism organisations*~~ SI

Commission proposal	Drafting suggestions and Comments
	(Comments): SI supports maintaining record-keeping and reporting obligations for recognized data altruism organizations. In the light of the proposed removal of certain transparency requirements (previously Article 20 DGA), these obligations remain necessary to enable competent authorities to carry out effective controls.
(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:	NL (Drafting suggestions): ~~(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;	NL (Drafting suggestions): ~~(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.	NL (Drafting suggestions): ~~(b) the location of the processing and the objectives of general interest for which it permits any processing carried out in a third country, where the processing is carried out by the recognised data altruism organisation.~~
(2) Recognised data altruism organisations shall not use the data for other objectives than the objectives of general interest for which the data subject or data holder allows the processing. The recognised data altruism organisation shall not use misleading marketing practices to solicit the provision of data.	NL (Drafting suggestions): ~~(2) Recognised data altruism organisations shall not use the data for other objectives than the objectives of general interest for which the data subject or data holder allows the processing. The recognised data altruism organisation shall not use misleading marketing practices to solicit the provision of data.~~

Commission proposal	Drafting suggestions and Comments
(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.	NL (Drafting suggestions): ~~(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.~~ PL (Drafting suggestions): ~~(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.~~ →see the comment PL (Comments): The provision on the obligation of the Commission to establish a uniform European data altruism consent form should be reinstated (former article 25). Leaving the data altruism content form unspecified and at the discretion of Member States may create unwanted differences between countries, hindering the activities of data altruism organisations.
(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.	NL (Drafting suggestions): ~~(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	NL (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
shall, where relevant, specify the third-country in which the data use is intended to take place.	~~(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	IT (Drafting suggestions): **Article 32fa** **Transparency requirements** **1. A recognised data altruism organisation shall keep full and accurate records concerning the categories of natural or legal persons that were given the possibility to process data held by that recognised data altruism organisations including a summary description of the objectives of general interest pursued by such data processing and the description of the technical means used for it, including a description of the techniques used to preserve privacy and data protection.** **2. A recognised data altruism organisation shall draw up and transmit to the relevant competent authority for the registration of data altruism organisations an annual activity report which shall contain at least an overview at least of:** **(a) categories of natural or legal persons that were allowed to process data it holds;** **(b) the sources of revenue of the recognised data altruism organisation, in particular all revenue from allowing access to the data, and on categories of expenditures** **3. The Commission shall adopt an implmenting act to determine the common elements to be included in the annual report.** IT

Commission proposal	Drafting suggestions and Comments
	(Comments): To foster trust in the label 'data altruism organisation recognised in the Union', effective public oversight should be ensured and appropriate accountability mechanisms should be put in place. For this reason, we recommend maintaining the record-keeping obligation envisaged by article 20(1) of the current DGA for data altruism organisations, in order to ensure that competent authorities can exercise their oversight in an effective manner. We also recommend maintaining certain elements of the reporting obligation for recognised data altruism organisations, envisaged by article 20(2) of the current DGA in order to foster effective oversight. In particular, an annual overview of the categories of all natural and legal persons that were allowed to process data could be required, as well as an overview on an annual basis of the sources of revenue of the recognised data altruism organisation, and notably all revenue from allowing access to the data, and on categories of expenditure. Harmonisation across the EU, for example through a Commission implementing act, could be considered to determine common elements for all annual reports NL (Drafting suggestions): ~~Article 32g~~
Monitoring of compliance	IT (Comments): In light of art. 37(1) of the current Data Act on the the designation of competent authorities, it is unclear why specific provisions defining the tasks

Commission proposal	Drafting suggestions and Comments
	of the competent authorities are also included in this Chapter, rather than in the overarching Chapter IX on enforcement. To ensure legal certainty, we recommend clarifying the relationship between the relevant provisions of this Chapter and Chapter IX NL (Drafting suggestions): ~~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.	IT (Comments): This provision which mandates competent authorities to initiate supervision upon their own initiative or on a request by a natural or legal person, seems to introduce a change from discretionary power to mandatory action in relation to the current articles 14 and 24 DGA. If this is the case, we recommend amending it to maintain the competent authorities' discretion to prioritise enforcement action. By maintaining this discretion, competent authorities will be in a better position to allocate resources more efficiently to take action where it is most needed NL (Drafting suggestions): ~~(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.~~ NL (Comments):

Commission proposal	Drafting suggestions and Comments
	It is better to have all comptent authorities articles in art. 37. This task from (1) is added to art. 37 (5). SI (Comments): SI considers that the obligation set out in the proposed Article 32g(1) is unnecessary and the draft regulation could only provide for the possibility to start controls at the request of a natural or legal person (in the same way as Articles 14 and 24 of Regulation (EU) 2022/868 on data management, mutatis mutandis).
(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.	NL (Drafting suggestions): ~~(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.~~ NL (Comments): Merged in art. 37(4). Text is similar. Text from art. 32g(2) 14. Competent authorities shall have the power to request from users, data holders, data recipients, recognised data intermediation services providers or their legal representatives, falling under the competence of their Member State all information necessary to verify compliance with this Regulation.

Commission proposal	Drafting suggestions and Comments
	Any request for information shall be proportionate to the performance of the underlying task and shall be reasoned.
(3) Where a competent authority finds that a recognised data intermediation services provider or a recognised data altruism organisation does not comply with one or more of the requirements laid down in this Chapter, it shall notify that entity, or its legal representative, of those findings and give it the opportunity to state its views, within 30 days of the receipt of the notification.	NL (Drafting suggestions): ~~(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.~~ NL (Comments): It is better to have all comptent authorities articles in chapter IX. In new article 37a about non-compliance recognised data intermediation services providers
(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.	NL (Drafting suggestions): ~~(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.~~ NL (Comments): It is better to have all comptent authorities articles in chapter IX. In new article 37a about non-compliance recognised data intermediation services providers

Commission proposal	Drafting suggestions and Comments
(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:	NL (Drafting suggestions): ~~(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:~~ NL (Comments): It is better to have all comptent authorities articles in chapter IX. In new article 37a about non-compliance recognised data intermediation services providers
(a) lose its right to use the label referred to in Article 32a in written and spoken communication;	NL (Drafting suggestions): ~~(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.	NL (Drafting suggestions): ~~(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.	DE (Drafting suggestions): **(6) Within six months after [Digital Omnibus Regulation] has entered into force the Commission shall adopt guidelines on how to best protect, in the context of this Regulation, commercially sensitive non-personal data, in particular trade secrets, but also non-personal data representing content protected by intellectual property rights from unlawful access that risks intellectual property theft or industrial espionage. The guidelines shall be updated at least annually.**

Commission proposal	Drafting suggestions and Comments
	DE (Comments): **DE**: German Position Paper on the European Commission's Digital Omnibus, p. 1 ("[legal acts] should be formulated in a clear and precise manner ensuring legal clarity and certainty"), p. 2 ("ensure uniform implementation and harmonization"). Guidelines should be developed on specific topics and updated annually. The role of the EDIB in the creation of all guidelines should be laid down in the Data Act. NL (Drafting suggestions): ~~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'	FR (Drafting suggestions): **Free flow of non-personal data within the Union'** FR (Comments): We propose to amend the title to align with the wording of the repealed Regulation EU 2018/1807.
'Article 32h	FR

Commission proposal	Drafting suggestions and Comments
	(Comments): France expresses concerns on the deletion of articles 5 and 7 of Regulation EU 2018/1807. This should not lead to a reduction in the investigative powers of judicial investigation services and the investigative powers of the various administrative authorities of the Member States.
Prohibition of localisation requirements for non-personal data within the Union	SI (Comments): SI supports consolidating relevant provisions of the FFDR into the Data Act. It is important for MS to meet the objectives of removing unjustified obstacles to the free flow of non-personal data.
(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.'	

Commission proposal	Drafting suggestions and Comments
Chapter VIIc	PL (Comments): **General comment:** EU acts should be drafted according to their type, in particular whether they are directly binding (regulations) or require national implementation (directives). Since regulations are directly applicable and are binding in their entirety, their provisions should be drafted in such a way that the addressees have no doubts as to the rights and obligations resulting from them. Some of the currently proposed provisions do not meet these standards. The rules of the directive (meant for Member States and implemented nationally) have been transferred into a regulation to be applied directly. This approach is problematic. The proposed provisions should be amended accordingly and re-drafted by the Commission to reflect the nature of a regulation as a legal act. In particular, amendments should be introduced to provisions governing the conditions for re-use, the charging of fees, and the procedure for handling requests for the re-use of data and documents. These provisions should be precise and ready for direct application and **need redrafting.**
Re-use of data and documents held by public sector bodies	PL (Comments): **General comment:** The challenge when applying the new Chapter VIIc (Re-use of data and documents held by public sector bodies) will be to determine, in a quickly and unambiguous way whether Chapter VIIc applies to specific data or documents, and if so, which of the two Sections (section 2 or 3) is relevant in a given case. The proposed list of exemptions is largely based on Directive 2019/1024, which was considered unclear. As a result, the list of exemptions long, complex, and difficult to use in practice.

Commission proposal	Drafting suggestions and Comments
SECTION 1	
GENERAL PROVISIONS	
Article 32i	
Subject matter and scope	DE (Comments): **DE**: The technical implementation seems to be legalistically sound. However, Recital 54 ODD also explicitly clarifies that the term "intellectual property" in the Open Data Directive only refers to copyright and related rights, meaning that the ODD does not apply to documents covered by industrial property rights such as patents, registered designs, and trademarks. This important exemption in favor of industrial property rights has not been included (to our understanding) in the provisions of the new Chapter VIIc of the Data Act, nor has it been enshrined in the corresponding recitals. The absence of this clarification gives the impression that the scope of the regulations on the reuse of data is to be extended and that industrial property rights are no longer to remain unaffected. This would be viewed very critically. Hence, it should be clarified in Article 32i that Chapter VIIc does not apply to data and documents that are subject to industrial property rights (in line with the previous recital 54 ODD).
(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;	

Commission proposal	Drafting suggestions and Comments
(b) existing data and documents held by public undertakings that are:	
(i) active in the areas referred to in Chapter II of Directive 2014/25/EU of the European Parliament and of the Council;	
(ii) acting as public service operators pursuant to Article 2 of Regulation (EC) No 1370/2007 of the European Parliament and of the Council;	
(iii) acting as air carriers fulfilling public service obligations pursuant to Article 16 of Regulation (EC) No 1008/2008 of the European Parliament and of the Council; or	
(iv) acting as Community shipowners fulfilling public service obligations pursuant to Article 4 of Council Regulation (EEC) No 3577/92 ;	
(c) research data pursuant to the conditions set out in Article 32t.	
(2) This Chapter does not apply to the following:	
(a) data and documents the supply of which is an activity falling outside the scope of the public task of the public sector bodies concerned as defined by law or by other binding rules in the Member State, or, in the absence of such rules, as defined in accordance with common administrative practice in the Member State in question, provided that the scope of the public tasks is transparent and subject to review;	PL (Comments): According to Article 32i (2) (a) and (b) chapter VIIc does not apply to: – data and documents the supply of which is an activity falling **outside the scope of the public task** of the public sector bodies, – data and documents held by public undertakings and produced **outside the scope of the provision of services in the general interest** The same concepts should be expressed using the same terms, without departing from their meaning in ordinary legal or technical language. Since the act uses different terms, we request clarification of the difference between “outside the scope of the public task” and “outside the scope of the provision

Commission proposal	Drafting suggestions and Comments
	of services in the general interest", and, if there is no difference, that a single term be used consistently.
(b) data and documents held by public undertakings and:	
(i) produced outside the scope of the provision of services in the general interest as defined by law or other binding rules in the Member State;	
(ii) related to activities directly exposed to competition and therefore, pursuant to Article 34 of Directive 2014/25/EU, not subject to procurement rules;	
(c) data and documents, such as sensitive data, which are excluded from access by virtue of the access regimes in the Member State on grounds of the protection of national security (namely, State security), defence, or public security;	
(d) data and documents held by public service broadcasters and their subsidiaries, and by other bodies or their subsidiaries for the fulfilment of a public service broadcasting remit.	
(3) Section 2 of this Chapter does not apply to:	
(a) data or documents, such as sensitive data or documents, which are excluded from access by virtue of the access regimes in the Member State, including on grounds of:	
(i) statistical confidentiality;	
(ii) commercial confidentiality (including business, professional or company secrets);	

Commission proposal	Drafting suggestions and Comments
(b) data or documents access to which is restricted by virtue of the access regimes in the Member States,	
(i) including cases whereby citizens or legal entities have to prove a particular interest to obtain access to documents;	
(ii) on grounds of protection of personal data, and parts of data or documents accessible by virtue of those regimes which contain personal data the re-use of which has been defined by law as being incompatible with the law concerning the protection of individuals with regard to the processing of personal data or as undermining the protection of privacy and the integrity of the individual, in particular in accordance with Union or national law regarding the protection of personal data; logos, crests and insignia;	
(c) data or documents for which third parties hold intellectual property rights;	
(d) data or documents held by cultural establishments other than libraries, including university libraries, museums and archives;	
(e) data or documents held by educational establishments of secondary level and below, and, in the case of all other educational establishments, data other than those referred to in paragraph 1, point (c);	
(f) data or documents other than those referred to in paragraph 1, point (c), held by research performing organisations and research funding organisations, including organisations established for the transfer of research results;	
(g) Data or documents access to which is excluded or restricted on grounds of critical entity or critical infrastructure protection related information as defined in points (1) and (4) of Article 2 of Directive (EU) 2022/2557.	

Commission proposal	Drafting suggestions and Comments
(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.	FI (Drafting suggestions): FI: (add after section 5 as new sections 6 and 7) 6) This Chapter does not create any obligation on public sector bodies to allow the re-use of data, nor does it release public sector bodies from their confidentiality obligations under Union or national law. 7) This Regulation does not create a legal basis for the processing of personal data, nor does it affect any of the rights and obligations set out in Regulations (EU) 2016/679 or (EU) 2018/1725 or Directives 2002/58/EC or (EU) 2016/680. FI (Comments): FI: We would like to see these principles from DGA Article 1(2) and 1(3) kept in Chapter VIIc. This clarifies interpretation and application of the Chapter, especially since the recitals of the ODD and DGA are lost in the process of merging the rules into the DA.

Commission proposal	Drafting suggestions and Comments
	The EDPB and EDPS joint opinion also recommends reinstating these in Chapter VIIc (sections 151 and 152 of the opinion). In our view these are applicable to both Section 2 and Section 3 and so their right place is here.
(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).	FI (Drafting suggestions): FI: **8)** 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). FI (Comments): FI: change numbering to reflect newly added sections
(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.	FI (Drafting suggestions): FI: **9)** 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. FI (Comments): FI: change numbering to reflect newly added sections
(8) This Chapter governs the re-use of existing data and documents held by public sector bodies and public undertakings of the Member States,	FI (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
including data and documents to which Directive 2007/2/EC of the European Parliament and of the Council applies.	FI: **10)** 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. FI (Comments): FI: change numbering to reflect newly added sections
(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).	FI (Drafting suggestions): FI: **(11)** 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). FI (Comments): FI: change numbering to reflect newly added sections IT (Drafting suggestions): **(10) This Chapter does not create any obligation on public sector bodies to allow the re-use of data, nor does it release public sector bodies from their confidentiality obligations under Union or national law. In**

Commission proposal	Drafting suggestions and Comments
	particular, this Chapter does not create a legal basis for the processing of personal data, nor does it affect any of the rights and obligations set out in Regulation (EU) 2016/679 IT (Comments): To ensure legal certainty, we recommend reinstating Article 1(2) of the current DGA which provides that the DGA 'does not create any obligations on public sector bodies to allow the re-use of data, nor does it release public sector bodies from their confidentiality obligations under Union or national law'. The specification under the current rules that there is no legal duty for public sector bodies to give access to personal data is important from a data protection viewpoint. In the same vein, we recommend inserting an equivalent provision to Article 1(3) of the current DGA, so as to clarify that this Chapter does not create a legal basis for the processing of personal data, nor does it affect any of the rights and obligations set out in the GDPR
	BE (Drafting suggestions): (10) This Chapter does not create any obligation on public sector bodies to allow the re-use of protected data, nor does it release public sector bodies from their confidentiality obligations under Union or national law.

Formatted: English (United Kingdom)
Formatted: English (United Kingdom)

Commission proposal	Drafting suggestions and Comments
	(11) This Chapter does not create a legal basis for the processing of personal data, nor does it affect any of the rights and obligation set out in Regulation (EU) 2016/679. BE (Comments): _The arguments for proposing the new (10) directly flow from the EDPB-EDPS JOINT OPINION 2/2026, p. 43/48 : "*151. As a general comment, applicable to all provisions of the new Chapter VIIc of the Data Act, the EDPB and the EDPS note that Article 1(2) DGA, which provides that the DGA 'does not create any obligation on public sector bodies to allow the re-use of data, nor does it release public sector bodies from their confidentiality obligations under Union or national law', is not retained in the Proposal.* ***The specification under the current rules that there is no legal duty for public sector bodies to give access to personal data is important from a data protection viewpoint. For this reason, the EDPB and the EDPS recommend reinstating Article 1(2) DGA167.*** ". (For the new (11), its motivation equally flows directly from the EDPB-EDPS JOINT OPINION 2/2026 p. 43/48 : "*152. The EDPB and the EDPS also note the Proposal would delete the provisions in Article 1(3) DGA, which clarify that 'the Regulation does not create a legal basis for the processing of personal data, nor does it affect any of the rights and obligation set out in Regulations (EU) 2016/679'.* ***For clarity, the EDPB and the EDPS recommend inserting an equivalent provision in the Proposal in relation to access granted by public bodies for re-use, governed by proposed Chapter VIIc, and in relation to activities of data intermediation services and data altruism organisations, governed by Chapter VIIa****.".* In any way these two sentences form an important part of the DGA and should, for clarity reasons, thus be integrated into the new chapter VIIc.

Commission proposal	Drafting suggestions and Comments
	Indirect inferral does not constitute legal clarity. Omitting the integration of the extisting articles 1(2) and 1(3) DGA leads to questions and unnecessary unclarity regarding the voluntary nature for allowing public sector bodies the re-use of protected data, the continued obligations for public sector in terms of confidentiality and create confusion regarding the fact that the provisions do not provide for a new legal basis for the processing of personal data, or the full application of all rights and obligations set out in Regulation (EU) 2016/679. The Commission has not provided any reasons for not integration the extisting articles 1(2) and 1(3) DGA into the nex text, perhaps this was simply forgetfulness?
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.	DE (Comments): **DE**: Paragraph 1 combines Art. 11(1) ODD and Art. 5(2) DGA; sentence 3 (ODD) is difficult to understand in terms of its meaning; according to hE, it is more of a clarification that different types of reuse should be non-discriminatory; please assess need for clarification by adding at the end of sentence 1 and introduction with “in particular”?
(2) If data or documents are re-used by a public sector body as input for its commercial activities which fall outside the scope of its public tasks, the same charges and other conditions shall apply to the supply of the data or documents for those activities as the ones that apply to other re-users.	
Article 32k	
Exclusive arrangements	
(1) The re-use of data or documents shall be open to all potential actors in the market, even if one or more market actors already exploit added-value products based on those data or documents. Agreements or other arrangements	

Commission proposal	Drafting suggestions and Comments
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.	PL (Drafting suggestions): (a) **unless national law provides one of methods of granting the exclusive right,** ~~the exclusive~~ **such** 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, PL (Comments): n Article 32k, we propose the following: • To clarify the rules concerning the choice of the form for granting an exclusive right (contract or administrative act). We propose that the provisions should stipulate by default that an exclusive right is granted by way of a contract or an administrative act, unless national law provides otherwise (e.g., allows only a contract). The purpose of this amendment is to eliminate any doubts as to the interpretation of the provision.

Commission proposal	Drafting suggestions and Comments
	• To clarify the use of the terms "contractual agreements (contract)" and "administrative acts."
(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.	PL (Drafting suggestions): (b) the agreements **or administrative acts** 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. PL (Comments): General comment: In accordance with Article 32k(2)(b), agreements granting an exclusive right, including the reasons for granting such a right, must be transparent and made publicly available online in a form that complies with relevant Union law on public procurement and national law. It is necessary to clarify this provision and include references to the relevant UE public procurement legislation (by indicating the specific provisions) regarding the publication of information.
(c) except for exclusive rights related to the digitisation of cultural resources, the validity of the reason for granting exclusive rights concerning data and documents within the scope of Section 2 shall be subject to regular review, and shall in any event, be reviewed every three years.	
(d) exclusive arrangements established on or after 16 July 2019 shall be made publicly available online at least two months before they come into effect. The final terms of such arrangements shall be transparent and shall be made publicly available online.	DE (Comments): **DE**: point d corresponds to Article 12(2) sentence 2 ODD and should be amended due to its obsolescence (deletion of ... on or after July 16, 2019);

Commission proposal	Drafting suggestions and Comments
(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.	PL (Drafting suggestions): 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 **or administrative act is adopted**, the duration of the ~~contract~~ **arrangements** 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:	

Commission proposal	Drafting suggestions and Comments
(a) exclusive arrangements concerning data and documents within the scope of Section 2existing on 17 July 2013 that do not qualify for the exceptions set out in paragraphs 2 and 3 and that were entered into by public sector bodies shall be terminated at the end of the contract and in any event not later than 18 July 2043;	
(b) exclusive arrangements concerning data and documents within the scope of Section 2 existing on 16 July 2019 that do not qualify for the exceptions set out in paragraphs 2 and 3, and that were entered into by public undertakings, shall be terminated at the end of the contract and in any event not later than 17 July 2049;	
Article 32l	
General principles relating to charging	
(1) Any charges set out under Section 2 or Section 3 shall be transparent, non-discriminatory, proportionate and objectively justified and shall not restrict competition.	
(2) In the case of standard charges for the re-use of data or documents, any applicable conditions and the actual amount of those charges, including the calculation basis for such charges, shall be established in advance and published, through electronic means where possible and appropriate.	
(3) In the case of charges for the re-use other than those referred to in paragraph 1, the factors that are taken into account in the calculation of those charges shall be indicated at the outset. Upon request, the holder of the data or documents in question shall also indicate the way in which such charges have been calculated in relation to a specific re-use request.	DE (Drafting suggestions): (3) In the case of charges for the re-use other than those referred to in paragraph ~~1~~**2**, 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. DE

Commission proposal	Drafting suggestions and Comments
	(Comments): **DE**: Please check reference. PL (Drafting suggestions): (3) In the case of charges for the re-use other than those referred to in paragraph ~~1~~ **2**, 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. PL (Comments): Incorrect reference to paragraph 1
(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.	DE (Comments): **DE**: The proposed changes have significant impact on the Open Data Directive regarding the setting of conditions for the re-use of data and documents for particularly large companies. This applies in particular to Articles 32q, 32r, 32k, and the associated Recital 25. While we welcome the basic idea of taking greater account of company size in the re-use of data and documents, the practical implications of the specific wording still need to be examined. We have received input from stakeholders involved, according to which there are concerns about the continuation of the current practice of dealing with standard licenses. Question: Does the Commission have any information on the expected impact of the new Articles 32q, 32r, 32k, and Recital 25 on standard licenses in particular?

Commission proposal	Drafting suggestions and Comments
	PL (Comments): The new obligation for public bodies to provide easy online payment modalities for fees and charges related both to re-use of open government data and to protected data requires preparations and modifications and additional budgets to organise. What timeline is foreseen for the entry into force of this obligation? Will a public sector body meet these requirements if it provides for the possibility of paying the fee by bank transfer to a bank account?
Article 32m	
Information on means of redress	IT (Comments): we recommend clarifying how this newly introduced provision on redress relates to the new Article 38 Data Act and Article 39 of the current Data Act.
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	DK (Drafting suggestions): *Chapter VIIc* Re-use of data and documents held by public sector bodies *Article 32i* **Subject matter and scope** 1. In order to promote the use of open data and stimulate innovation in products and services, this Chapter establishes a set of minimum rules governing the re-use and the practical arrangements for facilitating the re-use of: (a) existing documents held by public sector bodies of the Member States or by EU institutions; (b) existing documents held by public undertakings that are: (i) active in the areas defined in Directive 2014/25/EU; (ii) acting as public service operators pursuant to Article 2 of Regulation (EC) No 1370/2007; (iii) acting as air carriers fulfilling public service obligations pursuant to Article 16 of Regulation (EC) No 1008/2008; or (iv) acting as Community shipowners fulfilling public service obligations pursuant to Article 4 of Regulation (EEC) No 3577/92; (c) research data pursuant to the conditions set out in Article 32u. 2. This Chapter does not apply to: (a) 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;

Commission proposal	Drafting suggestions and Comments
	(documents held by public undertakings: b (produced outside the scope of the provision of services in the general) i interest as defined by law or other binding rules in the Member State;) (irelated to activities directly exposed to competition and therefore, i)pursuant to Article 34 of Directive 2014/25/EU, not subject to procurement rules; (c)documents for which third parties hold intellectual property rights; (documents, such as sensitive data, which are excluded from access by d virtue of the access regimes in the Member State, including on grounds of:) (ithe protection of national security (namely, State security), defence, or) public security; (documents access to which is excluded or restricted on grounds of sensitive e critical infrastructure protection related information as defined in point (d)) of Article 2 of Directive 2008/114/EC; 3. This Chapter builds on, and is without prejudice to, Union and national access regimes. 4. This Chapter is without prejudice to Union and national law on the protection of personal data, in particular Regulation (EU) 2016/679 and Directive 2002/58/EC and the corresponding provisions of national law. 5. 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, the TRIPS Agreement and the WCT. 6. 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 documents or to restrict re-use beyond the limits set by this Chapter . 7. This Chapter governs the re-use of existing documents held by public sector bodies and public undertakings of the Member States, including documents to which Directive 2007/2/EC applies.

Commission proposal	Drafting suggestions and Comments
	Article 32j **Definitions** For the purpose of this Chapter, the following definitions apply: (1) 'data' means any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audiovisual recording; (1a) 'public sector body' means the State, regional or local authorities, bodies governed by public law or associations formed by one or more such authorities or one or more such bodies governed by public law; (2) '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; and (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; (3) 'public undertaking' means any undertaking active in the areas set out in point (b) of Article 32i(1) over which the public sector bodies 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;

Commission proposal	Drafting suggestions and Comments
	(c) can appoint more than half of the undertaking's administrative, management or supervisory body; (4) 'university' means any public sector body that provides post-secondary-school higher education leading to academic degrees; (5) 'standard licence' means a set of predefined re-use conditions in a digital format, preferably compatible with standardised public licences available online; (6) 'document' means: (a) any content whatever its medium (paper or electronic form or as a sound, visual or audiovisual recording); or (b) any part of such content; (7) 'anonymisation' means the process of changing documents into anonymous documents which do not relate to an identified or identifiable natural person, or the process of rendering personal data anonymous in such a manner that the data subject is not or no longer identifiable; (8) 'dynamic data' means 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; (9) 'research data' means documents in a digital form, 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; (10) 'high-value datasets' means 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 of the number of potential beneficiaries of the value-added services and applications based on those datasets; (11) 're-use' means the use by persons or legal entities of documents held by:

Commission proposal	Drafting suggestions and Comments
	(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, 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; (12) 'personal data' means personal data as defined in point (1) of Article 4 of Regulation (EU) 2016/679; (13) '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; (14) '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; (15) '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; (16) 'reasonable return on investment' means a percentage of the overall charge, in addition to that needed to recover the eligible costs, not exceeding 5 percentage points above the fixed interest rate of the ECB;. (1 'third party' means any natural or legal person other than a public sector 7) body or a public undertaking that holds the data. (1 The definitions set out for datasets in the mobility category under 8) Directive 2007/2/EC and Directive 2005/44/EC shall apply. (1 'key attribute' means a characteristic of an object or an entity in a 9) dataset, such as a national identification code or name; (20) 'granularity' means the level of detail of the dataset;

Commission proposal	Drafting suggestions and Comments
	(21) 'application programming interface (API)' means a set of functions, procedures, definitions and protocols for machine-to-machine communication and the seamless exchange of data; (22) 'bulk download' means a function that enables a download of an entire dataset in one or several packages. (24) 'secure processing environment' means the physical or virtual environment and organisational means to ensure compliance with Union law, such as Regulation (EU) 2016/679, 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; *Article 32k* **General principle** 1. Subject to paragraph 2 of this Article, Member States shall ensure that documents to which this Chapter applies shall be re-usable for commercial or non-commercial purposes in accordance with Sections III and IV of this Chapter. 2. For documents in which libraries, including university libraries, museums and archives hold intellectual property rights and for documents held by public undertakings, Member States shall ensure that, where the re-use of such documents is allowed, those documents shall be re-usable for commercial or non-commercial purposes in accordance with Sections III and IV of this Chapter. **Section II** **REQUESTS FOR RE-USE**

Commission proposal	Drafting suggestions and Comments
	Article 32l **Processing of 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 documents. 2. Where no time limits or other rules regulating the timely provision of documents have been established, public sector bodies shall process the request and shall deliver the documents for re-use to the applicant or, if a licence is needed, finalise the licence offer to the applicant as soon as possible. Competent public sector bodies or the competent bodies shall adopt a decision on the request for the re-use of data held by them within two months of the date of receipt of the request. 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 of the provisions of this Regulation. Where a negative decision is based on point (c) of Article 32i(2), 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. Any decision on re-use shall contain a reference to the means of redress where the applicant wishes to challenge the decision. The means of redress shall include the possibility of review by an impartial review body with the appropriate expertise, such as the national competition authority, the relevant access to 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.

Commission proposal	Drafting suggestions and Comments
	5. For the purposes of this Article, Member States shall establish practical arrangements to facilitate effective re-use of documents. Those arrangements may in particular include the means to supply adequate information on the rights provided for in this Chapter and to offer relevant assistance and guidance. **Section III** **CONDITIONS FOR RE-USE** *Article 32m* **Access to protected data** 1. Particular conditions of reuse can be applied to data within the definition in Article 32i which are protected on 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; 2. Public sector bodies which are competent under national law to grant or refuse access for the re-use of one or more of the categories of data referred to in paragraph 1 shall make publicly available the conditions for allowing such re-use and the procedure to request the re-use. 3. Conditions for re-use shall be non-discriminatory, transparent, proportionate and objectively justified with regard to the categories of data and the purposes of re-use and the nature of the data for which re-use is allowed. Those conditions shall not be used to restrict competition. 4. Public sector bodies shall, in accordance with Union and national law, ensure that the protected nature of data is preserved. They may provide for the following requirements:

Commission proposal	Drafting suggestions and Comments
	(a) to grant access for the re-use of data only where the public sector body or the competent body, following the request for re-use, has ensured that data has been: (i) anonymised, in the case of personal data; and (i modified, aggregated or treated by any other method of disclosure i) 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 remotely within a secure processing environment that is provided or controlled by the public sector body; (c) to access and re-use the data 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. 5. In the case of re-use allowed in accordance with paragraph 4, 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. The public sector body shall reserve the right to verify the process, the means and any results of processing of data undertaken by the re-user to preserve the integrity of the protection of the data and 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. 6. Unless national law provides for specific safeguards on applicable confidentiality obligations relating to the re-use of data referred to in paragraph 1, the public sector body shall make the re-use of data provided in accordance with paragraph 4 of this Article 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 that the re-user may have acquired despite the safeguards put in place. Re-users shall be prohibited from re-identifying any data subject to whom the data relates and shall take technical and operational measures to prevent re-identification

Commission proposal	Drafting suggestions and Comments
	and to notify any data breach resulting in the re-identification of the data subjects concerned to the public sector body. In the event of the unauthorised re-use of non-personal data, the re-user shall, without delay, where appropriate with the assistance of the public sector body, inform the legal persons whose rights and interests may be affected. 7. Where the re-use of data cannot be allowed in accordance with the obligations laid down in paragraphs 3 and 4 of this Article and there is no legal basis for transmitting the data under Regulation (EU) 2016/679, 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 it 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 32o(1). 8. Re-use of data shall be allowed only in compliance with intellectual property rights. The right of the maker of a database as 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 or to restrict re-use beyond the limits set by this Regulation. 9. Where data requested is considered to be confidential, in accordance with Union or national law on commercial or statistical confidentiality, the public sector bodies shall ensure that the confidential data is not disclosed as a result of allowing re-use, unless such re-use is allowed in accordance with paragraph 6. 10. Where a re-user intends to transfer non-personal data protected on the grounds set out in paragraph 1 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 such data. In the case of re-use in accordance with paragraph 6 of this Article, the re-user shall, where appropriate with the assistance of the public sector body, inform the legal person whose rights and interests may be affected of that intention, purpose

Commission proposal	Drafting suggestions and Comments
	and the appropriate safeguards. The public sector body shall not allow the re-use unless the legal person gives permission for the transfer. 11. 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 13 only if the re-user contractually commits to: (a) complying with the obligations imposed in accordance with paragraphs 8 and 9 even after the data is transferred to the third country; and (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 paragraphs 8 and 9. 12. 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 11 of this Article. In order to assist public sector bodies and re-users, the Commission may adopt implementing acts establishing model contractual clauses for complying with the obligations referred to in paragraph 11 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 46(2). 13. 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. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 46(2).

Commission proposal	Drafting suggestions and Comments
	14. 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. Those special conditions shall be based on the nature of the non-personal data categories identified in the specific Union legislative act and on the grounds for deeming those categories to be highly sensitive, taking into account the risks of re-identification of non-personal, anonymised data. They shall be non-discriminatory and limited to what is necessary to achieve the Union public policy objectives identified in that act, in accordance with the Union's international obligations. If required by specific Union legislative acts as 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. 15. The natural or legal person to which the right to re-use non-personal data was granted may not transfer the data to third countries unless the requirements in paragraphs 11, 13 and 14 are met. *Article 32n* **Available formats** 1. Without prejudice to Section V, public sector bodies and public undertakings shall make their documents available in any pre-existing format or language. Where possible and appropriate, data shall be made available in formats that are open, machine-readable, accessible, findable and re-usable,

Commission proposal	Drafting suggestions and Comments
	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 make documents falling within the scope of this Chapter available 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 documents or provide extracts in order to comply with that paragraph where this would involve disproportionate effort, going beyond a simple operation. 4. Paragraphs 1 to 3 shall apply to existing documents held by public undertakings which are available for re-use. 5. The high-value datasets, as listed in accordance with Article 32x(1) shall be made available for re-use in machine-readable format, via suitable APIs and, where relevant, as a bulk download. *Article 32o* **Principles governing charging** 1. The re-use of documents shall be free of charge. However, the recovery of the marginal costs incurred for the reproduction, provision and dissemination of documents as well as for anonymisation of personal data and measures taken to protect commercially confidential information may be allowed. 2. By way of exception, paragraph 1 shall not apply to the following: (public sector bodies that are required to generate revenue to cover a 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. (d) data referred to in Article 32m 3. Member States shall publish online a list of the public sector bodies referred to in point (a) of paragraph 2. 4. In the cases referred to in points (a) and (c) of paragraph 2, the total charges shall be calculated in accordance with *transparent, non-*

Commission proposal	Drafting suggestions and Comments
	discriminatory, proportionate and objectively justified criteria *and shall not restrict competition*. *5. Any fees shall be derived from the costs related to conducting the procedure for requests for the re-use of the 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 32m(4);* *(d) the maintenance of the secure processing environment;* *(e) the acquisition of the right to allow re-use in accordance with this Chapter by third parties outside the public sector; and* *(f) 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.* *6. 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.* The total income from supplying and allowing the re-use of 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. 7. Where charges are made by the public sector bodies referred to in point (b) of paragraph 2, the total income from supplying and allowing the re-use of 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

Commission proposal	Drafting suggestions and Comments
	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. *8. Where public sector bodies charge fees, they shall take measures to provide incentives for the re-use of the categories of data referred to in Article 32m for non-commercial purposes, such as scientific research purposes, and by SMCs, SMEs and start-ups in accordance with 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 SMCs, SMEs and start-ups, civil society and educational establishments. To that end, public sector bodies may establish a list of categories of re-users to which data 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.* 9. 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. 10. The re-use of the following shall be free of charge for the user: (subject to Article 32y(3), (4) and (5), the high-value datasets, as listed in a accordance with paragraph 1 of that Article;) (b) research data referred to in point (c) of Article 32i(1). *Article 32p* **Transparency**

Commission proposal	Drafting suggestions and Comments
	1. In the case of standard charges for the re-use of documents, any applicable conditions and the actual amount of those charges, including the calculation basis for such charges, shall be pre-established and published, through electronic means where possible and appropriate. 2. 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 documents in question shall also indicate the way in which such charges have been calculated in relation to a specific re-use request. 3. Public sector bodies shall ensure that applicants for re-use of documents are informed of available means of redress relating to decisions or practices affecting them. *Article 32q* **Standard licences** 1. The re-use of documents shall not be subject to conditions, unless such conditions are objective, proportionate, non-discriminatory and justified on grounds of a public interest objective. 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. 2. In Member States where licences are used, Member States shall ensure that standard licences for the re-use of public sector documents, which can be adapted to meet particular licence applications, are available in digital format and can be processed electronically. Member States shall encourage the use of such standard licences. 3. 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 32r* **Practical arrangements**

Commission proposal	Drafting suggestions and Comments
	1. Member States shall make practical arrangements facilitating the search for documents available for re-use. Where possible, Member States shall facilitate the cross-linguistic search for documents. Member States shall also encourage public sector bodies to make practical arrangements facilitating the preservation of 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 information point and by progressively making available suitable datasets held by public sector bodies with regard to the documents to which this Chapter applies, as well as to data held by Union institutions, in formats that are accessible, readily findable and re-usable by electronic means. Article 32s **Single information points** 1. Member States shall ensure that all relevant information concerning the access to data covered by this Chapter is available and easily accessible through a single information point. 2. The single information point shall be competent to receive enquiries or requests for the re-use of the categories of data referred to in Article 32m(1) and shall transmit them, where possible and appropriate by automated means, to the competent public sector bodies, or the competent bodies referred to in Article 32t, where relevant. The single information point shall make available by electronic means a searchable asset list containing an overview of all available data resources including, where relevant, those data resources that are available at sectoral, regional or local information points, with relevant information describing the available data, including at least the data format and size and the conditions for their re-use. 3. The Commission shall establish a European single access point offering a searchable electronic register of data available in the national single information points and further information on how to request data via those national single information points. *Article 32t* **Competent bodies**

Commission proposal	Drafting suggestions and Comments
	1. For the purpose of carrying out the tasks referred to in this Article, each Member State shall designate one or more competent bodies, which may be competent for particular sectors, to assist the public sector bodies which grant or refuse access for the re-use of the categories of data referred to in Article 32m. 2. The competent bodies may be empowered to grant access for the re-use of the categories of data referred to in Article 32m pursuant to Union or national law which provides for such access to be granted. 3. The assistance provided for 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; (b) providing guidance and technical support on how to best structure and store data to make that data easily accessible; c) providing technical support for pseudonymisation and ensuring data processing in a manner that effectively preserves the privacy, confidentiality, integrity and accessibility of the information contained in the data for which re-use is allowed, including techniques for the anonymisation, generalisation, suppression and randomisation of personal data or other state-of-the-art privacy-preserving methods, and the deletion of commercially confidential information, including trade secrets or content protected by intellectual property rights; (d) assisting the public sector bodies, where relevant, to provide support to re-users in requesting consent for re-use from data subjects or permission from data holders in line with their specific decisions, including on the jurisdiction in which the data processing is intended to take place and assisting the public sector bodies in establishing technical mechanisms that allow the transmission of requests for consent or permission from re-users, where practically feasible; (e) providing public sector bodies with assistance in assessing the adequacy of contractual commitments made by a re-user pursuant to Article 32m(11).

Commission proposal	Drafting suggestions and Comments
	4. Each Member State shall notify the Commission of the identity of the competent bodies designated pursuant to paragraph 1 and of any subsequent change to the identity of those competent bodies. *Article 32u* **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 point (c) of Article 32i(2), research data shall be re-usable for commercial or non-commercial purposes in accordance with Sections III and IV, insofar as they are publicly funded and researchers, research performing organisations or research funding organisations have already made them publicly available through an institutional or subject-based repository. In that context, legitimate commercial interests, knowledge transfer activities and pre-existing intellectual property rights shall be taken into account. **Section IV** **NON-DISCRIMINATION AND FAIR TRADING** *Article 32v* **Non-discrimination** 1. Any applicable conditions for the re-use of documents shall be non-discriminatory for comparable categories of re-use, including for cross-border re-use.

Commission proposal	Drafting suggestions and Comments
	2. If 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 documents for those activities as apply to other users. *Article 32w* **Exclusive arrangements** ~~1.~~ The re-use of 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 documents. 2. Agreements or other practices pertaining to the re-use of data held by public sector bodies containing categories of data referred to in Article 32m(1) which grant exclusive rights or which have as their objective or effect to grant such exclusive rights or to restrict the availability of data for re-use by entities other than the parties to such agreements or other practices shall be prohibited. 3. By way of derogation from paragraph 2, an exclusive right to re-use data referred to in that paragraph may be granted to the extent necessary for the provision of a service or the supply of a product in the general interest that would not otherwise be possible. 4. An exclusive right as referred to in paragraph 3 shall be granted through an administrative act or contractual arrangement in accordance with applicable Union or national law and in compliance with the principles of transparency, equal treatment and non-discrimination. 5. 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. Notwithstanding paragraph 5, 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 subject to review during the 11th year and, if applicable, every seven years thereafter. Such arrangements granting

Commission proposal	Drafting suggestions and Comments
	exclusive rights shall be transparent and made public and 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. 7. The grant of an exclusive right pursuant to paragraphs 3 and 6, including the reasons as to why it is necessary to grant such a right, shall be transparent and be made publicly available online, in a form that complies with relevant Union law on public procurement. 4. Legal or practical arrangements 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 documents by entities other than the third party participating in the arrangement, shall 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. 5. Exclusive arrangements existing on 17 July 2013 that do not qualify for the exceptions set out in paragraphs 3 and 4 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 on 18 July 2043. Exclusive arrangements existing on 16 July 2019 that do not qualify for the exceptions set out in paragraphs 3 and 4, and that were entered into by public undertakings, shall be terminated at the end of the contract and in any event not later than on 17 July 2049. **Section V** **HIGH-VALUE DATASETS** *Article 32x* **Thematic categories of high-value datasets**

Commission proposal	Drafting suggestions and Comments
	1. In order to provide for conditions to support the re-use of high-value datasets, a list of thematic categories of such datasets is set out in Annex I. 2. The Commission is empowered to adopt delegated acts in accordance with Article 32y in order to amend Annex I by adding new thematic categories of high-value datasets in order to reflect technological and market developments. *Article 32y* **Specific high-value datasets and arrangements for publication and re-use** 1. -Specific high-value datasets listed in Annex I and held by public sector bodies and public undertakings among the documents to which this Chapter applies shall be: (a) available free of charge. The requirement to make high-value datasets available free of charge shall not apply to libraries, including university libraries, museums and archives. (b) made available in machine-readable formats via APIs corresponding to the reasonable needs of re-users; (c) made available as a bulk download where indicated in Annex I; (d) made available for re-use under the conditions of the Creative Commons Public Domain Dedication (CC0) or, alternatively, the Creative Commons BY 4.0 licence, or any equivalent or less restrictive open licence, as set out in the Annex, allowing for unrestricted re-use. A requirement of attribution, giving the credit to the licensor, can additionally be required by the licensor. (e) made available in accordance with the arrangements for the publication and re-use as set out in the Annex. 2. Those public sector bodies referred to in paragraph 1 shall set out and publish the terms of use of the API and the quality of service criteria on its performance, capacity and availability. The terms of use shall be available in a human-readable and machine-readable format. Both the terms of use and the quality of service criteria shall be compatible with the arrangements for the re-use of high-value datasets laid down in accordance with this Article.

Commission proposal	Drafting suggestions and Comments
	3. API terms of use shall be accompanied by API documentation in a Union or internationally recognised open, human-readable and machine-readable format. 4. Public sector bodies referred to in paragraph 1 shall designate a point of contact for questions and issues related to the API with a view to ensure the availability and maintenance of the API and ultimately the smooth and effective publication of the high-value datasets. 5. Public sector bodies holding high-value datasets listed in Annex I shall ensure that the datasets are denoted as high-value datasets in their metadata description. 6. The Commission may adopt implementing acts specifying high-value datasets beyond those described in Annex 1 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 SMCs and SMEs; (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, with respect to the re-use of documents. That impact assessment shall include a cost-benefit analysis and an analysis of whether providing high-value datasets free of charge by public sector bodies that are required to generate revenue to cover a substantial part of their costs relating to the performance of their public tasks would lead to a substantial impact on the budget of such bodies. With regard to high-value datasets held by public undertakings, the impact assessment shall give special consideration to the role of public undertakings in a competitive economic environment. DK

Commission proposal	Drafting suggestions and Comments
	(Comments): The chapter as proposed by the Commission seems to primarily combining the two rulesets on re-use of public sector information, rather than merging them, in effect making it more difficult for actors to determine which rules apply to the different data sets. Hence, DK proposes an alternative draft for the re-use of open government data with the intention of truly merging the ODD and the DGA, in order to clarify which rules apply and to simplify and streamline. We have inserted the proposed draft here, which is to replace "Section 2" in its entirety. IT (Comments): We recommend to further clarify the relationship between the different access regimes in Sections 2 and 3 in order to achieve the objective of providing greater legal clarity to public sector bodies and potential re-users, while not lowering the level of protection of personal data. Otherwise, the relationship between the access regimes under the new Data Act and national rules (see new art. 32(i)(5) above), which govern the re-use of personal data in this contex (see new art. 32i(9) Data Act), continues to be complex and unclear. One source of complexity is the definition of 'certain categories of protected data' under the new Art. 2(54) Data Act, which is dependent on whether personal data falls outside the scope of Section 2 of Chapter VIIc. In turn, the scope of Section 2 of Chapter VIIc is dependent on the scope of national access regimes (see new Art. 32i(3)(b)(ii) Data Act). Understanding the scope of Section 3 of Chapter VIIc requires reading (at least) new Articles 32i(4)(a) and 2(54) Data Act together, containing three negations: 'Section 3 of this Chapter does not apply to (a) data and documents that are not certain categories of protected data', meaning data 'protected on the grounds of ... (d) the protection of personal data, insofar as such data fall outside the scope of Section 2 of Chapter VIIc'

Commission proposal	Drafting suggestions and Comments
	PL (Comments): General comment: It is necessary to appropriately adapt the provisions of Section 2 of Chapter VIIc to the requirements applicable to an EU Regulation, which is directly applicable. A substantial part of the provisions of Section 2 has been transferred from Directive 2019/1024 to the proposed Chapter VIIc, in most cases without any amendments. Any changes introduced have been minimal. A comparison of the respective parts of Directive 2019/1024 and the proposed Section 2 leads to the conclusion that they are, in principle, the same provisions. Union acts should be drafted with due regard to the nature of the instrument concerned, in particular whether it is binding in its entirety and directly applicable (a regulation) or requires transposition (a directive). The wording of the provisions should reflect the type of legal act. Regulations are binding in their entirety and directly applicable. For this reason, their provisions must be formulated in such a way that the addressee has no doubts as to the rights and obligations arising from them. In some cases, the currently proposed provisions do not meet these requirements. The drafter has transferred provisions of a directive—addressed to Member States and implemented in national law—into a regulation that is to be applied directly. Such an approach cannot be endorsed. Appropriate amendments to the proposed provisions should therefore be introduced.
RE-USE OF OPEN GOVERNMENT DATA	
Subsection 1 Scope and General Principles	
Article 32n	
General principle for re-use of open government data	

Commission proposal	Drafting suggestions and Comments
(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	PL (Comments): General comment: Art. 32o should be re-drafted in order to reflect the type of the act that is regulation. Since regulations are directly applicable and are binding in their entirety, their provisions should be drafted in such a way that the addressees have no doubts as to the rights and obligations resulting from them
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.	

Commission proposal	Drafting suggestions and Comments
(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.	PL (Drafting suggestions): (2) ~~Where no time limits or other rules regulating the timely provision of data or documents have been established~~ **Unless shorter time limits have been established in accordance with national law,** 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~~ **one month** of receipt. That time frame may be extended by a further ~~20 working days~~ **one month** 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. PL (Comments): This will make the regulations in Sections 2 and 3 more consistent, as the timeframe in Section 3 is 2 months.
(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.	DE (Comments): **DE**: Paragraph 3 corresponds to Article 4(3); the deviations implement the new arrangement of exceptions to the scope of application of Article 1(2) ODD in Article 31i; the addition in brackets to Article 32n at the end of sentence 1 should be reviewed from a legalistic perspective. PL (Comments): **General comment:** There must be a clear and unambiguous regulation specifying when a refusal is required.

Commission proposal	Drafting suggestions and Comments
	This provision must be amended. It has been mechanically transferred from the directive to the regulation. In a directive, such wording was acceptable because a directive is not directly applicable. A regulation, however, must be unambiguous in this respect. If Member States are to decide on these matters, this must be clearly stated in the provisions. At present, it is unclear who is to determine which rules are to apply. **It is necessary to establish precise grounds for refusing access to data or documents within the procedure for handling requests for re-use (under Section 2). Such rules should be precise and uniform across all Member States. The regulation should clearly indicate when a public sector body is required to refuse access to data or documents under the provisions of Section 2.** **The reference to article 32i and 32n in this article is unsufficient – these provisions do not determine the grounds for refusal and they add confusion rather than clarity.**
(4) The means of redress shall include the possibility of review by an impartial review body with the appropriate expertise, such as the national competition authority, the relevant access to data or documents authority, the supervisory authority established in accordance with Regulation (EU) 2016/679 or a national judicial authority, whose decisions are binding upon the public sector body concerned.	IT (Comments): We recommend clarifying how this newly introduced provison on redress relates to the new Article 38 and Article 39 of the current Data Act.
(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:	

Commission proposal	Drafting suggestions and Comments
(a) public undertakings;	
(b) educational establishments, research performing organisations and research funding organisations.	
Subsection 3	IT (Comments): As stated above, we recommend to further clarify the relationship between the different access regimes in Sections 2 and 3 in order to achieve the objective of providing greater legal clarity to public sector bodies and potential re-users, while not lowering the level of protection of personal data. Otherwise, the relationship between the access regimes under the new Data Act and national rules, which govern the re-use of personal data in this contex, continues to be complex and unclear
Conditions for re-use	
Article 32p	PL (Comments): General comments: The regulation should establish clear rules for determining the conditions for the reuse of data and documents. In this regard, efforts should also be made at the European level to introduce an obligation to make data and documents available for reuse under standard licenses (within Section 2). Such an obligation has already been introduced in the HVD Implementing Regulation. Furthermore, consideration should be given to creating a single, harmonized European license for the reuse of data and documents. National licenses, such as Germany's Datenlizenz Deutschland and the United Kingdom's Open Government Licence, may serve as useful models. It is also worth noting that, to facilitate the sharing and reuse of software developed by the public

Commission proposal	Drafting suggestions and Comments
	administrations of Member States, the European Commission introduced a common EU Public License for open-source software (EUPL) a few years ago. This provides valuable experience that can be drawn upon. Introducing a European-level obligation to make data and documents available for reuse under standard licenses (in the framework of Section 2) would further help to reduce disparities between national regulations and practices in the field of open data. Standardizing licensing for data made available for reuse will simplify cross-border access to public resources for users.
Available formats	
(1) Without prejudice to Subsection 5, public sector bodies and public undertakings shall make their data or documents available in any pre-existing format or language and, where possible and appropriate, by electronic means, in formats that are open, machine-readable, accessible, findable and re-usable, together with their metadata. Both the format and the metadata shall, where possible, comply with formal open standards.	
(2) Member States shall encourage public sector bodies and public undertakings to produce and make available data or documents falling within the scope of this Section in accordance with the principle of 'open by design and by default.	PL (Comments): This provision should be amended and aligned with the requirements of the Regulation. This provision should be established for authorities and enterprises providing clear guidance on the application of these principles. The provision should be formulated in a manner that allows for direct applicability. The word "encourage" is not appropriate for the language of the regulation.
(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	

Commission proposal	Drafting suggestions and Comments
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.	PL (Drafting suggestions): Public sector bodies shall not be required to continue the production and storage of a certain type of **data or** 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.	FI (Drafting suggestions): FI: ~~(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.~~ FI (Comments): FI: We propose removing the obligation regarding dynamic data. It was introduced in the ODD/PSI recast of 2019, but it has (combined with the exemptions in the following paragraph) resulted in a great deal of confusion. What the obligation is is really just that data should be kept up to date at a degree and level which is fundamental to preserve the re-use value of the data. This applies to all kinds of data, not just data considered particularly "dynamic", but by creating a separate category of "dynamic data", the ODD has prompted an *a contrario* conclusion where data other than dynamic data does not need to be kept up to date. The need for data to be up to date is something that can be tackled by guidelines and applying the open data rules as a whole, rather than a very specific and technical legal rule.
(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	FI (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
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.	FI: ~~(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.~~ FI (Comments): FI: see above PL (Comments): General comment: We propose supplementing the provision with a regulation addressing the issue of "temporariness." We suggest that the authority is obliged to indicate the date from which it will comply with the requirements of paragraph 5, and to develop an action plan to bring it closer to that point. Otherwise, the provision would remain ineffective. Temporariness may turn into a permanent situation.
(7) Paragraphs 1 to 6 shall apply to existing data or documents held by public undertakings which are available for re-use.	FI (Drafting suggestions): FI: **(5)** Paragraphs **1** to **4** shall apply to existing data or documents held by public undertakings which are available for re-use. FI (Comments): FI: see above. Technical change.
(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.'	FI (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
	FI: **(6)** 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.' FI (Comments): FI: see above. Technical change.
Article 32q	
Principles governing charging for open government data	
(1) The re-use of data or documents within the scope of this Section shall be free of charge. However, the recovery by the public sector body holding the data of the marginal costs incurred for the reproduction, provision and dissemination of such data or documents as well as for anonymisation of personal data and measures taken to protect commercially confidential information may be allowed.	PL (Drafting suggestions): [...]However, the recovery by the public sector body holding the data **or documents** of the marginal costs incurred for the reproduction [...] PL (Comments): General comment: We propose introducing a more precise catalogue of costs that may be taken into account when determining the amount of the fee. Such a catalogue should be modeled on the solutions set out in Section 3. This would ensure internal consistency within the chapter and provide public sector authorities with a clear provision. The provision could be supplemented with a "in particular" catalogue.
(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.	

Commission proposal	Drafting suggestions and Comments
(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.	PL (Comments): The criteria and methodology for calculating fees should be determined at the EU level rather than at the national level. Allowing the criteria for calculating fees to be determined by the Member States would result in the introduction of 27 divergent pricing regimes and would undermine Europe's objective of making public data widely reusable. This would also be contrary to the nature of a regulation as a legislative act, which is intended to ensure uniform and unambiguous application. We believe that any criteria or methodologies concerning the calculation of fees should be developed and adopted exclusively at the European Union level. This would ensure uniform standards and principles for charging fees across all Member States. Even under the previous Directive 2003/98/EC, the European Commission issued such guidelines: (https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX:52014XC0724(01).
(5) Where charges are made by the public sector bodies referred to in paragraph 2, point (b), the total income from supplying and allowing the re-use of data or documents over the appropriate accounting period shall not exceed the cost of collection, production, reproduction, dissemination, data storage, preservation and rights clearance and, where applicable, the anonymisation of personal data and measures taken to protect commercially confidential information, together with a reasonable return on investment. Charges shall be calculated in accordance with the accounting principles applicable to the public sector bodies involved.	PL (Drafting suggestions): Where charges are made by the public sector bodies referred to in paragraph 2, point (b), the total income from supplying and allowing the re-use of data or documents over the appropriate accounting period shall not exceed the cost of collection, production, reproduction, dissemination, data **or documents** storage,[...]
(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	BE

Commission proposal	Drafting suggestions and Comments
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.	(Drafting suggestions): ~~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~~ BE (Comments): (Despite supporting the objective pursued by this proposed provision, to promote fair competition and innovation amongst small & medium sized businesses, Belgium has some concerns regarding the exception for very large enterprises set out in the proposed Articles 32q(6), 32r(4) and 32y(5). These provisions raise several difficulties: • Leaving the definition of the term 'very large enterprise' to the national authorities as well as the possibility to impose additional conditions may lead to fragmentation and additional administrative burdens. • The practical application of these provisions by public authorities may prove particularly complex and burdensome from an administrative point of view. Furthermore, questions may be raised about the ability of public authorities to identify these enterprises. • Finally, it should be noted that Article 32y.2 allows for a limitation of the costs borne by SMEs/SMCs, which therefore amounts to a de facto heavier financial burden for larger enterprises.

Commission proposal	Drafting suggestions and Comments
	• Therefore, we consider that this provision raises concerns regarding its effectiveness and practicability and would impose an additional administrative burden on public authorities. Even if the application is optional, the proposed articles 32q(6), 32r(4) and 32y(5) lead to additional complexity, including a multitude of administrative and legislative tasks for MS, for determining objective criteria and/or special or stricter conditions an/of higher fees and for its application and follow-up, and could in turn also create more fragmentation between MS. Finally, the regime is highly likley to be circumvented by VLE, who could eaisily set up 'strawman' like structures and who have the means use other alternative ways to avoid stricter conditions and higher fees. Even though Belgium is opposing the adoption of the exception (alternative treatment) regime for very large enterprises set out in the proposed Articles 32q(6), 32r(4) and 32y(5), *if these exceptions for VLE's are adopted in the end,* this will lead to a multitude of administrative and legislative tasks for MS, in order to ensure the exceptions will not be applied in an arbitraty manner. This in turn clearly requires a reasonable period of time. For this reason, *if the exception regime for very large enterprises set out in the proposed Articles 32q(6), 32r(4) and 32y(5), is adopted in the end*, Belgium proposes to pospone the entry into application of the new chapter VIIc (article 1(18)) : and have this new chapter enter into application 18 months from the entry into force of this Regulation. DE (Comments): **DE**: Paragraph 6 has been newly added and allows for higher fees if the recipient is a very large company, especially if it is a gatekeeper within the

Commission proposal	Drafting suggestions and Comments
	meaning of the DMA; it is questionable whether the definition of very large companies is clear enough. FI (Drafting suggestions): (6) ~~Public sector bodies may set out higher~~ **Charges higher than the charges provided for in paragraphs 1, 4 and 5 may be set out for the re-use of data and documents by very large enterprises.** 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. FI (Comments): FI: As the principles for charging fees can be set at the national level through legislation, rather than by the public sector bodies themselves, we propose changing the wording to a more general level to accommodate differences in Member States. (cf. Article 6 of the ODD) Otherwise, due to TFEU Article 288, this would allow public sector bodies to independently apply higher charges to very large enterprises regardless of national legislation. This would also be in line with paragraph 4 of Article 32q (this Article), requiring Member States to lay down criteria for charges. NL (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
	~~(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.~~ NL (Comments): NL doesn't support different conditions and higher rates. A variety of conditions for different enterprises increases complexity, and thus doesn't contribute to simplification PL (Comments): The provision uses the term "very large enterprise," which has not been defined. The provision is therefore imprecise.
(7) The re-use of the following shall be free of charge for the user:	PL (Drafting suggestions): The re-use of the following shall be free of charge for ~~the user:~~ **the re-user:** PL (Comments): An incorrect definition has been used. In the new Data Act, the definitions of "user" and "re-user" constitute two distinct concepts. The term "user" should therefore be replaced with the term "re-user.":

Commission proposal	Drafting suggestions and Comments
	(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; (12) 'user' means a natural or legal person that owns a connected product or to whom temporary rights to use that connected product have been contractually transferred, or that receives related services;
(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	PL (Comments): General comment: This regulation should lay down clear rules for determining the conditions for the re-use of data and documents. The current provision has been moved from the Directive and does not meet the requirements of direct applicability. We therefore propose introducing a catalogue of possible conditions for re-use based on standard licences. In this respect, Commission Implementing Regulation (EU) 2023/138 may serve as a model. Pursuant to that Regulation, high-value datasets shall be made available for re-use under the conditions of the Creative Commons Public Domain Dedication (CC0) or, alternatively, the Creative Commons BY 4.0 licence, or any equivalent or less restrictive open licence. The basic conditions for making data or documents available should be those indicated above. At the same time, it should be possible to provide for more restrictive conditions where the data or documents are protected by intellectual property rights. In such cases, those conditions should be justified by the existence of intellectual property rights. Furthermore, the possibility (as proposed in the

Commission proposal	Drafting suggestions and Comments
	Omnibus draft) of establishing more restrictive conditions for very large enterprises should be maintained. The use of standardised licences will facilitate the cross-border re-use of data and documents.
(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.	PL (Drafting suggestions): 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.~~ PL (Comments): As stated above
(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.	PL (Drafting suggestions): **2. By way of derogation of paragraph 1, where a conditions are justified by objective grounds, public sector bodies and public undertakings may establish conditions for the re-use of data and documents by the Creative Commons Public Domain Dedication (CC0) or, alternatively, the Creative Commons BY 4.0 licence, or any equivalent or less restrictive open licence allowing for unrestricted re-use. A requirement of attribution, giving the credit to the licensor, can additionally be required by the licensor. Such licenses shall be objective, proportionate, non-discriminatory and justified on grounds of a public interest objective.** ~~(2) When re-use is subject to conditions, those conditions shall not unnecessarily restrict possibilities for re-use and shall not be used to restrict competition.~~ PL

Commission proposal	Drafting suggestions and Comments
	(Comments): As stated above
(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.	PL (Drafting suggestions): **3. For data or documents covered by intellectual property rights, public sector bodies, in particular libraries, museums and archives and public undertakings, may establish more restrictive licensing terms for the re-use than those referred to in paragraph 2. Such licenses shall be objective, proportionate, non-discriminatory, justified on grounds of a public interest objective and of intellectual property rights.** ~~(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.~~ PL (Comments): As stated above
(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.	BE (Drafting suggestions): ~~(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.~~ BE

Formatted: Strikethrough

Commission proposal	Drafting suggestions and Comments
	(Comments): Despite supporting the objective pursued by this proposed provision, to promote fair competition and innovation amongst small & medium sized businesses, Belgium has some concerns regarding the exception for very large enterprises set out in the proposed Articles 32q(6), 32r(4) and 32y(5). These provisions raise several difficulties: • Leaving the definition of the term 'very large enterprise' to the national authorities as well as the possibility to impose additional conditions may lead to fragmentation and additional administrative burdens. • The practical application of these provisions by public authorities may prove particularly complex and burdensome from an administrative point of view. Furthermore, questions may be raised about the ability of public authorities to identify these enterprises. • Finally, it should be noted that Article 32y.2 allows for a limitation of the costs borne by SMEs/SMCs, which therefore amounts to a de facto heavier financial burden for larger enterprises. • Therefore, we consider that this provision raises concerns regarding its effectiveness and practicability and would impose an additional administrative burden on public authorities. Even if the application is optional, the proposed articles 32q(6), 32r(4) and 32y(5) lead to additional complexity, including a multitude of administrative and legislative tasks for MS, for determining objective criteria and/or special or stricter conditions an/of higher fees and for its application and follow-up, and could in turn also create more fragmentation between MS. Finally, the regime is highly likley to be circumvented by VLE, who could eaisily set up 'strawman' like structures and who have the means use other alternative ways to avoid stricter conditions and higher fees. Even though Belgium is opposing the adoption of the exception (alternative treatment) regime for very large enterprises set out in the proposed Articles

Commission proposal	Drafting suggestions and Comments
	32q(6), 32r(4) and 32y(5), *if these exceptions for VLE's are adopted in the end,* this will lead to a multitude of administrative and legislative tasks for MS, in order to ensure the exceptions will not be applied in an arbitraty manner. This in turn clearly requires a reasonable period of time. For this reason, *if the exception regime for very large enterprises set out in the proposed Articles 32q(6), 32r(4) and 32y(5), is adopted in the end*, Belgium proposes to pospone the entry into application of the new chapter VIIc (article 1(18)) : and have this new chapter enter into application 18 months from the entry into force of this Regulation. DE (Comments): **DE**: allows for exceptions reagrding standard licenses in case of very large companies / gatekeepers; cf. comment above regarding Article 32q(6); NL (Drafting suggestions): ~~(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.~~ NL (Comments): NL doesn't support different conditions and higher rates. A variety of conditions for different enterprises increases complexity, and thus doesn't contribute to simplification

Commission proposal	Drafting suggestions and Comments
	PL (Drafting suggestions): (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.~~ **Public sector bodies and public undertakings may establish more restrictive licensing terms for the re-use of data and documents by very large enterprises. Such licenses 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. After par. (4) add par. (5) **5. In the cases referred to in paragraph 3 and 4, public sector bodies and public undertakings shall indicate justified for establish conditions for the re-use of data and documents in relation to a specific re-use request.** PL (Comments): As stated above
Article 32s	PL (Comments): General comment: We propose amendments to Article 32s(1) to explicitly emphasise the role of data portals. We propose considering a revision of the title of the Article 32s (into "Data portals"). We also propose adding a new paragraph 3 to highlight the role of data portals maintained and dynamically developed by regional and local authorities.
Practical arrangements	PL

Commission proposal	Drafting suggestions and Comments
	(Drafting suggestions): ~~*Practical arrangements*~~ ***Data portals***
(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.	PL (Drafting suggestions): (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~~ **in data** portal**s** ~~sites that are linked to the asset lists~~. Where possible, Member States shall facilitate the cross-linguistic search for data or documents, in particular by enabling metadata aggregation at Union level.
Member States shall also encourage public sector bodies to make practical arrangements facilitating the preservation of data or documents available for re-use.	
(2) Member States shall, in cooperation with the Commission, continue efforts to simplify access to datasets, in particular by providing a single point of access and by progressively making available suitable datasets held by public sector bodies with regard to the data or documents to which this Section applies, as well as to data held by Union institutions, in formats that are accessible, readily findable and re-usable by electronic means.	PL (Drafting suggestions): After par. (2) add par. (3): **(3) Where possible practical arrangements as referred to in paragraph 1 shall be made by regional or local authorities.**
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	

Commission proposal	Drafting suggestions and Comments
principle of 'open by default' and compatible with the FAIR principles. In that context, concerns relating to intellectual property rights, personal data protection and confidentiality, security and legitimate commercial interests, shall be taken into account in accordance with the principle of 'as open as possible, as closed as necessary'. Those open access policies shall be addressed to research performing organisations and research funding organisations.	
(2) Without prejudice to Article 32n, paragraph 3, point (d), research data shall be re-usable for commercial or non-commercial purposes in accordance with Section 1 and Section 2 Subsection 3, insofar as they are publicly funded and researchers, research performing organisations or research funding organisations have already made them publicly available through an institutional or subject-based repository. In that context, legitimate commercial interests, knowledge transfer activities and pre-existing intellectual property rights shall be taken into account.	DE (Comments): **DE**: Paragraph 2 has been amended in line with the new order of exceptions to the scope of application of Article 1(2)(c) ODD in Article 32i(3)(c); the reference to Article 32n(3)(d) is likely to be an error and should be corrected to Article 32i(3)(c); PL (Comments): In Article 32t(2), a reference is made to an incorrect provision: "*Without prejudice to Article 32n, paragraph 3, point (d).*" No such provision exists.
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	

Commission proposal	Drafting suggestions and Comments
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.	BE (Comments): Do we understand well that the eralier proposed transistion an implementing act to a delegated act is no longer being pursued, since the proposed text specifies that it will be done through an implementing act? *If* the Commission still pursues the transition to a delegated act, we urge the Commission to conduct a thourough impact assessment to expand the categories and the list. We would like the Commission to confirm this and also confirm the possibility of Member States being directly and closely involved. PL (Drafting suggestions): (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. **Exemptions referred to in Article 32i paragraph 2 and 3 do not apply to such specific high-value datasets.** PL (Comments): According to art. 32v (1) Pursuant to Article 32v(1), the Commission shall adopt implementing acts laying down a list of specific high-value datasets (HVDs) 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. In Poland, a case has arisen in which the HVD was held by an entity excluded from the scope of the Directive (currently Section 2). We therefore

Commission proposal	Drafting suggestions and Comments
	propose an appropriate amendment to the provisions so that, in the case of HVDs, the general exemptions from the scope of the Directive would not apply. We also propose splitting the current paragraph 1 into three separate paragraphs. This would improve the clarity of the regulation. The new paragraphs would also be organised thematically.
Such specific high-value datasets shall be:	PL (Drafting suggestions): **(2)** ~~Such~~ specific high-value datasets **referred to in paragraph 1** shall be: (a) available free of charge, subject to paragraphs ~~3, 4 and 5~~ **5, 6 and 7;** (b) machine readable; (c) provided via APIs; and (d) provided as a bulk download, where relevant.
(a) available free of charge, subject to paragraphs 3, 4 and 5;	
(b) machine readable;	
(c) provided via APIs; and	
(d) provided as a bulk download, where relevant.	
Those implementing acts may specify the arrangements for the publication and re-use of high-value datasets. Such arrangements shall be compatible with open standard licences.	BE (Comments): Do we understand well that the eralier proposed transistion an implementing act to a delegated act is no longer being pursued, since the proposed text specifies that it will be done through an implementing act? *If* the Commission still pursues the transition to a delegated act, we urge the Commission to conduct a thourough impact assessment to expand the categories and the list. We would like the Commission to confirm this and

Commission proposal	Drafting suggestions and Comments
	also confirm the possibility of Member States being directly and closely involved. PL (Drafting suggestions): **(3)** ~~Those~~ implementing acts **referred to in paragraph 1** 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).	BE (Comments): Do we understand well that the eralier proposed transistion an implementing act to a delegated act is no longer being pursued, since the proposed text specifies that it will be done through an implementing act? *If* the Commission still pursues the transition to a delegated act, we urge the Commission to conduct a thourough impact assessment to expand the categories and the list. We would like the Commission to confirm this and also confirm the possibility of Member States being directly and closely involved.
(2) The identification of specific high-value datasets pursuant to paragraph 1 shall be based on the assessment of their potential to:	PL (Drafting suggestions): ~~(2)~~ **(4)** The identification of specific high-value datasets pursuant to paragraph 1 shall be based on the assessment of their potential to:

Commission proposal	Drafting suggestions and Comments
	PL (Comments): Change in the numbering of paragraphs
(a) generate significant socioeconomic or environmental benefits and innovative services;	
(b) benefit a high number of users, in particular SMEs and SMCs;	
(c) assist in generating revenues; and	
(d) be combined with other datasets.	
For the purpose of identifying such specific high-value datasets, the Commission shall carry out appropriate consultations, including at expert level, conduct an impact assessment and ensure complementarity with existing legal acts, such as Directive 2010/40/EU of the European Parliament and of the Council, with respect to the re-use of data or documents. That impact assessment shall include a cost-benefit analysis and an analysis of whether providing high-value datasets free of charge by public sector bodies that are required to generate revenue to cover a substantial part of their costs relating to the performance of their public tasks would lead to a substantial impact on the budget of such bodies. With regard to high-value datasets held by public undertakings, the impact assessment shall give special consideration to the role of public undertakings in a competitive economic environment.	BE (Comments): We would like the Commission to confirm the possibility of Member States being directly and closely involved in the impact assessment and the analysis for ensuring complementarity with existing legal acts.
(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.	PL (Drafting suggestions): (~~3~~) **(5)** 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

Commission proposal	Drafting suggestions and Comments
	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.	PL (Drafting suggestions): (~~4~~) **(6)** 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.	PL (Drafting suggestions): (~~5~~) **(7)** 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	DE (Comments): **DE**: In line with our comments with respect to the new definitions of “data” and “document” (p. 47/48): it is not advisable to broaden the scope of chapter II DGA by replacing “data” by “data or document”. DGA defines “data” as any digital content including (hence digital) documents. Omnibus defines “data” as all digital content excluding documents since “document” is defined to be non-digital content. Hence, by using “data or document” instead of “data” the DGA is broadened to apply to non-digital content. This is outside the scope of the original regulation and is not necessary
Re-use of certain categories of protected data held by public sector bodies	PL

Commission proposal	Drafting suggestions and Comments
	(Comments): General comment on Section 3: It is **necessary to clarify the provisions governing the requirements that may be imposed by public sector bodies to ensure that the protected nature of data is preserved.** Currently, the regulation does not allow for the introduction of requirements involving modification, aggregation, or the application of other disclosure control methods in the case of data protected for reasons of statistical confidentiality. Such measures are currently provided only for information constituting trade secrets and content protected by intellectual property rights. The obligation for public sector bodies to publish in advance the conditions for allowing re-use of protected data under the provisions of Section 3 is problematic. In this respect, the solution applied in Chapter II of Regulation 2022/868 has been copied. For protected data, the conditions for re-use must be determined on a case-by-case basis, individually, during the assessment of a specific re-use request. In doing so, the public sector body must take into account a range of factors, criteria, and variables, such as the type of data, the nature of the data, the size of the data set, the intended method of use (e.g., transfer of non-personal data to third countries), applicable legal provisions, the need to obtain consents and authorisations, and so on. All of this makes it **impossible to set the conditions for re-use in advance**. The conditions for a specific data set cannot be anticipated before a request is submitted, as the content of the conditions is determined by the intended manner and scope of use by the user. Moreover, such an "advance" specification of conditions could be inconsistent with the actual manner and scope of re-use and could consequently pose a risk of infringing third-party rights. It could also prove ineffective, as it would not address the specific manner and scope of the

Commission proposal	Drafting suggestions and Comments
	intended re-use. For these reasons, consideration should be given to removing this obligation. Furthermore, **clarification is needed as to whether Section 3 applies exclusively to data or also to documents**. The current title of Section 3 indicates that it concerns only certain categories of protected data. At the same time, some provisions within Section 3 also refer to documents. This approach may give rise to doubts and requires further clarification or specification. **We also propose that the provisions of Section 3 clearly indicate when a public sector body should refuse access to protected data**. Such a provision should be included in the article governing the procedure for submitting re-use requests (under Section 3) and should provide that a public sector body must refuse access to protected data when it is not possible to ensure that the protected nature of the data will be maintained. Questions also arise regarding the solution whereby the criteria and methodology for calculating fees (under Section 3) are determined by the Member States. Any additional criteria or methodologies concerning the determination of fees should be developed and adopted exclusively at the European Union level. This would ensure uniform standards and principles for charging fees across all Member States.
Article 32w	DE (Drafting suggestions): **Article 32va**
Conditions for re-use	DE

Commission proposal	Drafting suggestions and Comments
	(Drafting suggestions): ***General Principle relating to certain categories of protected data***
(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).	DE (Drafting suggestions): **This Section does not create any obligation on public sector bodies to allow the re-use of data or documents, nor does it release public sector bodies from their confidentiality obligations under Union or national law. It sets out minimum conditions for situations foreseen in national legislation on the re-use of protected data held by public sector bodies.** DE (Comments): **DE**: In COM(2025) 837 final it says in the EXPLANATORY MEMORANDUM: ”It sets out the general principle relating to the re-use of certain categories of protected data. This is the principle set out under Chapter II of Regulation (EU) 2022/868 (Data Governance Act), that the section does not create an obligation on public sector bodies to allow the re-use of protected data, but rather sets out minimum conditions where public sector bodies decide to make such data available for re-use.” This should become clearer either in Article 32i or in Section 3 of Chapter VIIc.
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:	DE (Comments):

Commission proposal	Drafting suggestions and Comments
	DE: Paragraph 2 transfers Art. 5 (7), (8) DGA to points a and b; point c merely clarifies that the provisions of the GDPR must be complied with (Art. 5 (2) DGA was transferred to Art. 32j (1)); However, Recital 17 of the DGA also contains an explicit clarification that the DGA does not affect the intellectual property rights of third parties and that it is not intended to restrict existing intellectual property rights of public bodies or their exercise in any way. This important clarifying statement is not found in either the regulatory part or the recitals of the proposal. In this regard, this corresponding statement is also transferred, at least in the Recitals.
(a) in compliance with intellectual property rights.	
(b) if data that is considered confidential in accordance with Union or national law on commercial or statistical confidentiality, is not disclosed, as a result of allowing re-use, unless such re-use is allowed based on the data subject's consent or the data holder's permission in accordance with paragraph 5.	
(c) in compliance with Regulation (EU) 2016/679.	
(3) To ensure the preservation of the protected nature as referred to in paragraph 2, public sector bodies may establish the following requirements:	
(a) to grant access for the re-use of data or documents only where the public sector body or the competent body, following the request for re-use, has ensured that those data or documents have been:	
(i) anonymised, in the case of personal data;	
(ii) subject to other forms of preparation of personal data;	DE (Comments):

Commission proposal	Drafting suggestions and Comments
	DE: Regarding personal data, an alternative to anonymization has been introduced in letter a, ii (subject to other forms of preparation of personal data), although it is unclear what forms are meant by this; in particular, it is unclear what is specifically meant here by "other forms" of processing personal data in addition to the anonymization mentioned in (i), except possibly pseudonymization. But then it is not clear why this would not be explicitly stated or given as an example. FI (Comments): FI: As recommended in section 154 of the EDPB/EDPS joint opinion, it is necessary to further explain and clarify what these prepations of personal data are. Otherwise this addition should be removed from the text. IT (Comments): This provision seems to imply that access could be granted to personal data for re-use without anonymising this data. If this is the case, the necessity of this possibility should be analysed and duly justified in a recital, keeping in mind the principle of data minimisation. In addition, we recommend clarifying what technical measures, other than pseudonymisation, are covered by these 'preparations' or at least to set out the objectives to be achieved by those technical measures. SI (Comments): SI considers that the proposed regulation (in point (a) (ii) of the third paragraph of Article 32w) of 'other forms of preparation of personal data' for allowing the re-use of data is particularly problematic in the part of the proposal for a regulation under consideration. From the proposed text it is not clear what is meant by "other forms of preparation of personal data" - whether it is a pseudonymization of personal data or some other technique -

Commission proposal	Drafting suggestions and Comments
	since pseudonymisation is not mentioned in the proposal as a technique for the protection of personal data (such as the anonymization, aggregation, alterations, etc. mentioned). As this are sensitive data, SI considers that it is necessary to regulate this matter in an appropriate manner in order to ensure transparency, security and maintain trust in such processing and data holders, as is currently regulated by the provision of Article 7 in DGA.
(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	

Commission proposal	Drafting suggestions and Comments
re-user to preserve the integrity of the protection of the data or documents. It shall also reserve the right to prohibit the use of results that contain information jeopardising the rights and interests of third parties. The decision to prohibit the use of the results shall be comprehensible and transparent to the re-user.	
Unless national law provides for specific safeguards on applicable confidentiality obligations relating to the re-use of certain categories of protected data, the public sector body shall make the re-use of data or documents provided in accordance with paragraph 3 conditional on the adherence by the re-user to a confidentiality obligation that prohibits the disclosure of any information that jeopardises the rights and interests of third parties and that the re-user may have acquired despite the safeguards put in place. In the event of the unauthorised re-use of non-personal data, the re-user shall be obliged, without delay, where appropriate with the assistance of the public sector body, to inform the natural or legal persons whose rights and interests may be affected.	
(5) Where the re-use of data or documents cannot be allowed in accordance with paragraphs 3 and 4, re-use shall only be possible:	DE (Drafting suggestions): Where the re-use of data or documents cannot be allowed in accordance with paragraphs **2**~~3~~ and **3**~~4~~, re-use shall only be possible: DE (Comments): **DE**: Please check references.
(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;	FI (Comments): FI: This should be deleted as superfluous, cf. the EDPB/EDPS joint opinion, section 155. IT

Commission proposal	Drafting suggestions and Comments
	(Drafting suggestions): ~~**(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;**~~ IT (Comments): This provision seems superfluous also in light of the new art. 32w(2)(c) Data Act. Against this background and bearing in mind that this provision could cause confusion, we recommend deleting it
(b) with the permission from the data holders whose rights and interests may be affected by such re-use.	
The public sector body shall make best efforts, in accordance with Union and national law, to provide assistance to potential re-users in seeking consent of the data subjects or permission from the data holders whose rights and interests may be affected by such re-use, where this is feasible without a disproportionate burden on the public sector body.	
Where it provides such assistance, the public sector body may be assisted by the competent bodies referred to in Article 32z.	
Article 32x	
Requirements for transfers of non-personal data to third countries by re-users	
(1) Where a re-user intends to transfer certain categories of protected data that are non-personal to a third country, it shall inform the public sector body of its intention to transfer such data and the purpose of such transfer at the time of requesting the re-use of the data. In the case of re-use based on the data holder's permission the re-user shall, where appropriate with the assistance of the public sector body, inform the natural or legal person whose rights and	

Commission proposal	Drafting suggestions and Comments
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:	DE (Drafting suggestions): (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 **5**~~7~~ only if the re-user contractually commits to: DE (Comments): **DE**: Please check references.
(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.	

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.	

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.	FI (Drafting suggestions): (2) Where ~~public sector bodies charge~~ **fees are charged, Member States** 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~~ **data may be made** 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 **may be established**. That list, together with the criteria used to establish it, shall be made public. FI (Comments): FI: As the principles for charging fees can be set at the national level through legislation, rather than by the public sector bodies themselves, we propose changing the wording to a more general level to accommodate differences in Member States. (cf. Article 6 of the ODD)

Commission proposal	Drafting suggestions and Comments
(3) Any fees shall be derived from the costs related to conducting the procedure for requests for the re-use of certain categories of protected data and limited to the necessary costs in relation to:	
(a) the reproduction, provision and dissemination of data;	
(b) the clearance of rights;	
(c) anonymisation or other forms of preparation of personal data and commercially confidential data as provided for in Article 32w(3)[conditions for re-use];	
(d) the maintenance of the secure processing environment;	
(e) the acquisition of the right to allow re-use in accordance with this Section by third parties outside the public sector; and assisting re-users in seeking consent from data subjects and permission from data holders whose rights and interests may be affected by such re-use.	
(4) The criteria and methodology for calculating fees shall be laid down by the Member States and published. The public sector body shall publish a description of the main categories of costs and the rules used for the allocation of costs.	
(5) Public sector bodies may charge higher fees than those allowed in accordance with paragraph 2 and 3 of this Article with respect to very large enterprises, based on objective criteria, taking into account the economic power, or the ability of the entity to acquire data, including in particular a designation as a gatekeeper under Regulation (EU) 2022/1925. Any such calculated fees shall be proportionate. In addition to the elements listed in paragraph 3 of this Article, they can cover the cost of collection and production of the data, together with a reasonable return on investment.	BE (Drafting suggestions): ~~(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~~

Formatted: Strikethrough

Commission proposal	Drafting suggestions and Comments
	~~paragraph 3 of this Article, they can cover the cost of collection and production of the data, together with a reasonable return on investment.~~ BE (Comments): Despite supporting the objective pursued by this proposed provision, to promote fair competition and innovation amongst small & medium sized businesses, Belgium has some concerns regarding the exception (alternative treatment) for very large enterprises set out in the proposed Articles 32q(6), 32r(4) and 32y(5). These provisions raise several difficulties: • Leaving the definition of the term 'very large enterprise' to the national authorities as well as the possibility to impose additional conditions may lead to fragmentation and additional administrative burdens. • The practical application of these provisions by public authorities may prove particularly complex and burdensome from an administrative point of view. Furthermore, questions may be raised about the ability of public authorities to identify these enterprises. • Finally, it should be noted that Article 32y.2 allows for a limitation of the costs borne by SMEs/SMCs, which therefore amounts to a de facto heavier financial burden for larger enterprises. • Therefore, we consider that this provision raises concerns regarding its effectiveness and practicability and would impose an additional administrative burden on public authorities. Even if the application is optional, the proposed articles 32q(6), 32r(4) and 32y(5) lead to additional complexity, including a multitude of administrative and legislative tasks for MS, for determining objective criteria and/or special or stricter conditions an/of higher fees and for its application and follow-up, and could in turn also create more fragmentation between MS. Finally, the regime is highly likley to be circumvented by VLE, who could eaisily set up

Commission proposal	Drafting suggestions and Comments
	'strawman' like structures and who have the means use other alternative ways to avoid stricter conditions and higher fees. Even though Belgium is opposing the adoption of the exception (alternative treatment) regime for very large enterprises set out in the proposed Articles 32q(6), 32r(4) and 32y(5), *if these exceptions for VLE's are adopted in the end,* this will lead to a multitude of administrative and legislative tasks for MS, in order to ensure the exceptions will not be applied in an arbitraty manner. This in turn clearly requires a reasonable period of time. For this reason, *if the exception regime for very large enterprises set out in the proposed Articles 32q(6), 32r(4) and 32y(5), is adopted in the end*, Belgium proposes to pospone the entry into application of the new chapter VIIc (article 1(18)) : and have this new chapter enter into application 18 months from the entry into force of this Regulation. NL (Drafting suggestions): ~~(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.~~ NL (Comments):

Commission proposal	Drafting suggestions and Comments
	NL doesn't support different conditions and higher rates. A variety of conditions for different enterprises increases complexity, and thus doesn't contribute to simplification
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.	FI (Drafting suggestions): FI: 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. FI (Comments): FI: Our proposal is to remove Chapter VIIc from the scope of Article 37 and keep the rules regarding competent bodies within Section 3 of Chapter VIIc to avoid ambiguity and confusion (see later for details on this). Accordingly the reference to Article 37 in Article 32z needs to be removed; what remains is basically the existing DGA Article 7 which has already been a sufficient legal basis for competent bodies.
(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.	

Commission proposal	Drafting suggestions and Comments
(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).	DE (Drafting suggestions): (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~~ **certain** categories of protected data referred to in in Article 2(54). DE (Comments): **DE**: Paragraph 3 corresponds to Article 7(3) of the DGA; for reasons of consistency, reference should be made here to the definition of "certain categories of protected data" instead of to 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	

Commission proposal	Drafting suggestions and Comments
sector bodies in establishing technical mechanisms that allow the transmission of requests for consent or permission from re-users, where practically feasible;	
(e) providing public sector bodies with assistance in assessing the adequacy of contractual commitments made by a re-user pursuant to Article 32x(2).	
Article 32aa	
Single information point	
(1) Each Member State shall designate a single information point. That point shall make available easily accessible information concerning the application of Articles 32w, 32x and 32y.	FI (Drafting suggestions): FI: (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. **The single information point may be linked to sectoral, regional or local information points.** FI (Comments): FI: In light of the removal of the recitals of the DGA, we would prefer to reinstate this element from Article 8(1) DGA to clarify that the existence of and linking to sectoral, regional or local information points is possible. The Finnish implementation relies heavily on sectoral information points.
(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.	

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).	DE (Drafting suggestions): (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~~ **certain** categories of data referred to in Article 2(54). DE (Comments): **DE**: Paragraph 3 corresponds to Article 8(3) of the DGA, but adds SMC; for reasons of consistency, reference should be made here to the definition of "certain categories of protected data" instead of to 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.	DE (Comments): **DE**: Paragraph 4 corresponds to Art. 8(2) sentence 2 DGA; it should read "data or document resources", see comment with respect to „data" and „document" above (p. 132) – we suggest to either be consistent or to delete „or document" for the entire section 3.
(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	

Commission proposal	Drafting suggestions and Comments
for the re-use of certain categories of protected data within two months of the date of receipt of the request.	
(2) In the case of exceptionally extensive and complex requests for re-use, that two-month period may be extended by up to 30 days. In such cases the competent public sector bodies or the competent bodies referred to in paragraph 1 of Article 32z shall notify the applicant as soon as possible that more time is needed for conducting the procedure, together with the reasons for the delay.	
(3) Any natural or legal person directly affected by a decision as referred to in paragraph 1 shall have an effective right of redress in the Member State where the relevant body is located. Such a right of redress shall be laid down in national law and shall include the possibility of review by an impartial body with the appropriate expertise, such as the national competition authority, the relevant access-to-documents authority, the supervisory authority established in accordance with Regulation (EU) 2016/679 or a national judicial authority, whose decisions are binding upon the public sector body or the competent body concerned.'	IT (Comments): we recommend clarifying how this newly introduced provision on redress relates to the new Article 38 and Article 39 of the current Data Act.
19. Article 38 is replaced by the following:	DE (Drafting suggestions): Article 33 (1) […] (d) where applicable, the means to enable the interoperability of tools for automating the execution of data sharing agreements~~, such as smart contracts~~ shall be provided. […] (11) The Commission may adopt guidelines taking into account the proposal of the EDIB in accordance with Article 30, point (h), of Regulation (EU)

Commission proposal	Drafting suggestions and Comments
	2022/868 laying down interoperable frameworks for common standards and practices for the functioning of common European data spaces. **Within six months after [Digital Omnibus Regulation] has entered into force the Commission shall adopt guidelines laying down frameworks for common standards and practices for the functioning of common EU data spaces, taking into account existing standards. The guidelines shall be updated at least annually.** Article 37 […] **(17) For the purposes of cooperation under this Regulation, the Commission shall provide and operate at their own expense a secure information sharing system to facilitate communication and information exchange between competent authorities and with the Commission. It shall ensure an appropriate level of security and data protection in accordance with Union law."** **(18) The Commission shall adopt implementing acts laying down the practical and operational arrangements for the functioning of the information sharing system and its interoperability with other relevant systems.** DE (Comments): **DE**: Deletion in Paragraph 1 as consequence of deletion of smart contracts from scope of Data Act (see. Art. 36 Data Act).

Commission proposal	Drafting suggestions and Comments
	German Position Paper on the European Commission's Digital Omnibus, p. 1 ("[legal acts] should be formulated in a clear and precise manner ensuring legal clarity and certainty"), p. 2 ("ensure uniform implementation and harmonization"). Guidelines should be developed on specific topics and updated annually. The role of the EDIB in the creation of all guidelines should be laid down in the Data Act. **DE**: legal basis for digital platform for competent authorities to communicate and exchange information inter alia on pending cases. FI (Drafting suggestions): FI: 4. This Article shall not apply to Chapter VIIc. FI (Comments): FI: We propose that Article 37 have the following paragraph 17 added: 17. This Article shall not apply to Chapter VIIc. We also propose that Article 38 and Article 39 also have the following paragraph 4 added to both:

Commission proposal	Drafting suggestions and Comments
	4. This Article shall not apply to Chapter VIIc. These changes would mirror the proposed Article 40(6) and be in line with the goal of transposing the existing ODD and DGA Chapter II into the Data Act while also simplifying the data acquis and not creating new burdens. The ODD as it is currently does not provide for a competent authority to monitor it, and the DGA does not require a competent authority to enforce Chapter II of the DGA. Therefore a competent authority is not necessary to enforce the provisions of Chapter VIIc, as the provisions obligate public sector bodies and publicly controlled undertakings and because Chapter VIIc already requires access to remedies and a complaint mechanism if the party requesting re-use of data or a document has had their rights under Chapter VIIc infringed. Requiring the appointment of a competent authority for rules that did not require them previously would increase administrative burden and complicate regulation. Similarly, neither the ODD nor the DGA Chapter II contain a provision on lodging complaints. Instead both of them have provisions for remedies when a re-use request is rejected, which would be maintained in Chapter VIIc, making a separate complaint mechanism through Article 38 and separate requirements for remedies through Article 39 superfluous and contribute to making the data acquis more complicated. The EDPB/EDPS joint opinion of February 11 has also pointed out the need to clarify the relationship between Chapter VIIc and Chapter IX (see section 157 of the joint opinion). The proposed changes would accomplish this. IT (Drafting suggestions): **19a Article 37(3) is replaced by the following:**

Commission proposal	Drafting suggestions and Comments
	The supervisory authorities responsible for monitoring the application of Regulation (EU) 2016/679 shall be responsible for monitoring the application of this Regulation insofar as the protection of personal data is concerned on the basis of their existing competences and responsibilities under the GDPR. **Article 37(5)(g) is replaced by the following:** **cooperating with the relevant competent authorities responsible for the implementation of other Union or national legal acts, including with authorities competent in the field of data and electronic communication services, with the supervisory authority responsible for monitoring the application of Regulation (EU) 2016/679 or with sectoral authorities. In accordance with their respective competences under Union and national law. Those authorities shall establish strong cooperation and exchange information, including information obtained in the context of encorcements activities, as is necessary for the exercise of their tasks,and shall aim to achieve consistency in the decisions taken in applying this Regulation.** IT (Comments): The allocation of responsibilities between competent authorities under Article 37(1) of the current Data Act and supervisory authorities, related to

Commission proposal	Drafting suggestions and Comments
	the monitoring of the application of the Data Act insofar as the processing of personal data is concerned (Article 37(3) of the current Data Act), is ambiguous and further clarification is warranted. Therefore, to ensure legal certainty, it should be clearly indicated under Article 37(3) Data Act that data protection supervisory authorities participate in the monitoring of the application of the Data Act only on the basis of their existing competences and responsibilities under the GDPR. In addition, we recommend providing an explicit legal basis in art. 37(1)(g) Data Acr for the exchange of all relevant information, including information obtained on ongoing investigations, between competent authorities under the Data Act and competent authorities responsible for other Union or national legal acts. This would enable the effective and consistent enforcement of the Data Act and other Union or national legal acts, but also provide legal certainty for the enforcers and limit possible legal disputes on procedural matters. In particular, it should be clarified even in a recital that, as part of such cooperation, the supervisory authority under the GDPR must be consulted by the authority designated under Article 37(1) of the current Data Act to provide their assessment in cases that require an assessment of EU and national data protection law (for example, on whether a data holder correctly qualifies which data should be considered personal data or whether a valid legal basis under the GDPR exists for a user who is not a data subject) NL (Drafting suggestions): **19. In article 37 is amended as follows:** **(a) Paragraph 5 is amended as follows:** **(i) To point (g) is added:** **"including the exchange of all relevant information."**

Commission proposal	Drafting suggestions and Comments
	(ii) The following point is added to paragraph 5. **k) monitor and supervise whether recognised data intermediation services providers comply with the requirements laid down in Chapter VIIa, including whether they continue to comply with the requirements for registration laid down therein, either on their own initiative or on a request by a natural or legal person.** **(b) the following paragraph is added:** **8a. The competent authorities responsible for the application and enforcement of Chapter VIIa shall be set up in a manner so that their independence from any recognised data intermediation services provider is guaranteed.** **(c) Parapgraphs 11, 12 and 13 are replaced by the following:** **11. Any entity falling within the scope of this Regulation that makes connected products available or offers services in the Union, data intermediation servies providers that are not established in the Union, shall designate a legal representative in one of the Member States.** **12. For the purpose of ensuring compliance with this Regulation, a legal representative shall be mandated by an entity falling within the scope of this Regulation that makes connected products available or offers services in the Union, data intermediation servies providers to be addressed in addition to or instead of it by competent authorities with regard to all issues related to that entity. That legal representative shall cooperate with and comprehensively demonstrate to the competent authorities, upon request, the actions taken and provisions put in place by the entity falling within the scope of this Regulation that makes connected products available or offers services in the Union, data intermediation servies providers to ensure compliance with this Regulation.**

Commission proposal	Drafting suggestions and Comments
	13. An entity falling within the scope of this Regulation that makes connected products available or offers services in the Union, and data intermediation servies providers shall be considered to be under the competence of the Member State in which its legal representative is located. The designation of a legal representative by such an entity shall be without prejudice to the liability of, and any legal action that could be initiated against, such an entity. Until such time as an entity designates a legal representative in accordance with this Article, it shall be under the competence of all Member States, where applicable, for the purposes of ensuring the application and enforcement of this Regulation. Any competent authority may exercise its competence, including by imposing effective, proportionate and dissuasive penalties, provided that the entity is not subject to enforcement proceedings under this Regulation regarding the same facts by another competent authority. **(d) Parapgraph 14 is replaced by the following:** **14. Competent authorities shall have the power to request from users, data holders, data recipients, recognised data intermediation services providers or their legal representatives, falling under the competence of their Member State all information necessary to verify compliance with this Regulation. Any request for information shall be proportionate to the performance of the underlying task and shall be reasoned.** **20. After article 37 a new article is inserted:** ***Article 37a Non-compliance recognised data intermediation services providers or recognised data altruism organisations*** **(1) Where a competent authority finds that a recognised data intermediation services provider does not comply with one or more of the requirements laid down in this Regulation, 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.**

Commission proposal	Drafting suggestions and Comments
	(2) The competent authority shall have the power to require the cessation of the non-compliance either immediately or within a reasonable time limit and shall take appropriate and proportionate measures with the aim of ensuring compliance. **(3) If a recognised data intermediation services provider does not comply with one or more of the requirements laid down in this Regulation even after having been notified in accordance with paragraph 1, 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.** **~~19.~~ 21. Article 38 is replaced by the following:** NL (Comments): 19. It is better to have all comptent authorities articles in art. 37 for consistency and to avoid doubeling. (a) (i) In line with art. 13(3) DGA and art. 37(5)(f) DA the exchange of information is added. (a) (ii) This task from art. 32g(1) is added to art. 37 (5). (b) Text from art. 32b(2). (c) Text from art. 32e(2) is merged into art. 37(11)(12)(13). (d) Text from art. 32g(2). Text is similar.

Commission proposal	Drafting suggestions and Comments
	20. It is better to have all comptent authorities articles in chapter IX. In new article 37a about non-compliance recognised data intermediation services providers. Rules come from art. 32g (3)(4)(5).
(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.	NL (Drafting suggestions): (b) any matter falling within the scope of this Regulation specifically against a recognised data intermediation services provider ~~or a recognised data altruism organisation~~, with the relevant competent authority for the registration of data intermediation services ~~or the relevant competent authority for the registration of data altruism organisations.~~
(2) The data coordinator shall, upon request, provide all the necessary information to natural and legal persons for the lodging of their complaints with the appropriate competent authority.	
(3) The competent authority with which the complaint has been lodged shall inform the complainant, in accordance with national law, of:	
(a) the progress of the proceedings, of the decision taken; and	
(b) the judicial remedies provided for in Article 39.'	IT (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
	(4) competent authorities shall cooperate to handle and resolve complaints effectively and in a timely manner, including by exchanging all relevant information by electronic means, without undue delay. IT (Comments): We would recommend re inserting Article 38(3) of the current Data Act to allow cooperation, including the exchange of information, between competent authorities when handling complaints so as to provide more legal certainty for how cooperation should function and reduce the risk of possible future legal disputes on procedural matters
20. in Article 40, paragraph (6) is inserted:	
'6. This Article shall not apply to Chapter VIIc.'	FI (Comments): FI: As above regarding Articles 37 through 39, we consider this a necessity to support integrating the proposed Chapter VIIc into the Data Act. NL (Drafting suggestions): '6. This Article shall not apply to Chapters VIIb and VIIc.' NL (Comments): No sanctions are needed for chapter VIIb. PL (Drafting suggestions): This Article shall not apply to Chapters **VIIa and** VIIc. PL

Commission proposal	Drafting suggestions and Comments
	(Comments): This new drafting only clarifies the evident omission and makes sure that this article's provision do not apply to data intermetiation provieds and data altrisum organisaations and that both are only subject to penaties stipulated in Chapter VIIa (losing the right to use the label – Art. 32g(5)).
21. after Article 41, the following heading is inserted:	DE (Drafting suggestions): Chapter IX IMPLEMENTATION AND ENFORCEMENT **Article […] Transitional provision** **Where a Member State has designated one or more competent authorities or a competent body for the application and enforcement of [name inserted legal act here], such designation shall remain valid and shall apply to the application and enforcement of Chapter [name Chapter of Data Act, in which legal act is inserted] of this Regulation in analogy, until the Member State designates one or more other authorities or bodies for the application and enforcement of these Chapters in accordance with Article 37 paragraph 1.** DE (Comments): **DE**: wording taken from Article 1 Number 71 Digital Omnibus (concerning competent authority according to DGA)
'CHAPTER IXa	
European Data Innovation Board';	FI (Comments):

Commission proposal	Drafting suggestions and Comments
	FI: Detailed references to the EDIB articles should be reviewed throughout the Regulation since some references are no longer accurate (Technical comment)
22. the following Article 41a is inserted:	
‘Article 41a	SI (Comments): SI generally supports streamlining the governance framework in order to avoid regulatory fragmentation. We agree that the European Data Innovation Board (EDIB) should evolve into a forum capable of steering the broader strategic direction of the European data economy, including in light of the geopolitical dimension of data flows. However, SI would welcome further clarification on the operational consequences of the proposed simplification in Article 41a. While supporting a stronger focus on strategic discussions, we caution against any dilution of the technical expertise necessary for effective implementation of the Regulation. In particular, if the statutorily mandated subgroups (previously Article 29(2) DGA) are removed, it is important to ensure that the EDIB retains the capacity to address detailed interoperability and standardisation issues. SI therefore welcomes safeguards ensuring that the increased involvement of high-level policy representatives does not marginalise the contribution of technical competent authorities, whose expertise remains essential for the effective functioning of Common European Data Spaces.
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.	ES (Drafting suggestions): The European Data Innovation Board is established as a means to advising and assisting the Commission in coordinating **and monitoring** the

Commission proposal	Drafting suggestions and Comments
	enforcement of this Regulation and to serve as a forum of **strategic** discussion for the development of a European data economy and data policies. ES (Comments): This change elevates the EDIB from a purely advisory role to an active role. Adding "monitoring" ensures the Board tracks the actual impact of the Regulation on the market, while "strategic" empowers it to shape long-term policy rather than just reacting to Commission requests. FI (Drafting suggestions): 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. **The Board will convene both at a strategic level and in focused operational compositions.** FI (Comments): FI: Finland wishes to further strengthen the role of EDIB by establishing a clearer governance structure that allows it to convene both at a strategic level and in a focused operational composition. LV (Comments): Clarification is required regarding the future model for expert working groups that are currently engaged in sector-specific legislative work.
(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	BE (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
European Data Protection Board, the European Data Protection Supervisor, ENISA, the EU SME Envoy or a representative appointed by the network of SME envoys. The Commission may decide to add additional categories of members. In its appointments of individual experts, the Commission shall aim to achieve gender and geographical balance among the members of the group.	(2) It shall be composed at least of representatives of Member States competent for matters related to data, the competent authorities for enforcement of Chapters II, III, V, VIIa and VIIc of this Regulation, the European Data Protection Board, the European Data Protection Supervisor, ENISA, the EU SME Envoy or a representative appointed by the network of SME envoys. The Commission may decide to add additional categories of members. In its appointments of individual experts, the Commission shall aim to achieve gender and geographical balance among the members of the group. **Member States shall ensure that their representatives have the relevant competences and powers in their Member State so as to contribute actively to the achievement of the Board's tasks referred to in Article 42.** BE (Comments): Belgium agrees with and supports the proposed changes to simplify the structure of the EDIB. However, it is important to ensure appropriate representation of the Member States within the EDIB in order to enable effective strategic policy discussions. We would like to thank the Commission for the clarifications provided in the Q&A at the AGS on 13 February, particularly with regard to the intention to address enforcement and strategic issues separately within the EDIB. We consider that such clarifications should be reflected in the provision itself. As discussed in the AGS on 13 February, we suggest to reflect on a structure similar to the AI Board, mainly competent for coordination and strategic discussion, and the subgroups for the different topics on enforcement questions, such as the re-use of public data, data intermediation services, IoT data sharing and cloud. In addition, we suggest clarifying Art. 41a(2) by inserting wording similar to that set out in Art. 65(4)(a) of the AI Act, to ensure that Member States can designate their national representatives for the different areas of this regulation. DK

Commission proposal	Drafting suggestions and Comments
	(Drafting suggestions): (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, **VI,** VIIa and VIIc of this Regulation, the European Data Protection Board, the European Data Protection Supervisor, ENISA, the EU SME Envoy or a representative appointed by the network of SME envoys. The Commission may decide to add additional categories of members. In its appointments of individual experts, the Commission shall aim to achieve gender and geographical balance among the members of the group. DK (Comments): DK supports widening the scope of participating competent authorities, so as to ensure that competent authorities for all the relevant data legislation are represented. DK further supports that the Commission can decide to add additional categories of members. DK would prefer that the competent authorities for Chapter VI of the Data Act is included. It would be prudent to merge the powers and tasks related to the data legislation under one body, namely EDIB, to ensure consistency across the Data Act, why Chapter VI on cloud switching should be covered by EDIB. ES (Drafting suggestions): 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~~ **Board** may decide to add additional categories of members. In its appointments of individual experts, the ~~Commission~~ **Board**

Commission proposal	Drafting suggestions and Comments
	shall aim to achieve gender and geographical balance among the members of the group. **Member States shall ensure that their representatives on the Board:** **(a) have the relevant competences and powers in their Member State so as to contribute actively to the achievement of the Board's tasks referred to in Article 42;** **(b) are designated as a single contact point vis-à-vis the Board and, where appropriate, taking into account Member States' needs, as a single contact point for stakeholders;** **(c) are empowered to facilitate consistency and coordination between national competent authorities in their Member State as regards the implementation of this Regulation, including through the collection of relevant data and information for the purpose of fulfilling their tasks on the Board.** ES (Comments): This amendment aligns the requirements for Board members with Article 65(4) of the AI Act. It ensures that Member State representatives possess not only technical expertise but also the necessary 'competences and powers' at the national level to ensure the actual enforcement of the Board's decisions. Furthermore, transferring the power to add member categories from the Commission to the Board itself mirrors the institutional independence of the AI Board, allowing the body to adapt to evolving technical needs autonomously and reducing political dependency. FI (Drafting suggestions): (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

Commission proposal	Drafting suggestions and Comments
	European Data Protection Board, the European Data Protection Supervisor, ENISA, the EU SME Envoy or a representative appointed by the network of SME envoys. **If a Member State has designated more than one competent authority or competent body, they are represented in the plenary meetings of the Board by the designated data coordinator. Other competent authorities or competent bodies entrusted with specific operational responsibilities for the application and enforcement of this Regulation may par-ticipate in the thematic subgroups of the Board relevant for their responsibilities.** The Commission may decide to add additional categories of members. In its appointments of individual experts, the Commission shall aim to achieve gender and geographical balance among the members of the group. FI (Comments): FI: To avoid an overly large plenary, its composition should be further specified, drawing on the DSA Board model where the data coordinator represents the national competent authorities, while additional competent authorities may participate in sub groups where relevant.
(3) The Commission shall decide on the composition of the different configurations in which the Board will fulfil its tasks.	ES (Drafting suggestions): ~~The Commission shall decide on the composition of the different configurations in which the Board will fulfil its tasks.~~ **The Board shall be organised and operated so as to safeguard the objectivity and impartiality of its activities.** **The Board shall establish at least the following three permanent standing sub-groups to ensure specialized technical expertise and consistent enforcement across the pillars of this Regulation:**

Commission proposal	Drafting suggestions and Comments
	(a) a sub-group for Data Rights and Access (Chapters II, III, IV, and V), focusing on product data access, B2B fair contractual terms, and B2G data sharing **(b) a sub-group for Data Intermediation and Trust (Chapters VIIa and VIIc), focusing on the oversight of data intermediation services and data altruism organizations;** **(c) a sub-group for Open Data and High-Value Datasets (Chapter VIIb), focusing on the re-use of public sector data and the implementation of high-value dataset requirements.** ES (Comments): This amendment, inspired by article 65(7) of the AI Act, shifts the Board from a Commission-led advisory group to a structured, independent, and specialized Board. By replacing 'Commission-decided configurations' with a mandate for 'objectivity and impartiality,' the Board gains the institutional independence necessary to act as a neutral arbiter for the data economy. Furthermore, the establishment of permanent standing sub-groups follows the successful model of Article 65(6) of the AI Act, ensures that the EDIB has the specialized technical expertise required to manage the distinct pillars consolidated by the Digital Omnibus. This structure prevents technical dilution and ensures that dedicated experts handle the specific complexities of Data Rights (Chapters II-V), Data Intermediation (Chapters VIIa/c), and Open Data (Chapter VIIb) simultaneously, leading to more consistent enforcement across the Union. FI (Drafting suggestions): ~~(3) The Commission shall decide on the composition of the different configurations in which the Board will fulfil its tasks.~~

Commission proposal	Drafting suggestions and Comments
	(3) (NEW) The Board shall adopt its an annual work programme and rules of procedure after hearing the Commission. The rules of procedure shall include principles for the organisation of the Board's activities and those of its sub-groups. FI (Comments): FI: We propose that paragraph 3 be deleted and a new paragraph 3 added. We find it essential that the EDIB has a real opportunity to shape the organisation of its own work, and that its operations are planned in a way that facilitates the efficient use of national authorities' resources. Sub groups should be established where necessary, particularly for supervisory and enforcement matters, which should remain limited to competent authorities to ensure consistent implementation across the Union. Clear coordination and delineation of responsibilities are needed to avoid overlapping structures. In addition, Finland sees a need to find a solution for cooperation concerning data processing services under the Data Act. This could either be added to the tasks of the EDIB, or alternatively, assigned to another body, such as BEREC.
(4) The Commission shall chair the meetings of the European Data Innovation Board.'	DE (Drafting suggestions): […] **(5) The Board shall have a permanent set of subgroups to ensure consistent practice of competent authorities in the enforcement of Chapters II, III, V, VII, VIIa and VIIc across all member states.**

Commission proposal	Drafting suggestions and Comments
	(6) Within six months after [Digital Omnibus Regulation] has entered into force, the EDIB shall suggest and the Commission shall publish guide-lines, especially addressing SMEs in the scope of this Regulation and covering, at least, the following topics: **(a) Roles and scope: users, data holders, data recipients and SME status (ad-dressing parallel roles of SMEs and specification of SME exemptions);** **(b) Data categories and mixed data sets: what is product data, related service data and how to apply Regulation (EU) 2016/679;** **(c) Contract drafting and remuneration: FRAND, unfair terms and model clauses.** **The guidelines shall be updated at least an-nually.** DE (Comments): **DE**: German Position Paper on the European Commission‘s Digital Omnibus, p. 2:

Commission proposal	Drafting suggestions and Comments
	„Streamlining and harmonizing of EU governance (e.g., European Data Innovation Board, Art. 29/30 DGA…) to ensure uniform implementation and harmonization of data related legal acts and measures across the EU." Subgroups within EDIB should be maintained as the past year has shown that the added value of the EDIB is not limited to advising the Commission. Rather, a body is also needed to ensure a coherent application practice among the participating competent authorities. The existing shadow groups are merely a temporary measure. The stated goal should be achieved by setting up subgroups based in Union law. **DE**: German Position Paper on the European Commission's Digital Omnibus, p. 1 ("[legal acts] should be formulated in a clear and precise manner ensuring legal clarity and certainty"), p. 2 ("ensure uniform implementation and harmonization"). Guidelines should be developed on specific topics and updated annually. The role of the EDIB in the creation of all guidelines should be laid down in the Data Act. ES (Drafting suggestions): The Commission shall chair the meetings of the European Data Innovation Board.' **The Board shall be chaired by one of the representatives of the Member States, who shall be elected by the Board by a two-thirds majority of its members. The Comission shall provide the secretariat for the Board, convene the meetings upon request of the Chair, and prepare the agenda**

Commission proposal	Drafting suggestions and Comments
	in accordance with the tasks of the Board pursuant to this Regulation and its rules of procedure ES (Comments): This amendment adopts the governance structure established in Article 65(8) of the AI Act and is essential to ensure the institutional independence and technical autonomy of the Board. By transitioning from a Commission-led chair to a representative elected by the Member States through a qualified majority (two-thirds), the Board gains the legitimacy needed to act as an impartial arbiter. This structure creates a necessary balance of power: the Member States lead the strategic and decision-making functions, while the Commission provides vital administrative support through the secretariat. This ensures that the Board's agenda and outputs reflect the collective expertise of national authorities, fostering greater trust and more effective cooperation across the Union. FI (Drafting suggestions): (4) The Commission shall chair the meetings of the European Data Innovation Board.' **(5)** (NEW) **The European Data Innovation Board shall be assisted by a secretariat provided by the Commission.** **For the purposes of cooperation under this Regulation, the Commission shall provide and maintain a reliable and secure information sharing system to facilitate communication and information exchange between competent authorities and the Commission. It shall ensure an appropriate level of security and data protection in accordance with Union law and interoperability with other relevant systems**.

Commission proposal	Drafting suggestions and Comments
	FI (Comments): FI: We suggest new section (5) after section (4). It is important that the EDIB receives adequate support to carry out its expanded tasks under the consolidated Data Act. The Commission should have a mandate to develop an electronic information-exchange system to facilitate co-operation. Provisions to this effect could alternatively be added to Article 37. NL (Drafting suggestions): (4) The Commission shall chair the meetings of the European Data Innovation Board.[2] **(5) <u>The European Data Innovation Board shall be assisted by a secretariat provided by the Commission.</u>'** NL (Comments): In order to make sure the EDIB is able to operate at full capacity, secretarial support and functional digital infrastructure enabling collaboration should be provided. PL (Drafting suggestions): (4) The Commission shall chair the meetings of the European Data Innovation Board. **<u>(5) The Board shall be assisted by a pernament secretariat provided by the Commission.</u>**

Commission proposal	Drafting suggestions and Comments
	(6) The Board shall operate on the basis of annual work programs prepared by the Commission in consultation with members of the Board. The Commission shall prepare each year reports on the implementation of the Board's annual work programs.' PL (Comments): As the role of EDIB and its composition expands and it becomes a central coordination and harmonisation body in most data-related topics it is necessart to provide a professionalised and pernament assistance to the Commission and Member States to help organised and coordinate its functioning. In oder to ensur the Board works consistently and efficently it is advisaable to conduct its operation according to annual work programs followed by reports on their implementation.
23. Article 42 is replaced by the following:	DE (Comments): **DE**: The provision combines the lists of tasks in Article 30 DGA and Article 42 GDPR. • It is generally to be welcomed that individual enumeration has been replaced by a sector-specific allocation of tasks. • The addition of the EDIB's role as a strategy forum (Article 42(1)(a)) is also to be welcomed, as is the addition of improving the exchange of best practices (Article 42(1)(d). • An obligation to consult when adopting delegated regulations and exercising implementing powers, as well as when drafting harmonized standards, should be added (see, for example, Art. 29(7), Art. 32u(2), Art. 32v, Art. 32x(2), (5), (7), 33(2), (4), (5), (11), 35(4), (5), (8), Art. 36(6) GDPR);
'Article 42	

Commission proposal	Drafting suggestions and Comments
Role of the EDIB	LU (Comments): Luxembourg is not opposed to simplifying the structure of the EDIB. We would, however, welcome further details from the Commission on how they consider the organization of the work of the simplified EDIB, including with regard to governance and sub-groups. For instance, does the Commission plan to organize the simplified EDIB similarly to the AI Board? In the proposed text, EDIB is no more set up as an expert group pursuant to Article 29 of Regulation (EU) 2022/868. What will be the legal basis for the governance of the simplified 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;	DE (Drafting suggestions): (b) advising and assisting the Commission with regard to developing consistent practice of competent authorities in the enforcement of Chapters II, III, V, **VI,** VII, VIIa and VIIc; DE (Comments): **DE**: Proposal to designate EDIB to advise and assist the Commission with regard to cloud switching according to Chapter VI DK

Commission proposal	Drafting suggestions and Comments
	(Drafting suggestions): (b) advising and assisting the Commission with regard to developing consistent practice of competent authorities in the enforcement of Chapters II, III, V, **VI,** VII, VIIa and VIIc; DK (Comments): DK suggests that Chapter VI is included, as it would be prudent to merge the powers and tasks related to the data legislation under one body, namely EDIB, to ensure consistency across the Data Act. ES (Drafting suggestions): advising and assisting the Commission with regard to ~~developing consistent practice of competent authorities~~ **coordinating the activities of national authorities and** developing consistent practice of competent authorities in the enforcement of Chapters II, III, V, VII, VIIa and VIIc; ES (Comments): This amendment expands the Board's mandate from providing theoretical advice to active operational support. By explicitly including the 'coordination of activities of national authorities,' the Board is empowered to harmonize how different Member States enforce the Regulation in practice. This prevents a fragmented regulatory landscape, ensuring that businesses operating across the Union face uniform requirements and that national competent authorities share technical expertise and enforcement strategies effectively. IT (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
	(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, **as well as guidelines ans harmonised standards** IT (Comments): For the sake of clarity, we recommend clarifying that one of the tasks of the EDIB is to advise and assist the Commission with the development of guidelines and standards. We also recommend empowering the Commission to issue guidelines on any topic concerning the Data Act, in order to facilitate its effective application and enforcement. Where appropriate, such guidance should be drafted in close cooperation with relevant sectoral authorities or bodies, including with the EDPB as a sectoral body, where the protection of personal data is concerned (also in light of Article 8(3) of the Charter and in line with Article 1(5) of the Data Act). These changes would also allow the EDIB to advise and assist the Commission on the development of these guidelines NL (Comments): In the current omnibus proposal, the EDIB would no longer coordinate regulatory oversight for those aspects of the Data Act pertaining to cloud, thus leaving no mechanism in place for the competent authorities on the cloud provisions. We strongly urge the creation of a coordination mechanism on cloud provisions in order to solve this hiatus. We would be interested to hear from the Commission how they envision the facilitation of coordination between competent authorities regarding cloud services and which mechanisms, such as the EDIB or BEREC.

Commission proposal	Drafting suggestions and Comments
(c) facilitating cooperation between competent authorities through capacity-building and the exchange of information;	IT (Drafting suggestions): **(c) facilitating cooperation between competent authorities through capacity-building and the exchange of information, in particular by establishing methods for the efficient exchange of information relating to the enforcement of the rights and obligations under this Regulation in cross-border cases, including coordination with regard to the setting of penalties** IT (Comments): We recommend that the EDIB's role in 'facilitating cooperation between competent authorities through capacity-building and the exchange of information remains the same as under the current Data Act. Therefore, for the sake of clarity, we recommends reinserting in the new Art. 42(1)(c) Data Act the phrase '*in particular by establishing methods for the efficient exchange of information relating to the enforcement of the rights and obligations (...) in cross-border cases, including coordination with regard to the setting of penalties'* NL (Drafting suggestions): **(c) facilitating cooperation between competent authorities through capacity-building and the exchange of information, in particular by establishing methods for the efficient exchange of information relating to the enforcement of the rights and obligations under Chapters II, III and V in cross-border cases, including coordination with regard to the setting of penalties;** **(d) advising and assisting the Commission with regard to:**

Commission proposal	Drafting suggestions and Comments
	(i) whether to request the drafting of harmonised standards referred to in Article 33(4), Article 35(4) and Article 36(5); **(ii) the preparation of the implementing acts referred to in Article 33(5), Article 35(5) and (8) and Article 36(6);** **(iii) the preparation of the delegated acts referred to in Article 29(7) and Article 33(2); and** **(iv) the adoption of the guidelines laying down interoperable frameworks for common standards and practices for the functioning of common European data spaces referred to in Article 33(11)** NL (Comments): In general, The Netherlands sees the merits of the proposed direction simplifying the EDIB structure. However, in addition to strategic discussions the EDIB should also remain focused on the coordination of regulatory oversight and standardization efforts. Therefore, we would suggest to retain the text of the existing article 42b and 42c in the Data Act to keep the efforts of the EDIB focused.
(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.’;	DE (Drafting suggestions): **(e) advising and assisting the Commission with regard to developing guidelines according to Article 24, 32 (3), 32g(6), 33(11), 41a(6).** **(2) The Commission upon recommendation of the EDIB and facilitated by the Data Act Legal Helpdesk will publish FAQs addressing the implementation of [the Data Act] in at least three new sectors (e.g. automotive, health, energy etc.) – in total at least 15 sectors should be covered. Additionally, the EDIB will publish exemplary use cases for the respective sectors for connected products visualizing exemplary business cases with extended information such as implication of [the Data Act] on**

Commission proposal	Drafting suggestions and Comments
	product design, fulfillment of information requirements, important relating contractual clauses etc. The FAQs and use cases shall be updated at least annually. DE (Comments): **DE** DK (Drafting suggestions): (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.'; **(e) advising and assisting the Commission with regard to supporting the implemenation of Chapters II, III, V, VI, VII, VIIa and VIIc by suggesting development of guidance, tools and templates for businesses and public organizations;** **(f) advising and assisting the Commission with regard to supporting the implemenation of Chapters II, III, V, VI, VII, VIIa and VIIc by making standardization requests and/or developing common specifications;** DK (Comments): DK suggests to add a litra (e) to Article 42, with further tasks for the EDIB in line with existing EDIBs existing tasks to ensure coordinated and effective implementation across Member States.

Commission proposal	Drafting suggestions and Comments
	ES (Drafting suggestions): *Add new point 42 1 e):* **At the request of the Commission or on its own initiative, issue recommendations and written opinions on any relevant matters related to the implementation of this Regulation and to its consistent and effective application, including:** **(i) on the development and application of codes of conduct and codes of practice pursuant to this Regulation, as well as the Commission's guidelines on data sharing and fair contractual terms;** **(ii) the evaluation and review of this Regulation, including the functioning of the common European data spaces, the preparation of delegated or implementing acts, and the alignment of this Regulation with the Union legislation on sectoral data spaces;** **(iii) on technical specifications or existing standards regarding the interoperability requirements and the protection of trade secrets;** **(iv) on the use of harmonised standards or common specifications for interoperability of data, data sharing mechanisms and service and common European data spaces referred to in Articles 33 and 35;** **(v) trends, such as European global competitiveness in the data economy, and the uptake of data-sharing technologies in the Union.** **(vi) trends on the evolving typology of data value chains** **(vii) on the potential need for amendment to the list of high-value datasets and the potential need for revision of the rules on Business-to-Government (B2G) data sharing, taking into account the latest technological developments and societal needs.**

Commission proposal	Drafting suggestions and Comments
	Add new point 42 1 (f): **Ensure active cooperation and structured coordination with other relevant Union institutions, bodies, and expert groups to ensure policy consistency in the digital single market, in particular with:** **(i) the European Artificial Intelligence Board (AI Board) regarding the interplay between data and AI;** **(ii) the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) on matters related to personal data and privacy;** **(iii) sectoral data gobernance bodies;** **(iv) the European Statistical System Committee (ESSC);** **(v) ENISA and the European Digital Services Board.** ES (Comments): New point 42 1 (e): This section incorporates a comprehensive task list similar to the Article 66 of the AI Act. The proposed enhancement of the European Data Innovation Board (EDIB) introduces a critical Right of Initiative, allowing the Board to act on its own volition rather than waiting for a formal request from the European Commission. By granting the EDIB the power to issue recommendations and opinions independently, it can proactively identify and flag market failures, emerging bottlenecks, or technical gaps in the data economy as they arise. This autonomy ensures that the Board remains a dynamic actor capable of addressing urgent issues without administrative delay. In terms of Technical Standards, the new mandate empowers the EDIB to oversee technical specifications and existing standards. This oversight is vital for ensuring cross-sectoral interoperability, allowing data to flow seamlessly between different industries, such as from a smart vehicle to an insurance provider, without being hindered by technical barriers. By harmonizing these

Commission proposal	Drafting suggestions and Comments
	requirements, the EDIB acts as the bridge that connects disparate data silos into a unified European data space. By monitoring global competitiveness, the uptake of data-sharing technologies, and the development of digital skills, the Board becomes the primary "think tank" for the EU's data strategy. This ensures that Europe remains competitive against global data giants by identifying strategic trends and fostering the necessary talent and infrastructure within the Union. Finally, the proposal ensures Regulatory Agility by allowing the EDIB to recommend timely amendments to the Data Act. As technology evolves, introducing new types of sensor data, AI-generated synthetic data, or changing value chain structures, the Board can suggest revisions to the legal text and its annexes. This proactive monitoring prevents the Regulation from becoming obsolete and ensures that the legal framework remains fit for purpose in a rapidly changing technological landscape. New point 42 1 (f): Data is the foundational layer for all emerging technologies; therefore, the EDIB cannot function in isolation. By requiring the EDIB to synchronize with the AI Board, the EDPB, and sectoral bodies, this provision prevents 'regulatory silos' and contradictory guidance. This is particularly critical for the 'Data-AI-Privacy' nexus, where a single dataset may be subject to three different Regulations. A structured coordination mechanism ensures that technical standards and interoperability requirements are harmonized across the Union, providing legal certainty for businesses and avoiding the duplication of administrative efforts."
24. Article 45 is amended as follows:	
(a) paragraph 2 is replaced by the following:	
'2. The power to adopt delegated acts referred to in Article 29(7), Article 32u(2) and Article 33(2) shall be conferred on the Commission for an indeterminate period of time.'	DE (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
	2. The power to adopt delegated acts referred to in Article 29(7), Article 32u(2)**, Article 32x(7)** 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.'	DE (Drafting suggestions): 3. The delegation of power referred to in Article 29(7), Article 32u(2)**, Article 32x (7)** 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. DE (Comments): **DE**: Paragraph 3 supplements the power to adopt delegated regulations in Article 32u; it is questionable whether a reference to Article 32x(7) is also necessary. The previous parallel provision in Art. 32 DGA, which is being deleted, also mentions the previous power to adopt delegated acts under Art. 5(13) DGA, which is why it seems logical to now also include reference to Art. 32x(7).
(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	DE (Drafting suggestions): 6. A delegated act adopted pursuant to Article 29(7), Article 32u(2)**, Article 32x(7)** 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

Commission proposal	Drafting suggestions and Comments
extended by three months at the initiative of the European Parliament or of the Council.	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:	ES (Drafting suggestions): No amendment necessary. Delete this modification.
'The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.'	NL (Drafting suggestions): 'The Commission shall be assisted by the **European Data Innovation Board** ~~a committee~~. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.' NL (Comments): Not just any committee, it is the EDIB.
(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:	

Commission proposal	Drafting suggestions and Comments
(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:'	NL (Drafting suggestions): 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:' **(a) The operation and effectiveness of the EDIB** NL (Comments): The Netherlands thinks it is important to also evaluate then functioning of the EDIB.
(ii) point (m) is replaced by the following:	
'(m) the impact of this Regulation on SMEs and SMCs with regard to their capacity to innovate and to the availability of data processing services for users in the Union and the burden of complying with new obligations'	
(b) the following paragraph 2a is inserted:	
'2a. By [date = entry into force plus 5 years], the Commission shall carry out an evaluation of chapters VIIa, VIIb and VIIc of this Regulation and submit a report on its main findings to the European Parliament and to the Council as well as to the European Economic and Social Committee.	
The report shall assess, in particular:	

Commission proposal	Drafting suggestions and Comments
(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.'	NL (Drafting suggestions): ~~(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.'	NL (Drafting suggestions): ~~(g)~~ Member States shall provide the Commission with the Information necessary for the preparation of that report.' NL (Comments): Not part of the enumeration.
(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.'	

Commission proposal	Drafting suggestions and Comments
27. Annex I is added as set out in the Annex II to this Regulation.	DE (Drafting suggestions): Article 50 This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union. It shall apply from 12 September 2025. The obligation resulting from Article 3(1) shall apply to connected products and the services related to them placed on the market after 12 September 2026. **Chapter II shall apply from 1 January 2027 to the obligation of medium-sized and small-mid-cap enterprises to make product data and related service data accessible to user.** […] **Article 40 shall apply from 12 September 2027 to providers of data processing services.** DE (Comments): **DE**: The exemption in Art. 7 (1) Data Act should include “medium-sized” and “small mid-cap” companies and they should be given more time to adapt to the new rules. Therefore, a new transition period (ending January 1st 2027) relating to Chapter II for the companies mentioned should be introduced for these companies in Art. 50 Data Act (Entry into force and

Commission proposal	Drafting suggestions and Comments
	application) on the entry into force and application of Chapter II, taking into account an evaluation of the impact of the Data Act on medium-sized and small mid-cap companies. **DE**: as counterweight to legal uncertainty and given legal uncertainties in time of transition.
Article 2	
Amendments to Regulation (EU) 2018/1724	
In the table in Annex II to Regulation (EU) 2018/1724, the entry 'Starting, running and closing a business' is replaced by the following:	
[Table]	
[…]	
Article 6	
Amendments to Directive (EU) 2022/2555	
Directive (EU) 2022/2555 is amended as follows:	
1. The following Article 23a is added:	ES (Drafting suggestions): REPLACE the proposed Article 23a (Single-entry point) with the following: 'Article 23a Single Information Point

Commission proposal	Drafting suggestions and Comments
	1. ENISA shall develop and maintain a publicly accessible Single Information Point ('SIP') consisting of a website providing: (a) clear and regularly updated information on incident reporting obligations under the applicable Union legal acts, including applicable thresholds, timelines and notification formats. (b) identification of competent national CSIRTs, competent authorities and national reporting entry points for each Member State and relevant sector; (c) direct links and, where available, redirection to national reporting forms and entry points of competent authorities. 2. The Single Information Point shall not collect, process or store any data relating to incident notifications. All incident notifications shall be submitted directly to the competent national CSIRTs or competent authorities in accordance with the applicable Union and national legal acts. 3. Member States shall cooperate with ENISA by providing accurate and up-to-date information on national competent authorities, entry points and notification requirements for the purposes of this Article. 4. ENISA shall develop the Single Information Point in cooperation with the CSIRTs network and the competent authorities under the relevant Union legal acts, within ENISA's existing mandate under Regulation (EU) 2019/881. ' ES (Comments): ES: The operational SEP is replaced by a non-operational Single Information Point (SIP), an ENISA-managed information website with no data collection/storage functions. Consistent with the non-paper co-signed by ES, FR, DE, IT, NL, SE. No modification to NIS2 Art 23 notification channels required.
‘Article 23a	SK

Commission proposal	Drafting suggestions and Comments
	(Comments): **SK suggestions for amendment of the Article 23a** **National Single-entry point for incident reporting** **General comments** **Slovakia supports the objectives pursued by the Commission in the Digital Omnibus proposal to simplify incident reporting obligations across multiple Union legal acts through the introduction of a Single-Entry Point (SEP). In particular, Slovakia recognises the need to reduce administrative burden for reporting entities and to facilitate the "report once" principle where entities are currently required to submit similar notifications under different Union frameworks.** **At the same time, discussions among Member States have shown that there is not yet a common position regarding the establishment of a single technical solution operated at Union level by the European Union Agency for Cybersecurity (ENISA).** **Several Member States have expressed concerns regarding the potential risks associated with a centralised technical platform. These concerns include, inter alia:** • **the risk of creating a single point of failure in a system intended to support critical cybersecurity reporting;** • **the aggregation of sensitive incident-related information in one central system;** • **potential implications for national competences in the area of cybersecurity incident handling;** • **the possibility of information sharing beyond what is required under the relevant Union legal acts; and** • **uncertainty regarding the preceding financial investment into the already existing national solutions.**

Commission proposal	Drafting suggestions and Comments
	In light of these concerns, Slovakia considers it important to explore alternative technical solutions that would still achieve the simplification objectives of the proposal while addressing the sensitivities expressed by Member States.
Single-entry point for incident reporting	DE (Drafting suggestions): *Single-**information** ~~entry~~ point for incident reporting* FR (Drafting suggestions): *Single-**information** ~~entry~~ point for incident reporting* IT (Drafting suggestions): *Single-**information** ~~entry~~ point for incident reporting* LV (Comments): National Cybersecurity Centre (NCSC) of Latvia does not support a development and maintenance of a single-entry point by ENISA due to: - Security concerns of the platform itself – protection of sensitive information as a national security concern; management and response to cyberthreats and cyberincidents targeting platform; - Already established and functioning national incident reporting channels in place. Direct incident reporting at the EU level could undermine

Commission proposal	Drafting suggestions and Comments
	confidence in national authorities and their competences. It may not be clear to companies and authorities who is responsible for the incident handling and follow-up actions. That can weaken national cybersecurity governance and public confidence in national competent authorities. Subjects might face difficulties accessing external platform (vs one integrated with other governmental services). It could also have possible negative effect on relationships between subjects and national competent authorities. Building culture of trust and reporting between subjects and national competent authorities has been a long and thorough work. An individual approach has played a significant role to build trust supplemented with state-sponsored services to strengthen subjects' cyber resilience and cybersecurity. Overall, a technical intermediate platform could increase the complexity of the system, create accessibility risks and potentially jeopardize timely incident reporting by subjects. - Disproportionate and not fully assessed administrative and financial burden for Member States' competent authorities to develop and maintain reporting platforms/systems; adapt incident reporting processes already in place; ensure integration with other systems; train staff and maintain current processes at the same time. NCSC believes that an viable option would be for ENISA to develop and maintain a website providing links to each Member States' national incident reporting authorities/reporting platforms etc. in accordance with the each legal act. ENISA shall consult each Member State on the content of the website. NL (Drafting suggestions): *Single-**information** entry point for incident reporting*

Commission proposal	Drafting suggestions and Comments
	SE (Comments): Sweden proposes that the provisions be amended so that incidents do not go via a conduit at ENISA; and instead focus is placed on ENISA's supportive role regarding information, guidance, and other expertise related to incident reporting. Instead of incidents being reported via ENISA single entry point, we propose that ENISA should provide to entities an information point with information and e.g. links to the Member States' platforms for incident reporting. SK (Comments): ***Rationale of the proposed Article 23a amendments*** **Slovakia proposes to introduce into the discussion a compromise approach based on the establishment and operation of national single-entry points at the level of Member States rather than a single centralised technical solution operated by ENISA.** **Under this approach, each Member State would establish and maintain its own national single-entry point for incident reporting in accordance with harmonised technical specifications. This would ensure the proportionality principle and also that reporting entities benefit from a simplified and unified interface at national level while preserving Member States' control over incident-related information.** **To support the consistent implementation of such national single-entry points across the Union, ENISA would develop and publish common technical specifications and a reference implementation made available under an open-source licence. This reference implementation could be**

Commission proposal	Drafting suggestions and Comments
	used by Member States that do not currently operate their own reporting platforms or that wish to adopt a ready-made solution. **At the same time, Member States that already operate national incident reporting systems would be able to adapt their existing systems to comply with the agreed common technical specifications.** **This approach would allow the Union to achieve the main objective of simplification for reporting entities while avoiding the creation of a centralised repository of incident reports at Union level and preserving the existing balance of competences between the Union and the Member States in the area of cybersecurity incident handling.** **Slovakia therefore presents the accompanying draft of Article 23a as a possible compromise solution for further discussion among Member States.**
(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.	BE (Drafting suggestions): 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'). **The single-entry point shall operate without prejudice to the possibility for entities to report directly to the competent national authorities where such national reporting mechanisms exist.** 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. BE (Comments):

Commission proposal	Drafting suggestions and Comments
	Belgium supports the objective of simplifying incident reporting through the Single Entry Point (SEP). However, as its practical functioning and added value have not yet been sufficiently demonstrated, its use should not be made mandatory for entities at this stage. Entities should remain free to choose the reporting channel that is simplest and safest for them, including direct reporting to existing national reporting mechanisms National authorities will in any case maintain their own reporting infrastructures for registration, redundancy and non-mandatory notifications. DE (Drafting suggestions): (1) ENISA shall develop and maintain a single-**information** ~~entry~~ point to support **entities in fulfilling their** obligations, **pertaining** to **the** report**ing of** incidents and related events under the Union legal acts where those Union legal acts provide so ('single-**information** ~~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.~~ ES (Drafting suggestions): DELETE paragraph (1) — covered by replacement Article 23a (SIP) proposed above. FI (Comments): FI would welcome major amendmends in the Article 23(a) in order to easen incident reporting while simultainously avoiding unnecessary administrative costs. Instead of ENISA's obligation to develop and maintain SEP, FI would preliminary find more suitable to impose obligation on each Member State to

Commission proposal	Drafting suggestions and Comments
	develop and maintain a single-entry point for incident reporting in each MS. For this option, Article 23(a) should be amended accordingly and FI can provide drafting suggestions at later stage. FR (Drafting suggestions): (1) ENISA shall develop and maintain a single-**information** ~~entry~~ point to support **entities in fulfilling their** obligations, **pertaining** to **the** report**ing of** incidents and related events under the Union legal acts where those Union legal acts provide so ('single-**information** ~~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.~~ IT (Drafting suggestions): (1) ENISA shall develop and maintain a single-**information** ~~entry~~ point to support **entities in fulfilling their** obligations, **pertaining** to **the** report**ing of** incidents and related events under the Union legal acts where those Union legal acts provide so ('single-**information** ~~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.~~ IT (Comments): This is to institute a single information point capable of guiding entities through existing incident reporting obligations that the Omnibus proposal does not modify. Such measure is to be considered a short term improvement to be complemented with actions having a longer term impact, as outlined in Article 23(c) 'Harmonising incident notification framework'. NL

Commission proposal	Drafting suggestions and Comments
	(Drafting suggestions): (1) ENISA shall develop and maintain a single-**information** ~~entry~~ point to support **entities in fulfilling their** obligations, **pertaining** to **the** report**ing of** incidents and related events under the Union legal acts where those Union legal acts provide so ('single-**information** ~~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.~~ PL (Drafting suggestions): ~~ENISA~~Member States shall each develop and maintain a national 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').Member States should take into account the guidelines developed by ENISA in line with par. 3 ~~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.~~ RO (Drafting suggestions): ~~(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~~

Commission proposal	Drafting suggestions and Comments
	~~Parliament and of the Council, ENISA may ensure that the single-entry point builds on the single reporting platform established under that Regulation.~~ RO (Comments): Our position is in accordance with the comment on recital (49). This should also operate on the following provisions regarding the subject. SI (Drafting suggestions): Member State shall each develop and maintain a national 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'). SK (Drafting suggestions): (1) **Member States shall each develop, operate and maintain a national single-entry point to support the obligations to report incidents and related events under the Union legal acts where those Union legal acts provide so. Unless otherwise stated by a Member State, development, operation and maintenance of a national single-entry point is provided by a national competent authority according to Directive (EU) 2022/2555.** **The national single-entry point shall constitute the online technical interface through which entities may fulfil their reporting obligations under the Union legal acts referred to in this paragraph.**
(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	BE (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
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.	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 **for national security** of **the** information submitted or disseminated pursuant to the Union legal acts referred to in paragraph (1) and **shall** ensure that **incident notifications are transmitted automatically and without delay to the competent national authorities under those legal acts and that these competent authorities ~~under those Union legal acts~~ have access to and process the information as required under those Union legal acts**. **The single-entry point shall operate exclusively as a secure transmission conduit and shall not entail centralised storage of incident data at Union level. Incident data shall remain under the control of the competent national authorities and shall not be transferred to or processed on infrastructure located outside outside their control.** BE (Comments): Belgium underlines that incident notifications must be transmitted immediately and automatically, without any delay, to all authorities concerned and this in a secure manner in which no information pertinent to national security passes through infrastructure that is outside the control of that member state(s). DE (Drafting suggestions): ~~(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~~

Commission proposal	Drafting suggestions and Comments
	~~Union legal acts have access to and process the information as required under those Union legal acts.~~ **(1a) The single-information point should** **(a) enable entities to identify the applicable reporting obligations, including at least:** - **references to the definitions of (significant) incidents as defined under relevant Union legal acts, including incident reporting thresholds;** - **an indication of the competent authorities and CSIRTs, including contact information;** - **information on applicable deadlines, formats, procedures, required content of the reporting, and admissible languages, available in easily-accessible formats, such as guidelines, tutorials, or knowledge databases** - **a guided and interactive navigation, allowing entities, on the basis of relevant information to identify the applicable reporting obligations and to be redirected to the appropriate national authorities and procedures.** **(1b) When developing the single-information point, ENISA shall consult the relevant national competent authorities under the Union legal acts, the Cooperation Group and the CSIRTs Network. ENISA shall establish strutured communication channels ensuring that information available on the single-information point is updated swtiftly and effectively.** **(1c) ENISA shall not enable the submission, transmission, storage or processing of any incident notification or related data via the single-**

Commission proposal	Drafting suggestions and Comments
	information point, and shall not collect any information allowing the identification of the notifying entity or of any incident. **(1d) Within [12] months from the entry into force of this Regulation, ENISA shall pilot the functioning of the single-information ~~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 pursuant to Article 23a (1a) (a).** **(1e) After establishing the single-information point for incident reporting and in cooperation with the Cooperation Group, ENISA shall explore the possibility to extend the single-information point by providing recommendations on:** **(a) regulatory mapping of relevant EU legal acts imposing cybersecurity risk management and incident reporting obligations;** **(b) national measures, including transposition measures, implementing relevant Union legal acts imposing cybersecurity risk management and incident reporting obligations;** **(c) content to support entities in complying with obligations, in particular regarding entity registration, cybersecurity risk-management, incident reporting, and the reporting of other relevant events;** **(d) cybersecurity educational benchmark comparison tools, designed to enable entities to understand, assess and compare the obligations they are required to implement pursuant to a relevant national or Union legal act, or within the framework of a non-regulatory certification scheme.**

Commission proposal	Drafting suggestions and Comments
	ES (Drafting suggestions): DELETE paragraph (2) — covered by replacement Article 23a (SIP) proposed above. FR (Drafting suggestions): ~~(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.~~ **(1a) The single information point should** **(b) enable entities to identify the applicable reporting obligations, including at least:** - **references to the definitions of significant incidents and incidents as defined under relevant Union legal acts, including incident reporting thresholds;** - **an indication of the competent authorities and CSIRTs, including contact information;** - **applicable deadlines;** - **formats;** - **procedures;** - **language.** **(c) be designed to enable a guided and dynamic navigation, allowing entities, on the basis of relevant information provided, to identify**

Commission proposal	Drafting suggestions and Comments
	the applicable reporting obligations and to be redirected to the appropriate national authorities and procedures. **(d) make available simplified and well-documented information channels enabling entities to notify incidents, such as help guides, tutorials and a knowledge base compiling information.** **(1b) When developing the single-information point, ENISA shall consult the relevant national competent authorities under the Union legal acts, the NIS Cooperation Group and the CSIRT Network. ENISA shall establish strutured communication channels ensuring that information available on the single-information point is swtiftly and effectively updated.** **(1c) The single information point shall not enable the submission, transmission, storage or processing of any incident notification or related data, and shall not collect any information allowing the identification of the notifying entity or of any incident.** **(1d) Within [12] months from the entry into force of this Regulation, ENISA shall pilot the functioning of the single information-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 pursuant to Article 23a (1a) (a).** **(1e) After establishing the Single-Information Point for incident reporting and in cooperation with the NIS Cooperation Group, ENISA shall explore the possibility to extend the Single-Information Point by providing guidelines on:** **(e) regulatory mapping of relevant EU legal acts imposing cybersecurity risk management and incident reporting obligations;**

Commission proposal	Drafting suggestions and Comments
	(f) national measures, including transposition measures, implementing relevant Union legal acts imposing cybersecurity risk management and incident reporting obligations; **(g) content to support entities in complying with obligations, in particular regarding entity registration, cybersecurity risk-management, incident reporting, and the reporting of other relevant events;** **(h) cybersecurity educational benchmark comparison tools, designed to enable entities to understand, assess and compare the obligations they are required to implement pursuant to a relevant national or Union legal act, or within the framework of certification schemes.** IT (Drafting suggestions): ~~(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.~~ **(1a) The single information point should** **(e) enable entities to identify the applicable reporting obligations, including at least:** **- references to the definitions of (significant) incidents as defined under relevant Union legal acts, including incident reporting thresholds;**

Commission proposal	Drafting suggestions and Comments
	- **an indication of the competent authorities and CSIRTs, including contact information;** - **applicable deadlines;** - **formats;** - **procedures;** - **language.** **(f) be designed to enable a guided and dynamic navigation, allowing entities, on the basis of relevant information provided, to identify the applicable reporting obligations and to be redirected to the appropriate national authorities and procedures.** **(g) make available simplified and well-documented information channels enabling entities to notify incidents, such as help guides, tutorials and a knowledge base compiling information.** **(1b) When developing the single-information point, ENISA shall consult the relevant national competent authorities under the Union legal acts, the NIS Cooperation Group and the CSIRT Network. ENISA shall establish strutured communication channels ensuring that information available on the single-information point is swtiftly and effectively updated.** **(1c) The single information point shall not enable the submission, transmission, storage or processing of any incident notification or related data, and shall not collect any information allowing the identification of the notifying entity or of any incident.** **(1d) Within [12] months from the entry into force of this Regulation, ENISA shall pilot the functioning of the single information-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**

Commission proposal	Drafting suggestions and Comments
	respective Union legal act, and after consulting the Commission and the relevant competent authorities pursuant to Article 23a (1a) (a). **(1e) After establishing the Single-Information Point for incident reporting and in cooperation with the NIS Cooperation Group, ENISA shall explore the possibility to extend the Single-Information Point to:** **(i) regulatory mapping of relevant EU legal acts imposing cybersecurity risk management and incident reporting obligations;** **(j) national measures, including transposition measures, implemeting relevant Union legal acts imposing cybersecurity risk management and incident reporting obligations;** **(k) content to support entities in complying with obligations, in particular regarding entity registration, cybersecurity risk- management, incident reporting, and the reporting of other relevant events.;** (l) **Cybersecurity educational benchmark comparison tools, designed to enable entities to understand, assess and compare the obligations they are required to implement pursuant to a relevant national or Union legal act, or within the framework of a certification scheme.** IT (Comments): The timeframe for piloting could be shorter as the single information point should be less complex to establish. Moreover, the information point may be expanded beyond incident notification so to support compliance with other obligations. NL

Commission proposal	Drafting suggestions and Comments
	(Drafting suggestions): ~~(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.~~ **(1a) The single information point should** **(a) enable entities to identify the applicable reporting obligations, including at least:** **- references to the definitions of (significant) incidents as defined under relevant Union legal acts, including incident reporting thresholds;** **- an indication of the competent authorities and CSIRTs, including contact information;** **- applicable deadlines;** **- formats;** **- procedures;** **- language.** **(b) be designed to enable a guided and dynamic navigation, allowing entities, on the basis of relevant information provided, to identify the applicable reporting obligations and to be redirected to the appropriate national authorities and procedures.**

Commission proposal	Drafting suggestions and Comments
	(c) make available simplified and well-documented information channels enabling entities to notify incidents, such as help guides, tutorials and a knowledge base compiling information. **(1b) When developing the single-information point, ENISA shall consult the relevant national competent authorities under the Union legal acts, the NIS Cooperation Group and the CSIRT Network. ENISA shall establish strutured communication channels ensuring that information available on the single-information point is swtiftly and effectively updated.** **(1c) The single information point shall not enable the submission, transmission, storage or processing of any incident notification or related data, and shall not collect any information allowing the identification of the notifying entity or of any incident.** **(1d) Within [12] months from the entry into force of this Regulation, ENISA shall pilot the functioning of the single information-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 pursuant to Article 23a (1a) (a).** **(1e) After establishing the Single-Information Point for incident reporting and in cooperation with the NIS Cooperation Group, ENISA shall explore the possibility to extend the Single-Information Point by providing guidelines on:**

Commission proposal	Drafting suggestions and Comments
	(a) regulatory mapping of relevant EU legal acts imposing cybersecurity risk management and incident reporting obligations; **(b) national measures, including transposition measures, implementing relevant Union legal acts imposing cybersecurity risk management and incident reporting obligations;** **(c) content to support entities in complying with obligations, in particular regarding entity registration, cybersecurity risk-management, incident reporting, and the reporting of other relevant events;** **(d) cybersecurity pedagogical benchmark comparison tools, designed to enable entities to understand, assess and compare the obligations they are required to implement pursuant to a relevant national or Union legal act, or within the framework of a non-regulatory certification scheme.** PL (Drafting suggestions): ~~ENISA~~Member States 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~~Member States 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. SI

Commission proposal	Drafting suggestions and Comments
	(Drafting suggestions): Member States 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. Member states 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. SK (Drafting suggestions): (2) **Member States shall take appropriate and proportionate technical, operational and organisational measures to ensure the security, confidentiality, integrity and availability of the single-entry point and of the information submitted via its technical infrastructure.** **Member States shall ensure that competent authorities under the Union legal acts referred to in paragraph (1) have access to and process the information as required under those 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:	DE (Drafting suggestions): ~~(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:~~

Commission proposal	Drafting suggestions and Comments
	2. The following Article 23b is added: ***'Article 23b*** ***National entry points for incident reporting*** **(1) Member States shall establish and maintain one or more national entry points for incident reporting, taking into account their specific needs, existing national structures and the most effective arrangements for incident reporting. Incident reporting shall remain the sole responsibility of each Member State.** **(2) ENISA shall, in consultation with the CSIRTs network and the Cooperation Group, develop recommendations to support Member States in the establishment, maintenance and secure operation of national entry points. Those recommendations shall address technical, operational and organisational measures, taking into account experiences and lessons learned from existing reporting structures.** **(3) The recommendations may include technical and organisational measures to ensure that entities using the national entry point can retrieve and, if necessary, supplement information previously submitted, and that a single submission of information can be reused to fulfil multiple reporting obligations via the same national entry points.** **(4) Member States shall regularly inform ENISA about the development of national entry points.** **(5) At the request of Member States, the CSIRTs Network can support the development of national entry points within the Union.** ES

Commission proposal	Drafting suggestions and Comments
	(Drafting suggestions): DELETE paragraph (3) — covered by replacement Article 23a (SIP) proposed above. FR (Drafting suggestions): ~~(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:~~ **2. The following Article 23b is added:** ***'Article 23b*** ***National entry points for incident reporting*** **(6) Member States shall establish and maintain one or more national entry points for incident reporting, taking into account their specific needs, existing national structures and the most effective arrangements for incident reporting. Incident reporting shall remain the sole responsibility of each Member State.** **(7) ENISA shall, in consultation with the CSIRTs network and the NIS Cooperation Group, develop guidelines to support Member States in the establishment, maintenance and secure operation of national entry points. Those guidelines shall address technical, operational and organisational measures, taking into account experiences and lessons learned from existing reporting structures.**

Commission proposal	Drafting suggestions and Comments
	(8) The guidelines may include technical and organisational measures to ensure that entities using the national entry point can retrieve and, if necessary, supplement information previously submitted, and that a single submission of information can be reused to fulfil multiple reporting obligations via the same national entry points. **(9) Member States shall regularly inform ENISA about the development of national entry points.** **At the request of Member States, the CSIRT Network can support the development of national entry points within the Union.** IT (Drafting suggestions): ~~(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:~~ **2. The following Article 23b is added:** ***'Article 23b*** ***National entry points for incident reporting*** **(10) Member States shall establish and maintain one or more national entry points for incident reporting, taking into account their specific needs, existing national structures and the most effective arrangements for incident reporting. Incident reporting shall remain the sole responsibility of each Member State.**

Commission proposal	Drafting suggestions and Comments
	(11) ENISA shall, in consultation with the CSIRTs network and the NIS Cooperation Group, develop guidelines to support Member States in the establishment, maintenance and secure operation of national entry points. Those guidelines shall address technical, operational and organisational measures, taking into account experiences and lessons learned from existing reporting structures. **(12) The guidelines may include technical and organisational measures to ensure that entities using the national entry point can retrieve and, if necessary, supplement information previously submitted, and that a single submission of information can be reused to fulfil multiple reporting obligations via the same national entry points.** **(13) Member States shall regularly inform ENISA about the development of national entry points.** **(14) At the request of Member States, the CSIRT Network can support the development of national entry points within the Union.** NL (Drafting suggestions): ~~(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:~~ **2. The following Article 23b is added:** ***'Article 23b***

Commission proposal	Drafting suggestions and Comments
	National entry points for incident reporting **(1) Member States shall establish and maintain one or more national entry points for incident reporting, taking into account their specific needs, existing national structures and the most effective arrangements for incident reporting. Incident reporting shall remain the sole responsibility of each Member State.** **(2) ENISA shall, in consultation with the CSIRTs network and the NIS Cooperation Group, develop guidelines to support Member States in the establishment, maintenance and secure operation of national entry points. Those guidelines shall address technical, operational and organisational measures, taking into account experiences and lessons learned from existing reporting structures.** **(3) The guidelines may include technical and organisational measures to ensure that entities using the national entry point can retrieve and, if necessary, supplement information previously submitted, and that a single submission of information can be reused to fulfil multiple reporting obligations via the same national entry points.** **(4) Member States shall regularly inform ENISA about the development of national entry points.** **(5) At the request of Member States, the CSIRT Network can support the development of national entry points within the Union.** PL

Commission proposal	Drafting suggestions and Comments
	(Drafting suggestions): ENISA shall ~~provide and implement the~~, in consultation with the CSIRTs network and the NIS Cooperation Group develop and provide Member States with guidelines concerning 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~~ within 12 months from the entry into force of this Regulation. The guidelines shall includethe technical specifications necessary toensure interoperability between all national single entry points. The guidelines shall take into account experiences and lessons learned from existing national single entry points. The guidelines shall cover in particular the following aspects: SI (Drafting suggestions): ENISA shall, in consultation with the CSIRTs network and the NIS Cooperation Group develop and provide Member States with guidelines concerning specifications on the technical, operational and organisational measures regarding the establishment, maintenance and secure operation of the single-entry point within 12 months from the entry into force of this Regulation. The guidelines shall includethe technical specifications necessary to ensure interoperability between all national single entry points. The guidelines shall take into account experiences and lessons learned from existing national single entry points. The guidelines shall cover in particular the following aspects: SK

Commission proposal	Drafting suggestions and Comments
	(Drafting suggestions): **(3)** **ENISA shall, in consultation with the CSIRTs Network and the NIS Cooperation Group, develop and publish, within 12 months from the entry into force of this Regulation:** **(a) a common technical specification defining the minimum functional, security and interoperability requirements for national single-entry points;** **(b) common data formats and reporting templates necessary to enable entities to submit a single notification capable of fulfilling multiple reporting obligations under the Union legal acts referred to in paragraph (1);** **(c) a reference implementation of a national single-entry point made available under an open-source licence. The reference implementation shall be made available for voluntary use by Member States.**
(a) the necessary capability for interoperability with regard to other relevant reporting obligations referred to in paragraph (1) is ensured;	DE (Drafting suggestions): ~~(a) the necessary capability for interoperability with regard to other relevant reporting obligations referred to in paragraph (1) is ensured;~~ ES (Drafting suggestions): DELETE paragraph (3)(a) — covered by replacement Article 23a (SIP) proposed above. FR (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
	~~(a) the necessary capability for interoperability with regard to other relevant reporting obligations referred to in paragraph (1) is ensured;~~ IT (Drafting suggestions): ~~(a) the necessary capability for interoperability with regard to other relevant reporting obligations referred to in paragraph (1) is ensured;~~ NL (Drafting suggestions): (a) the necessary capability for interoperability with regard to other relevant reporting obligations referred to in paragraph (1) is ensured; PL (Drafting suggestions): (a) technical and operational measures to ensure the necessary capability for interoperability with regard to other relevant reporting obligations referred to in paragraph (1) ~~is ensured;~~ in each national entry point; SI (Drafting suggestions): a) technical and operational measures to ensure the necessary capability for interoperability with regard to other relevant reporting obligations referred to in paragraph (1) in each national entry point;
(b) technical arrangements for the relevant entities and authorities under the Union legal acts referred to in paragraph (1) to access, submit , retrieve, transmit or otherwise process information from the single-entry point, are in place and, provide technical protocols and tools that allow the entities and authorities to further process the receive information within their systems;	BE (Drafting suggestions): technical arrangements for the relevant entities and authorities under the Union legal acts referred to in paragraph (1) to ~~**access,**~~ submit , ~~**retrieve**~~, transmit or otherwise process information from the single-entry point, are in place and, provide technical protocols and tools that allow the entities and authorities to further process the receive information within their systems

Commission proposal	Drafting suggestions and Comments
	BE (Comments): Belgium considers that the Single Entry Point (SEP) should function strictly as a secure transmission conduit and not as a centralised EU-level database. Incident notifications must remain under the control of the competent national authorities and be transmitted immediately and automatically to all authorities concerned. DE (Drafting suggestions): ~~(b) technical arrangements for the relevant entities and authorities under the Union legal acts referred to in paragraph (1) to access, submit , retrieve, transmit or otherwise process information from the single entry point, are in place and, provide technical protocols and tools that allow the entities and authorities to further process the receive information within their systems;~~ ES (Drafting suggestions): DELETE paragraph (3)(b) — covered by replacement Article 23a (SIP) proposed above. FR (Drafting suggestions): ~~(b) technical arrangements for the relevant entities and authorities under the Union legal acts referred to in paragraph (1) to access, submit , retrieve, transmit or otherwise process information from the single entry point, are in place and, provide technical protocols and tools that allow the entities and authorities to further process the receive information within their systems;~~ IT (Drafting suggestions):

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

Commission proposal	Drafting suggestions and Comments
	(Comments): Strike out the whole paragraph
(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;	DE (Drafting suggestions): ~~(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;~~ ES (Drafting suggestions): DELETE paragraph (3)(c) — covered by replacement Article 23a (SIP) proposed above. FR (Drafting suggestions): ~~(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;~~ IT (Drafting suggestions): ~~(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;~~ NL (Drafting suggestions): ~~(c) the specificities of the incident reporting requirements set out under the Union legal acts referred to in paragraph (1) are duly taken into account;~~
(d) where relevant, the single-entry point is interoperable and compatible with European Business Wallets referred to in *[Proposal for a Regulation: Insert title of the proposal]* and that the European Business Wallets can be used at least to identify and authenticate entities using the single-entry point;	DE (Drafting suggestions): ~~(d) where relevant, the single-entry point is interoperable and compatible with European Business Wallets referred to in *[Proposal for a Regulation:*~~

Commission proposal	Drafting suggestions and Comments
	~~*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;~~ ES (Drafting suggestions): DELETE paragraph (3)(d) — covered by replacement Article 23a (SIP) proposed above. FR (Drafting suggestions): ~~(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;~~ IT (Drafting suggestions): ~~(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;~~ NL (Drafting suggestions): (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; PL (Drafting suggestions): ~~where relevant, the single-entry point is interoperable and compatible with European Business Wallets referred to in *[Proposal for a*~~

Commission proposal	Drafting suggestions and Comments
	~~*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;~~ SI (Drafting suggestions): ~~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;~~ SI (Comments): Strike out the whole paragraph
(e) entities using the single-entry point can retrieve and supplement information that they have previously submitted via the single-entry point;	BE (Drafting suggestions): entities using the single-entry point can ~~**retrieve**~~ and supplement information that they have previously submitted via the single-entry point; DE (Drafting suggestions): ~~(e) entities using the single-entry point can retrieve and supplement information that they have previously submitted via the single-entry point;~~ ES (Drafting suggestions): DELETE paragraph (3)(e) — covered by replacement Article 23a (SIP) proposed above. FR

Commission proposal	Drafting suggestions and Comments
	(Drafting suggestions): ~~(e) entities using the single-entry point can retrieve and supplement information that they have previously submitted via the single-entry point;~~ IT (Drafting suggestions): ~~(e) entities using the single-entry point can retrieve and supplement information that they have previously submitted via the single-entry point;~~ LU (Comments): Recital 49 states that the SEP should also be capable for operators to retrieve information of incident notifications done via SEP. But since no data will be stored on the SEP, we are wondering how the retrieval of incident notifications by operators will be feasible. NL (Drafting suggestions): (e) entities using the single-entry point can retrieve and supplement information that they have previously submitted via the single-entry point; PL (Drafting suggestions): technical measures to ensure that entities using the single-entry point can retrieve and supplement information that they have previously submitted via the national single-entry point; SI (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
	d) technical measures to ensure that entities using the single-entry point can retrieve and supplement information that they have previously submitted via the national single-entry point;
(f) a single notification of information submitted by an entity via the single-entry point can be used to fulfil reporting obligations as set out under any of the other Union legal acts which provide for incident reporting to the single-entry point.	BE (Drafting suggestions): Add the following paragraph (g): "**The single-entry point shall be designed in a manner that prevents any unauthorised access, alteration, retention or centralised storage of incident data at Union level and shall ensure that incident notifications are transmitted automatically and without delay to the competent national authorities concerned.**" Add the following paragraph (h): **"The single-entry point shall allow entities to submit notifications in any official language of the Union."** BE (Comments): (g) Belgium considers that the Single Entry Point (SEP) should function strictly as a secure transmission conduit and not as a centralised EU-level database. The platform should not entail central storage of incident data, nor introduce delays in the reporting process. Incident notifications must remain under the control of the competent national authorities and be transmitted immediately and automatically to all authorities concerned. (h) To ensure accessibility and legal certainty for entities, reporting via the Single Entry Point (SEP) should be possible in the official language(s) of the Union. DE (Drafting suggestions): ~~(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~~

Commission proposal	Drafting suggestions and Comments
	~~any of the other Union legal acts which provide for incident reporting to the single-entry point.~~ ES (Drafting suggestions): DELETE paragraph (3)(f) — covered by replacement Article 23a (SIP) proposed above. FR (Drafting suggestions): ~~(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.~~ IT (Drafting suggestions): ~~(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.~~ NL (Drafting suggestions): (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. PL (Drafting suggestions): (f) technical and organisational measures to ensure that a single notification of information submitted by an entity via the single-entry point

Commission proposal	Drafting suggestions and Comments
	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. SI (Drafting suggestions): f) technical and organisational measures to ensure that a single notification of information submitted by an entity via the single-entry point can be used to fulfil reporting obligations as set out under any of the other Union legal acts which provide for incident reporting to the single-entry point.
(4) Unless provided for in the Union legal acts referred to in paragraph (1) of this, ENISA shall not have access to the notifications submitted through the single-entry point.	BE (Drafting suggestions): 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. **The single-entry point shall operate exclusively as a secure transmission conduit and shall not entail centralised storage of incident data at Union level. Incident data shall remain under the control of the competent national authorities and shall not be transferred to or processed on infrastructure located outside their control.** BE (Comments): Given the sensitive and potentially national security-related nature of incident reporting data, the security requirements applicable to the Single Entry Point (SEP) must be clearly defined in advance. The platform should only become operational once its security, resilience and reliability are demonstrably ensured. DE (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
	~~(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.~~ ES (Drafting suggestions): DELETE paragraph (4) — covered by replacement Article 23a (SIP) proposed above. FR (Drafting suggestions): ~~(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.~~ IT (Drafting suggestions): ~~(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.~~ NL (Drafting suggestions): ~~(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.~~ PL (Drafting suggestions): ~~Unless provided for in the Union legal acts referred to in paragraph (1) of this, ENISA~~ 4a) Member States shall ~~not have access to the notifications~~

Commission proposal	Drafting suggestions and Comments
	~~submitted through~~ inform ENISA about the establishment of the single~~-~~ entry point~~.~~ SI (Drafting suggestions): (4a) Member States shall inform ENISA about the establishment of the single entry point no later than 1 month after the single-entry point is operational, and any changes that impact the fulfilment of reporting obligations. (4b) ENISA shall develop and maintain a website providing links to all national single-entry points established in line with paragraph (1) including a description of each national single entry point. ENISA shall consult the NIS Cooperation Group on the content of the website. (4c) Member States shall ensure that the national entry points are interoperable and able to exchange information. The single-entry point shall: (a) Allow entities to select whether the report is to be automatically shared with other single-entry points when the entity has obligation to report also in other Member States. (b) Allow CSIRTs or, where applicable, competent authorities to share a report with other single-entry points when deemed necessary. (4d) ENISA shall in consultation with the CSIRTs network [and the NIS Cooperation Group] develop and provide technical protocols and tools to ensure the interoperability and exchange of information between the national single-entry points withing 12 months from the entry into force of this Regulation. SI

Commission proposal	Drafting suggestions and Comments
	(Comments): Delete Commission proposal and replace by drafting suggestion. SK (Drafting suggestions): **(4)** **Member States shall ensure that their national single-entry points comply with the common technical specification referred to in paragraph (3). Member States may thus:** **(a) adopt the reference implementation developed by ENISA; or** **(b) adapt their existing national systems to ensure compliance with the common technical specification.**
(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.	BE (Drafting suggestions): 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, **and following the signing of a Protocol agreement with each competent authority involved. Prior to becoming operational, the single-entry point shall undergo independent security testing, including penetration testing and vulnerability assessments.** BE

Commission proposal	Drafting suggestions and Comments
	(Comments): Given the sensitive and potentially national security-related nature of incident reporting data, the security requirements applicable to the Single Entry Point (SEP) must be clearly defined in advance. The platform should only become operational once its security, resilience and reliability are demonstrably ensured. Before the platform becomes operational for specific legal acts and countries, ENISA shall conclude a protocol agreement e.g. on use, interoperability and (security) maintenance with each of the national competent authorities to whose systems and control the portal would connect, thereby also assuring Member States Authorities agree with the security standards set. DE (Drafting suggestions): ~~(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.~~ ES (Drafting suggestions): DELETE paragraph (5) — covered by replacement Article 23a (SIP) proposed above. FI (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
	Within [**24**] 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. FI (Comments): FI considers necessary to ensure sufficient and realistic implementation timeline, considering complex technical implementation of the SEP. FR (Drafting suggestions): ~~(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.~~ IT (Drafting suggestions): ~~(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~~

Commission proposal	Drafting suggestions and Comments
	~~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.~~ NL (Drafting suggestions): ~~(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.~~ PL (Drafting suggestions): ~~(5) Within [18] months from the entry into force of this Regulation, ENISA shall pilot the functioning of~~ no later than 1 month after the single-entry point ~~for each added Union legal act, including testing~~is operational, and any changes 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~~

Commission proposal	Drafting suggestions and Comments
	~~and after the Commission published a notice pursuant to paragraph 6.~~impact the fulfilment of reporting obligations. SI (Drafting suggestions): (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.~~ (5)Member States shall establish the single entry point within 36 months from the entry into force of this Regulation. SI (Comments): Delete the proposed Commission paragraph and replace with suggested. SK (Drafting suggestions): **(5)** **The national single-entry point shall enable entities to:**

Commission proposal	Drafting suggestions and Comments
	(a) submit a single notification capable of fulfilling reporting obligations under multiple Union legal acts referred to in paragraph (1); **(b) retrieve, supplement and update informat ion previously submitted;** **(c) receive confirmation of receipt and information regarding the competent authority to which the notification has been transmitted.**
(6) The Commission shall, in cooperation with ENISA, assess the proper functioning, reliability, integrity and confidentiality of the single-entry point. When the Commission, after consultation of the CSIRTs network and the competent authorities under the Union legal acts referred to in paragraph 1, finds that the single-entry point ensures the proper functioning, reliability, integrity and confidentiality, it shall publish a notice to that effect in the Official Journal of the European Union.	DE (Drafting suggestions): ~~(6) The Commission shall, in cooperation with ENISA, assess the proper functioning, reliability, integrity and confidentiality of the single-entry point. When the Commission, after consultation of the CSIRTs network and the competent authorities under the Union legal acts referred to in paragraph 1, finds that the single-entry point ensures the proper functioning, reliability, integrity and confidentiality, it shall publish a notice to that effect in the Official Journal of the European Union.~~ **3. The following article 23c is added :** ***'Article 23c*** ***Harmonising incident notification framework*** **(1) By [6 months after the entry into force of this Regulation] the Commission shall submit a report to the European Parliament and to the Council outlining common definitions, thresholds, deadlines, formats and procedures with regard to Article 23 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.**

Commission proposal	Drafting suggestions and Comments
	The report shall in particular envisage concrete steps and a credible timeline for introducing the proposed unified approach to incident reporting under the Union legal acts. **(2) Member States shall, in cooperation with the CSIRTs network, work on the exchange and interoperability of information regarding incident notification, with the aim of improving the efficiency and consistency of notification processes.** **(3) Building on the report referred in paragraph (1), ENISA shall, in cooperation with the Cooperation Group, develop recommendations to foster the harmonization of reporting obligations pursuant to Article 23. These recommendations shall, in particular:** **(a) Identify ways to harmonise templates for entities but also between CSIRTs across different sectors and legislative frameworks.** **(b) Provide a thorough analysis on the different sectoral thresholds, and, where appropriate, provide suggestions with regards to possible harmonization to improve efficiency.** **(c) Review the stages of incident notifications under different Union legal acts and recommend measures to streamline the process for entities.** **ENISA shall present a first draft of these guidelines within 12 months of the entry into force of this regulation, and shall update them regularly thereafter.** ES

Commission proposal	Drafting suggestions and Comments
	(Drafting suggestions): DELETE paragraph (6) — covered by replacement Article 23a (SIP) proposed above. FR (Drafting suggestions): ~~(6) The Commission shall, in cooperation with ENISA, assess the proper functioning, reliability, integrity and confidentiality of the single entry point. When the Commission, after consultation of the CSIRTs network and the competent authorities under the Union legal acts referred to in paragraph 1, finds that the single entry point ensures the proper functioning, reliability, integrity and confidentiality, it shall publish a notice to that effect in the Official Journal of the European Union.~~ **3. The following article 23c is added :** ***'Article 23c*** ***Harmonising incident notification framework*** **(1) By [6 months after the entry into force of this Regulation] the Commission shall submit a report to the European Parliament and to the Council outlining common definitions, thresholds, deadlines, formats and procedures applying to Article 23 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.** **The report shall in particular envisage concrete steps and a credible timeline for introducing the proposed unified approach to incident reporting under the Union legal acts.**

Commission proposal	Drafting suggestions and Comments
	(2) Member States shall, in cooperation with the CSIRT network, work on the exchange and interoperability of information regarding incident notification, with the aim of improving the efficiency and consistency of notification processes. **(3) Building on the report referred in paragraph (1), ENISA shall, in cooperation with the NIS Cooperation Group, develop guidelines to foster the harmonization of incident notifications. These guidelines shall, in particular:** **(a) Identify ways to harmonise templates for entities but also between CSIRTs across different sectors and legislative frameworks.** **(b) Provide a thorough analysis on the different sectoral thresholds, and, where appropriate, provide suggestions with regards to possible harmonization to improve efficiency.** **(c) Review the stages of incident notifications under different Union legal acts and recommend measures to streamline the process for entities.** **ENISA shall present a first draft of these guidelines within 12 months of the entry into force of this regulation, and shall update them regularly thereafter.** IT (Drafting suggestions): ~~(6) The Commission shall, in cooperation with ENISA, assess the proper functioning, reliability, integrity and confidentiality of the single entry point. When the Commission, after consultation of the CSIRTs network and the competent authorities under the Union legal acts referred to in paragraph 1,~~

Commission proposal	Drafting suggestions and Comments
	~~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.~~ **3. The following article 23c is added :** ***'Article 23c*** ***Harmonising incident notification framework*** **(1) By [6 months after the entry into force of this Regulation] the Commission shall submit a report to the European Parliament and to the Council outlining common definitions, thresholds, deadlines, formats and procedures applying to Article 23 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.** **The report shall in particular envisage concrete steps and a credible timeline for introducing the proposed unified approach to incident reporting under the Union legal acts.** **(2) Member States shall, in cooperation with the CSIRT network, work on the exchange and interoperability of information regarding incident notification, with the aim of improving the efficiency and consistency of notification processes.** **(3) Building on the report referred to in paragraph (1), ENISA shall, in cooperation with the NIS Cooperation Group, develop guidelines to foster the harmonization of incident notifications. These guidelines shall, in particular:**

Commission proposal	Drafting suggestions and Comments
	(a) Identify ways to harmonise templates for entities but also between CSIRTs across different sectors and legislative frameworks. **(b) Provide a thorough analysis on the different sectoral thresholds, and, where appropriate, provide suggestions with regards to possible harmonization to improve efficiency.** **(c) Review the stages of incident notifications under different Union legal acts and recommend measures to streamline the process for entities.** **ENISA shall present a first draft of these guidelines within 12 months of the entry into force of this regulation, and shall update them regularly thereafter.** IT (Comments): This is to outline a process, consituting of a Commission's report and ENISA's guidelines, for providing structural simplification of incident reporting across legal acts. In the medium term it should lead to the streamlining of thresholds, deadlines, formats and procedures. NL (Drafting suggestions): ~~(6) The Commission shall, in cooperation with ENISA, assess the proper functioning, reliability, integrity and confidentiality of the single entry point. When the Commission, after consultation of the CSIRTs network and the competent authorities under the Union legal acts referred to in paragraph 1, finds that the single entry point ensures the proper functioning, reliability,~~

Commission proposal	Drafting suggestions and Comments
	~~integrity and confidentiality, it shall publish a notice to that effect in the Official Journal of the European Union.~~ **3. The following article 23c is added :** ***'Article 23c*** ***Harmonising incident notification framework*** **(1) By [6 months after the entry into force of this Regulation] the Commission shall submit a report to the European Parliament and to the Council outlining common definitions, thresholds, deadlines, formats and procedures applying to Article 23 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.** **The report shall in particular envisage concrete steps and a credible timeline for introducing the proposed unified approach to incident reporting under the Union legal acts.** **(2) Member States shall, in cooperation with the CSIRT network, work on the exchange and interoperability of information regarding incident notification, with the aim of improving the efficiency and consistency of notification processes.** **(3) Building on the report referred in paragraph (1), ENISA shall, in cooperation with the NIS Cooperation Group, develop guidelines to**

Commission proposal	Drafting suggestions and Comments
	foster the harmonization of incident notifications. These guidelines shall, in particular: **(a) Identify ways to harmonise templates for entities but also between CSIRTs across different sectors and legislative frameworks.** **(b) Provide a thorough analysis on the different sectoral thresholds, and, where appropriate, provide suggestions with regards to possible harmonization to improve efficiency.** **(c) Review the stages of incident notifications under different Union legal acts and recommend measures to streamline the process for entities.** **ENISA shall present a first draft of these guidelines within 12 months of the entry into force of this regulation, and shall update them regularly thereafter.** PL (Drafting suggestions): ~~The Commission shall, in cooperation with ENISA, assess the proper functioning, reliability, integrity and confidentiality of the single entry point. When the Commission, after consultation of the CSIRTs network and the competent authorities under the Union legal acts referred to in paragraph 1, finds that the single entry point ensures the proper functioning, reliability, integrity and confidentiality, it shall publish a notice to that effect in the Official Journal of the European Union~~ SI (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
	~~(6) The Commission shall, in cooperation with ENISA, assess the proper functioning, reliability, integrity and confidentiality of the single-entry point. When the Commission, after consultation of the CSIRTs network and the competent authorities under the Union legal acts referred to in paragraph 1, finds that the single-entry point ensures the proper functioning, reliability, integrity and confidentiality, it shall publish a notice to that effect in the Official Journal of the European Union.~~ SI (Comments): Deletion of the paragraph SK (Drafting suggestions): **(6)** **Information submitted via a national single-entry point shall remain under the control of the Member State concerned.** **Nothing in this Article shall affect existing obligations under Union legal acts concerning cross-border information sharing or cooperation in the event of significant or large-scale incidents.**
(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.'	DE (Drafting suggestions): ~~(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~~

Commission proposal	Drafting suggestions and Comments
	~~proper functioning, reliability, integrity or confidentiality of the single-entry point and shall publish a notice in accordance with paragraph 6.~~[2] ~~(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] **4. The following article 23d is added :** ***'Article 23d*** ***Cross-border incident notification*** **(1) Member States should aim at facilitating cross-border notifications to multiple national reporting structures. ENISA, in cooperation with the cooperation group and the CSIRTs network, shall develop and maintain mechanisms to facilitate the alignment of incident notifications submitted via national entry points with cross-border reporting obligations, including the use of relevant tools.** **(2) ENISA shall, in cooperation with the CSIRTs Network, harmonise its relevant tools with national incident notification templates and facilitate an automatisation process to exchange information about cross-border impacts.** **(3) Information submitted through relevant tools shall not be automatically transmitted to ENISA in full, Member States shall have the possibility to select information shared.** ES

Commission proposal	Drafting suggestions and Comments
	(Drafting suggestions): DELETE paragraph (7) — covered by replacement Article 23a (SIP) proposed above. FR (Drafting suggestions): ~~(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.'~~ ~~(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.'~~ **4. The following article 23d is added :** ***'Article 23d*** ***Cross-border incident notification*** **(4) Member States should aim at facilitating cross-border notifications to multiple national reporting structures. ENISA, in cooperation with the NIS cooperation group and the CSIRT network, shall develop and maintain mechanisms to facilitate the alignment of incident**

Commission proposal	Drafting suggestions and Comments
	notifications submitted via national entry points with cross-border reporting obligations, including the use of relevant tools. **(5) ENISA shall, in cooperation with the CSIRT Network, harmonise its relevant tools with national incident notification templates and facilitate an automatisation process to exchange information about cross-border impacts.** **(3) Information submitted through relevant tools -shall not be automatically transmitted to ENISA in full, Member States shall have the possibility to select information shared.** IT (Drafting suggestions): ~~(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.'~~ **4. The following article 23d is added :** ***'Article 23d*** ***Cross-border incident notification*** **(6) Member States shall aim at faciliting cross-border notifications to multiple national reporting structures. ENISA, in cooperation with the NIS cooperation group and the CSIRT network, shall develop and maintain mechanisms to facilitate the alignment of incident**

Commission proposal	Drafting suggestions and Comments
	notifications submitted via national entry points with cross-border reporting obligations, including the use of relevant tools. **(7) ENISA shall, in cooperation with the CSIRT Network, harmonise its relevant tools with national incident notification templates and facilitate an automatisation process to exchange information about cross-border impacts.** **(8) Information submitted through relevant tools provided by ENISA shall not be automatically transmitted to ENISA in full, Member States shall have the possibility to select information shared.** IT (Comments): The purpose is to ensure that ENISA, including through the use of tools such as CIRAS (see corresponding recital (51)) contributes to making cross-border incident notification becomes more effective. NL (Drafting suggestions): ~~(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] ~~(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~~

Commission proposal	Drafting suggestions and Comments
	~~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.'~~ **4. The following article 23d is added :** ***'Article 23d*** ***Cross-border incident notification*** **(1) Member States should aim at facilitating cross-border notifications to multiple national reporting structures. ENISA, in cooperation with the NIS cooperation group and the CSIRT network, shall develop and maintain mechanisms to facilitate the alignment of incident notifications submitted via national entry points with cross-border reporting obligations, including the use of relevant tools.** **(2) ENISA shall, in cooperation with the CSIRT Network, harmonise its relevant tools with national incident notification templates and facilitate an automatisation process to exchange information about cross-border impacts.** **(3) Information submitted through relevant tools -shall not be automatically transmitted to ENISA in full, Member States shall have the possibility to select information shared.** PL (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
	~~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~~ (4b) ENISA shall develop and maintain a website providing links to all national single entry points established in line with paragraph (1) including a description of each national single entry point. ENISA shall consult the NIS Cooperation Group on the content of the website. (4c) Member States shall ensure that the national entry points are interoperable and able to exchange information. The single-entry point shall: (c) Allow entities to select whether the report is to be automatically shared with other single-entry points when the entity has obligation to report also in other Member States . (d) Allow CSIRTs or, where applicable, competent authorities to share a report with other single-entry points when deemed necessary. (4d) ENISA shall in consultation with the CSIRTs network [and the NIS Cooperation Group] develop and provide technical protocols and tools to ensure the interoperability and exchange of information between the national single-entry points withing 12 months from the entry into force of this Regulation. (5) Member States shall establish the single entry point within 36 months from the entry into force of this Regulation.

Commission proposal	Drafting suggestions and Comments
	SI (Drafting suggestions): (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] SI (Comments): Deletion of the paragraph SK (Drafting suggestions): **(7)** **ENISA shall maintain a publicly accessible website providing links to national single-entry points and general information regarding the common technical specification and reference implementation.** **(8)** **Member States shall establish or adapt their national single-entry points in accordance with this Article within 36 months from the entry into force of this Regulation.** **Member States opting voluntarily for reference implementation of a single-entry point developed by ENISA will be responsible for its operation and maintenance.**

Commission proposal	Drafting suggestions and Comments
2. Article 23 is amended as follows:	DE (Drafting suggestions): **5**. Article 23 is amended as follows: FR (Drafting suggestions): Article 23 is amended as follows: IT (Drafting suggestions): ~~2~~ **5**. Article 23 is amended as follows: NL (Drafting suggestions): **5**. Article 23 is amended as follows:
(a) in paragraph 1, the first sentence is replaced by the following:	DE (Drafting suggestions): (a) ~~in paragraph 1, the first sentence is replaced by the following:~~ **The following paragraph 1a is added :** FR (Drafting suggestions): (a) ~~in paragraph 1, the first sentence is replaced by the following:~~ **The following paragraph 1a is added :** IT (Drafting suggestions): (a) ~~in paragraph 1, the first sentence is replaced by the following:~~ **The following paragraph 1a is added :**

Commission proposal	Drafting suggestions and Comments
	NL (Drafting suggestions): (a) ~~in paragraph 1, the first sentence is replaced by the following:~~ **The following paragraph 1a is added :**
'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.'	BE (Drafting suggestions): '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). **Each Member State shall ensure that essential and important entities are able to submit such notifications** via the single-entry point established pursuant to Article 23~~a.~~ **Where a national reporting platform or other national reporting mechanism exists, Member States shall also ensure that entities are permitted to submit notifications directly to the competent national authority through that national mechanism'** BE (Comments): Member States should make it possible for Entities to notify via the SEP. Yet, if national reporting mechanisms exists, Member States should still be allowed to let entities choose the notification method that is most simple to them, be that via the SEP or directly to (all) the national platform(s). Such a voluntary mechanism would also ensure that a back-up system is in place as long as the SEP is not there. It will also allow the SEP to prove it is indeed the simpelest form. DE (Drafting suggestions):

Formatted: Spanish (Spain)

Commission proposal	Drafting suggestions and Comments
	~~'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.'~~ **(1a) ENISA shall, in cooperation with the Cooperation Group, provide a mapping of all the competent authorities and CSIRTs referred to in paragraph 1 in the single-information point established pursuant to Article 23a.** ES (Drafting suggestions): DELETE Article 6(2) in its entirety. No amendment to Article 23 NIS2 is necessary or justified. The sole purpose of the proposed modification to paragraph 1 is to introduce the single-entry point as the mandatory notification channel. With the SEP replaced by the Single Information Point, Article 23 NIS2 should remain unchanged. The addition of paragraph 12 (CRA manufacturer reporting) is also unnecessary, as the CRA platform shall remain a separate matter to the SIP and the SEP is never to be created in the first place. ES (Comments): ES: The modification to Article 23(1) has no independent regulatory purpose beyond routing notifications via the SEP. In line with the non-paper co-signed by ES, FR, DE, IT, NL, SE, no European single entry point should be created. Article 23 NIS2 must remain intact. FI

Commission proposal	Drafting suggestions and Comments
	(Drafting suggestions): 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). **Member States shall ensure that notifications can be submitted via the single-entry point established pursuant to Article 23a.** FI (Comments): FI: Entities should be able to choose how to report an incident. Therefore, reporting via SEP should not be mandated in the legal text. FR (Drafting suggestions): ~~'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.'~~ **(1a) ENISA shall, in cooperation with the NIS Cooperation Group, provide a maping of all the competent authorities and CSIRTs referred to in paragraph 1 in the single information point established pursuant to Article 23a.** IT (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
	~~'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.'~~ **(1a) ENISA shall, in cooperation with the NIS Cooperation Group, provide a mapping of all the competent authorities and CSIRTs referred to in paragraph 1 in the single information point established pursuant to Article 23a.** LU (Drafting suggestions): '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.' **When submitting an incident notification, essential and important entities becoming aware of, or being informed about, the unavailability or malfunctioning of the single-entry point shall inform its CSIRT or, where applicable, its competent authority by any means** LU (Comments): Recital 52 states that a continuity and interoperability with existing national solutions should be guaranteed and Recital 57 states that an alternative solution should be available in the case of technical issues, however the proposed amendments to NIS2 (Art6) but also the changes for GDPR as well

Commission proposal	Drafting suggestions and Comments
	as CER, do not foresee an alternative solution and does not provide the possibility to use a national platform. Therefore, LU would suggest to include the aforementioned sentence to Article 23a in article 6. paragraph 2 for the amendment to article 23 of NIS2, and also in paragraph 3 for the amendment to article 30 of NIS2. The same should apply for amendements to other Directives or Regulations. The same approach should apply to amendments to other Directives or Regulations. NL (Drafting suggestions): ~~'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.'~~ **(1a) ENISA shall, in cooperation with the NIS Cooperation Group, provide a maping of all the competent authorities and CSIRTs referred to in paragraph 1 in the single information 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)	DE (Drafting suggestions): When **an essential or important entity that is also** a manufacturer **pursuant to Article 3(13) of Regulation (EU) 2024/2847** notifies a severe

Commission proposal	Drafting suggestions and Comments
2024/2847 shall constitute reporting of information under paragraph 4 of this Article.'; 3. in Article 30, paragraph 1 is replaced by the following: '1. Member States shall ensure that, in addition to the notification obligation provided for in Article 23, notifications can be submitted to the CSIRTs or, where applicable, the competent authorities, on a voluntary basis via the single-entry point established pursuant to Article 23a, by:	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 **according to the national incident reporting specification pursuant to this Directive**, 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. DE (Comments): These are German modifications to prevent regulatory gaps and misunderstandings DE (Drafting suggestions): '1. Member States shall ensure that, in addition to the notification obligation provided for in Article 23, notifications can be submitted to the CSIRTs or, where applicable, the competent authorities, on a voluntary basis via ~~the single-entry point established pursuant to Article 23a~~ **national reporting structures**, by: ES (Drafting suggestions): DELETE Article 6(3) in its entirety. No amendment to Article 30 NIS2 is necessary or justified. The sole modification introduced is the addition of "via the single-entry point established pursuant to Article 23a", which has no purpose if the SEP is replaced by the Single Information Point. Article 30 NIS2 should remain unchanged. ES (Comments):

Commission proposal	Drafting suggestions and Comments
	ES: As with Article 23, this modification exists exclusively to route voluntary notifications via the SEP. Without the SEP, no amendment to Article 30 is needed. In line with the non-paper co-signed by ES, FR, DE, IT, NL, SE. FR (Drafting suggestions): '1. Member States shall ensure that, in addition to the notification obligation provided for in Article 23, notifications can be submitted to the CSIRTs or, where applicable, the competent authorities, on a voluntary basis via ~~the single-entry point established pursuant to Article 23a~~ **national reporting structures**, by: IT (Drafting suggestions): '1. Member States shall ensure that, in addition to the notification obligation provided for in Article 23, notifications can be submitted to the CSIRTs or, where applicable, the competent authorities, on a voluntary basis via ~~the single-entry point established pursuant to Article 23a~~ **national reporting structures**, by: LU (Drafting suggestions): '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.' **When submitting an incident notification, essential and important entities becoming aware of, or being informed about, the unavailability or malfunctioning of the single-entry**

Commission proposal	Drafting suggestions and Comments
	point shall inform its CSIRT or, where applicable, its competent authority by any means LU (Comments): Recital 52 states that a continuity and interoperability with existing national solutions should be guaranteed and Recital 57 states that an alternative solution should be available in the case of technical issues, however the proposed amendments to NIS2 (Art6) but also the changes for GDPR as well as CER, do not foresee an alternative solution and does not provide the possibility to use a national platform. Therefore LU would suggest to include the aforementioned sentence to Article 23a in article 6. paragraph 2 for the amendment to article 23 of NIS2, and also in paragraph 3 for the amendment to article 30 of NIS2. The same approach should apply to amendments to other Directives or Regulations. NL (Drafting suggestions): '1. Member States shall ensure that, in addition to the notification obligation provided for in Article 23, notifications can be submitted to the CSIRTs or, where applicable, the competent authorities, on a voluntary basis via ~~the single entry point established pursuant to Article 23a~~ **national reporting structures**, by:
(a) essential and important entities with regard to incidents, cyber threats and near misses;	

Commission proposal	Drafting suggestions and Comments
(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.';	BE (Drafting suggestions): '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 **or directly through national reporting mechanisms, where they should exist.**'; DE (Drafting suggestions): '1a. **Recommendations on how entities shall ensure compliance with** ~~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 available through the single-**information**~~-entry~~ point pursuant to Article 23a of Directive (EU) 2022/2555.'; ES

Commission proposal	Drafting suggestions and Comments
	(Drafting suggestions): DELETE new paragraph entirely. Notifications under Art 19a(1a) should continue to be made as before ES (Comments): ES: Delete. Routes notifications via SEP. Without SEP, existing direct notification channels under eIDAS apply. FI (Drafting suggestions): '1a. **Member States shall ensure that** notifications pursuant to paragraph 1, point (b) of this Article to the supervisory body and, where applicable, to other relevant competent authorities, **can** be made through the single-entry point pursuant to Article 23a of Directive (EU) 2022/2555.' FI (Comments): FI: Entities should be able to choose how to report an incident. Therefore, reporting via SEP should not be mandated in the legal text. FR (Drafting suggestions): '1a. **Guidance on how entities shall ensure compliance with** ~~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 **information** ~~entry~~ point pursuant to Article 23a of Directive (EU) 2022/2555.'; IT

Commission proposal	Drafting suggestions and Comments
	(Drafting suggestions): '1a. **Guidance on how entities shall ensure compliance with** ~~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 **information** ~~entry~~ point pursuant to Article 23a of Directive (EU) 2022/2555.'; IT (Comments): The wording is adjusted to ensure cohrence with the single information point proposed under Article 23a. NL (Drafting suggestions): '1a. **Guidance on how entities shall ensure compliance with** ~~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 **information** ~~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.';	BE (Drafting suggestions): 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 **or directly through national reporting mechanisms, where they should exist.**';

Commission proposal	Drafting suggestions and Comments
	DE (Drafting suggestions): '2a. **Recommendations on how entities shall ensure compliance with** 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-**information** ~~-entry~~ point pursuant to Article 23a of Directive (EU) 2022/2555.'; ES (Drafting suggestions): DELETE new paragraph entirely. Notifications under Art 24(2a) should continue to be made as before. ES (Comments): ES: Delete. Routes notifications via SEP. Without SEP, existing direct notification channels under eIDAS apply. FI (Drafting suggestions): **Member States shall ensure that** notifications pursuant to in paragraph 2, point (fb), of this Article to the supervisory body and, where applicable, to other relevant competent bodies, **can** be made through the single-entry point pursuant to Article 23a of Directive (EU) 2022/2555 FI (Comments): FI: Entities should be able to choose how to report an incident. Therefore, reporting via SEP should not be mandated in the legal text. FR (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
	'2a. **Guidance on how entities shall ensure compliance with** 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 **information**-entry point pursuant to Article 23a of Directive (EU) 2022/2555.'; IT (Drafting suggestions): '2a. **Guidance on how entities shall ensure compliance with** 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 **information**~~-entry~~ point pursuant to Article 23a of Directive (EU) 2022/2555.'; IT (Comments): See above. NL (Drafting suggestions): '2a. **Guidance on how entities shall ensure compliance with** 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 **information**-entry point pursuant to Article 23a of Directive (EU) 2022/2555.';
3. in Article 45a the following paragraph 3a is inserted:	
'3a. Notifications pursuant to in paragraph 3 to the Commission and to the competent supervisory body, shall be made through the single-entry point pursuant to Article 23a of Directive (EU) 2022/2555.'	BE (Drafting suggestions): '3a. Notifications pursuant to in paragraph 3 to the Commission and to the competent supervisory body, shall be made through the single-entry point

Commission proposal	Drafting suggestions and Comments
	pursuant to Article 23a of Directive (EU) 2022/2555 **or directly through national reporting mechanisms, where they should exist.**'; DE (Drafting suggestions): '3a. **Recommendations on how entities shall ensure compliance with** ~~Notifications pursuant to in~~ paragraph 3 ~~to the Commission and to the competent supervisory body,~~ shall be made available through the single-**information** ~~entry~~ point pursuant to Article 23a of Directive (EU) 2022/2555.' ES (Drafting suggestions): DELETE new paragraph entirely. Notifications under Art 45a(3a) should continue to be made as before. ES (Comments): ES: Delete. Routes notifications via SEP. Without SEP, existing direct notification channels under eIDAS apply. FI (Drafting suggestions): **Member States shall ensure that** notifications pursuant to in paragraph 3 to the Commission and to the competent supervisory body, **can** be made through the single-entry point pursuant to Article 23a of Directive (EU) 2022/2555 FI (Comments): FI: Entities should be able to choose how to report an incident. Therefore, reporting via SEP should not be mandated in the legal text.

Commission proposal	Drafting suggestions and Comments
	FR (Drafting suggestions): '3a. **Guidance on how entities shall ensure compliance with** ~~Notifications pursuant to in~~ paragraph 3 ~~to the Commission and to the competent supervisory body,~~ shall be made through the single **information-**~~entry~~ point pursuant to Article 23a of Directive (EU) 2022/2555.' IT (Drafting suggestions): '3a. **Guidance on how entities shall ensure compliance with** ~~Notifications pursuant to in~~ paragraph 3 ~~to the Commission and to the competent supervisory body,~~ shall be made through the single **information-**~~entry~~ point pursuant to Article 23a of Directive (EU) 2022/2555.' IT (Comments): See above. NL (Drafting suggestions): '3a. **Guidance on how entities shall ensure compliance with** ~~Notifications pursuant to in~~ paragraph 3 ~~to the Commission and to the competent supervisory body,~~ shall be made through the single **information-**~~entry~~ point pursuant to Article 23a of Directive (EU) 2022/2555.'
Article 8	
Amendments to Regulation (EU) 2022/2554	
Article 19 of Regulation (EU) 2022/2554 is amended as follows:	

Commission proposal	Drafting suggestions and Comments
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.'	BE (Drafting suggestions): 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 **or directly via national reporting mechanisms, where they should exist.**'; DE (Drafting suggestions): '**Recommendation to** ~~F~~financial entities **which** shall report major ICT-related incidents to the relevant competent authority as referred to in Article 46 **shall be provided** via the single-**information** ~~-entry-~~point established pursuant to Article 23a of Directive (EU) 2022/2555 ~~in accordance with paragraph 4 of this Article~~.' ES (Drafting suggestions): DELETE new paragraph entirely. Notifications under DORA should continue to be made as before. ES (Comments): ES: DORA's existing notification channel to the relevant competent authority must be preserved. FI (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
	Member States shall ensure that financial entities **can** 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 FI (Comments): FI: Entities should be able to choose how to report an incident. Therefore, reporting via SEP should not be mandated in the legal text. FR (Drafting suggestions): '**Guidance to** ~~F~~financial entities **which** shall report major ICT-related incidents to the relevant competent authority as referred to in Article 46 **shall be provided** via the single **information** ~~-entry~~ point established pursuant to Article 23a of Directive (EU) 2022/2555 ~~in accordance with paragraph 4 of this Article~~.' IT (Drafting suggestions): '**Guidance to** ~~F~~financial entities **which** shall report major ICT-related incidents to the relevant competent authority as referred to in Article 46 **shall be provided** via the single **information** ~~-entry~~ point established pursuant to Article 23a of Directive (EU) 2022/2555 ~~in accordance with paragraph 4 of this Article~~.' IT (Comments): See above. NL

Commission proposal	Drafting suggestions and Comments
	(Drafting suggestions): '**Guidance to** ~~F~~financial entities **which** shall report major ICT-related incidents to the relevant competent authority as referred to in Article 46 **shall be provided** via the single **information** ~~-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:	DE (Drafting suggestions): ~~2. in paragraph 2, the first subparagraph is replaced by the following:~~ FR (Drafting suggestions): ~~2. in paragraph 2, the first subparagraph is replaced by the following:~~ IT (Drafting suggestions): ~~2. in paragraph 2, the first subparagraph is replaced by the following:~~ NL (Drafting suggestions): ~~2. in paragraph 2, the first subparagraph is replaced by the following:~~
'Financial entities may, on a voluntary basis, notify via the single-entry point established pursuant to Article 23a of Directive (EU) 2022/2555 significant cyber threats to the relevant competent authority when they deem the threat to be of relevance to the financial system, service users or clients. The relevant competent authority may provide such information to other relevant authorities referred to in paragraph 6.'	BE (Drafting suggestions): 'Financial entities may, on a voluntary basis, notify via the single-entry point established pursuant to Article 23a of Directive (EU) 2022/2555 **or directly via national reporting mechanisms, where they should exist,** 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

Commission proposal	Drafting suggestions and Comments
	relevant competent authority may provide such information to other relevant authorities referred to in paragraph 6.' DE (Drafting suggestions): ~~'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.'~~ ES (Drafting suggestions): DELETE new paragraph entirely. Notifications under DORA should continue to be made as before ES (Comments): ES: Voluntary threat notifications under DORA should remain direct to the relevant competent authority. FR (Drafting suggestions): ~~'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.'~~ IT (Drafting suggestions):

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.'~~ IT (Comments): See above. NL (Drafting suggestions): ~~'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:	DE (Drafting suggestions): 1. in paragraph 1, the first sentence is replaced as follows: **the following paragraph 1a is inserted:** FR

Commission proposal	Drafting suggestions and Comments
	(Drafting suggestions): 1. in paragraph 1, the first sentence is replaced as follows: **the following paragraph 1a is inserted:** IT (Drafting suggestions): 1. in paragraph 1, the first sentence is replaced as follows: **the following paragraph 1a is inserted:** NL (Drafting suggestions): 1. in paragraph 1, the first sentence is replaced as follows: **the following paragraph 1a is inserted:**
'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.';	BE (Drafting suggestions): Member States shall ensure that critical entities notify **either** via the single-entry point established pursuant to Article 23a of Directive (EU) 2022/2555 the competent authority, **or via national reporting mechanisms, where they should exist** ,without undue delay, of incidents that significantly disrupt or have the potential to significantly disrupt the provision of essential services.'; DE (Drafting suggestions): '**Recommendation on how critical entities shall notify national competent authorities** ~~Member States~~ shall **be made available** ~~ensure that critical entities notify~~ via the single-**information** ~~-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~~.';

Commission proposal	Drafting suggestions and Comments
	ES (Drafting suggestions): DELETE new paragraph entirely. Notifications under CER should continue to be made as before ES (Comments): ES: CER notification must remain a direct channel to national competent authorities. FI (Drafting suggestions): Member States shall ensure that critical entities notify the competent authority, without undue delay, of incidents that significantly disrupt or have the potential to significantly disrupt the provision of essential services. **Member Statess shall ensure that such notifications can be submitted via the single-entry point established pursuant to Article 23a of Directive (EU) 2022/2555** FI (Comments): FI: Entities should be able to choose how to report an incident. Therefore, reporting via SEP should not be mandated in the legal text. FR (Drafting suggestions): ‘**Guidance on how critical entities shall notify national competent authorities** ~~Member States~~ shall **be made available** ~~ensure that critical entities notify~~ via the single-**information** ~~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~~.’;

Commission proposal	Drafting suggestions and Comments
	IT (Drafting suggestions): '**Guidance on how critical entities shall notify national competent authorities** ~~Member States~~ shall **be made available** ~~ensure that critical entities notify~~ via the single-**information** ~~-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~~.'; IT (Comments): See above. NL (Drafting suggestions): '**Guidance on how critical entities shall notify national competent authorities** ~~Member States~~ shall **be made available** ~~ensure that critical entities notify~~ via the single-**information** ~~-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:	DE (Drafting suggestions): 2. in paragraph 2, the following sub-paragraph is added: FR

Commission proposal	Drafting suggestions and Comments
	(Drafting suggestions): 2. in paragraph 2, the following sub-paragraph is added: IT (Drafting suggestions): ~~2. in paragraph 2, the following sub-paragraph is added:~~ NL (Drafting suggestions): 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).'	DE (Drafting suggestions): ~~'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).'~~ ES (Drafting suggestions): DELETE new paragraph entirely. Notifications under CER should continue to be made as before ES (Comments): ES: CER notification must remain a direct channel to national competent authorities. FR (Drafting suggestions): ~~'The Commission may adopt implementing acts further specifying the type and format of information notified pursuant to Article 15(1). Those~~

Commission proposal	Drafting suggestions and Comments
	~~implementing acts shall be adopted in accordance with the examination procedure referred to in Article 24(2).'~~ IT (Drafting suggestions): ~~'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).'~~ IT (Comments): See above. NL (Drafting suggestions): ~~'The Commission may adopt implementing acts further specifying the type and format of information notified pursuant to Article 15(1). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 24(2).'~~
Article 10	
Repeals and transitory clauses	
1. Regulation 2019/1150/EU is repealed with effect from [date = entry into application of this Regulation].	
2. By way of derogation from paragraph 1, the following provisions shall continue to apply until 31 December 2032:	

Commission proposal	Drafting suggestions and Comments
(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	LV (Comments): We note that the timelines for application can only be objectively assessed once a compromise has been reached on all essential aspects and the overall alignment of the regulatory framework within the Digital Omnibus has been achieved; therefore, no comments can be submitted on this matter at this stage.

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*.	PL (Drafting suggestions): This Regulation shall enter into force on the ~~third~~ **twentieth** day following that of its publication in the *Official Journal of the European Union*. **It shall apply from 24 months after its entry into force.** PL (Comments): The proposed time of entry into force of this Regulation (on the third day after its publication) is unfeasible for us. We need more transitional period to adapt the existing regulations, especially to repeal the law implementing the ODD.
Deviating from paragraph 3, Article 5(2) shall enter into application 6 months after the publication in the Official Journal of the European Union.	PL (Drafting suggestions): Delete in case of adopting longer time of entry into application as above. PL (Comments): The proposed time of entry into force of this Regulation (on the third day after its publication) is unfeasible for us. We need more transitional period to adapt the existing regulations, especially to repeal the law implementing the ODD.
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	BE (Drafting suggestions): Article 1 (18) with regard to the insertion of a new chapter VIIc, 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

Formatted: Not Highlight

Commission proposal	Drafting suggestions and Comments
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.	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. BE (Comments): Entering into application on the third day following its publication would be unreasonable for the modifications that are required to national legal systems for the following reasons: - Member States must be attributed sufficient time to properly prepare the merging of their corresponding legal systems with a view to clarity and efficiency just as is intended by the Omniobus itself. - Given the fact that the OOD will be transformed to a regulation instead of a directive, MS also need to repeal or modify national transpositions laws for the Open Data Directive and effectively need a reasonable periode of time to adapt existing the laws on implementing measures for the Data Governance Act. Besides merging legal systems, the Commission also effectively includes several new elements and obligations in this proposal. These not only necessitate changes to extisting national legal frameworks and practical preparations, adequate resources and budgets are also required. This is the case for: - the broadening of the scope of application for the reuse of protected data to include all non-electronic protected documents (article 32w). The fact that it is 'not obligatory' for public bodies to approve requests for protected documents or electonic data, does not change

Commission proposal	Drafting suggestions and Comments
	the fact that public sector bodies must treat and analyse the requests for protected documents that they will receive, motivate their decisions on these requests and provide for an effective right of redress regarding requests for protected documents (article 32ab). - furthermore, the completely new obligation for public bodies charging fees for re-use of their informations of the establishment of a specific system for online payment (article 32k) cannot be completed within three days following the publication of the proposed regulation, adequate resources and budgets are also required to be able to effectively organise such system. - Even though Belgium is opposing the adoption of the exception (alternative treatment) regime for very large enterprises set out in the proposed Articles 32q(6), 32r(4) and 32y(5), *if these exceptions for VLE's are adopted,* this will lead to a multitude of administrative and legislative tasks for MS, in order to ensure the exceptions will not be applied in an arbitraty manner. This in turn clearly requires a reasonable period of time. For the reasons mentioned above, we propose to pospone the entry into application of the new chapter VIIc (article 1(18)) : and have this new chapter enter into application 18 months from the entry into force of this Regulation. In addition the COM admitted in its presentation on Omnibus VII: Digital Omnibus – Presentation by the Commission (AGS on 13 February 2026) - WK 2134/2026 INIT that the COM "*understand[s] the need for MS to repeal national transpositions laws for the Open Data Directive and the potential need to adapt the laws on implementing measures for the Data Governance Act. Reasonable time can be given for this.*". (slide 47).

Commission proposal	Drafting suggestions and Comments
	Regarding the new obligation of a mandatory online electronic payment system for fees for re-use the COM stated: *"•Commission is open to discuss with MS the practical effects of the extension of scope.* *•It is correct to note that the obligation to provide the means to pay online in Article 32l (4) also for data previously covered by the Open Data Directive is a new element. The Commission is open to discuss practical issues in relation to the entry into application of this obligation."* ES (Drafting suggestions): DELETE the entire SEP-contingent proviso (second sentence of the third paragraph of Article 11): '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 [...]' — DELETE in full. The entry into application provision should read: '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.' without any contingency on SEP operational assessment. ES (Comments): ES: Without the SEP, the contingency mechanism in Article 11 is redundant. Template harmonisation provisions should apply on standard timeline. FI (Drafting suggestions): Article 3(8), points (a) to (c), Articles 6 (2) and (3) and 7 to 9, shall enter into application **24** months from the entry into force of this Regulation. Deviating from the first sentence, where the Commission finds in its assessment

Commission proposal	Drafting suggestions and Comments
	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 **30** months from the entry into force of this Regulation. FI (Comments): FI finds necessary to ensure sufficient and realistic implementation timeline, considering complex technical implementation of the SEP. PL (Drafting suggestions): Delete in case of adopting longer time of entry into application as above. PL (Comments): The proposed time of entry into force of this Regulation (on the third day after its publication) is unfeasible for us. We need more transitional period to adapt the existing regulations, especially to repeal the law implementing the ODD.
This Regulation shall be binding in its entirety and directly applicable in all Member States.	

Commission proposal	Drafting suggestions and Comments
Done at Brussels,	
For the European Parliament *For the Council*	
The President *The President*	
	NL (Drafting suggestions): Annex I NL (Comments): Comments in seperate document. It is important that the annex is correct since art. 10(3) Omnibus is refering to this annex.
Annex II	
List of thematic categories of high-value datasets, as referred to in Article 32ab(1) of Regulation (EU) 2023/2854	
1. Geospatial	
2. Earth observation and environment	
3. Meteorological	
4. Statistics	
5. Companies and company ownership	
6. Mobility	

Commission proposal	Drafting suggestions and Comments