Council of the European Union
General Secretariat

PUBLIC

Interinstitutional files:
2025/0360 (COD)

Brussels, 31 July 2026

WK 11020/2026 INIT

LIMITE

SIMPL
ANTICI
DATAPROTECT
CYBER
TELECOM
CODEC
PROCIV
COMPET
MI

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): Written comments and drafting suggestions from Member States on the Presidency revised compromise text

Delegations will find attached the comments and drafting suggestions on the Presidency revised compromise text set out in document ST 10677/2026 (deadline: 28 July 2026) submitted by the following Member States: CZ, DK, EE, EL, ES, FR, IT, LV, LU, HU, NL, AT, PL, SI, SK and FI.

Comments on the Presidency revised compromise text Deadline: ***28 July 2026***
From: CZ, DK, EE, EL, ES, FR, IT, LV, LU, HU, NL, AT, PL, SI, SK, FI **Updated: 31/07/2026 14:18**

PUBLIC

Guidelines to be followed

Please kindly provide your contributions in the table below.

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

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

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

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

Thank you for your cooperation!

Commission proposal	Drafting suggestions and Comments
General Comments	DK (Comments): It is important to increase the level of ambition to deliver concrete simplification benefits for businesses. In our opinion, this is possible without making any significant compromises to the level of data protection. We are generally satisfied with the current approach on ePrivacy parts and welcome the continued efforts to simplify the framework while preserving a high level of protection for users. In particular, we would welcome the reintroduction of exemptions fraud detection and prevention, provided that it is limited to what is strictly necessary and accompanied by appropriate safeguards, preventing misuse. The same goes for the reintroduction of the exemption on contextual advertising. Finally, we are still scrutinising the suggestions from PL, but are, at this stage, positive towards the suggestions. EE

Commission proposal	Drafting suggestions and Comments
	(Comments): Estonia thanks for the opportunity to provide comments and drating suggestions. Estonia welcomes the progress made in the compromise text and thanks the Cyprus Presidency for its work. Therefore we will focus on the points where we still see a need for further clarification. We would first like to make a general observation on the proposed Data Act Estonia supports the aim of simplifying the EU digital rulebook and the idea of one single EU data regulation that brings together the rules from the Open Data Directive, the Data Governance Act and the Regulation on the free flow of non-personal data. The terms “data” and “documents” remain insufficiently clear and are used inconsistently throughout the articles. At the same time, the fundamentally changed definition of „document“ does instead add additional complexity and confusion. Thus, these laws do not align within themselves. Furthermore, the new Data Regulation does not clearly set out under which conditions personal data can be made available as open data. The definition of data has to be stable throughout the data act. If the scope of these terms is unclear, public authorities and users may not know which rules apply. This could lead to different interpretations in Member States and create more, not less, administrative burden. „Document“, as defined in the Open Data Directive, was understood as information in any format or medium, while the Digital Omnibus redefines „Document“ as „.. non-digital ..“. This change is problematic for multiple reasons: a. It has been stated that the current aim of the Omnibus is to consolidate available legal acts, not to make fundamental changes in the content. As the change of core definitions is a fundamental change, we risk breaking the rules set by ourselves.

PUBLIC

Commission proposal	Drafting suggestions and Comments
	b. The updated definition is not in line with international best practices and definitions, incl. definitions provided within the Tromso Convention, and international standards on documents, records and information management c. The content of the Digital Omnibus has not been thoroughly reviewed in regard to the change, leading to inconsistencies and impossible requirements (e.g. requiring to make high value „documents“ machine-readable and available via APIs). Though Estonia has highlighted some of the most obvious errors in prior consultations, there must be a full review of all occurencies of „data“, „documents“, „data and documents“, „data or documents“ etc. d. Fundamentally, the availability and reusability of information should be concentrating on the value and usefulness of publishing this information, not on whether this information is available in digital or non-digital form, meaning that the issues raised by the changed definitions are unnecessary in the first place. e. The title „Data Act“ implies, that issues regarding the specific issues of the availability of non-digital information (i.e. paper documents) are not in scope. Based on these arguments, Estonia prefers to continue using the definition of „document“ as provided in the current Open Data Directive, or scope the Data Act / Digital Omnibus to regulate only „data“. Alternatively, if we are not willing to revert the definition of „document“, a thorough review of the Digital Omnibus must be undertaken, to ensure the consistency and relevance of the act. We would like to emphasise once more that this clarification is necessary to ensure legal certainty and a simpler framework in practice. ES (Comments):

Commission proposal	Drafting suggestions and Comments
	The comments and drafting proposals on the cyber-related provisions in the table reflect a joint proposal supported by Spain, France, Austria, Italy and the Netherlands. We consider that the Presidency compromise text currently used as the basis for discussions (REV4) does not provide Member States with the flexibility needed to implement the national entry point. We do, however, support the wording proposed for the cyber-related provisions on 22 June (REV5). Our comments therefore seek to restore the wording of REV5 and to introduce the corresponding consequential amendments to the sectoral acts. FR (Comments): The comments and drafting proposals on the cyber part in the table are a joint proposal supported by Spain, Austria, Italy, The Netherlands and France. We believe that the compromised text currently used by the Presidency (REV4) do not provide the flexibility needed by Member States in implementing the national entry point. We however support the drafting on the cyber part proposed on the 22nd of June (REV5). Therefore, our comments aim at coming back to the wording of the REV5 and asks for consequential amendments to the sectoral acts. IT (Drafting suggestions): **OVERALL DRAFTING APPROACH** Replace procedure-centred and risk-based compliance with outcome-based accountability. Controllers should retain discretion to determine the technical and organisational means most appropriate to their processing operations, provided that they demonstrably achieve the substantive requirements of the GDPR, including lawfulness, purpose limitation, data minimisation, accuracy, confidentiality, integrity, availability, resilience and effective protection against unauthorised processing. A reduction of ex ante procedural and documentary obligations should be accompanied by stronger ex post supervision. Supervisory authorities should concentrate resources on

Commission proposal	Drafting suggestions and Comments
	effective inspections, technical audits and verification of actual processing practices rather than prescribing organisational methods, templates or additional paperwork. The supervisory and judicial functions should be expressly distinguished. Supervisory authorities should determine regulatory compliance with the GDPR and exercise administrative corrective powers. Courts should adjudicate contested subjective rights, civil liability, damages, compensation and other inter partes claims. IT (Comments): **General comment** The simplification exercise should remove formalism without weakening substantive protection. The proposed regulatory bargain is greater operational freedom for controllers in choosing means of compliance, combined with materially stronger ex post inspection by supervisory authorities. The central organising principle should therefore be achievement of objectively verifiable legal, safety and security outcomes rather than completion of prescribed risk assessments. This requires operative amendments to Articles 24, 25, 32, 33 and 35, not merely interpretative recitals. As regards institutional competence, Article 8(3) of the Charter requires independent supervision of data-protection compliance, while Article 47 protects effective judicial adjudication. The proposed text therefore reserves regulatory compliance and corrective enforcement to supervisory authorities, while reserving civil rights, compensation and other inter partes claims to courts. This would be a substantive legislative adjustment to the present relationship between Articles 77-79 GDPR, interpreted in CJEU Case C-132/21 as providing concurrent and independent remedies. With reference to the SEP, this submission has been jointly developed with France, the Netherlands, Spain and Austria as a common approach. LU (Comments): **Luxembourg strongly supports the continuation of the drafting proposal submitted by the Cypriot Presidency on Article 49 of the GDPR, concerning exchange of tax information with third countries.**

Commission proposal	Drafting suggestions and Comments
	SI (Comments): We support the direction in which the text has developed so far as it strikes an appropriate balance between simplification and preserving the core principles of the data protection framework. We consider the latest version of the text under the CY PCY to be a good compromise and solid basis for negotiations with the European Parliament Should there be strong support for additional amendments, we could only support them insofar as they do not interfere with the definition of "personal data", lower data subjects' rights or generally lower protection standards by opening new avenues for interpreting the nature of the data being processed. It is precisely these additional and potentially divergent rules, introduced without prior impact assessments, that could disproportionately affect legal certainty, clarity, and increase the burden on data controllers in achieving compliance. SK (Comments): **SK: All SK comments are considered a preliminary.** Slovakia supports the objective of consolidating and simplifying the Union data acquis. However, simplification should not weaken trust, neutrality or effective access to data. The final text should preserve proportionate baseline safeguards, ensure adequate implementation resources for public sector bodies and avoid creating parallel national infrastructures. **Comment for the GDPR are relevant also for same for EUDPR and they are not repeated there.**

PUBLIC

Commission proposal	Drafting suggestions and Comments
	We welcome that proposal for amendment of Article 49 (1)(d) GDPR and accompanying recital are not included in this document. We have strong reservation about this proposal as we consider the area of international transfers to be a sensitive issue. In our view, the proposed amendment regulates precisely the situation that is currently being held by the CJEU in case C-804/25. In this respect, we believe that the timing of the proposal is not right. In our view, the proposed amendment to Article 49(1)(d) and (4) of Regulation 2016/679 is only an editorial change. However, the accompanying recital 40b already shifts the interpretation of this exception. Specifically, it concerns the part *„where personal data are exchange on a periodic or automated basis“*. This is in direct contradiction with the second subparagraph of Article 49(1), which states that transfers under the exceptions may take place *“only if the transfer is not repetitive”*. Exceptions should be interpreted restrictively so that the exception does not become the rule. GDPR has in Article 46 tools for the transfer of personal data between public authorities based on an international treaty, which take precedence over the exceptions. Specifically, Article 46(2)(a) – legally binding and enforceable instrument and Article 46 (3)(b) – administrative arrangements. We are concerned that the proposed recital 40b may lead to circumvention of the hierarchy of tools for transfer. We are worried that the proposed recital 40b will in practice lead to a situation where public authorities, instead of seeking to incorporate appropriate safeguards under Article 46 GDPR, will take the easier route and rely on the exemption under Article 49(1)(d) GDPR. FI (Comments):

Commission proposal	Drafting suggestions and Comments
	FI thanks the Presidency for advancing the negotiations and the opportunity to submit written comments and for considering our drafting suggestions. In general, FI considers it vital to find a balanced solution that clarifies the application of the GDPR and reduces unnecessary administrative burden without affecting the current level of data protection. FI supports in general the approach of this compromise proposal regarding the amendments on the ePrivacy rules, including the "whitelist" exemptions, but wishes to raise questions on centralised and automated consent and the impact on the media sector. FI supports the current solution of keeping the cookie regulation in the ePD. Regardless of the solution on Article 88a and 88b, it is important to ensure the interplay between the GDPR and the ePD as well as to ensure that current level of data protection would not weaken. If the provisions related to cookies were transferred to the GDPR, it should be ensured that non-personal data would not get higher level of protection than personal data. Overall, FI finds it important that the Commission continues the work on updating ePrivacy rules. FI remains open for discussing the below points in further detail and advancing a balanced outcome.
2025/0360 (COD)	
Proposal for a	
REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL	EL (Comments):

PUBLIC

Commission proposal	Drafting suggestions and Comments
	We welcome the Presidency's targeted approach and offer the following comments, while reserving our position on the remaining issues, falling under a different competence.
amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2019/1150, (EU) 2023/2854, (EU) 2022/2554, and (EU) 910/2014~~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. […].	
Having regard to the opinion of the Committee of the Regions[3],	

PUBLIC

PUBLIC

Commission proposal	Drafting suggestions and Comments
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 **of** fundamental rights, not least privacy and data protection.	
(3) Union digital legislation has evolved incrementally over the past years, in response to the rapidly growing footprint of digital technologies in the Union's economy and societal dynamic, and in view of addressing	

Commission proposal	Drafting suggestions and Comments
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. 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)	

PUBLIC

Commission proposal	Drafting suggestions and Comments
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.	
(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	

PUBLIC

Commission proposal	Drafting suggestions and Comments
streamline the regime. With respect to data altruism, certain rules of Regulation (EU) 2022/868, notably the obligation on Member States to have national policies on data altruism in place, the establishment of a 'rulebook' and developing a European data altruism consent form appear unnecessary regulation, also in light of on-going work by the European Data Protection Board referred to in Article 68 of Regulation (EU) 2016/679 of the European Parliament and of the Council[9] on guidance on the processing of personal data in the context of scientific research. 7 Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (OJ L 152, 3.6.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/868/oj). 8 Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (OJ L 172, 26.6.2019, p. 56, ELI: http://data.europa.eu/eli/dir/2019/1024/oj). 9 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).	
(8) While the importance of data intermediation services is recognised in the context of many initiatives supporting data sharing and collaboration, the rules of Regulation (EU) 2022/868 on data intermediation service providers should be clarified. In particular, the definition of such providers should be made more precise. It should eliminate elements that served merely as illustrative examples, rather than exceptions. Moreover, it should address loopholes resulting from ambiguous formulations, notably as regards the notion of 'closed group'. Services should not be eligible to register as data intermediation services where they are exclusively used by a closed group of	SK (Comments): :Slovakia considers the complete replacement of the mandatory notification regime for data intermediation services by purely voluntary registration premature. Minimum requirements on neutrality, transparency, security, complaints and non-misuse of data should apply to all providers. Voluntary registration could then operate as an enhanced Union trust label.

PUBLIC

Commission proposal	Drafting suggestions and Comments
companies and where any extension of that group of companies can only be decided by that group and not the service provider. More importantly, making this emerging market subject to a compulsory regime has created unnecessary compliance costs. At this stage of market development, a voluntary regime, allowing neutral players to distinguish themselves from other players, appears sufficient. Also, in order to enable sustainable business models, the regime should be made less strict by abolishing the requirement for a legal separation between data intermediation services and other value-added services that a **data intermediation** service **provider** should be allowed to offer, replacing it with a functional separation while keeping certain safeguards. The administrative monitoring regime should be simplified. Instead of national and a Union public register for data intermediation services providers and data altruism organisations, there should only be Union public registers, namely one for data intermediation service providers and another for data altruism organisations. Competent authorities overseeing the award of the label and the compliance of the entities with the requirements for obtaining it should be independent in this task. This should be understood to mean that they are legally and functionally independent from a data intermediation service or data altruism organisation, including at the level of their top-management. It should be possible for government organisations to financially support data intermediation services or data altruism organisations, in particular given the emerging nature of these entities, provided that they are legally separate entities. In order to ensure that recognised entities are easily identifiable throughout the Union, the Commission established Implementing Regulation (EU) 2023/1622 ~~**on the design of common logos to identify data intermediation services providers and data altruism organisations recognised in the Union**. on the design of common logos to identify data intermediation services providers and data altruism organisations recognised in the Union.~~	
(9) Regulation (EU) 2023/2854 removes barriers to data access and use, unlocks data-driven innovation and competitiveness, and safeguards the incentives of those who invest in data technologies.	

PUBLIC

Commission proposal	Drafting suggestions and Comments
(10) Chapter II of Regulation (EU) 2023/2854 requires data holders to make data available, including data protected as trade secrets, to users and their selected third parties, provided confidentiality measures established by the data holder are maintained. This requirement of maintaining confidentiality complements Directive (EU) 2016/943 of the European Parliament and of the Council [10], which sets the standard for protecting trade secrets within the Union. However, disclosure of trade secrets to third-country entities may increase risks to their integrity and confidentiality where there is exposure to jurisdictions with inadequate protections or difficulties in their actual enforcement, potentially resulting in unauthorised use, economic damage and legal uncertainty. 10 Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (OJ L 157, 15.6.2016, p. 1).	
(11) It is necessary to strengthen Regulation (EU) 2023/2854 by introducing an additional ground for data holders to refuse **access to data where such access could lead to** 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 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, non-equivalent, or weaker legal frameworks than the applicable Union rules. The new provision also covers instances where the third country legal framework, in theory, is robust or exceeds such Union rules, but lacks appropriate enforcement in practice. Such risks highlight the possibility that trade secrets could be acquired, used, or disclosed in violation of Union law, threatening the integrity and confidentiality of trade secrets.	

PUBLIC

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

PUBLIC

Commission proposal	Drafting suggestions and Comments
another entity's management or strategic decisions, whether through ownership of capital or voting rights, financial participation, contractual arrangements, or intermediary entities. Control may be exercised directly or through other means, even without majority ownership. Data holders should use best efforts to obtain the relevant information, which may include searches in public registers or requesting it from the user or third party directly, while ensuring it remains appropriately non-intrusive.	
(14) Protecting trade secrets from those vulnerabilities is essential for European **businesses** ~~industries~~ to sustain their market position and competitive advantage. While data holders may exercise discretion in protecting their trade secrets, refusals to share data should be limited to justified, exceptional circumstances, in order to preserve the objectives of Regulation (EU) 2023/2854 of fostering data-driven innovation and a thriving digital economy in the Union. Safeguards against misuse of the refusal mechanism should remain in place, including the data holder's obligation to demonstrate in a duly substantiated manner that disclosure poses a high risk and to notify competent authorities. This demonstration should be provided in writing without undue delay to the user or third party and proportionate to the case at hand. All parties involved should treat the decision and supporting demonstration as confidential in order to uphold the confidential nature of the trade secrets concerned. Users and third parties, as the case may be, may challenge the data holder's decision with the competent authority, in court, or through dispute settlement bodies.	
(15) To simplify the business-to-government data sharing framework under Regulation (EU) 2023/2854 and to clarify ambiguities that previously imposed broader obligations on businesses, it is necessary to narrow the scope of Chapter V of that Regulation from 'exceptional need' to 'public emergencies'. The concept of 'public emergencies', which is defined under Article 2(29) of Regulation (EU) 2023/2854, ~~thus~~ ensures that the obligations laid down in that Chapter are invoked only **in**~~under~~ well-defined, urgent situations, reducing the technical, administrative and legal challenges that **businesses**~~business~~ faced under the previous regime. This would ensure	SK (Comments): From a public-authority perspective, Slovakia cannot support limiting Chapter V exclusively to declared public emergencies. A narrowly defined mechanism should remain available for statutory public-interest tasks, including official statistics and evidence-based public policy, where the necessary data cannot reasonably be obtained by alternative means. At the same time, Slovakia recognises the need to ensure that such access remains strictly circumscribed and acceptable to affected economic operators. Any

Commission proposal	Drafting suggestions and Comments
that data requests are relevant and proportionate to responding, ~~mitigating,~~ or supporting the recovery from **public emergencies. While 'responding to' a public emergency presupposes an ongoing public emergency, which has been determined or officially declared in accordance with the relevant procedures under Union or national law, 'supporting the recovery from' a public emergency covers measures undertaken after the public emergency has been determined or officially declared over. The third alternative of 'mitigating' a public emergency under Regulation (EU) 2023/2854 should be deleted because it is already covered by the notion of 'responding to'** 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**~~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**~~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**~~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).	requests should therefore remain subject to necessity, proportionality, compensation, trade-secret protection, transparency, and effective redress. Further consultation with business associations / private sector representatives may be useful, to clarify the position of stakeholders towards a well-balanced restrictive approach.
(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	

Commission proposal	Drafting suggestions and Comments
(EU) 2023/2854. The absence of harmonised standards and clear definitions for key concepts such as 'robustness', 'access control', and 'consistency with contractual terms', combined with the requirement for a 'safe termination or interruption mechanism' potentially incompatible with decentralised or public blockchain architectures built on immutable ledgers, posed challenges to innovators from a cost and opportunity perspective. Additionally, the ambiguity surrounding the performance of the conformity assessment under Article 36(2) of that Regulation risks imposing disproportionate burdens. The elimination of Article 36 of Regulation (EU) 2023/2854 would therefore promote the development and market introduction of new business models, foster innovation, and reduce barriers for emerging technologies.	
(17) Certain data processing services, which do not fall within the Infrastructure as a Service (IaaS) delivery model, are custom-made to the needs or ecosystem of a customer. The provision of such data processing services is based on time-intensive pre-contractual and contractual negotiations to determine the specific requirements of 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	

Commission proposal	Drafting suggestions and Comments
remove switching and egress charges, custom-made services provided according to contracts concluded before or on 12 September 2025 should not fall within scope of Chapter VI of Regulation (EU) 2023/2854.	
(18) For reasons relating to financial planning and attracting investment, providers of data processing services, especially SMEs and SMCs, may prefer and offer contracts of a fixed duration. It is necessary to clarify that providers of data processing services may include provisions on proportionate early termination penalties in those contracts as long as they do not constitute an obstacle to switching. In addition, providers of data processing services that are SMEs or SMCs are particularly burdened by the need to align existing contracts for the provision of data processing services to Regulation (EU) 2023/2854. It is therefore necessary to establish a specific regime for those providers if they provide data processing services, other than IaaS, based on contracts concluded before or on 12 September 2025. Taking into account the aim of Regulation (EU) 2023/2854 to enable switching between data processing services and given that switching charges, including egress charges, constitute a serious obstacle to switching, the new lighter regimes for data processing services that are custom-made or are provided by SMEs or SMCs should not undermine the gradual withdrawal of those charges. Contractual provisions running contrary to that objective should be considered to never have existed, if they are included in contractual agreements on the provision of services falling within the scope of those two new specific regimes.	
(19) Regulation (EU) 2018/1807 of the European Parliament and of the Council[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' **within**~~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 Commission should continue monitoring deviations from this principle**. The provision does not affect the data processing in so far as it is carried out as part of an activity	

PUBLIC

Commission proposal	Drafting suggestions and Comments
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).	
(20) The concept of 'public security', within the meaning of Article 52 TFEU and as interpreted by the Court of Justice, covers both the internal and external security of a Member State, as well as issues of public safety, in order, in particular, to facilitate the investigation, detection and prosecution of criminal offences. It presupposes the existence of a genuine and sufficiently serious threat affecting one of the fundamental interests of society, such as a threat to the functioning of institutions and essential public services and the survival of the population, as well as the risk of a serious disturbance to foreign relations or the peaceful coexistence of nations, or a risk to military interests. In compliance with the principle of proportionality, data localisation requirements that are justified on grounds of public security should be suitable for attaining the objective pursued, and should not go beyond what is necessary to attain that objective.	
(21) Both Directive (EU) 2019/1024 and Chapter II of Regulation (EU) 2022/868 regulate the re-use of public sector information for innovation purposes. The interplay of the two sets of rules has created legal uncertainty, mainly for public sector bodies. An alignment of the rules in one legal	

PUBLIC

Commission proposal	Drafting suggestions and Comments
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 **in** ~~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. **However, the consolidation respects and allows to maintain national organisational specificities to ensure flexibility for national, regional and local administrations.** 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. **In line with this rationale, it should be recalled that the intellectual property rights of third parties are not affected by Chapter VIIc. The term 'intellectual property rights' refers to copyright and related rights only, including sui generis forms of protection. Section 2 of Chapter VIIc does not apply to data or documents covered by industrial property rights, such as patents and registered designs and trade marks.**	PL (Drafting suggestions): Since both Directive (EU) 2019/1024 and Regulation (EU) 2022/868 share the goal of enhancing the re-use of public sector information, and in order to simplify rules from the perspective of both public sector bodies and re-users of public sector information, it is rational to repeal Directive (EU) 2019/1024 and Regulation (EU) 2022/868, 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. However, the consolidation respects and allows to maintain national organisational specificities to ensure flexibility for national, regional and local administrations. **To this end, the current approach should be maintained, and it should be ensured that Member States are able to adopt policies, practical arrangements and rules that exceed the minimum standards laid down in this Regulation, thus allowing for more extensive re-use. In particular Member States should be able to adopt more advanced regulatory frameworks and instruments such as well-developed open data portals, open data officers' networks or multiannual open data strategies.** 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. In

PUBLIC

Commission proposal	Drafting suggestions and Comments
	line with this rationale, it should be recalled that the intellectual property rights of third parties are not affected by Chapter VIIc. The term 'intellectual property rights' refers to copyright and related rights only, including sui generis forms of protection. Section 2 of Chapter VIIc does not apply to data or documents covered by industrial property rights, such as patents and registered designs and trade marks.
(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 **to** 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.	
(24a) The consolidation of the rules should in particular maintain the principle that the rules under Section 3 of Chapter VIIc should not create an obligation to allow the re-use of certain categories of protected data held by public sector bodies. In particular, Member States should therefore be able to decide whether such protected data is made accessible for re-use, also in terms of the purposes and scope of such access. This Regulation should complement and be without prejudice to	

Commission proposal	Drafting suggestions and Comments
more specific obligations on public sector bodies to allow re-use of protected 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 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. **The re-use regime provided for under Section 3 of Chapter VIIc should apply to protected data the supply of which forms part of the public tasks of the public sector bodies concerned under law or other binding rules in the Member States. In the absence of such rules, the public tasks should be defined in accordance with common administrative practice in the Member States, provided that the scope of the public tasks is transparent and subject to review. The public tasks could be defined generally or on a case-by-case basis for individual public sector bodies. The protected data held by public undertakings should not be covered by this Regulation. Protected data held by cultural establishments, such as libraries, archives and museums as well as orchestras, operas, ballets and theatres, and by educational establishments should not be covered by the rules under Section 3 of Chapter VIIc, since the works and other documents they hold are predominantly covered by third party intellectual property rights. Research-performing organisations and research-funding organisations could also be organised as public sector bodies or bodies governed by public law. The rules relating to protected data should apply to such hybrid organisations only in their capacity as research-performing organisations. If a research-performing organisation holds protected data as a part of a specific public-private association with private sector organisations or other public sector bodies, bodies governed by public law or hybrid research-performing**	

PUBLIC

Commission proposal	Drafting suggestions and Comments
organisations, i.e. organised as either public sector bodies or public undertakings, with the main purpose of pursuing research, those protected data should also not be covered by the rules governing the re-use of protected data. Where relevant, Member States should be able to apply the rules on protected data under Section 3 Chapter VIIc to public undertakings or private undertakings that exercise public sector duties or provide services of general interest. The exchange of protected data, purely in pursuit of their public tasks, among public sector bodies in the Union or between public sector bodies in the Union and public sector bodies in third countries or international organisations, as well as the exchange of protected data between researchers for non-commercial scientific research purposes, should not be subject to the provisions concerning the re-use of certain categories of protected data held by public sector bodies.	
(24b) Member States should establish a single information point as an interface for re-users seeking to re-use specific categories of data held by public sector bodies. The single information point should have a cross-sector remit, complement sectoral arrangements where necessary, and may rely on automated means to transmit enquiries or requests for re-use, subject to appropriate human oversight. Existing arrangements, such as open data portals, may be used for that purpose. It should maintain an asset list providing an overview of available data resources, including, where relevant, data resources accessible through sectoral, regional or local information points, together with relevant descriptive information. Member States should also designate, establish or facilitate the establishment of one or more competent bodies to support public sector bodies in enabling the re-use of protected data. Such bodies may, where provided for under Union or national sectoral law, grant access to data. They should assist public sector bodies by providing expertise on state-of-the-art techniques for structuring, storing and making data accessible, including through application programming interfaces, and for ensuring interoperability, transferability and searchability. They	SK (Comments): Slovakia supports a single information point and competent support bodies, provided that existing national open-data portals, catalogues and sectoral arrangements may be reused. The single information point should function as a federated interface rather than requiring a new central repository. Adequate Union and national funding, common standards and a realistic transition period are essential.

PUBLIC

Commission proposal	Drafting suggestions and Comments
should also support the use of best practices, applicable regulatory and technical standards, and secure processing environments that enable data analysis while preserving privacy, confidentiality and other protected interests. Competent bodies should act in accordance with the instructions of the public sector body concerned. They may also support data subjects and data holders in managing consent or permissions for re-use, including for scientific research conducted in accordance with recognised ethical standards. Without prejudice to the powers of data protection authorities, any processing of personal data should remain under the responsibility of the public sector body responsible for the relevant register, which remains the controller within the meaning of Regulation (EU) 2016/679. Member States should be able to designate one or more competent bodies, including internal services of public sector bodies. A competent body may assist other public sector bodies in enabling re-use of data or may itself enable such re-use. Assistance may include providing guidance on compliance with this Regulation, including on secure processing environments and technical measures to ensure privacy and confidentiality. Where competent bodies grant or refuse access for the re-use Articles 32k, 32w, 32x, 32y and 32ab should apply to those competent bodies.	
(25) Start-ups, small enterprises and enterprises that qualify as medium-sized enterprises under **point**~~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	CZ (Drafting suggestions): (25) Start-ups, small enterprises and enterprises that qualify as medium-sized enterprises under **point**~~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

Commission proposal	Drafting suggestions and Comments
should be able to introduce special conditions in licences pertaining to the re-use of data and documents by very large enterprises. **Member States may further specify the criteria for what constitutes a very large enterprise for the purpose of Regulation (EU) 2023/2854.** 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 **(EU)**~~€~~ 2022/1925, other such criteria, where appropriate. Such special conditions may, inter alia, pertain to the charges and fees or the purposes of re-use. 13 Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36, ELI: http://data.europa.eu/eli/reco/2003/361/oj). 14 Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (OJ L 265, 12.10.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/1925/oj).	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. ~~**Member States may further specify the criteria for what constitutes a very large enterprise for the purpose of Regulation (EU) 2023/2854.**~~ 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 **(EU)**~~€~~ 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. CZ (Comments): CZ is not convinced that 'very large enterprise' should be defined individually by each Member State, and would appreciate further information justifying this change. So far, no explanation was provided.
(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 **public sector** 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	FR (Comments): Ces modalités d'accès ne doivent être ni discriminantes ni génératrice de charge administrative pour les entreprises. En effet, le considérant 26 de l'omnibus permettraient aux autorités publiques: • d'imposer des conditions particulières aux "très grandes entreprises"; • et de moduler les redevances ou conditions de réutilisation selon la taille ou la puissance économique des acteurs. Or, cette approche est problématique à plusieurs titres :

PUBLIC

Commission proposal	Drafting suggestions and Comments
to acquire data. This measure serves to safeguard opportunities for smaller businesses and new market entrants to innovate and compete in the digital economy.	• elle remet en cause le principe de neutralité de la réutilisation des informations publiques; • elle fragilise la logique d'un accès non discriminatoire aux données publiques; • elle crée un risque important de fragmentation entre États membres ; • elle va introduire une complexité technique de distribution des données importantes ; • et elle s'écarte de l'esprit du cadre open data européen et français, historiquement fondé sur l'ouverture la plus large possible, indépendamment du profil du réutilisateur. Au-delà des intentions poursuivies vis-à-vis des *gatekeepers*, ces dispositions introduiraient une logique de différenciation économique dans l'accès à la donnée publique qui pourrait affaiblir la prévisibilité et l'attractivité du cadre européen de sa réutilisation.
(26a) While Member State are required to designate one or more competent authorities to be responsible for the application and enforcement of Regulation (EU) 2023/2854 (competent authorities), uncertainty persists about the role of supervisory authorities responsible for monitoring and enforcement of Regulation (EU) 2016/679 and Regulation (EU) 2018/1725 under Regulation (EU) 2023/2854. Regulation (EU) 2023/2854 recalls that Regulation (EU) 2016/679 applies to the processing of personal data by private and public authorities of the Member States and Regulation (EU) 2018/1725 applies to the processing of personal data by all Union institutions and bodies when these organisations are data holders, data users or third parties under this regulation. It further stipulates that the powers and competences of supervisory authorities under Regulation (EU) 2016/679 and (EU) 2017/1725 remain unaffected by Regulation (EU) 2023/2854. In addition, the current rules of Regulation (EU) 2023/2854 state that these authorities are responsible for monitoring the application of Regulation	

PUBLIC

Commission proposal	Drafting suggestions and Comments
(EU) 2023/2854 insofar as the protection of personal data is concerned and impose fines for the infringement of this regulation. To clarify the role and responsibilities of the supervisory authorities responsible for monitoring and enforcing Regulation (EU) 2016/679 and Regulation (EU) 2018/1725 when personal data are processed pursuant to this regulation and to increase legal certainty, it is necessary to amend Regulation (EU) 2023/2854 by deleting Articles 37(3) and 40(4) and (5) of that Regulation.	
(26b) The European Data Innovation Board's character as a consultative body as regards the implementation and the enforcement of the Data Act should be maintained. However, its structure should be simplified and should allow for more strategic discussions. Notwithstanding these changes, the Board should continue to serve as a forum to develop consistent practice of competent authorities in the enforcement of Chapters II, III, V and VII, VIIa and VIIc. To this end, technical exchanges relating to best practices and dialogue between national enforcement bodies, including information sharing shall continue to be possible in various subgroups. These subgroups should also be able to discuss matters relating to the newly added Chapters VIIa and VIIc. The European Data Innovation Board should also be consulted on guidelines the Commission may issue to support the sectorial implementation of the Data Act.	
(26c) The special provision of the Data Act on the right to lodge a complaint and the right to an effective judicial remedy should not apply to Chapters VIIb and VIIc. It is clarified that this is without prejudice to any rights or obligations stemming from the Charter of Fundamental Rights.	
(27) This Regulation proposes a series of targeted amendments to Regulation (EU) 2016/679 for clarification and simplification, whilst preserving the same level of data protection. ~~**Article 4 of Regulation (EU) 2016/679 provides that personal data is any information relating to an identified or identifiable natural person. In order to determine whether**~~	DK (Comments): We support a higher degree of harmonisation and simplification on the issue of the definition of personal data and pseudonymisation.

Commission proposal	Drafting suggestions and Comments
~~a natural person is identifiable, account should be taken of all the means reasonably likely to be used to identify the natural person directly or indirectly. Taking into account the case-law of the Court of Justice of the European Union concerning the definition of personal data, it is necessary to provide further clarity on when a natural person should be considered to be identifiable. The existence of additional information enabling the data subject to be identified does not, in itself, mean that pseudonymised data must be regarded as constituting, in all cases and for every person or entity, personal data for the purposes of the application of Regulation (EU) 2016/679. In particular, it should be clarified that information is not to be considered personal data for a given entity where that entity does not have means reasonably likely to be used to identify the natural person to whom the information relates. A potential subsequent transmission of that information to third parties who have means reasonably allowing them to identify the natural person to whom the information relates, such as cross-checking with other data at their disposal, renders that information personal data only for those third parties who have such means at their disposal. An entity for which the information is not personal data, in principle, does not fall within the scope of application of Regulation (EU) 2016/679. In this respect the Court of Justice of the European Union has held that a means of identifying the data subject is not reasonably likely to be used where the risk of identification appears in reality to be insignificant, in that the identification of that data subject is prohibited by law or impossible in practice, for example because it would involve a disproportionate effort in terms of time, cost and labour. An example of a prohibition against reidentification can be found in the obligations of health data users in Article 61(3) of Regulation (EU) 2025/327 of the European Parliament and of the Council[15]. The Commission, together with the European Data Protection Board, should support controllers in the application of this updated definition by stipulating technical criteria in an implementing act.~~	There is room to go further than the proposed Article 29a without compromising data protection. We can support the proposal previously put forward by GER and SWE on the matter. However, we are of course open to discus the specific wording. IT (Drafting suggestions): **Replace recital (27) with:** (27) This Regulation proposes targeted amendments to Regulation (EU) 2016/679 intended to simplify compliance while preserving a high level of protection of personal data. In determining whether information relates to an identifiable natural person, identifiability should be assessed in relation to the person or entity processing or receiving that information. The existence of additional information capable of identifying a natural person should not in itself render information personal data for every person or entity. In particular, where personal data have undergone pseudonymisation and are disclosed to a recipient which neither possesses nor has reasonable legal, technical or practical means of obtaining or using the information necessary to identify the data subject, those data should be regarded as anonymous information in relation to that recipient for as long as those circumstances persist. A means of identification should be regarded as reasonably likely to be used only where it is realistically accessible to that recipient and its use is reasonably practicable, taking account of legal restrictions, contractual restrictions, technical and organisational measures, the cost and time required for identification and the technology actually available. A merely theoretical possibility of identification, the existence of identifying information held by another person, or the possibility that future technological developments might permit identification should not be sufficient. Where the recipient subsequently obtains means reasonably likely to permit identification, the information should constitute personal data for that recipient from that moment. IT (Comments): The present compromise correctly moves towards a recipient-relative concept of identifiability, but the rule should be made categorical enough to prevent remote or purely theoretical re-identification possibilities from keeping information indefinitely within the GDPR.

Commission proposal	Drafting suggestions and Comments
15 ~~Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 (OJ L, 2025/327, 5.3.2025, ELI: http://data.europa.eu/eli/reg/2025/327/oj~~)	AT (Comments): • AT **continues to support** that the current definition of 'personal data' remains unchanged SI (Comments): We support retaining the deletion in this recital as proposed and related provisions in the substantive part. The definition of "personal data" should remain unchanged. FI (Comments): FI supports this recital text.
(27a) In order to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used to identify the natural person directly or indirectly. The identifiability of a natural person should be assessed by the controller, considering the actual technical and organisational measures, and applicable prohibitions by law . In light of the interpretation provided in the case-law of the Court of Justice of the European Union, it is important to provide further clarity on when a natural person should be considered to be identifiable following the application of pseudonymisation to personal data and the transmission to a recipient. The European Data Protection Board should ensure consistency and support controllers and processors by adopting an opinion on pseudonymisation and anonymisation, assessing and specifying the state of the art of available techniques, as well as the technical and organisational measures and criteria to apply pseudonymisation and anonymisation to personal data effectively and by clarifying circumstances whether and when the application of pseudonymisation to personal data may effectively prevent persons other	CZ (Comments): CZ believes that standard comitology should be used. (redline pertaining to Article 29a) Consequently, references to EDPB opinions should be deleted. IT (Drafting suggestions): **Replace recital (27a) with:** (27a) The determination of identifiability should follow directly from the objective test laid down in this Regulation and should not depend upon prior authorisation, approval, guidance or an opinion of a supervisory authority or of the Board. The Board and the Commission may identify voluntary technical safe harbours and examples capable of supporting controllers, processors and recipients, but such guidance should not restrict the statutory test or prevent a controller, processor or recipient from demonstrating by other appropriate evidence that identification is not reasonably possible. IT

Commission proposal	Drafting suggestions and Comments
than the controller from identifying the data subject in such a way that, for them, the data subject is not or is no longer identifiable. The opinion should also address the processing to be undertaken and other measures to be applied in order to effectively render personal data anonymous. It is important that the Board carries out a public consultation with relevant stakeholders prior to issuing its opinion. While controllers remain fully responsible to determine and demonstrate whether pseudonymised data do not lead to re-identification of data subjects by persons other than the controller, the opinion should support and provide guidance to controllers regarding the effective application of pseudonymisation to personal data.	(Comments): The legal test should be contained in the Regulation itself. EDPB or Commission guidance may assist compliance, but should not become a de facto authorisation mechanism determining whether the GDPR applies. LU (Drafting suggestions): **(27a) In order to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used to identify the natural person directly or indirectly. The identifiability of a natural person should be assessed ~~by the controller~~, considering the actual technical and organisational measures, and applicable prohibitions by law . In light of the interpretation provided in the case-law of the Court of Justice of the European Union, it is important to provide further clarity on when a natural person should be considered to be identifiable following the application of pseudonymisation to personal data and the transmission to a recipient. The European Data Protection Board should ensure consistency ~~and support controllers and processors~~ by adopting an opinion on pseudonymisation and anonymisation, assessing and specifying the state of the art of available techniques, as well as the technical and organisational measures and criteria to apply pseudonymisation and anonymisation to personal data effectively and by clarifying circumstances whether and when the application of pseudonymisation to personal data may effectively prevent persons other than the controller from identifying the data subject in such a way that, for them, the data subject is not or is no longer identifiable. The opinion should also address the processing to be undertaken and other measures to be applied in order to effectively render personal data anonymous. It is important that the Board carries out a public consultation with relevant stakeholders prior to issuing its opinion. While controllers remain fully responsible to determine and demonstrate whether pseudonymised data do not lead to re-identification of data subjects by**

PUBLIC

Commission proposal	Drafting suggestions and Comments
	persons other than the controller, the opinion should support and provide guidance ~~to controllers~~ regarding the effective application of pseudonymisation to personal data. LU (Comments): One gets the impression that such an assessment only needs to be done by the controller. We consider that the assessment needs to be carried out by the concerned party independent of its qualification regarding the GDPR (controller, processor, recipient, third party…etc.). Luxembourg therefor suggests deleting a part of the sentence to keep the recital neutral. NL (Drafting suggestions): 27a) In order to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used to identify the natural person directly or indirectly. The identifiability of a natural person should be assessed by the controller, considering the actual technical and organisational measures, and applicable prohibitions by law. In light of the interpretation provided in the case-law of the Court of Justice of the European Union, it is important to provide further clarity on when a natural person should be considered to be identifiable following the application of pseudonymisation to personal data and the transmission to a recipient, **as well as when such recipient further discloses, transmits or otherwise makes such data available to a third party. Data which are in themselves impersonal may become 'personal' in nature where they are put at the disposal of other persons who have means reasonably likely to enable the data subject to be identified. This applies to both the party that transmits this data and the third party that subsequently processes this data.**

Commission proposal	Drafting suggestions and Comments
	Whether means are reasonably likely to be used will depend on the relevant entity's perspective, which depends on the specific nature and context of the processing, such as who has access to or control over the data, whether the data is being transmitted from one party to another, the relationship between those parties, and whether a receiver of the data might process it on behalf of another party. The European Data Protection Board should ensure consistency and support controllers and processors by adopting an opinion on pseudonymisation and anonymisation, assessing and specifying the state of the art of available techniques, as well as the technical and organisational measures and criteria to apply pseudonymisation and anonymisation to personal data effectively and by clarifying circumstances whether and when the application of pseudonymisation to personal data may effectively prevent persons other than the controller from identifying the data subject in such a way that, for them, the data subject is not or is no longer identifiable. The opinion should also address the processing to be undertaken and other measures to be applied in order to effectively render personal data anonymous. It is important that the Board carries out a public consultation with relevant stakeholders prior to issuing its opinion. While controllers remain fully responsible to determine and demonstrate whether pseudonymised data do not lead to re-identification of data subjects by persons other than the controller, the opinion should support and provide guidance to controllers regarding the effective application of pseudonymisation to personal data. NL (Comments): The first proposed additions in recital 27a reflect the added §2a in Article 29a and are based upon §84 of the SRB-case: "(…) *data which are in themselves impersonal may become 'personal' in nature where the controller puts them at the disposal of other persons who have means reasonably likely to enable the data subject to be identified. It is apparent, in particular, from the latter*

Commission proposal	Drafting suggestions and Comments
	judgment that – where those data are put at their disposal – those data are personal data both for those persons and, indirectly, for the controller." The last added sentence is based on the EDPB Guidelines on Anonymisation (02/2026), §11-13 AT (Comments): • AT **continues to support** assigning the competence to issue guidelines regarding pseudonymisation and identifiability of natural persons to the EDPB. • AT **continues to support** the proposed Recital 27a. SK (Comments): **SK:** We propose to delete this recital. An explanation is provided in the comments to Article 29a. FI (Drafting suggestions): **(27a) In order to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used to identify the natural person directly or indirectly. The identifiability of a natural person should be assessed by the controller, considering the actual technical and organisational measures, and applicable prohibitions by law. In light of the interpretation provided in the case-law of the Court of Justice of the European Union, it is important to provide further clarity on when a natural person should be considered to be identifiable following the application of pseudonymisation to personal data and the transmission to a recipient, including where that recipient discloses, transmits or otherwise makes available such data to a third party. Data which are as such impersonal may become personal in**

Commission proposal	Drafting suggestions and Comments
	nature where they are made available to other persons who possess or can obtain means reasonably likely to enable the data subject to be identified. In such a case, both the transmission of the data to a third party and the subsequent processing of the data by that third party should be considered as processing of personal data. The European Data Protection Board should ensure consistency and support controllers and processors by adopting an opinion on pseudonymisation and anonymisation, assessing and specifying the state of the art of available techniques, as well as the technical and organisational measures and criteria to apply pseudonymisation and anonymisation to personal data effectively and by clarifying circumstances whether and when the application of pseudonymisation to personal data may effectively prevent persons other than the controller from identifying the data subject in such a way that, for them, the data subject is not or is no longer identifiable. The opinion should also address the processing to be undertaken and other measures to be applied in order to effectively render personal data anonymous. It is important that the Board carries out a public consultation with relevant stakeholders prior to issuing its opinion. While controllers remain fully responsible to determine and demonstrate whether pseudonymised data do not lead to reidentification of data subjects by persons other than the controller, the opinion should support and provide guidance to controllers regarding the effective application of pseudonymisation to personal data. FI (Comments): FI considers that the CY Presidency's latest compromise proposal on Article 30a and Recital 27a found a balance that clarifies pseudonymisation in accordance with the relevant case law of the CJEU and maintains the current level of protection of personal data.

Commission proposal	Drafting suggestions and Comments
	It is important that the proposed para. 2a in Article 30a (ST 10729/26) is included in new Article 29a as it would codify appropriately the rulings of the CJEU in the case EDPS v SRB (see C-413/23 P, para 84). Similarly, the changes proposed in recital 27a in the previous compromise version (ST 10729) should be included in the text. See proposal underlined and bolded. This would also be in line with the new anonymisation guidelines of the EDPB (see para 21 in guidelines 2/2026 on Anonymisation). *"(2a) Where a person other than the controller referred to in paragraph 2 discloses, transmits or otherwise makes such data available to a third party and it cannot be ruled out that this third party possesses or can obtain means reasonably likely to enable the data subject to be identified, both the transmission of the data to this third party and the subsequent processing of the data by this third party is to be considered as processing of data relating to an identifiable natural person. "*
(27b) Pseudonymisation is one of the possible security measures within the meaning of Article 32 of Regulation (EU) 2016/679 and does not necessarily have to be applied in all cases. Whether pseudonymisation is appropriate, should be assessed on a case-by-case basis and depends on the context, the nature of the personal data and the existence of other appropriate technical and organisational measures. The effective application of pseudonymisation may also be clarified for controllers and processors through the approval of specific codes of conduct in accordance with Article 40 of Regulation (EU) 2016/679, taking account of the specific characteristics of the processing carried out in certain sectors and the specific needs of micro, small and medium enterprises.	EE (Drafting suggestions): **(27b) Pseudonymisation is one of the possible security measures within the meaning of Article 32 of Regulation (EU) 2016/679 and does not necessarily have to be applied in all cases. Apart from pseudonymisation, other Privacy Enhancing Techonogies could be applied as appropriate. Whether pseudonymisation is appropriate, should be assessed on a case-by-case basis and depends on the context, the nature of the personal data and the existence of other appropriate technical and organisational measures. The effective application of pseudonymisation may also be clarified for controllers and processors through the approval of specific codes of conduct in accordance with Article 40 of Regulation (EU)**

Commission proposal	Drafting suggestions and Comments
	2016/679, taking account of the specific characteristics of the processing carried out in certain sectors and the specific needs of micro, small and medium enterprises. EE (Comments): We should also not focus only on pseudonymisation, but consider other relevant privacy-enhancing technologies (PETs) as well. IT (Drafting suggestions): **Replace recital (27b) with:** (27b) Pseudonymisation is one possible technical and organisational measure and does not have to be applied in every case. Its legal effect should depend upon its actual effectiveness in preventing attribution of information to a natural person by the relevant recipient. Controllers and processors should remain free to use other equally effective or more effective technical and organisational measures capable of achieving the substantive confidentiality, integrity and data-protection outcomes required by this Regulation. IT (Comments): This removes unnecessary case-by-case risk formalism and makes the criterion the actual effectiveness of the measure. It also preserves technological neutrality and operational discretion. AT (Comments): • AT **can support** the proposed Recital 27b. FI (Comments): See the comment above.
(28) In order to assess whether **scientific** research **activities meet**~~meets~~ the conditions of scientific research for the purpose of ~~this~~ Regulation **(EU)**	CZ

Commission proposal	Drafting suggestions and Comments
2016/679, account can be taken of elements such as **the purpose of the research, the** methodological ~~and systematic~~ approach **and ethical standards** applied **in the specific area** while conducting the research**, and adherence to the principles of transparency, reliability, accountability, oversight, verifiability, and rules for** ~~in the specific area.~~**research**~~Research~~**integrity.** **Transparency could, among other things, involve making research results publicly available with due regard to legitimate limitations to access such as protection of intellectual property and trade secrets.** **Scientific research activities**~~and technology development~~ should be conducted **autonomously and independently, free from undue pressure and contribute to the growth of society's general knowledge and wellbeing. This does not exclude that the outcome of scientific research activities may also aim to further commercial or private interests.** **It is important that processing for scientific research activities prevent individuals from being subjected to harm or other adverse effects due to their participation in scientific research and respect, amongst others, human autonomy and, to the extent necessary, the notion of consent to participate in research should be used as a safeguard and is to be considered distinctively from consent under Regulation (EU) 2016/679. Scientific research can, amongst others, be part of and support innovation, such as technology or medical development. The fact that scientific research activities are to be conducted autonomously and independently does not exclude that such activities can be mandated and conducted by public authorities or private entities, including small and medium sized undertakings,** in academic, industry and other settings **. The outcome of scientific research may be applied for public interest, private or commercial purposes.** **The qualification of processing as being carried out for scientific research purposes**~~, including small and medium-sized undertakings, (Article 179(2) TFEU) and~~ should be **assessed and substantiated by the controller on a case-by-case basis, considering the objective**	(Comments): CZ considers it essential that scientific research is defined by the objective characteristics of the research activity and not by the institutional status of the entity conducting it. Research carried out by private undertakings, including SMEs, should therefore be capable of qualifying as scientific research, in particular in the context of AI research, development and innovation. CZ proposes to delete: • „the purpose of the research“, as all scientific research should be supported • „reliability, accountability, oversight“ as they are not explained, and may be in contradiction with inherently uncertain nature of research and with „autonomy and independence“ that are also in the text. GDPR should not make research even more bureaucratic exercise. NL (Drafting suggestions): 28) In order to assess whether scientific research activities meet the conditions of scientific research for the purpose of Regulation (EU) 2016/679, account can be taken of elements such as the purpose of the research, the methodological approach and ethical standards applied in the specific area while conducting the research, and adherence to the principles of transparency, reliability, accountability, oversight, verifiability, and rules for research integrity. Transparency **should** ~~may~~, among other things, involve making research results publicly available with due regard to legitimate limitations to access such as protection of intellectual property and trade secrets. Scientific research activities should be conducted autonomously and independently, free from undue pressure and contribute to the growth of society's general knowledge and wellbeing. This does not exclude that the outcome of scientific research activities may also aim to

Commission proposal	Drafting suggestions and Comments
characteristics of the research activity, ~~**always of a of high quality**~~ and should **not undermine the obligation to apply appropriate safeguards as provided for in Article 89 of Regulation (EU** ~~**adhere to the principles of principles of reliability, honesty, respect and accountability (verifiability)**~~ **2016/679**.	further commercial or private interests. It is important that processing for scientific research activities prevent individuals from being subjected to harm or other adverse effects due to their participation in scientific research and respect, amongst others, human autonomy and, to the extent necessary, the notion of consent to participate in research should be used as a safeguard and is to be considered distinctively from consent under Regulation (EU) 2016/679. ~~**Scientific research can, amongst others, be part of and support innovation, such as technology or medical development.**~~ Scientific research activities may be conducted in academic, industry and other settings, by public authorities or private entities, including small and medium sized undertakings. The outcome of scientific research may be applied for public interest, private or commercial purposes. The qualification of processing as being carried out for scientific research purposes should be assessed on a case-by-case basis, considering the objective characteristics of the research activity, and should not rely solely on the declaration of the controller, nor undermine the obligation to apply appropriate safeguards as provided for in Article 89 of Regulation (EU) 2016/679. **Scientific research applies the scientific method of observing phenomena, formulating and testing a hypothesis for those phenomena, and concluding as to the validity of the hypothesis. The notion of scientific research may not be stretched beyond its common meaning.** NL (Comments): This amendment tries to prevent that the clarification of the definition of scientific data would create a very liberal application or loophole in practice, which could be misused to undermine fundamental rights. NL is still concerned that the proposed definition is prone to abuse and that it extends the scope of exceptions for scientific research also in unintended ways.

Commission proposal	Drafting suggestions and Comments
	The wording of the two added sentences at the end is derived from the EDPB Opinion 1/2026, para. 9; EDPB Guidelines 03/2020, para. 10; EDPS Preliminary Opinion on data protection and scientific research (January 6, 2020), para. 3.2. Furthermore, NL proposes to adapt the second sentence of this recital to the proposed definition, which reads: "(…) producing verifiable and transparent results". Therefore, transparency *should* in principle involve that research results become publicly available. AT (Comments): • AT **continues to have concerns** about the inclusion of a GDPR-specific definition of "scientific research". • The Recital should therefore be **deleted** (in line with proposed deletion of Art. 4(38)). Parts of this Recital could be moved to Recital 32, which also relates to scientific research. FI (Comments): FI supports the proposed definition of scientific research as it includes all the necessary elements for scientific research. FI also supports the recitals 28 and 32 which are balanced and consider both the public and private interests.
(29) It should be reiterated that further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. In such cases it **should not be**~~is not~~ necessary to ascertain on the basis of Article 6(4) of ~~this~~ Regulation **(EU) 2016/679** whether the purpose of the further processing is compatible with the purpose for which the personal data are initially collected. **Such further processing should be considered compatible, and should be carried out in compliance with the principles and appropriate safeguards laid down in Regulation (EU) 2016/679, in particular Article 89.**	EE (Drafting suggestions): It should be reiterated that further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible **purposeful** ~~lawful~~ processing operations. In such cases it **should not be**~~is not~~ necessary to ascertain on the basis of Article 6(4) of ~~this~~ Regulation **(EU) 2016/679** whether the purpose of the further processing is compatible with the purpose for which the personal data are initially collected. **Such further processing**

Commission proposal	Drafting suggestions and Comments
	should be considered compatible, and should be carried out in compliance with the principles and appropriate safeguards laid down in Regulation (EU) 2016/679, in particular Article 89. EE (Comments): Estonia would like to draw attention to the points 31 and 32 of the EDPB/EDPS joint opinion. 31. The EDPB and the EDPS note that current Recital 50 GDPR and Recital 25 EUDPR contain phrases similar to those in Recital 29 Proposal, which provides that '[i]t should be reiterated that further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible *lawful* processing operations.' [emphasis added] The existing Recitals have not, however, achieved their intended effect of clarifying whether, and under what conditions no legal basis separate from the legal basis for collection of the personal data is required for further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. The EDPB and the EDPS therefore recommend to further clarify this in the enacting terms of the GDPR and the EUDPR to ensure legal clarity. 32. The EDPB and the EDPS recall that, in cases where the initial legal basis is relied on for the further compatible processing, the rights of data subjects will then depend on that initial legal basis39. The EDPB and the EDPS consider that the fact that data subjects whose data are processed for scientific research may have different rights depending on the initial legal basis relied upon for collection of the data should also be addressed. According to the EDPB and the EDPS, the question of compatibility of purposes should not be confused with the principle of lawfulness under the GDPR and EUDPR.

Commission proposal	Drafting suggestions and Comments
	We do lack the legal clarity in what is regarded as compatible further processing. The principles of lawfulness and purpose limitation are separate ones and should not be mixed in our opinion. AT (Comments): • In line with the proposed deletion of Recital 27 and Article 4(38) the text **should be amended** as proposed in the 2nd compromise text. Explanations regarding the term 'scientific research' within the meaning of the GDPR would provide greater clarity and legal certainty. FI (Comments): FI supports this recital.
~~(30) Trustworthy AI is key in providing for economic growth and supporting innovation with socially beneficial outcomes. The development and use of AI systems and the underlying models such as large language models and generative video models rely on data, including personal data, in various phases in the AI lifecycle, such as the training, testing and validation phase and may in some instances be retained in the AI system or the AI model. The processing of personal data in this context may therefore be carried out for purposes of a legitimate interest within the meaning of Article 6 of Regulation (EU) 2016/679, where appropriate. This does not affect the obligation of the controller to ensure that the development or use (deployment) of AI in a specific context or for specific purposes complies with other Union or national law, or to ensure compliance where its use is explicitly prohibited by law. It also does not affect its obligation to ensure that all other conditions of Article 6(1)(f) of Regulation (EU) 2016/679 as well as all other requirements and principles of that Regulation are met.~~	IT (Drafting suggestions): **Replace recital (30) with:** (30) Trustworthy AI is important for economic growth, scientific and technological progress and socially beneficial outcomes. The development, training, testing, validation, evaluation and improvement of AI systems and AI models may serve substantial public-interest objectives, including public health, scientific and technological progress, cybersecurity, public safety, accessibility, environmental protection, energy sustainability, education, efficient public administration, prevention of fraud, resilience of essential services and the protection of fundamental rights. Where an AI system or AI model is developed for a substantial public-interest objective recognised by Union or Member State law, processing of personal data necessary for that development should be lawful pursuant to Article 6(1)(e). This Regulation should itself constitute a Union-law basis for such processing where the conditions specifically laid down therein are satisfied. Such processing should not additionally depend upon a case-by-case legitimate-interest balancing exercise. IT (Comments): The current wording merely states that AI development may fall within legitimate interests. That leaves major uncertainty. For AI development serving a substantial public interest, the

Commission proposal	Drafting suggestions and Comments
	Regulation should itself provide an express Article 6(1)(e) legal basis, including where development is undertaken by private entities AT (Comments): • AT **continues to support** the deletion of Recital 30.
~~(31) When the controller, in the light of the risk-based approach which informs the scalability of the obligations under this Regulation, is balancing the legitimate interest pursued by the controller or a third party and the interests, rights and freedoms of the data subject, consideration should be given to whether the interest pursued by the controller is beneficial for the data subject and society at large, which may for instance be the case where the processing of personal data is necessary for detecting and removing bias, thereby protecting data subjects from discrimination, or where the processing of personal data is aiming at ensuring accurate and safe outputs for a beneficial use, such as to improve accessibility to certain services. Consideration should also, among others, be given to reasonable expectations of the data subject based on their relationship with the controller, appropriate safeguards to minimise the impact on data subjects' rights such as providing enhanced transparency to data subjects, providing an unconditional right to object to the processing of their personal data, respecting technical indications embedded in a service limiting the use of data for AI development by third parties, the use of other state of the art privacy preserving techniques for AI training and appropriate technical measures to effectively minimise risks resulting, for example, from regurgitation, data leakage and other intended or foreseeable actions.~~	IT (Drafting suggestions): **Replace recital (31) with:** (31) Compliance with this Regulation should not depend upon speculative classifications of processing according to varying levels of risk. The substantive obligations laid down by this Regulation should apply according to their terms. Controllers should remain free to select the technical and organisational measures by which those obligations are achieved, subject to their ability to demonstrate effective compliance. Considerations concerning foreseeable adverse effects may inform the controller's selection and testing of safeguards but should not determine whether the substantive obligations of this Regulation apply. IT (Comments): This is the principal recital for moving from a risk-based architecture to outcome-based compliance. Risk may remain a factual consideration in engineering and testing, but should cease to be the legal trigger that determines the existence or intensity of core compliance obligations. AT (Comments): • AT **continues to support** the deletion of Recital 31.
(32) The processing of personal data for scientific research purposes and the application of the GDPR's provisions on scientific research are conditional on the adoption of appropriate safeguards for the rights and freedoms of data subjects, pursuant to Article 89(1) GDPR. To that end, the GDPR balances the right to protection of personal data, pursuant to Article 8	IT (Drafting suggestions): **Replace recital (32) with:** (32) The processing of personal data for scientific research and for the development, testing and validation of technologies serving a substantial public interest should be facilitated

Commission proposal	Drafting suggestions and Comments
CFREU, with the freedom of science, pursuant to Article 13 CFREU. The processing of personal data for the purpose of scientific research **can follow public interest within the meaning of Article 6(1)(e) of Regulation (EU) 2016/679 or be based on Member States and Union law. The processing of personal data for the purpose of scientific research may also be necessary for the purposes of the**~~therefore pursues a~~ legitimate **interests pursued by a controller or by a third-party**~~interest~~ within the meaning of Article 6(1)(f) of Regulation (EU) 2016/679, provided that such research is not contrary to Union or Member State law. This is without prejudice to the obligation of the controller to ensure that all other conditions of Article 6(1)(f) of Regulation (EU) 2016/679 as well as all other requirements and principles of that Regulation are met.	where effective safeguards protect data subjects. Such processing may be based on Article 6(1)(e) where the conditions of Article 6(3a) are met, including where the processing is performed by a private entity for a substantial public-interest objective. Where Article 6(3a) does not apply, another lawful basis under Article 6 may be relied upon in accordance with its conditions. The legal basis should be determined by the objective purpose and applicable law and should not depend upon the organisational form of the research body or developer. IT (Comments): This aligns scientific research and public-interest technology development with the new Article 6(3a), rather than forcing socially beneficial processing into an uncertain legitimate-interest balancing exercise. AT (Comments): • AT **continues to support** the proposed changes in Recital 32. FI (Comments): FI supports this recital text on scientific research.
(33) The development of certain AI systems and AI models may involve the collection of large amounts of data, **which can include**~~including~~ personal data and special categories thereof. Special categories of personal data may **incidentally and** residually exist in the training, testing or validation data sets or be retained in the AI system or the AI model, although the special categories of personal data are not necessary for the purpose of the processing **and while the controller did not intend to process such personal data and has taken the appropriate technical and organisational measures to avoid such processing, such as the filtering out of special categories of personal data at the collection stage.** ~~.~~In order not to disproportionately hinder the development and operation of AI and taking into account the capabilities of the controller to identify and **erase**~~remove~~ special categories of personal data**, including technical capabilities**, derogating from the prohibition on processing special categories	CZ (Drafting suggestions): The development of certain AI systems and AI models may involve the collection of large amounts of data, **which can include**~~including~~ personal data and special categories thereof. Special categories of personal data may **incidentally and** residually exist in the training, testing or validation data sets or be retained in the AI system or the AI model, although the special categories of personal data are not necessary for the purpose of the processing **and while the controller did not intend to process such personal data and has taken the appropriate technical and organisational measures to avoid such processing, such as the filtering out of special categories of personal data at the collection stage.** ~~.~~In order not to disproportionately hinder the development and operation of

Commission proposal	Drafting suggestions and Comments
of personal data under Article 9(2) of Regulation (EU) 2016/679 should be **limited to incidental and residual processing of special categories of data in the context of the development and technical operation of AI systems or AI models. The derogation should not be understood as covering the processing of special categories of personal data directly acquired by or provided to the AI system or AI model in the course of the deployment**~~allowed~~. The derogation should only apply where the controller has implemented appropriate technical and organisational measures in an effective manner to avoid the processing of those data, takes the appropriate measures **throughout**~~during~~ the entire lifecycle**, that is to say during the development and operation,** of an AI system or AI model and, once it identifies such data, effectively **erase them. If erasure**~~remove them. If removal~~ would **prove technically impossible or** require **manifestly** disproportionate effort, notably where the **erasure**~~removal~~ of special categories of data memorised in the AI system or AI model would require re-engineering the AI system or AI model, **or would be technically impossible,** the controller should effectively protect such data from **being further processed or processed for other purposes, in particular** being used to infer outputs, being disclosed or otherwise made available to third parties**. In line with the accountability principle, the controller should document its assessment and have processes in place to monitor and demonstrate the effectiveness of these measures**. This derogation should not apply where the processing of special categories of personal data is necessary for the purpose of the processing **for example if special categories of personal data relating to a natural person's voice, image or other personal characteristics are used in a way that goes beyond incidental or residual existence**. In this case, the controller should rely on the derogations pursuant to Article 9(2)(a) – (j) of Regulation (EU) 2016/679 **or on other Union law, such as Regulation (EU) 2024/1689 regarding the processing of special categories of personal data for the purpose of ensuring bias detection and correction**. **The notion of AI system and AI model should be understood in the same manner as in Regulation (EU) 2024/1689.**	AI and taking into account the capabilities of the controller to identify and **erase**~~remove~~ special categories of personal data**, including technical capabilities**, derogating from the prohibition on processing special categories of personal data under Article 9(2) of Regulation (EU) 2016/679 should be **limited to incidental and residual processing of special categories of data in the context of the development and technical operation of AI systems or AI models. The derogation should not be understood as covering the processing of special categories of personal data directly acquired by or provided to the AI system or AI model in the course of the deployment**~~allowed~~. The derogation should only apply where the controller has implemented appropriate technical and organisational measures in an effective manner to avoid the processing of those data, takes the appropriate measures **throughout**~~during~~ the entire lifecycle**, that is to say during the development and operation,** of an AI system or AI model and, once it identifies such data, effectively **erase them. If erasure**~~remove them. If removal~~ would **prove technically impossible or** require ~~**manifestly**~~ disproportionate effort, notably where the **erasure**~~removal~~ of special categories of data memorised in the AI system or AI model would require re-engineering the AI system or AI model, ~~**or would be technically impossible,**~~ the controller should effectively protect such data from **being** ~~**further processed or**~~ **processed for other purposes,** ~~**in particular**~~ being used to infer outputs, being disclosed or otherwise made available to third parties**. In line with the accountability principle, the controller should document its assessment and have processes in place to monitor and demonstrate the effectiveness of these measures**. This derogation should not apply where the processing of special categories of personal data is necessary for the purpose of the processing **for example if special categories of personal data relating to a natural person's voice, image or other personal characteristics are used in a way that goes beyond incidental or residual existence**. In this case, the controller should rely on the derogations pursuant to Article 9(2)(a) – (j) of Regulation (EU) 2016/679 **or on other Union law, such as Regulation (EU) 2024/1689 regarding the processing of special**

Commission proposal	Drafting suggestions and Comments
	categories of personal data for the purpose of ensuring bias detection and correction. The notion of AI system and AI model should be understood in the same manner as in Regulation (EU) 2024/1689. CZ (Comments): CZ believes that recital is no longer logically consistent – the fifth sentence requires deletion, the sixth sentence, solving situations where deletion is disproportionately difficult, still prohibits processing, including storage. Efforts to cumulate explanations made "technical impossibility" an example of "manifestly disproportionate effort". "Impossibility" is referred to twice. Some redrafting might be in order. CZ proposes at least some critical changes to keep the proposal within terminology of GDPR: - to delete "manifestly" - to delete "or would be technically impossible" - to keep the phrase "being processed for other purposes" To keep text in line with the normative text, "in particular" should be deleted as well. DK (Comments): With regard to Article 9(2)(k) and this related recital it is our understanding that it was intended to address the challenge with large datasets that potentially contain small amounts of special category personal data, where it would be imposible (or involve a disproportionate effort) to remove such data. This in order not to disproportionately hinder the development and operation of AI. It is still unclear to us what is meant by "incidental". We therefore worry that this requirement make the provision very limited in practice and fail to address the challenge. Maybe "unintended" is a better word than incidental?

PUBLIC

Commission proposal	Drafting suggestions and Comments
	EL (Drafting suggestions): Proposals to strengthen legal certainty and facilitate controller compliance: 1. Recital 33a should set out concrete, non-exhaustive examples of processing that may qualify for the legitimate-interest basis in the AI context, and/or the text should provide for dedicated EDPB guidelines. Given the breadth of the concept, worked examples are the most effective way to deliver the legal certainty that the simplification objective requires. 2. The clause "or where other Union or national laws explicitly require consent" should be removed. Whether another Union or national instrument requires consent as a legal basis is irrelevant to the balancing exercise under Article 6(1)(f); retaining it conflates two distinct questions and undermines legal clarity. 3. The sentence "Other provisions of this Regulation remain unaffected by the fact that a controller relies on this legal basis" should be removed. A recital cannot create or modify a legal basis: the basis remains Article 6(1)(f) GDPR. The sentence is superfluous and risks being read as attributing independent legal effect to the recital. 4. In line with Article 5(2) GDPR, where a controller relies on Article 6(1)(f) for such processing it should retain written documentation demonstrating that its legitimate interest is not overridden by the interests, rights and freedoms of others. This both facilitates compliance, by setting a clear and predictable expectation, and safeguards data subjects. 5. The processing should remain subject to appropriate technical and organisational measures and safeguards, in particular protection of children, consideration of the interests of artists and creative professionals, and protection against disclosure of data residually retained in the AI system or model. 6. The recital should retain the clarification that the controller remains obliged to select the appropriate lawful ground under Article 6 GDPR, including Article

Commission proposal	Drafting suggestions and Comments
	6(1)(e) for processing by public authorities. Thisdistinction is important for public-sector AI deployment. EL (Comments): We welcome recital 33a as a clarification that processing for the development and deployment of an AIsystem or AI model may, in certain cases, be carried out on the basis of the controller's legitimate interestunder Article 6(1)(f) GDPR. We consider, however, that a recital alone provides only limited legal certainty:legitimate interest is a broad and elastic concept that turns on a case-by-case balancing test, which leavesorganisations exposed to divergent assessments across Member States. LU (Comments): We reiterate our previous comment: We would be cautious to include the notion "the controller had not intended to process" since the intention of the controller needs to be assessed. We would suggest sticking to notions already used by the GDPR. In this case, we would suggest to only refer to the necessity of data processing in respect to the purpose. NL (Drafting suggestions): 33) The development of certain AI systems and AI models may involve the collection of large amounts of data, which can include personal data and special categories thereof, **subject to all requirements of Regulation (EU) 2016/679**. Special categories of personal data may incidentally and residually exist in the training, testing or validation data sets or be retained in the AI system or the AI model, although the special categories of personal data are not necessary for the purpose of the processing and while the controller did

Commission proposal	Drafting suggestions and Comments
	not intend to process such personal data and has taken the appropriate technical and organisational measures to avoid such processing~~, such as the filtering out of special categories of personal data at the collection stage.~~ . **Those measures should include filtering out, both at the collection stage – by avoiding collecting special categories of data in the first place – and immediately thereafter – by deleting or anonymising special categories of data prior to training AI models.** ~~In order not to disproportionately hinder the development and operation of AI and t~~ **T**aking into account the capabilities of the controller to **fully** identify and erase special categories of personal data, including technical capabilities, derogating from the prohibition on processing special categories of personal data under Article 9(2) of Regulation (EU) 2016/679 should be limited to incidental and residual processing of special categories of data in the context of the development and technical operation of AI systems or AI models. **The derogation should remain limited to strictly incidental, unintentional and residual cases, where the processing does not rely on such special categories of personal data.** The derogation should only apply where the controller has implemented appropriate technical and organisational measures in an effective manner to avoid the processing of those data, takes the appropriate measures throughout the entire lifecycle, that is to say during the development and operation, of an AI system or AI model and, once it identifies such data, effectively erase them. If erasure would prove technically impossible ~~or require manifestly disproportionate effort, notably where the erasure of special categories of data memorised in the AI system or AI model would require re-engineering the AI system or AI model, or would be technically impossible~~, the controller should effectively protect such data from being further processed or processed for other purposes, in particular being used to infer outputs, being disclosed or otherwise made available to third parties. In line with the accountability principle, the controller should document its assessment and have processes in place to monitor and demonstrate the effectiveness of these measures. This derogation should not apply where the processing of special categories of

Commission proposal	Drafting suggestions and Comments
	personal data is necessary for the purpose of the processing for example if special categories of personal data relating to a natural person's voice, image or other personal characteristics are used in a way that goes beyond incidental or residual existence. In this case, the controller should rely on the derogations pursuant to Article 9(2)(a) – (j) of Regulation (EU) 2016/679 or on other Union law, such as Regulation (EU) 2024/1689 regarding the processing of special categories of personal data for the purpose of ensuring bias detection and correction. **Therefore, this derogation should for example not apply where special categories of personal data would be used for training objectives, evaluation, optimisation, bias testing, profiling, output generation, model improvement, or deployment.** The notion of AI system and AI model should be understood in the same manner as in Regulation (EU) 2024/1689. NL (Comments): NL has repeatedly proposed deletion of recital 33 because of the proposed deletion of the corresponding Article 9(2)(k). However, if a majority of the Member States supports this provision, NL considers it crucial that recital 33 is formulated in a more stringent manner, and that article 9(2)(k) and 9(5) should be strictly limited. As further explained in the comments below on those provisions, NL remains seriously concerned about the exception to the prohibition on processing special categories of personal data for "residual" data when training and using AI. In the current from, recital 33 reinforces these concerns by accepting that special category data may be retained in AI systems or models and by not emphasising prevention and erasure, but mitigation where removal is difficult. The term "re-engineering" is not defined, so it is uncertain what it entails.

Commission proposal	Drafting suggestions and Comments
	It is important to emphasise the need to avoid the presence of sensitive data and to avoid large-scale retention of sensitive data as a result of the proposed derogation. NL finds support in this in the guidance of the EDPB, which has noted that the safeguards "*should involve filtering data categories falling under Article 9(1) GDPR. The filtering should apply to both, data collection (for example, selecting criteria for what data is collected) and immediately after data collection (deleting data).*" (EDPB, Report of the work undertaken by the ChatGPT Taskforce, adopted on 23.05.2024, p 7, §19 and §17). AT (Comments): • AT **continues to support** the proposed changes in Recital 33. FI (Comments): FI supports the derogation for AI-processing in Article 9 GDPR as well as recital 33, including the proposed text and safeguards. It is important that the derogation applies only to incidental and residual processing of special categories of personal data.
(33a) The processing of personal data in the context of the development and deployment of an AI system or of an AI model, may be regarded as carried out for a legitimate interest of the controller concerned and be carried out in accordance with Article 6(1)(f) of Regulation 2016/679, where appropriate, except where such interests are overridden by the interests, or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child, or where other Union or national laws explicitly require consent~~. The interests of artists and creative professionals are to be taken into account~~. This does not affect the obligation of the controller to choose an appropriate lawful ground of processing set out in Article 6 of Regulation (EU) 2016/679, such as Article 6(1)(e) with regard to	CZ (Comments): When it comes to AI – CZ believes that Digital Omnibus and changes to GDPR are not ambitious enough, because they do not provide higher level of legal certainty for AI developers and thus do not contribute to much needed simplification to allow AI development and training in the EU. CZ believes that reinstalment of Art. 88c (as proposed by DE or in other form) is essential element prior to closing Council position. As far as the text is concerned, CZ welcomes deletion of the sentence on artists. DK

Commission proposal	Drafting suggestions and Comments
processing by public authorities. Regardless of the lawful ground of processing, any such processing should be subject to appropriate organisational, technical measures and safeguards for the rights and freedoms of the data subject, such as to protect against non-disclosure of residually retained data in the AI system or AI model. Other provisions of this Regulation remain unaffected by the fact that a controller relies on this legal basis.	(Drafting suggestions): (33a) The processing of personal data in the context of the development and deployment of an AI system or of an AI model, may be regarded as carried out for a legitimate interest of the controller concerned and be carried out in accordance with Article 6(1)(f) of Regulation 2016/679, where appropriate, except where such interests are overridden by the interests, or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child, or where other Union or national laws explicitly require consent. ~~**The interests of artists and creative professionals are to be taken into account.**~~ This does not affect the obligation of the controller to choose an appropriate lawful ground of processing set out in Article 6 of Regulation (EU) 2016/679, such as Article 6(1)(e) with regard to processing by public authorities. Regardless of the lawful ground of processing, any such processing should be subject to appropriate organisational, technical measures and safeguards for the rights and freedoms of the data subject, such as to protect against non-disclosure of residually retained data in the AI system or AI model. Other provisions of this Regulation remain unaffected by the fact that a controller relies on this legal basis. DK (Comments): We acknowledge that the proposed recital 33a establishes that legitimate interest is potentially an appropriate legal basis. We have no issue with its inclusion. However, article 88c should be reintroduced, as it sends a clear signal that the provision is part of the operative text. Furthermore, the wording of the provision in article 88c is more explicit that legitimate interest can be an appropriate legal basis EE

Commission proposal	Drafting suggestions and Comments
	(Comments): Estonia considers that all legal bases provided for in the GDPR should remain available for the development and deployment of AI systems and AI models and at least the operative part of GDPR should remain technology neutral. Therefore we support replacing proposed article 88c with new recital 33a. Having said that, we are also in opinion that the text should not give the impression that legitimate interest is the only, or the preferred, legal basis for such processing. The appropriate legal basis must be chosen case by case, depending on the controller, the purpose of processing and the specific circumstances. Estonia has concerns about the current wording because its legal effect is not sufficiently clear. The term "where appropriate" should also be clarified. It is not clear what makes the use of legitimate interest appropriate in this context, who should make that assessment, and which criteria should be applied. Without clearer wording, this may lead to different interpretations and legal uncertainty across Member States. We would also welcome clarification on the relationship between this recital and the existing legitimate interest test under Article 6(1)(f) GDPR. The balancing test between the controller's interests and the rights and freedoms of the data subject already follows from the GDPR. It should therefore be clear whether the recital adds anything new, or simply recalls the existing GDPR framework. Overall, Estonia supports the aim of increasing legal certainty for AI development, but the current wording should be clarified so that it is clear, predictable and consistent with the GDPR. ES (Comments): We would have preferred to keep this point in the operative part, as it would provide greater legal certainty. In the spirit of compromise, we can accept that it remains in a recital.

PUBLIC

Commission proposal	Drafting suggestions and Comments
	IT (Drafting suggestions): **Replace recital (33a) with:** (33a) Processing of personal data in the context of development, training, testing, validation, evaluation, deployment or safety improvement of an AI system or AI model may be based on the lawful grounds set out in Article 6. Where the processing is necessary for a substantial public-interest objective referred to in Article 6(3a), it should be lawful pursuant to Article 6(1)(e) and should not require an additional balancing test under Article 6(1)(f). Regardless of the lawful ground relied upon, the controller should implement effective technical and organisational measures capable of preventing unauthorised disclosure, access, extraction or use of personal data retained in the AI system or model. IT (Comments): The public-interest route should be an autonomous lawful basis, while ordinary commercial AI development may continue to rely on the other grounds in Article 6 where their conditions are met. HU (Comments): HU: We do not consider it appropriate if a measure is put in the recitals instead of articles, but the content remains the same, and there is a mandatory law (ePrivacy) referenced in the case of cookies that makes consent mandatory, so this is a technical issue. As regards the substance, we do not see any added value of adding these stipulations to the preamble. The applicability of the legal basis and the requirement to ensure appropriate safeguards already stem from the GDPR, so explicitly restating them here among the recitals would not add any substantive normative value. NL (Drafting suggestions): **(33a) [deleted]**

Commission proposal	Drafting suggestions and Comments
	If a majority of member states want to retain recital 33a, NL proposes the following amendments: (33a) The processing of personal data **to the extent strictly necessary and proportionate for the purposes of the controller** in the context of the development and deployment of an AI system or of an AI model, may be regarded as carried out for a legitimate interest of the controller concerned and be carried out in accordance with Article 6(1)(f) of Regulation 2016/679, where appropriate, except where such interests are overridden by the interests, or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child, or where other Union or national laws explicitly require consent. **The reasonable expectations of data subjects should be taken into account in this assessment, which should include whether or not the personal data were publicly available, the nature of the relationship between the data subject and the controller and whether a link exists between the two, the nature of the service, the context in which the personal data were collected, the source from which the data were collected, the potential further uses of the model, and whether data subjects are actually aware that their personal data are online at all.** The interests of artists and creative professionals are to be taken into account. This does not affect the obligation of the controller to choose an appropriate lawful ground of processing set out in Article 6 of Regulation (EU) 2016/679, such as Article 6(1)(e) with regard to processing by public authorities. Regardless of the lawful ground of processing, any such processing should be subject to appropriate organisational, technical measures and safeguards for the rights and freedoms of the data subject, such as to protect against non-disclosure of residually retained data in the AI system or AI model. **Such mitigating measures could include, among others: ensuring that certain data categories are not collected or that certain sources are excluded by default from data collection, limiting the collection to freely accessible**

Commission proposal	Drafting suggestions and Comments
	data, establishing safeguards that contribute to increased transparency, facilitating the exercise of individuals' rights, deleting or anonymising personal data as soon as possible and pseudonymise personal data. Other additional measures relating to the subsequent stages of the AI development phase, such as including measures to limit the risks of memorisation, regurgitation or attack of AI models or systems are also relevant. Other provisions of this Regulation remain unaffected by the fact that a controller relies on this legal basis. NL (Comments): NL strongly supports the deletion of the regulation of a legitimate interest basis specifically for AI, the formerly proposed Article 88c GDPR. As the EDPB rightly noted, Article 88c would not bring any added value or further legal certainty. Article 88c would give the unjustified impression that the legal basis of a legitimate interest is given by default in case of AI. Furthermore, highlighting of a particular lawful ground for processing in the operative part of the GDPR would contradict with the absence of hierarchy between the different lawful grounds for processing under Article 6 GDPR and the responsibility of controllers to determine the most appropriate ground on a case-by-case basis. Article 88c is replaced by recital 33a. To increase legal certainty, NL underlines the importance to include a necessity and proportionality test in recital 33a. This could be done by adding the phrase "**to the extent strictly necessary and proportionate for the purposes of the controller**". This aligns with the example of the similar Recital 47 from the current GDPR and fits with the usual criteria for a legitimate interest.

Commission proposal	Drafting suggestions and Comments
	Furthermore, NL considers it essential to refer to the reasonable expectations of data subjects into recital 33a and to include the assessment factors which are given by the EDPB in this context (EDPB Opinion 28/2024, §93). An alternative could be to include a sentence about the factors from the EDPB Guidelines on web scraping for generative AI (2026/03), paragraph 64: "**The reasonable expectations of data subjects should be taken into account in this assessment, which should include the nature of the source of websites, the type of publication and the publicly accessible nature of the data, the restrictions imposed by the scraped website, the nature and characteristics of the relationship between the data subject and the controller and the characteristics of the data subjects**." On 7 July last, the EDPB published guidelines on web scraping for generative AI. NL is calling for incorporating useful elements of this guidelines in the recital, to increase legal certainty. The proposed added sentences at the end of recital 33a are derived from these guidelines, page 2-3 (summary) and paragraph 66. SI (Comments): We support this approach. FI (Comments): FI supports this recital and considers that it is balanced and includes all the necessary elements. It is important that the recital includes also the legal basis for public authorities. In case Article 88c is maintained, also the amendments proposed to it in the compromise text should be maintained [*similarly as proposed in recital 33a in ST 10677/26*]. In particular,

Commission proposal	Drafting suggestions and Comments
	- The joint opinion of the EDPB and EDPS should be taken into account in Article 88c; - The legal basis for public authorities should be clarified in the text; - Article 88c should also provide additional safeguards to AI-processing, such as an unconditional right to object.
(34) **Processing of biometric**~~Biometric~~ data, as defined in Article 4(14) of Regulation (EU) 2016/679, means processing of certain characteristics of a natural person through a specific technical means and which allows or confirms the unique identification of that person. **Processing**~~The notion~~ of biometric data **could be carried out for**~~includes~~ two distinct functions, namely the identification of a natural person or the verification (also called 'authentication') of his or her claimed identity, both of which rely on different technical processes. The identification process is based on a 'one-to-many' search of the data subject's biometric data in a database, while the verification process is based on a 'one-to-one' comparison of biometric data provided by the data subject, who is thereby claiming his or her identity. Derogating from the prohibition to process biometric data under Article 9(1) of ~~the~~ Regulation **(EU) 2016/679** should ~~also~~ be allowed where the verification of the claimed identity of the data subject is necessary for a purpose pursued by the controller~~,~~ and**, where applicable, subject to appropriate safeguards laid down under Union law or Member States law in accordance with Article 9(4) of Regulation (EU) 2016/679. Where biometric data are processed for the purpose of confirming the identity of a data subject, controllers should, where possible, prioritise authentication methods that do not involve the processing of biometric data. The controller should choose from equally effective means the less intrusive one. The processing of biometric data for identity verification should therefore only be used where necessary and proportionate and subject to appropriate safeguards. For example, such safeguards could include technical and organisational measures ensuring that original biometric samples of the data subject cannot be reconstructed from the template stored on a device or a database.**	CZ (Drafting suggestions): **Processing of biometric**~~Biometric~~ data, as defined in Article 4(14) of Regulation (EU) 2016/679, means processing of certain characteristics of a natural person through a specific technical means and which allows or confirms the unique identification of that person. **Processing**~~The notion~~ of biometric data **could be carried out for**~~includes~~ two distinct functions, namely the identification of a natural person or the verification (also called 'authentication') of his or her claimed identity, both of which rely on different technical processes. The identification process is based on a 'one-to-many' search of the data subject's biometric data in a database, while the verification process is based on a 'one-to-one' comparison of biometric data provided by the data subject, who is thereby claiming his or her identity. Derogating from the prohibition to process biometric data under Article 9(1) of ~~the~~ Regulation **(EU) 2016/679** should ~~also~~ be allowed where the verification of the claimed identity of the data subject is necessary for a purpose pursued by the controller~~,~~ and**, where applicable, subject to appropriate safeguards laid down under Union law or Member States law in accordance with Article 9(4) of Regulation (EU) 2016/679.** ~~**Where biometric data are processed for the purpose of confirming the identity of a data subject, controllers should, where possible, prioritise authentication methods that do not involve the processing of biometric data.**~~ **The controller should choose from equally effective means the less intrusive one.** ~~**The processing of biometric data for identity verification should therefore only be used where necessary and proportionate and subject to appropriate safeguards.**~~ **For example, such safeguards could**

Commission proposal	Drafting suggestions and Comments
For the purposes of this Regulation, biometric identification should be understood as the processing of biometric data through comparison against a database intended to determine the identity of a natural person, whereas biometric verification refers to a one-to-one comparison used solely to confirm a claimed identity. This derogation should apply where suitable safeguards apply to **ensure that the biometric data or the means needed for the verification are under the~~enable the data subject to have~~** sole control of the **data subject. Sole control means that the data subject can effectively decide when and how his or her biometric data are used for** verification**, without the controller having the technical capacity to access such biometric data in decrypted form or** process **them outside the strictly limited comparison process necessary for verification**. For example, **this is the case** where the biometric data are securely stored solely at the **device~~side~~** of the data subject or are securely stored **by~~at the side of~~** the controller in a state-of-the-art encrypted form and the encryption key or equivalent means is **securely** held solely by the data subject, **and subject to measures ensuring the overall security of~~that~~** processing**, including during the enrolment phase of data subject's ~~is not likely to create significant risks to his or her fundamental rights and freedoms. The controller does not gain knowledge of the~~** biometric data **and~~or only for a very limited time~~** during the verification process. **Such verification may in particular be required in the context of electronic identification systems and trust services under Union law. Other examples of appropriate safeguards are ensuring that end-to-end encryption is used when data are transmitted over a communication channel and providing data subjects with the possibility to securely erase their biometric data at any time.**	**include technical and organisational measures ensuring that original biometric samples of the data subject cannot be reconstructed from the template stored on a device or a database.** **For the purposes of this Regulation, biometric identification should be understood as the processing of biometric data through comparison against a database intended to determine the identity of a natural person, whereas biometric verification refers to a one-to-one comparison used solely to confirm a claimed identity. This derogation should apply where** suitable safeguards apply to **ensure that the biometric data or the means needed for the verification are under the~~enable the data subject to have~~** sole control of the **data subject. Sole control means that the data subject can effectively decide when and how his or her biometric data are used for** verification**, without the controller having the technical capacity to access such biometric data in decrypted form or** process **them outside the strictly limited comparison process necessary for verification**. For example, **this is the case** where the biometric data are securely stored solely at the **device~~side~~** of the data subject or are securely stored **by~~at the side of~~** the controller in a state-of-the-art encrypted form and the encryption key or equivalent means is **securely** held solely by the data subject, **and subject to measures ensuring the overall security of~~that~~** processing**, including during the enrolment phase of data subject's ~~is not likely to create significant risks to his or her fundamental rights and freedoms. The controller does not gain knowledge of the~~** biometric data **and~~or only for a very limited time~~** during the verification process. **Such verification may in particular be required in the context of electronic identification systems and trust services under Union law. Other examples of appropriate safeguards are ensuring that end-to-end encryption is used when data are transmitted over a communication channel and providing data subjects with the possibility to securely erase their biometric data at any time. This derogation should apply where** suitable safeguards apply to **ensure that the biometric data or the means needed for the verification are under the~~enable the data subject to have~~** sole control of the **data**

Commission proposal	Drafting suggestions and Comments
	subject. Sole control means that the data subject can effectively decide when and how his or her biometric data are used for verification**, without the controller having the technical capacity to access such biometric data in decrypted form or** process **them outside the strictly limited comparison process necessary for verification**. For example, **this is the case** where the biometric data are securely stored solely at the **device**~~side~~ of the data subject or are securely stored **by**~~at the side of~~ the controller in a state-of-the-art encrypted form and the encryption key or equivalent means is **securely** held solely by the data subject, **and subject to measures ensuring the overall security of**~~that~~ processing**, including during the enrolment phase of data subject's** ~~is not likely to create significant risks to his or her fundamental rights and freedoms. The controller does not gain knowledge of the~~ biometric data **and**~~or only for a very limited time~~ during the verification process. **Such verification may in particular be required in the context of electronic identification systems and trust services under Union law. Other examples of appropriate safeguards are ensuring that end-to-end encryption is used when data are transmitted over a communication channel and providing data subjects with the possibility to securely erase their biometric data at any time.** CZ (Comments): CZ proposes to delete the fifth and seventh sentences that unduly restrict biometric authentication which is low-risk kind of processing of biometric data. ES (Drafting suggestions): **Processing of** biometric data, as defined in Article 4(14) of Regulation (EU) 2016/679, means processing of certain characteristics of a natural person through a specific technical means and which allows or confirms the unique identification of that person. ~~The notion~~**Processing** of biometric data

Commission proposal	Drafting suggestions and Comments
	~~includes~~**could be carried out for** two distinct functions, namely the identification of a natural person or the verification (also called 'authentication') of his or her claimed identity, both of which rely on different technical processes. The identification process is based on a 'one-to-many' search of the data subject's biometric data in a database, while the verification process is based on a 'one-to-one' comparison of biometric data provided by the data subject, who is thereby claiming his or her identity. Derogating from the prohibition to process biometric data under Article 9(1) of ~~the~~ Regulation **(EU) 2016/679** should ~~also~~ be allowed where the verification of the claimed identity of the data subject is necessary for a purpose pursued by the controller~~, and, where applicable, subject to appropriate safeguards laid down under Union law or Member States law in accordance with Article 9(4) of Regulation (EU) 2016/679~~ **(…)** ES (Comments): (We recall our comments of 10/06) In line with the proposal in the new recital 27(a) on anonymization, we suggest the following text and the amendment of Article 9(4) so that it is used exclusively for biometric identificacion. In this way, we promote the innovative use of biometric verification based on current new low-risk technologies, avoiding the current fragmentation in this area within the EU: "The European Data Protection Board should ensure consistency and support controllers and processors by adopting an opinion on the processing of biometric data for verification purposes, assessing and specifying the state of the art of available decentralized architectures, as well as the technical and organisational measures and criteria to apply one-to-one verification effectively. The opinion should clarify the circumstances whether and when the retention of biometric templates or data under the sole control of the data subject effectively prevents the controller or any third party from accessing, storing, or centralizing such data. It is important that the Board carries out a

Commission proposal	Drafting suggestions and Comments
	public consultation with relevant stakeholders prior to issuing its opinion. While controllers remain fully responsible to determine and demonstrate that the chosen biometric system ensures strict necessity and maintains data under the user's exclusive control without leading to unauthorized tracking or secondary use, the opinion should support and provide guidance to controllers regarding the effective application of appropriate safeguards to protect the fundamental rights and interests of data subjects." AT (Comments): • AT can **support** the proposed changes. FI (Comments): Concerning the derogation for biometric verification in Article 9 GDPR [Art 3(3)(a) Digiomnibus], FI would have preferred to harmonise this matter in the GDPR, complemented with additional safeguards. FI can show flexibility in this (not a redline), if the majority of MS support it, although this proposal does not support the aim to simplify.
(35) **Chapter III of Regulation (EU) 2016/679 sets out rights of the data subject and corresponding obligations of the controller. Inter alia,** Article 15 of Regulation (EU) 2016/679 provides data subjects with the right to obtain **confirmation** from the controller ~~confirmation~~ as to whether or not personal data concerning him or her are being processed and, where that is the case, access to the personal data and certain additional information. The right of access should allow the data subject to be aware of, and to verify, the lawfulness of the processing and enable him or her to exercise his or her other rights under Regulation (EU) 2016/679. ~~By contrast, it should be clarified in~~ Article 12 **(5) of that** ~~of the~~ Regulation **already provides that where the request to exercise a** ~~that the~~ right **under Regulation 2016/679 is manifestly unfounded or excessive, the controller may either charge a**	NL (Drafting suggestions): (35) Chapter III of Regulation (EU) 2016/679 sets out rights of the data subject and corresponding obligations of the controller. Inter alia, Article 15 of Regulation (EU) 2016/679 provides data subjects with the right to obtain confirmation from the controller as to whether or not personal data concerning him or her are being processed and, where that is the case, access to the personal data and certain additional information. The right of access should allow the data subject to be aware of, and to verify, the lawfulness of the processing and enable him or her to exercise his or her other rights under Regulation (EU) 2016/679. Article 12 (5) of that Regulation already provides

Commission proposal	Drafting suggestions and Comments
reasonable fee or refuse to act on the request. The controller~~of access, which is from the outset favourable to data subjects,~~ should **provide**~~not be abused in the sense that~~ the data **subject with the reason thereof. A request is also to be considered excessive where an abusive intention on the part of the data subject submitting those requests can be demonstrated by the controller**~~subjects abuse them for purposes other than the protection of their data~~. For example, such an **abusive intention**~~abuse of the right of access~~ would arise where the data subject **submits**~~intends to cause the controller to refuse an access request, in order to subsequently demand the payment of compensation, potentially under the threat of bringing a claim for damages. Other examples of abuse include situations where data subjects make~~ excessive **numbers of identical or largely similar requests**~~use of the right of access~~ with the **sole**~~only~~ intent of causing damage or harm to the controller**. Repeated requests are not automatically excessive in nature but may indicate an abusive intent on the part of the data subject. Other examples include situations where**~~ or when~~ an individual **submits**~~makes~~ a request, but at the same time offers to withdraw it in return for some form of benefit from the controller~~. Moreover, in order to keep their burden to a reasonable extent, controllers should bear a lower burden of proof regarding the excessive character of~~**, when an subject submits** a request **with the sole purpose of obtaining compensation for an alleged infringement**~~than regarding the manifestly unfounded character of a request. The reason is that the manifestly unfounded character of a request depends on facts that lie principally within the controller's sphere of responsibility, whereas the excessive character of a request concerns the possibly abusive conduct of a data subject,~~ which **is deliberately provoked by**~~lies primarily outside the controller's sphere of influence, and therefore the controller may be able to prove such abuse only to a reasonable level. In any event, while requesting access under Article 15 of Regulation (EU) 2016/679~~ the data subject**, or when the exercise of a right is made with the intention to adversely affect a judicial procedure or with deliberate**	that where the request to exercise a right under Regulation 2016/679 is manifestly unfounded or excessive, the controller may either charge a reasonable fee or refuse to act on the request. The controller the data subject with the reason thereof. A request is also to be considered excessive where an abusive intention on the part of the data subject submitting those requests can be demonstrated by the controller. For example, such an abusive intention would arise where the data subject submits excessive numbers of identical or largely similar requests with the sole intent of causing damage or harm to the controller. Repeated requests are not automatically excessive in nature but may indicate an abusive intent on the part of the data subject. Other examples include situations when an individual submits a request, but at the same time offers to withdraw it in return for some form of benefit from the controller, when an subject submits a request with the sole purpose of obtaining compensation for an alleged infringement which is deliberately provoked by the data subject, or when the exercise of a right is made with the ~~intention to adversely affect a judicial procedure or with~~ deliberate intention to adversely affect and burden public authorities. NL (Comments): NL considers the wording that the "intention to adversely affect a judicial procedure", especially without further explanation, not in accordance with CJEU case law. (cf. CJEU CRIF, C-487/21, para. 35: "*In particular, that right of access is necessary to enable the data subject to exercise, depending on the circumstances, his or her* […] *right of action where he or she suffers damage, laid down in Articles 79 and 82 of the GDPR.*"; cf. CJEU Österreichische Post, C-154/21, para. 38; CJEU Rijkeboer, C-553/07, para. 52). AT (Comments):

Commission proposal	Drafting suggestions and Comments
intention to adversely affect and burden public authorities ~~**should be as specific as possible. Overly broad and undifferentiated requests should also be regarded as excessive**~~.	• AT **welcomes** the further clarification in Recital 35. FI (Comments): FI supports this recital. It is important that public authorities are mentioned in it. However, FI reiterates its earlier proposal to add "for instance by utilising AI agents for malicious automated requests" at the end of the recital but can support the recital as such too.
(35a) Article 57 of Regulation (EU) 2016/679 provides rules for situations where requests from a data subject to the supervisory authority, including complaints under Article 77 of Regulation (EU) 2016/679, are manifestly unfounded or excessive, in particular because of their repetitive character. Repeated requests are not automatically excessive in nature but may indicate an abusive intent on the part of the data subject. Articles 12 and 57 of Regulation (EU) 2016/679 use the same wording and pursue the same objective, namely to provide for an exception to the free-of-charge principle applicable to the tasks carried out by the supervisory authorities and the exercise of rights of the data subject, respectively. In order to reduce the burden of controllers with regard to excessive requests, which may also occur in relation to requests, including complaints, to the supervisory authority concerning the controller, the notion of excessiveness in Article 57 of Regulation (EU) 2016/679 should be adapted likewise.	AT (Comments): • AT **welcomes** the further clarification in Recital 35a. FI (Comments): FI supports the proposed recital 35a and Article 57(4) GDPR [Art. 3(11) Digiomnibus] concerning data protection authorities' (DPA) possibilities to refuse manifestly unfounded and excessive requests.
(36) Article 13 of Regulation (EU) 2016/679 requires the ~~data~~ controller to provide the data subject with certain information on the processing of his or her personal data as well as certain further information necessary to ensure fair and transparent processing, as defined in paragraphs 1, 2 and 3 of that provision. According to paragraph 4 of Article 13 of Regulation (EU) 2016/679, that obligation does not apply where and insofar as the data subject already has the information. To further reduce the burden of ~~data~~	AT (Drafting suggestions): (36) Article 13 of Regulation (EU) 2016/679 requires the ~~data~~ controller to provide the data subject with certain information on the processing of his or her personal data as well as certain further information necessary to ensure fair and transparent processing, as defined in paragraphs 1, 2 and 3 of that

Commission proposal	Drafting suggestions and Comments
controllers, without undermining the possibilities of the data subject to exercise his or her rights under Chapter III of **that**~~the~~ Regulation, this derogation should be extended to situations **where the personal data have been collected in the context of a direct and clearly circumscribed relationship between a data subject and a controller exercising an activity that does not involve processing a large amount of personal data,** where the processing is not likely to result in a high risk, within the meaning of Article 35 of **that**~~the~~ Regulation, and there are reasonable grounds to **believe**~~assume~~ that the data subject already has the information referred to in points (a) and (c) of paragraph 1 **of Article 13** in the light of the context in which the personal data have been collected**. A direct and clearly circumscribed**~~, in particular regarding the~~ relationship **is established for instance**~~between data subjects and the controller. These should be the situations~~ where ~~the context of the relationship between~~ the controller and the data subject **interact directly in a specific occasion** ~~is very clear and circumscribed and the controller's activity is not data-intensive~~, such as the relationship between a craftsman and their clients**.** **The application of the derogation from the information obligation should not undermine the principle of transparency and should be limited to situations where the controller has reasonable grounds to believe that the data subject already possesses the required information. These should be the situations where the personal data are collected in the context of a direct and clearly circumscribed relationship between data subjects and a controller and does not involve the processing of a large amount of personal data**, **and** where the scope of processing is limited to the minimum data necessary to perform the service. ~~The controller's activity is not data-intensive where it collects a low amount of personal data and its processing operations are not complex, which is not the case, for example, in the field of employment.~~ In such **cases**~~circumstances, that is to say when the processing is non data-intensive, non-complex and where the controller collects a low amount of personal data~~, it should be reasonable to expect, for instance, that the data	provision. According to paragraph 4 of Article 13 of Regulation (EU) 2016/679, that obligation does not apply where and insofar as the data subject already has the information. To further reduce the burden of ~~data~~ controllers, without undermining the possibilities of the data subject to exercise his or her rights under Chapter III of that~~the~~ Regulation, this derogation should be extended to situations where the personal data have been collected in the context of a direct and clearly circumscribed relationship between a data subject and a controller exercising an activity that does not involve **large scale** processing ~~**a large amount**~~ of personal data, where the processing is not likely to result in a high risk, within the meaning of Article 35 of that~~the~~ Regulation, and there are reasonable grounds to believe~~assume~~ that the data subject already has the information referred to in points (a) and (c) of paragraph 1 of Article 13 in the light of the context in which the personal data have been collected. A direct and clearly circumscribed~~, in particular regarding the~~ relationship is established for instance~~between data subjects and the controller. These should be the situations~~ where ~~the context of the relationship between~~ the controller and the data subject interact directly in a specific occasion ~~is very clear and circumscribed and the controller's activity is not data-intensive~~, such as the relationship between a craftsman and their clients. The application of the derogation from the information obligation should not undermine the principle of transparency and should be limited to situations where the controller has reasonable grounds to believe that the data subject already possesses the required information. These should be the situations where the personal data are collected in the context of a direct and clearly circumscribed relationship between data subjects and a controller and does not involve ~~the~~**large scale** processing ~~**of a large amount**~~ of personal data, and where the scope of processing is limited to the minimum data necessary to perform the service. ~~The controller's activity is not data-intensive where it collects a low amount of personal data and its processing operations are not complex, which is not the case, for example, in the field of employment.~~ In such cases~~circumstances, that is to say when the processing is non data-~~

Commission proposal	Drafting suggestions and Comments
subject has the information on the identity and contact details of the controller**,** as well as on the purpose of ~~the~~ processing ~~**when that processing is carried out for the performance of a contract to which a data subject is a party, or when the data subject has given his or her consent to that processing, in accordance with the requirements laid down in Regulation (EU) 2016/679**~~. The same should apply**, under the aforementioned conditions,** to associations and sport clubs where the processing of personal data is confined to the management of membership, communication with members and the organisation of activities. Nevertheless, this derogation from the obligations of Article 13 is without prejudice to the independent obligations of the controller under Article 15 of that Regulation, which applies in case the data subject requests access based on the latter provision. **This derogation should only apply to processing operations which are foreseeable and non-complex, which is not the case in the field of employment or in relations with public authorities or public bodies or private entities for the performance of a task in the public interest.** Where the derogation from the obligations of Article 13 does not apply, in order to balance the need for completeness and easy understanding by the data subject, controllers may adopt a layered approach when providing the information required, notably by allowing users to navigate to further information.	~~intensive, non-complex and where the controller collects a low amount of personal data~~, it should be reasonable to expect, for instance, that the data subject has the information on the identity and contact details of the controller, as well as on the purpose of ~~the~~ processing ~~when that processing is carried out for the performance of a contract to which a data subject is a party, or when the data subject has given his or her consent to that processing, in accordance with the requirements laid down in Regulation (EU) 2016/679~~. The same should apply, under the aforementioned conditions, to associations and sport clubs where the processing of personal data is confined to the management of membership, communication with members and the organisation of activities. Nevertheless, this derogation from the obligations of Article 13 is without prejudice to the independent obligations of the controller under Article 15 of that Regulation, which applies in case the data subject requests access based on the latter provision. This derogation should only apply to processing operations which are foreseeable and non-complex, which is not the case in the field of employment or in relations with public authorities or public bodies or private entities for the performance of a task in the public interest. Where the derogation from the obligations of Article 13 does not apply, in order to balance the need for completeness and easy understanding by the data subject, controllers may adopt a layered approach when providing the information required, notably by allowing users to navigate to further information. AT (Comments): • AT can **support** the compromise proposal on Article 13(5) and Recital 36 GDPR. The proposed amendments provide important clarifications. • In order to safeguard the consistent terminology of the GDPR, we would suggest that instead of using the term “processing of a large amount of personal data” the term “**large scale processing of personal data**” should be

Commission proposal	Drafting suggestions and Comments
	used. A term, that is already used in the GDPR, notably in Article 35 – which the proposed Article 13(4) itself refers to – as well as Article 37, and covered by relevant EDPB guidelines. • Alternatively, we would ask the Presidency for the reasoning for using the term "processing of large amounts of personal data" instead of "large scale processing of personal data". FI (Comments): FI supports this recital text.
(37) Where the **further** processing **by the same controller** takes place for the purpose of scientific research and the provision of information to the data subject proves to be impossible or would involve a disproportionate effort it should not be necessary to provide the information provided for under Article 13 of this Regulation. The controller should make reasonable efforts to acquire contact details if they are readily available and acquisition would not require a disproportionate effort. The provision of the information would involve a disproportionate effort in particular where the controller at the time of collection of the personal data did not know or anticipate that it would process personal data for scientific research purposes at a later stage, in which case it may not have easily available contact details of the data subjects. In such situations the controller should inform data subjects indirectly, such as by making the information publicly available. The provision of such information should ensure that as many data subjects concerned as possible are reached. Relevant means to make the information publicly available should be determined depending on the context of the research project and the data subjects involved.	FI (Comments): FI supports this recital text.
(38) Article 22 of Regulation (EU) 2016/679 provides **that data subject has the right not to be subject to a decision based solely on automated processing, except when specific conditions are met and in accordance with**~~for~~ rules governing the processing of personal data when the ~~data~~ controller makes decisions which have legal effects **concerning the data**	LU (Comments): Article 22 of the GDPR has long been regarded as offering limited legal clarity and is frequently perceived as difficult to understand in practice.

Commission proposal	Drafting suggestions and Comments
subject or similarly significant effects on the data subject, based solely on automated processing. In order to provide greater legal certainty, it should be clarified that **when assessing whether a decision**~~decisions~~ based solely on automated processing ~~are allowed when specific conditions are met, as set out in Regulation (EU) 2016/679. It should also be clarified that when assessing whether a decision~~ is necessary for entering into, or performance of, a contract between the data subject and a ~~data~~ controller, as set out in Article 22(2)(a) of Regulation (EU) 2016/679, it should not be required that the decision could be taken only by solely automated processing. ~~This means that~~ **The**~~the~~ fact that the decision could also be taken by a human does not prevent the controller from taking the decision by solely automated processing**.** When several equally effective automated processing solutions exist, the controller should use the less intrusive one.	Moreover, the concrete legal result of an explicit reference to a 'right' not to be subject to an automated decision remain uncertain, a point clearly reflected in the ongoing debate surrounding this provision. We would be more favourable to the initial proposal, submitted by the European Commission. AT (Comments): • AT continues to find it problematic to determine the meaning of the term **"necessary"** for the entering into or performance of a contract in accordance with Article 22 (1)a. This issue is currently the subject of a case pending before the CJEU (**Case C-568/25**). The CJEU should not be pre-empted in this regard. FI (Comments): FI supports this recital text.
(39) ~~In order to reduce the burden on controllers while ensuring that supervisory authorities have access to the relevant information and can act on violations of the Regulation, the threshold for notification of a personal data breach to the supervisory authority under Article 33 of Regulation (EU) 2016/679 should be aligned with that of communication of a personal data breach to the data subject under Article 34 of that Regulation.~~ In the case of a data breach that is not likely to result in a high risk to the rights and freedoms of natural persons, the controller should not be required to notify the competent supervisory authority. The higher threshold for notifying a data breach to the supervisory authority does not affect the obligation of the controller to document the breach in accordance with paragraph 5 of Article 33 of Regulation (EU) 2016/679, or its obligation to be able to demonstrate its compliance with that Regulation, in accordance with Article 5(2) of that Regulation. In order to facilitate compliance by	EE (Drafting suggestions): (39) ~~In order to reduce the burden on controllers while ensuring that supervisory authorities have access to the relevant information and can act on violations of the Regulation, the threshold for notification of a personal data breach to the supervisory authority under Article 33 of Regulation (EU) 2016/679 should be aligned with that of communication of a personal data breach to the data subject under Article 34 of that Regulation.~~ In the case of a data breach that is not likely to result in ~~a high risk~~ **an increased risk** to the rights and freedoms of natural persons, the controller should not be required to notify the competent supervisory authority. The higher threshold for notifying a data breach to the supervisory authority does not affect the obligation of the controller to document the

Commission proposal	Drafting suggestions and Comments
controllers and a harmonised approach in the Union, the Board should **establish and make public**~~prepare~~ a common template for notifying data breaches to the competent supervisory authority and a common list of circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person**, and a common list of circumstances in which a personal data breach does not result in such a high risk**~~. The Commission should take due account of the proposal prepared by the Board and review them, as necessary, prior to adoption~~. In order to take account of new information security threats, the common template and the list should be reviewed at least every three years and updated **where necessary. The Commission may adopt, by means of an implementing act, the common template as established by the Board, as well as its updates** where necessary. The lack of a common list of circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person should not affect the obligations of controllers to notify those breaches. **The alignment of notification thresholds should not affect the controller's obligation to carry out an individual risk assessment and to maintain complete documentation of personal data breaches in accordance with Article 33(5) of Regulation (EU) 2016/679. The common lists of circumstances in which a personal data breach is likely to result in a high risk to the rights and freedom of a natural person and in which a personal data breach is not likely to result in a high risk should also apply in order to determine when communicating the data breaches to the data subject, in accordance with Article 34.**	breach in accordance with paragraph 5 of Article 33 of Regulation (EU) 2016/679, or its obligation to be able to demonstrate its compliance with that Regulation, in accordance with Article 5(2) of that Regulation. In order to facilitate compliance by controllers and a harmonised approach in the Union, the Board should **establish and make public**~~prepare~~ a common template for notifying data breaches to the competent supervisory authority and a common list of circumstances in which a personal data breach is likely to result in ~~a high risk~~ **an increased risk** to the rights and freedoms of a natural person**, and a common list of circumstances in which a personal data breach does not result in such an increased risk** ~~**a high risk**~~**.** ~~**The Commission should take due account of the proposal prepared by the Board and review them, as necessary, prior to adoption**~~. In order to take account of new information security threats, the common template and the list should be reviewed at least every three years and updated **where necessary**~~**. The Commission may adopt, by means of an implementing act, the common template as established by the Board, as well as its updates** where necessary.~~ The lack of a common list of circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person should not affect the obligations of controllers to notify those breaches. **The alignment of notification thresholds should not affect the controller's obligation to carry out an individual risk assessment and to maintain complete documentation of personal data breaches in accordance with Article 33(5) of Regulation (EU) 2016/679. The common lists of circumstances in which a personal data breach is likely to result in an increased risk** ~~**a high risk**~~ **to the rights and freedom of a natural person and in which a personal data breach is not likely to result in an increased risk** ~~**a high risk**~~ **should also apply in order to determine when communicating the data breaches to the data subject, in accordance with Article 34.** EE (Comments):

Commission proposal	Drafting suggestions and Comments
	Estonia supports reducing unnecessary data breach notifications but notes that controllers might underestimate their impact on data subjects. Multiple low-risk breaches, when combined, could pose higher risks to individuals' rights and DPAs should be made aware of those. We recommend using terms like "impactful risks" or "increased risks." Estonia does not support the amendment as regards the division of competences in between EDPB and the Commission. In a situation where the Board's guidelines can be updated quickly in response to newly emerging possibilities, there is a risk that the guidelines may recommend an updated approach, while the Commission's implementing regulation in force contains outdated information. Amending both the EDPB guidelines and the implementing regulation will be a lengthy process and can result in different outcomes. This could result in a situation where controllers are unable to use up-to-date measures without committing a breach, thereby jeopardising the protection of individuals' personal data. We do understand that the EDPB's guidelines may be challenged in ECJ, but providing that its guidelines must be validated by an implementing regulation will jeopardise the EDPB's autonomy. For this reason, we suggest removing the clauses that permit the Commission to adopt implementing acts. IT (Drafting suggestions): **Replace recital (39) with:** (39) In order to reduce unnecessary notifications while ensuring that supervisory authorities receive information concerning materially significant personal data breaches, the notification obligation under Article 33 should be based on objective and harmonised materiality criteria established at Union level. Controllers should not be required to conduct a separate speculative assessment of the likelihood and severity of risk in every incident. A common set of technologically neutral criteria should identify the categories of breach requiring notification, while controllers should continue to document breaches and maintain evidence of the security and remediation measures actually taken. IT

Commission proposal	Drafting suggestions and Comments
	(Comments): A harmonised objective materiality threshold is more predictable and less bureaucratic than requiring each controller to reconstruct an abstract "high-risk" threshold after every incident. The authority retains access to material incidents and may inspect the controller's underlying records and remediation measures. NL (Drafting suggestions): (39) In the case of a data breach that is not likely to result in a high risk to the rights and freedoms of natural persons, the controller should not be required to notify the competent supervisory authority. The higher threshold for notifying a data breach to the supervisory authority does not affect the obligation of the controller to document the breach in accordance with paragraph 5 of Article 33 of Regulation (EU) 2016/679, or its obligation to be able to demonstrate its compliance with that Regulation, in accordance with Article 5(2) of that Regulation. In order to facilitate compliance by controllers and a harmonised approach in the Union, the Board should establish and make public a common template for notifying data breaches to the competent supervisory authority and a common list of circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person**,** and a common list of circumstances in which a personal data breach does not result in such a high risk. In order to take account of new information security threats, the common template and the list should be reviewed at least every three years and updated where necessary. ~~**The Commission may adopt, by means of an implementing act, the common template as established by the Board, as well as its updates where necessary**~~. The lack of a common list of circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person should not affect the obligations of controllers to notify those breaches. The alignment of notification thresholds should not affect the controller's obligation to carry out an individual risk assessment and to maintain complete documentation of personal data breaches in

Commission proposal	Drafting suggestions and Comments
	accordance with Article 33(5) of Regulation (EU) 2016/679. The common lists of circumstances in which a personal data breach is likely to result in a high risk to the rights and freedom of a natural person and in which a personal data breach is not likely to result in a high risk should also apply in order to determine when communicating the data breaches to the data subject, in accordance with Article 34. NL (Comments): NL refers to its amendment on Article 33(6). AT (Drafting suggestions): (39) ~~In order to reduce the burden on controllers while ensuring that supervisory authorities have access to the relevant information and can act on violations of the Regulation, the threshold for notification of a personal data breach to the supervisory authority under Article 33 of Regulation (EU) 2016/679 should be aligned with that of communication of a personal data breach to the data subject under Article 34 of that Regulation.~~ In the case of a data breach that is not likely to result in **~~a high risk~~an impactful/relevant/increased risk** to the rights and freedoms of natural persons, the controller should not be required to notify the competent supervisory authority. The higher threshold for notifying a data breach to the supervisory authority does not affect the obligation of the controller to document the breach in accordance with paragraph 5 of Article 33 of Regulation (EU) 2016/679, or its obligation to be able to demonstrate its compliance with that Regulation, in accordance with Article 5(2) of that Regulation. In order to facilitate compliance by controllers and a harmonised approach in the Union, the Board should establish and make public~~prepare~~ a common template for notifying data breaches to the competent supervisory authority and a common list of circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person,

Commission proposal	Drafting suggestions and Comments
	and a common list of circumstances in which a personal data breach does not result in such **~~a high risk~~an impactful/relevant/increased risk**~~. The Commission should take due account of the proposal prepared by the Board and review them, as necessary, prior to adoption~~. In order to take account of new information security threats, the common template and the list should be reviewed at least every three years and updated where necessary. The Commission may adopt, by means of an implementing act, the common template as established by the Board, as well as its updates where necessary. The lack of a common list of circumstances in which a personal data breach is likely to result in **~~a high risk~~an impactful/relevant/increased risk** to the rights and freedoms of a natural person should not affect the obligations of controllers to notify those breaches. The alignment of notification thresholds should not affect the controller's obligation to carry out an individual risk assessment and to maintain complete documentation of personal data breaches in accordance with Article 33(5) of Regulation (EU) 2016/679. The common lists of circumstances in which a personal data breach is likely to result in **~~a high risk~~an imactful/relevant/increased risk** to the rights and freedom of a natural person and in which a personal data breach is not likely to result in **~~a high risk~~an imactful/relevant/increased risk** should also apply in order to determine when communicating the data breaches to the data subject, in accordance with Article 34. AT (Comments): • AT **remains very sceptical** about raising the threshold for data breach notifications to the supervisory authority. According to the current legal framework, all data breaches have to be notified to the supervisory authority, those that pose a high risk to the rights and freedoms of data subject additionally have to be notified to the data subject. The proposed changes would eliminate any notification of data breaches that do not meet the requirements of "high risk to the rights and freedoms of data subjects".

Commission proposal	Drafting suggestions and Comments
	It would therefore depend solely on the processor to determin, what measures to take to remedy data breaches that pose **a significant but not necessarily high** risk to the rights and freedoms of data subjects. • As a consequence, the EDPB might need to update its guidelines on the assessment of a "high risk" in accordance with Article 70(1)h GDPR. • Furthermore, the raising of the material threshold ("high risk") **in combination** with the extended time limit for data breach notifications ("96h") substantially weakens the protection of the data subjects' rights. • A compromise would be to introduce a threshold between "a risk" and "a high risk", such as "**an impactful/relevant/increased risk**". FI (Comments): FI supports this recital text.
(39a) In order to facilitate compliance obligations and the establishment of the contract or other legal act governing the processing by a processor on behalf of the controller, the processor should also be subject to the general obligation of data protection by design and by default under Regulation (EU) 2016/679 to extent it relates to their own obligations under that Regulation. This obligation does not affect the level of responsibility and relationship between the controller and processor, nor does it affect the principle of accountability or the respective obligations of controller and processor as laid down under Article 28 of Regulation (EU) 2016/679). Accordingly, the controller remains solely responsible for determining the purpose and means of processing and for complying with related obligations, while the processor should ensure that data protection by design and by default is applied to its offered means and services to carry out processing.	EE (Drafting suggestions): ~~**(39a) In order to facilitate compliance obligations and the establishment of the contract or other legal act governing the processing by a processor on behalf of the controller, the processor should also be subject to the general obligation of data protection by design and by default under Regulation (EU) 2016/679 to extent it relates to their own obligations under that Regulation. This obligation does not affect the level of responsibility and relationship between the controller and processor, nor does it affect the principle of accountability or the respective obligations of controller and processor as laid down under Article 28 of Regulation (EU) 2016/679). Accordingly, the controller remains solely responsible for determining the purpose and means of processing and for complying with related obligations, while the processor should ensure that data protection by design and by default is applied to its offered means and services to carry out processing.**~~ EE

Commission proposal	Drafting suggestions and Comments
	(Comments): Estonia has concerns about extending the duty of data protection by design and by default to processors. This may create uncertainty in the division of responsibilities between controllers and processors and could run counter to the objective of reducing regulatory burden. By extending the principles of data protection by design and by default directly to processors as well, it blurs the controller's responsibility under Article 5(2) GDPR. In addition, if Article 28 still provides that the controller determines what the processor must do and how, and the processor acts accordingly, then the purpose of this amendment is not clear. Recital 39a states with regard to processors: "to the extent of its own obligations" – we kindly ask to specify what exactly does this mean in practice. Moreover, the current recital 78 already states that "When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations." We are of the opinion that the current text of GDPR already adresses the imbalance in between small controllers and large processors. AT (Comments): • AT **supports** the proposed changes. FI (Comments): Concerning Article 25 GDPR [Art. 3(7a) Digiomnibus] and this recital, FI has reservations as regards to adding processors in the Article without a proper assessment but understands that processors should also have responsibility especially in situations where SMEs use processors that

Commission proposal	Drafting suggestions and Comments
	provide services with “take it or leave it” conditions. However, this is not a redline.
(40) Article 35 of that Regulation (EU) 2016/679 requires controllers to conduct a data protection impact assessment where the processing of personal data is likely to result in a high risk to the rights and freedoms of natural persons. The supervisory authorities established pursuant to that Regulation are required to establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment. In addition, the Regulation provides that supervisory authorities may establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. In order to effectively contribute to the aim of convergence of the economies and to effectively ensure free flow of personal data between Member States, increase legal certainty, facilitate compliance by controllers and ensure a harmonised interpretation of the notion of a high risk to the rights and freedoms of data subjects, a single list of processing operations should be provided at EU level, to replace the existing national lists. In addition, the publication of a list of the type of processing operations for which no data protection impact assessment is required, which is currently optional, should be made mandatory. The lists of processing operations should be **established and made public**~~prepared~~ by the Board**. In establishing the lists, due account should be taken of the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons** ~~and adopted by the Commission as an implementing act~~. In order to facilitate compliance by controllers, the Board should also **establish and make public**~~prepare~~ a common template and a common methodology for conducting data protection impact assessments~~, to be adopted by the Commission as an implementing act. The Commission should take due account of the proposals prepared by the Board and review them, as necessary, prior to adoption~~. In order to take account of technological developments, the lists and the common template and methodology should be reviewed at least every three years and updated	EE (Drafting suggestions): (40) Article 35 of that Regulation (EU) 2016/679 requires controllers to conduct a data protection impact assessment where the processing of personal data is likely to result in a high risk to the rights and freedoms of natural persons. The supervisory authorities established pursuant to that Regulation are required to establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment. In addition, the Regulation provides that supervisory authorities may establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. In order to effectively contribute to the aim of convergence of the economies and to effectively ensure free flow of personal data between Member States, increase legal certainty, facilitate compliance by controllers and ensure a harmonised interpretation of the notion of a high risk to the rights and freedoms of data subjects, a single list of processing operations should be provided at EU level, to replace the existing national lists. In addition, the publication of a list of the type of processing operations for which no data protection impact assessment is required, which is currently optional, should be made mandatory. The lists of processing operations should be **established and made public**~~prepared~~ by the Board**. In establishing the lists, due account should be taken of the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons** ~~and adopted by the Commission as an implementing act~~. In order to facilitate compliance by controllers, the Board should also **establish and make public**~~prepare~~ a common template and a common methodology for conducting data protection impact assessments~~, to be adopted by the Commission as an implementing act. The Commission should take due account of the proposals prepared by the Board and~~

Commission proposal	Drafting suggestions and Comments
where necessary. **The Commission may adopt, by means of an implementing act, the common template as established by the Board, as well as its updates where necessary.**	~~review them, as necessary, prior to adoption~~. In order to take account of technological developments, the lists and the common template and methodology should be reviewed at least every three years and updated where necessary. ~~**The Commission may adopt, by means of an implementing act, the common template as established by the Board, as well as its updates where necessary.**~~ EE (Comments): Estonia does not support the amendment as regards the division of competences in between EDPB and the Commission. In a situation where the Board's guidelines can be updated quickly in response to newly emerging possibilities, there is a risk that the guidelines may recommend an updated approach, while the Commission's implementing regulation in force contains outdated information. Amending both the EDPB guidelines and the implementing regulation will be a lengthy process and can result in different outcomes. This could result in a situation where controllers are unable to use up-to-date measures without committing a breach, thereby jeopardising the protection of individuals' personal data. We do understand that the EDPB's guidelines may be challenged in ECJ, but providing that its guidelines must be validated by an implementing regulation will jeopardise the EDPB's autonomy. For this reason, we suggest removing the clauses that permit the Commission to adopt implementing acts. IT (Drafting suggestions): **Replace recital (40) with:** (40) The obligation to demonstrate compliance should focus on evidence of effective processing safeguards rather than on completion of a prescribed data protection impact assessment or risk methodology. For specified categories of processing, controllers should maintain concise evidence concerning purposes, categories of data, access and retention arrangements, applicable technical and organisational safeguards, testing performed and

Commission proposal	Drafting suggestions and Comments
	corrective action taken. No mandatory template or methodology should be required where the controller can demonstrate the same substantive outcomes by other reliable evidence. IT (Comments): The proposed EU-wide DPIA lists and methodology would harmonise formalities but could increase procedural bureaucracy. The better simplification is to replace a mandatory risk-assessment format with concise processing-assurance evidence that can be tested during inspection NL (Drafting suggestions): 40) Article 35 of that Regulation (EU) 2016/679 requires controllers to conduct a data protection impact assessment where the processing of personal data is likely to result in a high risk to the rights and freedoms of natural persons. The supervisory authorities established pursuant to that Regulation are required to establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment. In addition, the Regulation provides that supervisory authorities may establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. In order to effectively contribute to the aim of convergence of the economies and to effectively ensure free flow of personal data between Member States, increase legal certainty, facilitate compliance by controllers and ensure a harmonised interpretation of the notion of a high risk to the rights and freedoms of data subjects, a single list of processing operations should be provided at EU level, to replace the existing national lists. In addition, the publication of a list of the type of processing operations for which no data protection impact assessment is required, which is currently optional, should be made mandatory. The lists of processing operations should be established and made public by the Board. In establishing the lists, due account should be taken of the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons. In order

PUBLIC

Commission proposal	Drafting suggestions and Comments
	to facilitate compliance by controllers, the Board should also establish and make public a common template and a common methodology for conducting data protection impact assessments. In order to take account of technological developments, the lists and the common template and methodology should be reviewed at least every three years and updated where necessary. ~~**The Commission may adopt, by means of an implementing act, the common template as established by the Board, as well as its updates where necessary.**~~ NL (Comments): NL refers to its amendment on Article 35(6a) and 35(6b). FI (Comments): FI supports this recital text.
(40a) In order to ensure consistency of interpretation of this Regulation (EU) 2016/679, it is important that national supervisory authorities ensure that the adoption of guidelines, recommendations and best practices at national level on matters already covered by guidelines adopted by the Board, is consistent and does not contradict those issued by the Board, including by updating or repealing national relevant guidelines, recommendations and best practices when necessary. It is also important that national supervisory authorities and the Board duly consider matters of consistent application of this Regulation, including when such matters are identified and brought to their attention by controllers or other relevant stakeholders.	CZ (Drafting suggestions): New recital 40b: **Transfers of personal data to third countries or international organisations could be necessary for important reasons of public interest within the meaning of Article 49, paragraph (1), point (d) of Regulation (EU) 2016/679. Such important reasons of public interest include the implementation, application and compliance with international agreements or administrative arrangements on mutual assistance or cooperation in tax matters concluded by a Member State with a third country or an international organisation where personal data are exchanged on a periodic or automated basis. In such cases, Member States should ensure that appropriate safeguards are provided for under Union law or national law, so that the level of protection of natural persons guaranteed by Regulation (EU) 2016/679 is not undermined.**

Commission proposal	Drafting suggestions and Comments
	Where the competent authority responsible for the transfer considers that the rights and freedoms of the data subject concerned override the public interest pursued by the transfer, the transfer should not take place. CZ (Comments): CZ supports ES proposal for change of Art. 49 GDPR as regards tax cooperation. CZ strongly prefers that Article, but can, in the spirit of compromise, support a recital instead. Wording has been taken from document 10729/26 prepared by CY PRES. IT (Drafting suggestions): **Insert after recital (40a):** (40b) Greater flexibility for controllers in selecting the technical and organisational means by which they comply with this Regulation should be accompanied by more effective ex post supervision. Supervisory authorities should devote a greater proportion of their resources to inspections and technical verification of actual processing operations. Supervisory activity should focus on whether substantive legal, safety and security outcomes are achieved rather than on formal adherence to particular templates, methodologies or organisational models. (40c) Administrative investigations concerning compliance with Regulation (EU) 2016/679 should be conducted within a clear and mandatory maximum period. Legal certainty for data subjects, controllers and processors requires that all investigative activity be included within that period irrespective of the terminology used by the supervisory authority. In particular, a supervisory authority should not be able to postpone commencement of the applicable time limit by designating activities as preliminary enquiries, pre-investigative activities, screening, admissibility review, competence determination, fact finding, informal supervision or by any equivalent denomination. IT (Comments): These recitals state the quid pro quo underpinning the reform: less ex ante paperwork and more controller discretion must be counterbalanced by stronger technical inspection and

PUBLIC

Commission proposal	Drafting suggestions and Comments
	strict procedural discipline for supervisory authorities. The investigation clock must cover the entire factual investigation from its first substantive act. AT (Drafting suggestions): (40a) In order to ensure **consistency of the consistent interpretation** of this Regulation **(EU) 2016/679**, it is important that national supervisory authorities ensure that the **adoption of** guidelines, recommendations and best practices **adopted** at national level on matters already covered by guidelines adopted by the Board, **is are** consistent and **does do** not contradict those issued by the Board**., including by This includes** updating or repealing national relevant guidelines, recommendations and best practices when necessary. **It is also important that Moreover,** national supervisory authorities and the Board **should** duly consider matters of consistent application of this Regulation, including when such matters are identified and brought to their attention by controllers or other relevant stakeholders. AT (Comments): • AT **can support** the addition of Recital 40a but emphasises that the independence of supervisory authorities must be preserved. • Furthermore, AT proposes that the **wording** should be revised. PL (Drafting suggestions): (40a) In order to ensure consistency of interpretation of this Regulation (EU) 2016/679, it is important that national supervisory authorities ensure that the adoption of guidelines, recommendations and best practices at national level on matters already covered by guidelines adopted by the Board, is consistent and does not contradict those issued by the Board, including by updating or repealing national relevant guidelines, recommendations and best practices when necessary. It is also important that national supervisory authorities and the Board duly consider matters of

Commission proposal	Drafting suggestions and Comments
	consistent application of this Regulation, including when such matters are identified and brought to their attention by controllers or other relevant stakeholders. **<u>The consistent application of Regulation (EU) 2016/679 should also contribute to innovation and competitiveness of the Union.</u>** FI (Drafting suggestions): **(40a) In order to ensure consistency of interpretation of this Regulation (EU) 2016/679, ~~it is important that~~ national supervisory authorities should refrain from adopting and ensure that the adoption of guidelines, recommendations and best practices at national level on matters already covered by guidelines adopted by the Board, is consistent and does not contradict those issued by the Board. Where necessary, existing national relevant guidelines, recommendations and best practices should be repealed or updated. It is also important that national supervisory authorities and the Board duly consider matters of consistent application of this Regulation, including when such matters are identified and brought to their attention by controllers or other relevant stakeholders.** FI (Comments): FI can support recital 40a concerning the consistency of interpretation of the GDPR and the aim to ensure uniform guidelines from data protection authorities. It is important that when the EDPB has given guidance, national data protection authorities should repeal or amend their guidance appropriately.

Commission proposal	Drafting suggestions and Comments
	However, FI proposes that the recital would be more specific to ensure that national DPAs' guidelines are deleted or amended, if not in line with the EDPB guidance. See proposal underlined and bolded.
(41) Regulation (EU) 2018/1725 of the European Parliament and of the Council[16] applies to the processing of personal data by the Union institutions, bodies, offices and agencies. ~~Directive (EU) 2016/680 of the European Parliament and of the Council[17] applies to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.~~ Regulation (EU) 2018/1725 ~~and Directive (EU) 2016/680~~ should be brough into alignment with the amendments to Regulation (EU) 2016/679 introduced by this Regulation. 16 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj). 17 ~~Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89, ELI: **http://data.europa.eu/eli/dir/2016/680/oj**).~~	
(42) As clarified in recital 5 of Regulation (EU) 2018/1725, whenever the provisions of Regulation (EU) 2018/1725 follow the same principles as the provisions of Regulation (EU) 2016/679, those two sets of provisions should, under the case law of the Court of Justice of the European Union, be interpreted homogeneously. The scheme of Regulation (EU) 2018/1725	FI (Comments): FI supports this recital text.

Commission proposal	Drafting suggestions and Comments
should be understood as equivalent to the scheme of Regulation (EU) 2016/679. Therefore, this Regulation also amends the provisions of Regulation (EU) 2018/1725 that are concerned by the amendments of Regulation (EU) 2016/679, insofar as the latter amendments are also relevant in the context of the processing of personal data by the Union institutions, bodies, offices and agencies.	
~~(43) In order to provide a strong and coherent data protection framework in the Union, the necessary adaptations of Directive (EU) 2016/680 and any other Union legal act applicable to such processing of personal data should follow after the adoption of this regulation, in order to allow for their application as close as possible to the entry into application of the amendments to Regulation (EU) 2016/679 and Regulation (EU) 2018/1725.~~	
(43a) Directive 2002/58/EC on privacy and electronic communications ('ePrivacy Directive'), last revised in 2009, provides a framework for the protection of the right to privacy, including the confidentiality of communications. It also specifies Regulation (EU) 2016/679 in relation to processing of personal data in the context of electronic communication services. It protects the privacy and the integrity of subscriber's or user's terminal equipment used for such communications.	
(44) The storing of **information**~~personal data~~, or the gaining of access to **information**~~personal data~~ already stored, in a terminal equipment and the subsequent processing of such data should be regulated under a single legal framework, namely **Directive 2002/58/EC on privacy and electronic communications**~~Regulation (EU) 2016/679~~, where the subscriber of the electronic communications service or the user of the terminal equipment is a natural person. The amendments **to this Directive should**~~presented in this Regulation~~ continue to offer the highest levels of protection for personal data, while simplifying the experiences of data subjects in exerting their rights and expressing their choices online. The amendments concern in particular storage of information in that equipment, accessing or otherwise collecting information from that equipment that entails the processing of	

PUBLIC

Commission proposal	Drafting suggestions and Comments
personal data through cookies or similar technologies to gain information from the terminal equipment. ~~**The relevant rules should also apply regardless of whether the terminal equipment is owned by the natural person or by another legal or natural person.**~~	
(44a) The storing of **information**~~**personal data**~~, or the gaining of access to **information**~~**personal data**~~ already stored, in a terminal equipment should continue to be allowed only on the basis of consent. ~~**Similar to the approach in Directive 2002/58/EC, this requirement should not preclude storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person, when that is based on Union or Member State law within the meaning of Article 6 of Regulation (EU) 2016/679 and if it fulfils all conditions of lawfulness laid down in that provision, and is done for the objectives laid down in Article 23(1) of Regulation (EU) 2016/679.**~~	
(44b) With a view to reducing the compliance burden and providing legal clarity ~~**to controllers**~~, and given that certain purposes of processing pose a low risk to the rights and freedoms of data subjects or that such processing may be necessary to provide a service requested by **a subscriber or user**~~**the data subject**~~, it is necessary to define a limitative list of purposes for which the processing should be permitted without consent. As regards storing of **information**~~**personal data**~~, or the gaining of access to **information**~~**personal data**~~ already stored, in a terminal equipment, and subsequent processing that is necessary for those purposes, **the Directive**~~**this Regulation**~~ should therefore provide that **such**~~**the**~~ processing is lawful**, including when being carried out jointly with or on the behalf of a**~~**. The**~~ controller**. For example**~~**, such as**~~ a media service provider, may mandate a **third party**~~**processor**~~, such as a market research company, to carry out **such processing.** **Consent should not be required, where placing of information on or gaining access to information stored is necessary to provide a service explicitly requested by user or subscriber. This should include placing of information or gaining access to information stored for the purpose of**	CZ (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
ensuring certain functionalities necessary for the service explicitly requested by the user or subscriber. This could include memorising the user's choices and selected elements such as, among others, the user's language settings, configuration choices, items placed in shopping baskets~~ or memorising~~, information to facilitate filling in of online forms, or functionalities of a requested service related to information on vehicles. **Measuring the audience of an online service ~~in order to create~~by creating anonymous aggregated information about the usage of an online service, where it is carried out by the provider of that online service, or by a third party acting together with or on behalf of this provider, or by a third party such as a market research company or a Joint Industry Committee, acting together with or on behalf of this provider, ~~,~~also referred to as 'audience measurement' as defined in paragraph 16 of Article 2 and in accordance with Article 24 of Regulation (EU) 2024/1083, means~~the~~ processing such data and information to obtain insight into the performance and use of the online service in an instantly anonymised, aggregated and general manner. This includes the performance of audience by an entitled and independent third party performing audience measurement as defined in Regulation (EU) 2024/1083. The aggregated information should not relate to a specific data subject and should therefore be anonymous aggregated information. The anonymous aggregated information can be shared with third parties, including companies and non-commercial organizations. Processing of personal data with the aim of creating anonymous aggregated information contributes to the sustainability of the media ecosystem as highlighted in Regulation 2024/1083 and should be subject to strict limitations designed to ensure that the personal data is not reused for providing personalised advertising, profiling or other unrelated purposes. The personal data of users or subscribers initially collected should not be further processed for another purpose, combined with data from other services from the provider of the online service or**	

PUBLIC

Commission proposal	Drafting suggestions and Comments
from a third party, such as analytics information from other websites or apps, or shared with third parties. **Maintaining or restoring the security of a service provided by an information society service provider and requested by the subscriber or user, or the terminal equipment used for the provision of such service, should only be allowed without consent to the extent that the security updates are strictly necessary, proportionate, discretely packaged and do not in any way change the functionality of the software on the terminal equipment, including the interaction with other software or settings chosen by the subscriber or user, the subscriber or user is informed in advance each time an update is being installed, and the subscriber or user has the possibility to turn off the automatic installation of these updates~~on its behalf~~. The maintaining or restoring the security of the service or of the terminal equipment should include in particular cybersecurity and the necessary security requirements to ensure a proper functioning of the terminal equipment as well as the protection of personal data and privacy of the user.** ~~Measures taken for the detection and prevention of fraud should only be possible to be taken without consent insofar as they are strictly necessary and such measures do not override the fundamental rights and interests of users and subscribers.~~	

PUBLIC

Commission proposal	Drafting suggestions and Comments
	(…)**The measurement of the display and performance of advertising which is made solely on the basis of the immediate content displayed on the user's interface, also referred to as 'contextual advertising', may be lawful without the consent of the user provided if not based on any type of profiling, in other words based on a user's visit to a single web page or on a single search query, in case it does not involve any data retention or link with the user's past or future activity** CZ (Comments):

PUBLIC

Commission proposal	Drafting suggestions and Comments

PUBLIC

Commission proposal	Drafting suggestions and Comments

PUBLIC

Commission proposal	Drafting suggestions and Comments

PUBLIC

Commission proposal	Drafting suggestions and Comments
	CZ: To accompany our suggestion in art. 5(3)(e) DK (Drafting suggestions): […]meansthe processing such data and information to obtain insight into the performance and use of the online service in an ~~**instantly**~~ anonymised, aggregated and general manner[…]. DK (Comments): We question the reintroduction of the word "instantly" in the recital. While we support the objective of ensuring that audience measurement results in anonymous aggregated information, the additional qualifier does not reflect the technical realities and risks creating unnecessary legal uncertainty. We do not consider the word "instantly" necessary and we would like to see this streamlined with the operative text (art. 5(3), litra c of the ePrivacy Directive) and how the current market of independent audience measurements works in accordance with article 24 of the European Media Freedom Act (Regulation (EU) 2024/1083). In this regard, we would be positively inclined and eager to assess adjustments based on the oral comments made by the Italian and French delegation as well as the Commission representative at the last AGS meeting. EE (Comments): Question about **Measuring the audience of an online service:** how the proposed wording of Recital 44b interacts with Article 24 EMFA? In

PUBLIC

Commission proposal	Drafting suggestions and Comments
	particular, has it been assessed whether the requirements of "instant anonymisation" and the prohibition on combining data from other services could undermine the operation and verifiability of independent audience measurement systems that EMFA seeks to support? ES (Comments): We welcome the reinstatement of the requirement of da used for audience measurement to be “instantly” anonymised and aggregated. However, merely referring to this requirement in a recital is not sufficient. It is necessary to include clear provisions in the article in order to ensure its effective and legally binding application. FR (Drafting suggestions): **(44b)** With a view to reducing the compliance burden and providing legal clarity ~~to controllers~~, and given that certain purposes of processing pose a low risk to the rights and freedoms of data subjects or that such processing may be necessary to provide a service requested by **a subscriber or user**~~the data subject~~, it is necessary to define a limitative list of purposes for which the processing should be permitted without consent. As regards storing of **information**~~personal data~~, or the gaining of access to **information**~~personal data~~ already stored, in a terminal equipment, and subsequent processing that is necessary for those purposes, **the Directive**~~this Regulation~~ should therefore provide that **such**~~the~~ processing is lawful, **including when being carried out jointly with or on the behalf of a**~~. The~~ controller. **For example**~~, such as~~ a media service provider, may mandate a **third party**~~processor~~, such as a market research company, to carry out **such processing.** **Consent should not be required, where placing of information on or**

Commission proposal	Drafting suggestions and Comments
	gaining access to information stored is necessary to provide a service explicitly requested by user or subscriber. This should include placing of information or gaining access to information stored for the purpose of ensuring certain functionalities necessary for the service explicitly requested by the user or subscriber. This could include memorising the user's choices and selected elements such as, among others, the user's language settings, configuration choices, items placed in shopping baskets ~~or memorising~~, information to facilitate filling in of online forms, or functionalities of a requested service related to information on vehicles. **Measuring the audience of an online service in order to create ~~in order to create~~by ~~creating~~ anonymous aggregated information about the usage of an online service, where it is carried out by the provider of that online service, or by a third party acting together with or on behalf of this provider, or by a third party such as a market research company or a Joint Industry Committee, acting together with or on behalf of this provider, ~~,~~also referred to as 'audience measurement' as defined in paragraph 16 of Article 2 and in accordance with Article 24 of Regulation (EU) 2024/1083, means~~the~~ processing such data and information to obtain insight into the performance and use of the online service in ~~an instantly~~ anonymised, aggregated and general manner. This includes the performance of audience by an entitled and independent third party performing audience measurement as defined in Regulation (EU) 2024/1083. The aggregated information should not relate to a specific data subject and should therefore be anonymous aggregated information. The anonymous aggregated information can be shared with third parties, including companies and non-commercial organizations. Processing of personal data with the aim of creating anonymous aggregated information contributes to the sustainability of the media ecosystem as highlighted in Regulation 2024/1083 and should be subject to strict limitations designed to ensure that the personal data is not reused for providing personalised advertising, profiling or other**

Commission proposal	Drafting suggestions and Comments
	unrelated purposes. The personal data of users or subscribers initially collected should not be further processed for another purpose, combined with data from other services from the provider of the online service or from a third party, such as analytics information from other websites or apps, or shared with third parties <u>except for the operational needs for the sole purpose of providing audience measurement results in connection with Article 24(1) EMFA, or shared with third parties.</u> **Maintaining or restoring the security of a service provided by an information society service provider and requested by the subscriber or user, or the terminal equipment used for the provision of such service, should only be allowed without consent to the extent that the security updates are strictly necessary, proportionate, discretely packaged and do not in any way change the functionality of the software on the terminal equipment, including the interaction with other software or settings chosen by the subscriber or user, the subscriber or user is informed in advance each time an update is being installed, and the subscriber or user has the possibility to turn off the automatic installation of these updates~~on its behalf~~. The maintaining or restoring the security of the service or of the terminal equipment should include in particular cybersecurity and the necessary security requirements to ensure a proper functioning of the terminal equipment as well as the protection of personal data and** **privacy of the user.** **<u>The measurement of the display and performance of advertising which is made solely on the basis of the immediate content displayed on the user's interface, also referred to as 'contextual advertising', may be lawful without the consent of the user provided that it is not based on any type of profiling, that it is based on a user's current visit to a single web page or based on a single search query and does not involve any retention or link with the user's past or future activity.</u>** **Measures taken for the detection and prevention of fraud should only be possible to be taken without consent insofar as they are strictly necessary**

Commission proposal	Drafting suggestions and Comments
	and such measures do not override the fundamental rights and interests of users and subscribers. FR (Comments):

PUBLIC

Commission proposal	Drafting suggestions and Comments
	Inversion des étapes concernant la mesure d'audience afin de décrire correctement le processus : les données sont d'abord collectées puis agrégées afin de pouvoir mesurer l'audience. Suppression de la mention "Instantly", puisque l'agrégation ne peut pas avoir lieu de manière immédiate.

PUBLIC

Commission proposal	Drafting suggestions and Comments
	Assouplissement concernant la possibilité de combiner les données personnelles afin de permettre la constitution de panels dans le cadre de la mesure d'audience.

PUBLIC

Commission proposal	Drafting suggestions and Comments
	PUBLIC Réintroduction de l'exception relative à la publicité contextuelle. Réintroduction de l'exemption relative à la détection de la fraude IT (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
	Measuring the audience of an online service ~~in order to create~~by creating anonymous aggregated information about the usage of an online service, where it is carried out by the provider of that online service, or by a third party acting together with or on behalf of this provider, or by a third party such as a market research company or a Joint Industry Committee, acting together with or on behalf of this provider, ~~,~~also referred to as 'audience measurement' as defined in

PUBLIC

Commission proposal	Drafting suggestions and Comments
	paragraph 16 of Article 2 and in accordance with Article 24 of Regulation (EU) 2024/1083, means ~~the~~ processing **such data and information to obtain insight into the performance and use of the online service in an** ~~**instantly**~~ **anonymised, aggregated and general manner** IT (Comments):

PUBLIC

Commission proposal	Drafting suggestions and Comments
	PUBLIC We welcome the inclusion of audience measurement among the exemptions provided for in the whitelist under Article 5(2). This exemption, in line with Article 24 EMFA and the definition set out in Article 2(16) EMFA, is essential to preserve established industry methodologies and to safeguard the role of Joint Industry Committees (JICs), which are expressly recognized under the EMFA framework. At the same time, it is necessary to harmonize the text of Recital 44b by deleting the adverb “instantly” (which, incidentally, has already been removed from the previous version No. 10426/26), as its retention would create an inconsistency. Specifically, both the definition of “audience measurement” cited in Articles 24 and 2 of the EMFA and the practical operation of the JICs rely on multi-stage data processing methodologies that are incompatible with a requirement of instant anonymization. Maintaining such a requirement in Recital 44b could therefore have the unintended effect of rendering non-compliant the very audience measurement practices carried out by JICs. This outcome would be at odds with Article 24(5) EMFA, which explicitly recognizes and promotes these methodologies as industry best practices. NL

Commission proposal	Drafting suggestions and Comments
	(Drafting suggestions): (44b) With a view to reducing the compliance burden and providing legal clarity, and given that certain purposes of processing pose a low risk to the rights and freedoms of data subjects or that such processing may be necessary to provide a service requested by a subscriber or user, it is necessary to define a limitative list of purposes for which the processing should be permitted without consent. As regards storing of information, or the gaining of access to information already stored, in a terminal equipment, and subsequent processing that is **strictly** necessary for those purposes, the Directive should therefore provide that such processing is lawful, including when being carried out jointly with or on the behalf of a controller. For example, a media service provider, may mandate a third party, such as a market research company, to carry out such processing. Consent should not be required, where placing of information on or gaining access to information stored is **strictly** necessary to provide a service explicitly requested by user or subscriber. This should include placing of information or gaining access to information stored for the purpose of ensuring certain functionalities **strictly** necessary for the service explicitly requested by the user or subscriber. This could include memorising the user's choices and selected elements such as, among others, the user's language settings, configuration choices, items placed in shopping baskets, information to facilitate filling in of online forms, or functionalities of a requested service related to information on vehicles. Measuring the audience of an online service by creating anonymous aggregated information about the usage of an online service, where it is carried out by the provider of that online service, or by a third party acting together with or on behalf of this provider, or by a third party such as a market research company or a Joint Industry Committee, acting together with or on behalf of this provider, also referred to as 'audience measurement' as defined in paragraph 16 of Article 2 and in accordance with Article 24 of Regulation (EU) 2024/1083, means processing such data and information to obtain insight into the performance and use of the online service in an

Commission proposal	Drafting suggestions and Comments
	instantly anonymised, aggregated and general manner. This includes the performance of audience by an entitled and independent third party performing audience measurement as defined in Regulation (EU) 2024/1083. The aggregated information should not relate to a specific data subject and should therefore be anonymous aggregated information. The anonymous aggregated information can be shared with third parties, including companies and non-commercial organizations. Processing of personal data with the aim of creating anonymous aggregated information contributes to the sustainability of the media ecosystem as highlighted in Regulation 2024/1083 and should be subject to strict limitations designed to ensure that the personal data is not reused for providing personalised advertising, profiling or other unrelated purposes. The personal data of users or subscribers initially collected should not be further processed for another purpose, combined with data from other services from the provider of the online service or from a third party, such as analytics information from other websites or apps, or shared with third parties. Maintaining or restoring the security of a service provided by an information society service provider and requested by the subscriber or user, or the terminal equipment used for the provision of such service, should only be allowed without consent to the extent that the security updates are strictly necessary, proportionate, discretely packaged and do not in any way change the functionality of the software on the terminal equipment, including the interaction with other software or settings chosen by the subscriber or user, the subscriber or user is informed in advance each time an update is being installed, and the subscriber or user has the possibility to turn off the automatic installation of these updates~~on its behalf~~. The maintaining or restoring the security of the service or of the terminal equipment should include in particular cybersecurity and the necessary security requirements to ensure a proper functioning of the terminal equipment as well as the protection of personal data and privacy of the user. NL

Commission proposal	Drafting suggestions and Comments
	(Comments): NL proposes to add the wording “strictly” to the recital, to align the recital with the proposed phrasing of Article 5(3) ePrivacy Directive. Could it be further specified what the vehicles-exception is meant to cover (“*or functionalities of a requested service related to information on vehicles”*)? While the other examples are very specific this appears to apply

PUBLIC

Commission proposal	Drafting suggestions and Comments
	to the functionality of a requested service in general, which is already covered by the text above. PL (Drafting suggestions): To be added at the end: **(…) The measurement of the display and performance of advertising which is made solely on the basis of the immediate content displayed on the user's interface, also referred to as 'contextual advertising', may be lawful without the consent of the user provided if not based on any type of profiling, in other words based on a user's visit to a single web page or on a single search query, in case it does not involve any data retention or link with the user's past or future activity.** FI (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
	Measuring the audience of an online service ~~in order to create~~by creating anonymous aggregated information about the usage of an online service, where it is carried out by the provider of that online service, or by a third party acting together with or on behalf of this provider, or by a third party such as a market research company or a Joint Industry Committee, acting together with or on behalf of this provider, ~~,~~ also referred to as 'audience measurement' as defined in paragraph 16 of

PUBLIC

Commission proposal	Drafting suggestions and Comments
	Article 2 and in accordance with Article 24 of Regulation (EU) 2024/1083, means ~~the~~ processing **such data and information to obtain insight into the performance and use of the online service in an ~~instantly~~ anonymised, aggregated and general manner. This includes the performance of audience by an entitled and independent third party performing audience measurement as defined in Regulation (EU) 2024/1083. The aggregated information should not relate to a specific data subject and should therefore be anonymous aggregated information. The anonymous aggregated information can be shared with third parties, including companies and non-commercial organizations. Processing of personal data with the aim of creating anonymous aggregated information contributes to the sustainability of the media ecosystem as highlighted in Regulation 2024/1083 and should be subject to strict limitations designed to ensure that the personal data is not reused for providing personalised advertising, profiling or other unrelated purposes. The personal data of users or subscribers initially collected should not be further processed for another purpose, ~~combined with data from other services from the provider of the online service or from a third party, such as analytics information from other websites or apps,~~ or shared with third parties.** FI (Comments):

Commission proposal	Drafting suggestions and Comments
	FI underlines the importance of safeguarding the operating conditions of journalistic media in the digital age, in line with the European Democracy Shield. Article 24(1) of the EMFA mandates that audience measurement must be comparable and verifiable. The proposed specifications in recital 44, particularly the requirement to instantly anonymize data and the prohibition on combining data, would effectively render audience measurement, carried

PUBLIC

Commission proposal	Drafting suggestions and Comments
	out in compliance with the EMFA, impossible. FI calls for the deletion of requirements that would undermine the conditions necessary to ensure comparability and verifiability, thereby conflicting with article 24(1) of the EMFA.
(44c) For the **further**~~subsequent~~ processing of personal data for other purpose than those defined in the limitative list, Article 6 and, where relevant, Article 9 of Regulation (EU) 2016/679 should be applied. It is the responsibility of the controller in the light of the principle of accountability to choose the appropriate legal basis for the intended processing. In order to be able to rely on legitimate interest under Article 6(1), point f, of Regulation (EU) 2016/679 as a ground for the **further**~~subsequent~~ processing of personal data, the controller must show that it pursues the controller's or third parties' legitimate interest, the processing is necessary in order to achieve the purpose of that legitimate interest, and the interests or fundamental rights of the data subject do not override the interests pursued by the controller. In this context, controllers should take outmost account of the following elements: whether the data subject is a child; the reasonable expectations of data subject; the impact on the individual either because of the scale of data processed or the sensitivity of the data processed; the scale of the processing at issue in the sense that the processing cannot be particularly extensive either because of their amount or the range of categories of data; the processing should be based on data limited to what is necessary and cannot be based on monitoring of large parts of the online activity of the data subjects; and other relevant factors as appropriate. The processing should not give rise to the continuous monitoring of the data subject's private life.	
~~Where the controller cannot rely on legitimate interest as a legal ground for the subsequent processing, the processing should be based on another ground in Article 6(1), in particular on consent in accordance with~~	

Commission proposal	Drafting suggestions and Comments
~~Articles 6 and 7 of Regulation (EU) 2016/679, provided that all principles of Regulation (EU) 2016/679 are met.~~	
(45) Data subjects that have refused a request for consent are often confronted with a new request to give consent each time they visit the same controller's online service again. This may have detrimental effects to the data subjects which may consent just in order to avoid repeating requests. The controller should therefore be obliged to respect the data subject's choices to refuse a request for consent for at least a certain period. **This obligation is applicable to any** ~~controller~~**provider that accesses or stores** ~~personal data~~**information in the terminal equipment of** ~~the information~~**a subscriber or user, including** ~~third party~~**so-called third-party cookie** ~~providers~~**.**	
~~(46) Data subjects should have the possibility to rely on automated and machine-readable indications of their choice to consent or refuse a consent request or object to the processing of data. Such means should follow the state of the art. They can be implemented in the settings of a web browser or in the EU Digital Identity Wallet as set out by Regulation (EU) 914/2014, or any other adequate means. Rules set out in this Regulation should support the emergence of market-driven solutions with appropriate interfaces. The controller should be obliged to respect automated and machine-readable indications of data subject's choices once there are available standards. In light of the importance of independent journalism in a democratic society and in order not to undermine the economic basis for that, media service providers should not be obliged to respect the machine-readable indications of data subject's choices. The obligation for providers of web browsers to provide the technical means for data subjects to make choices with respect to the processing should not undermine the possibility for media service providers to request consent by data subjects.~~	
~~(47) Directive 2002/58/EC on privacy and electronic communications 'ePrivacy Directive'), last revised in 2009, provides a framework for the protection of the right to privacy, including the confidentiality of communications. It also specifies Regulation (EU) 2016/679 in relation to~~	

Commission proposal	Drafting suggestions and Comments
~~processing of personal data in the context of electronic communication services. It protects the privacy and the integrity of user's or subscriber's terminal equipment used for such communications. The current provision of Article 5(3) of Directive 2002/58/EC should remain applicable insofar as the subscriber or user is not a natural person, and the information stored or accessed does not constitute or lead to the processing of personal data.~~	
(48) Article 4 of Directive 2002/58/EC should be repealed. Article 4 of Directive 2002/58/EC sets requirements for providers of publicly available electronic communications services as regards safeguarding the security of their services and notification requirements. Subsequently, Directive (EU) 2022/2555 has set new requirements as regards cybersecurity risk-management measures and incident reporting for those providers. In order to reduce overlapping obligations for entities in the electronic communications sector, Article 4 of Directive 2002/58/EC should be repealed. As regards the security of processing of personal data pursuant to Article 4(1) and (1a) of this directive and the notification of personal data breaches pursuant to Article 4(3) to (5) of Directive 2002/58/EC this directive, the Regulation (EU) 2016/679 already provide for comprehensive and up-to-date rules. These rules should therefore apply to providers of publicly available electronic communication services and providers of public communications networks, thereby ensuring that one regime applies to the controllers and processors.	LV (Drafting suggestions): (48) Article 4 of Directive 2002/58/EC should be repealed. Article 4 of Directive 2002/58/EC sets requirements for providers of publicly available electronic communications services as regards safeguarding the security of their services and notification requirements. Subsequently, Directive (EU) 2022/2555 has set new requirements as regards cybersecurity risk-management measures and incident reporting for those providers. In order to reduce overlapping obligations for entities in the electronic communications sector, Article 4 of Directive 2002/58/EC should be repealed. As regards the security of processing of personal data pursuant to Article 4(1) and (1a) of this directive Directive 2002/58/EC and the notification of personal data breaches pursuant to Article 4(3) to (5) of Directive 2002/58/EC this directive, Regulation (EU) 2016/679 already provide provides for comprehensive and up-to-date rules. These rules should therefore apply to providers of publicly available electronic communication services and providers of public communications networks, thereby ensuring that one regime applies to the controllers and processors. LV (Comments): Repetiotion.
(49) Several horizontal or sectorial Union legal acts require the notification of the same event to different authorities using different technical	ES

Commission proposal	Drafting suggestions and Comments
means and channels. The **establishment by Member States of a national entry**~~single-entry~~ point for **the**~~incident~~ reporting **of incidents and related events** 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 **at national level**. Furthermore, the ~~single-entry point established at~~ **national** ~~level~~**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.	(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 establishment by Member States of a national entry point ~~for the reporting of incidents and related events~~ should ~~allow entities to fulfil reporting obligations~~ **support and facilitate the fulfillment of obligations pertaining to the reporting of incidents and related events** 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 at national level~~. Furthermore, the national entry point ~~should~~ **could** 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 (Comments): Spain supports the joint proposal to restore the wording of the compromise text of 22 June (REV5) for recital 49. For the avoidance of doubt, this includes, among other changes, removing the reference to notifications being submitted “to a single interface at national level”, which was already removed in REV5 and should not be reintroduced through the current compromise text. 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 **establishment by Member States of a national entry**~~single-entry~~ point ~~for~~ **should support and facilitate the fulfillment of obligations pertaining to the**~~incident~~ reporting **of incidents and related events** should allow entities to fulfil reporting obligations under Directive

Commission proposal	Drafting suggestions and Comments
	(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 **at national level**. Furthermore, the ~~**single-entry point** established at~~ **national** ~~level~~**entry point** ~~**should**~~ **could** 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. FR (Comments): Les autorités françaises estiment que la proposition de compromis présentée par la présidence irlandaise n'offre pas les garanties de flexibilité jugées nécessaires pour soutenir le texte. Les autorités françaises soulignent que la dernière proposition de compromis de la présidence chypriote (REV5 du 22 juin) offrait bel et bien la souplesse nécessaire en ce qui concerne le volet « cyber ». Elle garantissait à chaque État membre la possibilité d'adapter le point d'entrée national à ses dispositions et besoins nationaux, y compris ceux mis en œuvre pour protéger la sécurité nationale. Par conséquent, les autorités françaises demandent à modifier la formulation du volet «cybersécurité», en l'alignant sur le document REV5 (22/06) de la présidence chypriote. IT (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 establishment by Member States of a national entry point **should support and facilitate the fulfillment of obligations pertaining to** ~~**for**~~ the reporting of incidents and related events should allow entities to fulfil reporting obligations under Directive (EU) 2022/2555,

Commission proposal	Drafting suggestions and Comments
	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 at national level**~~. Furthermore, the national entry point ~~**should**~~ **could** 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): ACN estimates that the proposed compromise text does not provide the flexibility guarantees required to support the current wording. ACN underlines that the latest compromise proposal of the Cyprus Presidency of 22 June did provide the necessary flexibility for the cyber-related provisions. In particular, it ensured that each Member State could adapt the national entry point to its own national arrangements and requirements, including those established to safeguard national security. Therefore, ACN suggests amending the wording of the cyber-related provisions by aligning them with the text contained in the Cyprus Presidency's compromise proposal of 22 June. LV (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 **establishment by Member States of a national entry**~~single-entry~~ point for **the**~~incident~~ reporting **of incidents and related events** 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 **at national level**. Furthermore, the ~~single-entry point established at~~ **national** ~~level~~**entry point** should give a possibility

Commission proposal	Drafting suggestions and Comments
	for entities to retrieve information that they have previously submitted using the **national**~~single~~ entry point, thereby helping entities to keep track of their compliance with reporting obligations in connection with specific incidents. HU (Comments): HU The 96-hour deadline for reporting a breach proposed in Article 33 of the GDPR differs from the reporting regime under NIS2. Therefore, a report submitted through the national entry point does not automatically ensure the simultaneous fulfilment of the obligations under both regulations. The draft does not resolve this substantive discrepancy in a mandatory manner, so the simplification objective is only partially achieved. 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 **establishment by Member States of a national entrysingle-entry** point **for should support and facilitate the fulfillment of obligations pertaining to theincident** reporting **of incidents and related events** 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 **at national level**. Furthermore, the **single-entry point** established at **national** level**entry point should could** 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. NL

Commission proposal	Drafting suggestions and Comments
	(Comments): "The comments and drafting proposals on the cyber part in the table are a joint proposal supported by Spain, France, Austria, Italy and the Netherlands. We believe that the compromised text currently used by the Presidency (REV4) do not provide the flexibility needed by Member States in implementing the national entry point. We however support the drafting on the cyber part proposed on 22nd of June (REV5). Therefore, our comments aim at coming back to the wording of the REV5 and suggest consequential amendments to the sectoral acts."
(49a) In order to facilitate compliance with the obligation to report incidents and related events, including the identification of the applicable related obligations, ENISA should develop and maintain an incident reporting information point for incident reporting. That information point should serve as a clearly arranged source of information to support entities in identifying their reporting obligations and to guide them to the appropriate national entry point. Further information on related obligations, especially in terms of cybersecurity risk management, may be added. Structured communication channels should be established to ensure that the information available on the single information point is swiftly updated based on all the relevant and necessary information communicated by Member States.	
(50) To ensure the security of **national entry points in particular and with a view to designing interoperable national entry points**~~the single-entry point~~, ENISA should **develop non-binding recommendations addressing the**~~take~~ appropriate and proportionate technical, operational and organisational measures **for Member States to develop, maintain and securely operate their respective national entry**~~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~~	LV (Comments): LV would appreciate clarification on the proposal to establish a cross-border group to develop non-binding recommendations. Respectively regarding its functioning, effectiveness and expected results. How will it be possible to develop non-binding recommendations in 18 months if approximately more than 100 institutions would participate (national CSIRTs and competent authorities) in it? How will this group be organized? What will be the role of EU Member States and what will be the procedure for approving the non-binding recommendations?

Commission proposal	Drafting suggestions and Comments
~~disseminated pursuant to the relevant Union legal acts~~. ENISA should **establish a cross-sector working group to develop** ~~guidelines~~**these recommendations in cooperation with**~~consult~~ **CSIRTs and** competent authorities ~~and CSIRTs~~ under the relevant Union legal acts ~~when drafting~~**, making use of existing cooperation groups and networks of Member States established under these acts, with a view draft** the technical, operational and organisational measures necessary to establish, maintain and securely operate the **national entry**~~single entry~~ point ~~by making use of existing cooperation groups and networks of Member States established under these acts~~.	
(50a) The term 'national entry point' should be understood as a national infrastructure or arrangement, which may take the form of an online digital interface, platform or technical interoperability hub, established and maintained by the Member State, supporting entities to fulfil their incident notification obligations across multiple regulatory frameworks through ~~a single notification~~ **notifications at national level which will reach all competent authorities, CSIRTs and/or other designated authorities. Member States should retain flexibility to configure such infrastructure or arrangement in accordance with their specific needs, notably their national infrastructures and the allocation of competences among CSIRT's and competent and/or other designated authorities, including by connecting existing systems and enabling the sharing, routing or distribution of relevant information where needed. The creation of the national entry point does not necessarily interfere with the allocation of functions among competent authorities, CSIRT's and/or other designated authorities within each national system.**	
(50b) The national entry point could, depending on Member States' organisational arrangement and national structure, allow for tasks and functionalities supporting the reporting of relevant incidents, such as enabling the submission of notifications, receiving and processing notifications submitted by entities, ensuring or facilitating access to such notifications for the competent authorities under the relevant Union act,	

PUBLIC

Commission proposal	Drafting suggestions and Comments
transmitting or making available relevant information to other national authorities, where foreseen under Union or national law, supporting coordination among competent authorities in relation to reported incidents or information, or providing guidance or assistance to entities regarding notification procedures.	
(~~50b~~50c)The development and operation of national entry points may involve important costs for Member States, particularly where national reporting systems need to be built or existing ones need to be adapted. Further costs might be related to ensuring their cross-border interoperability. It is therefore important that, where applicable and foreseen in the relevant instruments, such activities are financially supported through relevant Union funding instruments, such as the Digital Europe Programme, the European Structural and Investment Funds and other relevant Union funding programmes.	
(51) **It is important to support the further harmonisation of incident**~~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~~**and reporting, including by working** on the **exchange and interoperability of information regarding incident reporting. For this purpose and in cooperation withhe**~~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**, the Cooperation Group and** ~~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,~~	LV (Drafting suggestions): (51) **It is important to support the further harmonisation of incident**~~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~~**and reporting, including by working** on the **exchange and interoperability of information regarding incident reporting. For this purpose and in cooperation withhe**~~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**, the NIS Cooperation Group and** ~~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~~

PUBLIC

Commission proposal	Drafting suggestions and Comments
ENISA should **develop guidelines to foster the harmonisation of incident notifications**~~take all necessary corrective measures, followed by a reassessment by the Commission~~.	~~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 **develop guidelines to foster the harmonisation of incident notifications**~~take all necessary corrective measures, followed by a reassessment by the Commission~~.
~~(52) To ensure the continuity and interoperability with existing national technical solutions that facilitate incident reporting, to the extent feasible, ENISA should take into account such national technical solutions when developing the specifications on the technical, operational and organisational measures necessary to establish, maintain and securely operate the single-entry point. Further, ENISA should consider technical protocols and tools such as application programming interfaces and machine-readable standards that enable entities to integrate reporting obligations into business processes, and authorities to connect the single-entry point with their national reporting systems.~~	
~~(53) To ensure that the single-entry point enables the relevant entities to submit the type of information and the format required under the relevant Union legal acts, ENISA should consult the Commission and the competent authorities under those acts. Where a Union legal act is not fully harmonized regarding the type of information and the format of notifications, Member States should inform ENISA about their national provisions.~~	
(54) Based on Regulation (EU) 2022/2554, the financial sector has been at the forefront in implementing a harmonised, comprehensive and effective framework, including with regard to incident reporting. In order to simplify compliance, it is appropriate to align the incident reporting framework established under Regulation (EU) 2022/2554 with the **national entry**~~single-entry~~ point, while ensuring continuity and stability of the existing reporting framework, and considering that the **national entry**~~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	CZ (Drafting suggestions): 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 national single-entry point, while ensuring continuity and stability of the existing reporting

Commission proposal	Drafting suggestions and Comments
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 **national entry**~~single-entry~~ point under Directive (EU) 2022/2555, Directive (EU) 2022/2557 or Regulation (EU) 2016/679, where appropriate. For this purpose, **Member States**~~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.	framework, and considering that the national 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 national single-entry point under Directive (EU) 2022/2555, Directive (EU) 2022/2557 or Regulation (EU) 2016/679, where appropriate. **The NIS2 reporting templates reflect the experience, lessons learned and best practices derived from the implementation of Regulation (EU) 2022/2554.** For this purpose, the Commission should take due account of the regulatory technical standards adopted pursuant to Regulation (EU) 2022/2554 **and the reporting templates developed under Directive (EU) 2022/2555 (NIS2),**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. CZ (Comments): CZ: CZ proposes this amendment to ensure that, alongside the experience and best practices derived from the implementation of Regulation (EU) 2022/2554 (DORA), the newly developed NIS2 common notification template by the NIS Cooperation Group as a key step in harmonization of

Commission proposal	Drafting suggestions and Comments
	incident notifications that will be shortly formally adopted by the Commission´s implementing act is also properly reflected. This is particularly relevant as the NIS2 common notification template was originally developed taking inspiration from and building upon the DORA reporting templates and related reporting requirements. Reflecting both DORA and the NIS2 common notification template would therefore support further harmonisation of incident reporting requirements and promote coherence across Union reporting frameworks.
(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 **national entry**~~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, **while remaining under the control of Member States,** should the Member States decide to make use of this additional feature.	
(56) To ensure that incident reporting is carried out via the **national entry**~~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 **national entry**~~single-entry~~ point should start being used for the purpose of reporting under those acts within **30**~~18~~ months from the entry into force of this Regulation. **Any new amendment to other Union legal acts or new proposals for Union legal acts should establish**~~When the Commission initiates the mechanisms of the notice delaying~~ the date **when national**~~of application to 24 months from the~~ entry **point**~~into force of the Regulation, the corresponding provisions of Directive (EU) 2022/2555, Regulation (EU) 910/2014, Regulation (EU) 2022/2554 and Directive~~	LV (Comments): LV sees that it would be valuable to keep reference that deadline for the obligation to report via the national entry point could be extended by 6 months if deemed necessary to keep flexibility as not all Member States have established national entry points that not only will have to be developed but also tested. Moreover, the guidelines by ENISA on technical, operational and organisational measures (Article 23b(4)) for national entry points and on harmonization of incident notifications (Article 23c(3)) should be developed

Commission proposal	Drafting suggestions and Comments
~~(EU) 2022/2557~~ should **be used for**~~continue to apply for the purpose of meeting the~~ reporting **incidents or related events.** ~~obligations laid down in the provisions.~~	before Regulation enters into force OR the 30 months deadline for the obligation to report via the national entry point should only start after work on these guidelines is concluded. If the development or adaptation of national entry points and work on these guidelines would occur in parallel, that would only create uncertainty for Member States and would hamper the overall process, including meeting the deadline.
(57) In the exceptional event that a technical impossibility prevents the submission of incident notifications using the **national entry**~~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 **and the European Data Protection Board were**~~was~~ consulted in accordance with Article **42**~~42(1)~~ of Regulation (EU) 2018/1725 of the European Parliament and of the Council[18], and delivered **their joint**~~its~~ opinion on **10 February 2026**~~[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]~~. 18 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).	
(59) Regulation (EU) 2019/1150 establishes a targeted set of mandatory rules at Union level to ensure a fair, predictable, sustainable and trusted online business environment within the internal market. Regulation (EU)	IT (Comments):

Commission proposal	Drafting suggestions and Comments
2022/2065 and Regulation (EU) 2022/1925 provide a comprehensive regulatory framework for a safe, predictable and trusted online environments for all end-users of online services, and establish a level playing field for businesses in digital markets. In the interest of simplification of Union legislation in the field of online intermediation services and online platforms, and given that the objectives and material provisions of the Platform-to-Business Regulation are largely covered by the Digital Services Act and the Digital Markets Act, **several provisions of** Regulation (EU) **2019/1150**~~2019/1050~~ should be **deleted**~~repealed~~. Regulation (EU) 2022/2065 and Regulation (EU) 2022/1925 contribute to a fully harmonised regulatory framework for digital services and digital markets, by approximating national measures concerning the requirements for providers of intermediary services and the contestability and fairness of core platforms services provided by gatekeepers. For purposes of legal certainty **and for purposes of keeping the necessary level of protection for business users**, selected definitions in Article 2, ~~the~~ provisions **on terms and conditions in Article 3,** on restrictions and suspensions in Article 4, **on ranking in Article 5, and on differentiated treatment in Article 7,**~~as well as~~ on the internal complaint-handling system in Article 11**, as well as provisions in** ~~of Regulation (EU) 2019/1150 that are cross-referenced by other legal acts, in particular Directive (EU) 2023/2831 on improving working conditions in platform work, and~~ Article 15 ensuring enforcement~~, will temporarily remain in application until the original acts are amended~~ **and in Article 18(1) mandating the Commission to evaluate that Regulation are maintained**.	ITALY acknowledges and supports the Commission's efforts to reduce administrative burdens by avoiding potential overlaps between the P2B Regulation and other EU legislation. Addressing those parts of the P2B Regulation that clearly overlap with other EU legislation, primarily the DSA and DMA, will simplify the applicable rules and increase legal certainty for businesses, making the EU more competitive and commercially attractive. However, the Commission's proposal to repeal the entire P2B Regulation, with only limited and time-gated exceptions, will lead to loopholes and weaknesses in the legal protections, that are disproportionate to the marginal reduction in administrative burdens that would be achieved. While simplification efforts are supported, they should not come at the expense of the essential safeguards for European SMEs. Such safeguards include transparency regarding general terms and conditions, predictability in the event of changes, insight into rankings and clear procedures in the event of restriction or suspension. Their importance is reflected in the growing awareness of P2B rights and the increasing number of complaints concerning non-compliant platforms. The P2B Regulation contributes to the proper functioning of the single market by harmonising rules that afford transparency, fairness and effective redress tools to business users of platforms. In this regard, it has a specific approach and constitutes a first step toward establishing a comprehensive EU legal framework for online intermediaries. The DMA and DSA have different targets and scopes. They do not provide the same substantive obligations, nor do they offer the subsidiarity and proximity afforded by the P2B Regulation. Therefore, they cannot offer the same level of protection in such situations.

Commission proposal	Drafting suggestions and Comments
	Simplification efforts should lead to a genuine reduction in regulatory burden. ITALY believes that targeted adjustments to remove clear overlaps with the DSA and DMA would streamline the regulatory framework without dismantling essential protections. The limited administrative burden associated with the remaining P2B provisions would be proportionate in light of the legal certainty and protection they afford SMEs. Therefore, ITALY proposes to maintaining certain essential P2B provisions on a permanent basis, while repealing the rest. This partial repeal reflects a more targeted and proportionate approach to reduce complexity and administrative burdens within the P2B Regulation while preserving the necessary protection this legislation offers for businesses, in particular SMEs. ITALY believes certain P2B provisions to be essential safeguards for SMEs, we therefore propose to maintaining them on a permanent basis, and not only until 31 December 2032, or , alternatevely, be repealed only only after a specific review has been carried out in accordance with Article 18 of the current P2B Regulation.
(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.	
(61) The amendments to Regulation (EU) 2016/679 and Regulation (EU) 2018/1725 are based on Article 16 TFEU. The amendments to Directive 2002/58/EC are based on Article 16 TFEU and Article 114 TFEU. All other amendments are based on Article 114 TFEU.	

PUBLIC

PUBLIC

Commission proposal	Drafting suggestions and Comments
(62) The reasons that led the European Parliament and the Council to adopt those provisions of Regulation (EU) 2022/868, Regulation (EU) 2018/1807, and Directive 2019/1024 which are being re-enacted in the present regulation remain valid.	
HAVE ADOPTED THIS REGULATION:	
Article 1 **Amendments to Regulation (EU) 2023/2854**	
Regulation (EU) 2023/2854 is amended as follows:	
1. Article 1 is amended as follows:	
(-a) in paragraph 1 point (c) is replaced by the following: **'(c) the making available of data by data holders to public sector bodies, the Commission, the European Central Bank and Union bodies, where there is the need for those data for the performance of a specific task carried out in the public interest;'**	
(a) in paragraph 1, the following points are inserted:	
'(ea) voluntary registration of data intermediation services;	
(eb) voluntary registration of entities which collect and process data made available for altruistic purposes;	
(ec) the establishment of a European Data Innovation Board;	
(ed) data localisation requirements ~~and the availability of data to competent authorities;~~	
(ee) the re-use of certain data and documents held by public sector bodies or by certain public undertakings, and of research data.;'	
(b) in paragraph 2, the following points are added:	
~~'(g) Chapter VIIa applies to personal and non-personal data;~~	
(h) Chapter VIIb applies to any non-personal data;	
~~(i) Chapter VIIc applies to personal and non-personal data, namely the following:~~	
~~(i) documents held by public sector bodies of Member States as referred~~	

Commission proposal	Drafting suggestions and Comments
~~(1) to in Article 32i(1), point (a) or by public undertakings as referred~~	
~~(2) to in Article 32i(1), point (b);~~	
~~(ii) research data as referred to in Article 32i(1), point (c);~~	
~~(iii) certain categories of protected data as referred to in Article 32i(1), point (a).'~~	
(c) in paragraph 3, point (g) is replaced by the following:	
'(g) participants in data spaces.;	
(ca) in paragraph (5) the following subparagraph is added:	
~~gb~~ **'The rules set out in Chapters VIIa and VIIc do not create a legal basis for the processing of personal data.''**	FI (Comments): FI can support this proposal.
(d) paragraph 7 is deleted.	
(e) the following paragraphs 11, 12 and 13 are added:	
'11. Chapter VIIb of this Regulation is without prejudice to laws, regulations, and administrative provisions that relate to the internal organisation of Member States and that allocate, among public authorities and bodies governed by public law, powers and responsibilities for the processing of data without contractual remuneration of private parties, as well as to laws, regulations, and administrative provisions of Member States that provide for the implementation of such powers and responsibilities.	
12. Where sector-specific Union or national law requires public sector bodies, data intermediation services providers or recognised data altruism organisations to comply with specific additional technical, administrative or organisational requirements that relate to Chapters VIIa and VIIb, including through an authorisation or certification regime, those provisions of that sector-specific Union or national law shall also apply. Any such specific additional requirements shall be non-discriminatory, proportionate and objectively justified.'	
13. With regards to data and documents in scope of Section II of Chapter VIIc, Chapter VIIc of this Regulation **establishes a set of minimum rules**	PL

PUBLIC

Commission proposal	Drafting suggestions and Comments
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.''	(Drafting suggestions): 13. With regards to data and documents in scope of Section II 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 **establish pracitical arrangements and** adopt more detailed or stricter rules, provided that those **arrangements and** rules allow for more extensive re-use of data and documents. **In particular Member States may adopt such arrangements and rules allowing for more extensive re-use with regards to conditions for re-use, principles governing charging and procedure for re-quests for re-use**.
2. Article 2 is amended as follows:	
(a) the following points (4a), (4b) and (4c) are inserted:	
'(4a) 'consent' means consent as defined in Article 4, point (11), of Regulation (EU) 2016/679;	CZ (Comments): CZ: CZ requests verification that the newly defined term does not conflict with Article 10(12) of the Data Act, where consent is used in connection with decisions by dispute settlement bodies and is not related to the processing of personal data. The term is also used elsewhere in the recitals. „12. The decision of a dispute settlement body shall be binding on the parties only if the parties have explicitly consented to its binding nature prior to the start of the dispute settlement proceedings. "
(4b) 'permission' **in the context of Chapters VIIa and VIIc** means giving data users the right to the processing of non-personal data;	
~~(4c) 'access' means data use, in accordance with specific technical, legal or organisational requirements, without necessarily implying the transmission or downloading of data;~~	
(b) point (10) is replaced by the following:	
~~4cb.~~ **'(10) 'data intermediation service' means a service which aims to establish relationships of an economic character for the purposes of data**	

PUBLIC

Commission proposal	Drafting suggestions and Comments
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 :	
~~4cc.~~ **(a) does not have as their main purpose the intermediation of copyright-protected content;**	EE (Drafting suggestions): (a) does not have as their ~~**main**~~ purpose ~~**the intermediation of copyright-protected content**~~ to intermediate the content protected by copyright or related rights. EE (Comments): In the current phrasing the provision is hard to apply in practise, since it means that we should have solutions, to establish what exactly qualifies as "main purpose" and how should regulators determine when copyright intermediation becomes the primary activity. It also raises a question whether the exclusion applies if copyright content intermediation is secondary or incidental. Therefore, we suggest avoiding ambiguous thresholds like "main purpose". We are proposing clearer phrasing that aligns with terminology used in EU copyright law.
~~4cd.~~ **(b) is not jointly procured by several legal persons for exclusive use among them; '**	EE (Comments): **We suggest additional point c:** **are not data sharing services offered by public sector bodies;** This is the part of the current definition as well, and there is no need to take it away. The data intermediation service regulation in the relevant chapter should focus on the private sector bodies, not public. Otherwise, it would create additional unneccessary burdens on MS.

Commission proposal	Drafting suggestions and Comments
(b) point (13) is replaced by the following:	
'(13) 'data holder' means a natural or legal person that has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation adopted in accordance with Union law, to use or make available data, including, where contractually agreed, product data or related service data, which it has retrieved or generated during the provision of a related service;'	EE (Drafting suggestions): '(13) 'data holder' means a natural or legal person that has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation adopted in accordance with Union law, to ~~use or~~ make available data, including, where contractually agreed, product data or related service data, which it has retrieved or generated during the provision of a related service; EE (Comments): "use or make available" includes also data recipients, i.e. everyone who can use the data but do not have the right or obligation to make it available. As the importance of a "data holder" is in making data available, the definition should concentrate on this aspect – the "right to use" the data is not relevant in data holder´s context and can be removed.
(ba) point (28) is replaced by the following: **'(28) 'public sector body' means the State, national, regional or local authorities of the Member States and bodies governed by public law of the Member States, or associations formed by one or more such authorities or one or more such bodies.**	
(c) the following points (28a) and (28b) are inserted:	
'(28a) 'bodies governed by public law' means bodies ~~as defined in Article 2(1)(4) of Directive 2014/24/EU.~~ that have all of the following characteristics:	
(a) they are established for the specific purpose of meeting needs in the general interest, not having an industrial or commercial character;	
(b) they have legal personality;	
(c) they are financed, for the most part by the State**, national**, regional or local authorities, or by other bodies governed by public law; or are subject to	

Commission proposal	Drafting suggestions and Comments
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**, national**, regional or local authorities, or by other bodies governed by public law;	
(28b) 'public undertaking' means any undertaking ~~as defined in Article 4(2) of Directive 2014/25/EU~~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;;'	
(e)~~(d)~~ the following **point (38a) is**~~points (38a) and (38b) are~~ inserted:	
~~'(38a) 'data intermediation service' means a service which aims to establish relationships of an economic character for the purposes of data sharing between an undetermined number of data subjects or data holders and data users, through technical, legal or other means, including for the purpose of exercising the rights of data subjects in relation to personal data, and which:~~	
~~(1) do not have as their main purpose the intermediation of copyright-protected content;~~	
~~(2) are not jointly procured by several legal persons for exclusive use among them;~~	
(**38a**~~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	

PUBLIC

PUBLIC

Commission proposal	Drafting suggestions and Comments
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;	
(ea) point (39) is deleted.	
(f) point (42) is amended as follows:	
~~38bc.~~ **(42) 'common specifications' means a set of technical requirements, other than a standard, that provides means of complying with certain requirements and obligations established under this Regulation.'**	
(e) the following points (44) to (**62**~~63~~) are added:	
'(44) 'medium-sized enterprise' means a medium-sized enterprise as defined in **point**~~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 **point**~~Article~~ 2 of the Annex to Commission Recommendation (EU) 2025/1099;	
(46) 'university' means **any**~~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:	CZ (Comments): CZ: CZ requests verification that the newly defined term does not conflict with Articles 2(42) and 19(1)c) of the Data Act and newly added point 53 to Artcile 2 ('certain categories of protected data'), given the fact that the new defition of document does not allow it to be in a digital format LU (Comments):

Commission proposal	Drafting suggestions and Comments
	As already mentionned in our previous comments, the extension of the scope of the DGA regarding 'documents' creates legal uncertainty. In our view it does not make sense for a regime that was designed for the digital sphere only. How would this work in practice?
(a) any content that is non-digital whatever its medium (paper or as a sound, visual or audiovisual recording); or	EE (Drafting suggestions): (a) any content ~~**that is non-digital**~~ whatever its medium (paper or as a sound, visual or audiovisual recording); or EE (Comments): The definition of document excluding digital forms is confusing as: 1) it opposes the common definition of document in archiving, information management, the Tromso convention etc. 2) it creates a lot of confusion in parts that have been copy-paste'd from previous acts (for example Open Data Directive) and which do not make sense with the new definition: a) the requirement to publish HVD documents in machine readable formats; b) definition of 'common specification' in the Data Act: ".. a document, other than a standard, containing technical solutions providing a means to comply with certain requirements and obligations established under this Regulation". As such all common specifications must be non-digital)
(b) any part of such content;	
(49) 'dynamic data' **in the context of Chapter VIIc** 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;	

PUBLIC

Commission proposal	Drafting suggestions and Comments
(50) '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 **or**~~and~~ results;	
(51) 're-use' means the use by natural ~~persons~~ or legal **persons of data or**~~entities of~~ documents held by:	
(a) public sector bodies, for commercial or non-commercial purposes other than the initial purpose within the public task for which the **data or** documents were produced, except for the exchange of **data or** 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 **data or** documents were produced, except for the exchange of **data or** documents between public undertakings and public sector bodies purely in pursuit of the public tasks of public sector bodies;	
(52) '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;	EE (Drafting suggestions): (52) 'high-value datasets' means data ~~and documents the re-use of~~ which is associated with important benefits for society, **including impact on smaller Member States,** 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 that data ~~and documents~~. **The disclosure of datasets which could jeopardise Union´s or Member States internal or external security must not be made publicly available;** EE (Comments):

Commission proposal	Drafting suggestions and Comments
	The disclosure of datasets which would jeopardise internal or external security must not be made publicly available. For example, data to related to energy. Especially, considering current geo-political situations. This principle should be well established in this act and HVD definition. When establishing additional categories of high-value datasets, one must take into account the impact on smaller Member States. Any further expansion should therefore be based on clear and reasoned impact assessments, considering not only the social and economic benefits of data re-use, but also the potential risks to security, fundamental rights and the competitiveness of undertakings.
(53) 'certain categories of protected data' means data and documents held by public sector bodies which are protected on the grounds of	EE (Drafting suggestions): 'certain categories of protected data' means data ~~and documents~~ held by public sector bodies which are protected on the grounds of EE (Comments): It creates confusion if data means data and documents at the same time. Since data in this act is digital content and documents are non-digital. Therefore, the current definition will mean that digital content means digital and non-digital at the same time.
(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;	
(54) '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,	

Commission proposal	Drafting suggestions and Comments
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;	
(55) '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;	
(56) '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;	
(57) '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 **data** ~~documents~~;	
(58) '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;	EE (Comments): Point 43 of the Data Act defines 'harmonised standard' as per 1025/2012 EU. Thus, we suggest that the definition of 'formal open standard' should clarify the difference between a harmonised and formal open standard. This would help a lot in practical implementation.
(59) '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;	
(60) '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	

PUBLIC

PUBLIC

Commission proposal	Drafting suggestions and Comments
territory of a specific Member State or hinders the processing of data in any other Member State;	
(61) '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;	
(**62**~~61~~) 'pseudonymisation' means pseudonymisation as referred to under Article 4(5) of Regulation (EU) 2016/679.'	CZ (Drafting suggestions): New point (63): **(63) '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;** CZ (Comments): CZ: Since the text frequently uses the term 'data user', which is defined under the DGA, and since the DGA is to be repealed, CZ considers it important to maintain this definition in the Digital Omnibus.
3. in Article 4, paragraph 8 is replaced by the following:	
'8. ~~**In exceptional circumstances,**~~ **Where**~~where~~ the data holder who is a trade secret holder is able to demonstrate that, despite the technical and organisational measures taken by the user pursuant to paragraph 6 of this Article, it is ~~highly~~ likely to suffer serious economic damage from the disclosure of trade secrets or that the disclosure of trade secrets to the user poses a high risk of unlawful acquisition, use, or disclosure to third country entities, or entities established in the Union under the direct or indirect control of such entities, which are subject to jurisdictions offering weaker or non-equivalent protection compared to that under Union law, that data holder may refuse ~~on a case-by-case basis~~ a request for access to the specific data in question. That demonstration ~~may be~~shall be duly substantiated on the	CZ (Comments): CZ: CZ considers it crucial that exemptions are limited to justifiable situations, and that the intention of the Data Act to support the creation of a data economy is preserved. CZ is conservative towards significant changes that go beyond simplification. Therefore, CZ has already expressed its reservations about the new exemption introduced by the Commission in the Digital Omnibus for disclosure to third countries, fearing it might be misused in situations beyond users' control (e.g. if a user employs third-country nationals or uses software unauthorised by the data holder). Nevertheless, CZ

Commission proposal	Drafting suggestions and Comments
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. **The Commission shall issue guidelines, in consultation with the European Data Innovation Board (EDIB), on the application of this paragraph, such as the assessment of serious economic damage, and the enforceability of trade secrets protection in third countries.**~~;'~~	recognises the complexity of the negotiation process and, in in a spirit of finding a compromise, can accept the text as it stands without further changes weakening the delicate balance between data protection and users' access rights. FR (Drafting suggestions): '8. **Trade secrets shall be preserved and do not have to be disclosed. Data from which trade secrets may be retrieved shall not be subject to disclosure. Pursuant to Regulation (UE) 2023/2854, unless the data holder and the user have reached an agreement on necessary measures to preserve their confidentiality and implemented those.** ~~In exceptional circumstances~~, Where~~where~~ the data holder who is a trade secret holder is able to demonstrate that, despite the technical and organisational measures taken by the user pursuant to paragraph 6 of this Article, it is ~~highly~~ likely to suffer serious economic damage from the disclosure of trade secrets or that the disclosure of trade secrets to the user poses a high risk of unlawful acquisition, use, or disclosure to third country entities, or entities established in the Union under the direct or indirect control of such entities, which are subject to jurisdictions offering weaker or non-equivalent protection compared to that under Union law, that data holder may refuse ~~on a case-by-case basis~~ a request for access to the specific data in question. That demonstration ~~may be~~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.

PUBLIC

Commission proposal	Drafting suggestions and Comments
	Circumstances that invoke the right to refuse a request for access may also arise if the disclosure of such data would increase cybersecurity risks affecting the security or resilience of the shared data, or the data holder's systems or connected products. The Commission shall issue guidelines, in consultation with the European Data Innovation Board (EDIB), on the application of this paragraph, such as the assessment of serious economic damage, and the enforceability of trade secrets protection in third countries.' FR (Comments): Rappel du principe de protection du secret de affaires. Proposition d'une clarification du Data Act afin de garantir que les obligations de partage de données ne conduisent pas à accroître les risques de cybersécurité.
4. in Article 5, paragraph 11 is replaced by the following:	
'11. ~~In exceptional circumstances,~~ **Where**~~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 ~~may be~~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	CZ (Comments): CZ: CZ considers it crucial that exemptions are limited to justifiable situations, and that the intention of the Data Act to support the creation of a data economy is preserved. CZ is conservative towards significant changes that go beyond simplification. Therefore, CZ has already expressed its reservations about the new exemption introduced by the Commission in the Digital Omnibus for disclosure to third countries, fearing it might be misused in situations beyond users' control (e.g. if a user employs third-country nationals or uses software unauthorised by the data holder). Nevertheless, CZ recognises the complexity of the negotiation process and, in in a spirit of finding a compromise, can accept the text as it stands without further changes

Commission proposal	Drafting suggestions and Comments
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. **The Commission shall issue guidelines, in consultation with the European Data Innovation Board (EDIB), on the application of this paragraph, such as the assessment of serious economic damage, and the enforceability of trade secrets protection in third countries.'**~~;~~	weakening the delicate balance between data protection and users' access rights. FR (Drafting suggestions): '11. **Trade secrets shall be preserved and do not have to be disclosed. Data from which trade secrets may be retrieved shall not be subject to disclosure. Pursuant to Regulation (UE) 2023/2854, unless the data holder and the user have reached an agreement on necessary measures to preserve their confidentiality and implemented those.** ~~In exceptional circumstances~~, Where~~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 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 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 be~~ 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. **Circumstances that invoke the right to refuse a request for access may also arise if the disclosure of such data would increase cybersecurity risks affecting the security or resilience of the shared data, or the data holder's systems or connected products.**

Commission proposal	Drafting suggestions and Comments
	The Commission shall issue guidelines, in consultation with the European Data Innovation Board (EDIB), on the application of this paragraph, such as the assessment of serious economic damage, and the enforceability of trade secrets protection in third countries.' FR (Comments): Rappel du principe de protection du secret des affaires. Proposition d'une clarification du Data Act afin de garantir que les obligations de partage de données ne conduisent pas à accroître les risques de cybersécurité.
4a. in Article 11 paragraph 1 is replaced by the following:	
~~11b.~~ **'(1) A data holder may apply appropriate technical protection measures, including 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 with Union law. Users, third parties and data recipients shall not alter or remove such technical protection measures unless agreed by the data holder.'**	
5. the title of Chapter V is replaced by the following:	
'MAKING DATA AVAILABLE TO PUBLIC SECTOR BODIES, THE COMMISSION, THE EUROPEAN CENTRAL BANK AND UNION BODIES ON THE BASIS OF A PUBLIC EMERGENCY;'	
6. Articles 14 and 15 are deleted;	
7. the following Article 15a is inserted:	
'Article 15a	EE

Commission proposal	Drafting suggestions and Comments
	(Comments): Estonia supports amending the EU Data Act to allow public authorities to request data from the private sector in situations of public emergency, but stresses that such powers must be exercised with full respect for fundamental rights and on the basis of clear and harmonised criteria across Member States. Estonia's key concerns are the primary use of non-personal data, the systematic consideration of privacy-enhancing technologies (including pseudonymisation) when personal data is necessary, and avoiding divergent national interpretations of what constitutes a public emergency.
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 **the**~~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.	CZ (Drafting suggestions): 1. Where a public sector body, the Commission, the European Central Bank or a Union body demonstrates the need **limited in time and scope** to use certain data to carry out its statutory duties in the public interest when responding to, 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. CZ (Comments): CZ: CZ suggests keeping the limitation of the (exceptional) need as it is in Art. 15(1).

Commission proposal	Drafting suggestions and Comments
	EE (Drafting suggestions): 1. Where a public sector body, the Commission, the European Central Bank or a Union body demonstrates ~~the~~ **an exceptional** need to use certain data to carry out its statutory duties in the public interest when responding to, 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. EE (Comments): The addition exceptional need is important to us. Not every need consitutes public emergency. LU (Comments): There is however further need to clarify this provision since the last sentence of paragraph 1 is too ambiguous. It will, in practice, not be possible for competent authorities to assess the request since the scope of the request is not clear. Does “in relation to” mean “responding to” AND “supporting the recovery from”? Or can it even be outside of these two scopes? Can these requests contain personal data? Can these requests be made to microentreprises and small enterprises? We consider that this provision entails too much legal uncertainty.

Commission proposal	Drafting suggestions and Comments
	Additionally, if requests for official statistics are considered as its own category of requests, Article 18(2) of the DA needs to be adapted in the sense that an additional deadline to respond to requests needs to be foreseen. We consider that this should be clarified.
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 **respond to**~~address~~ the public emergency, personal data may also be requested and, ~~where possible~~, made available in **pseudonymised**~~pseudonymized~~ form, subject to appropriate technical and organisational measures to ensure their protection.	EE (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 respond to ~~address~~ the public emergency, personal data may also be requested and, where possible, made available in pseudonymised~~pseudonymized~~ **or with the use of equivalent privacy-enhancing technologies** form, subject to appropriate technical and organisational measures to ensure their protection. EE (Comments): Requests should primarily concern non-personal data, and where personal data is necessary, privacy-enhancing technologies, including pseudonymisation, should be used. This should always be the case. Currently, the provision is allowing only pseudonymisation, but it might not be justified or necessary restriction considering fast development of technologies and innovation.
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	

Commission proposal	Drafting suggestions and Comments
the recovery from a public emergency. Such requests shall not be made to microenterprises and small enterprises.;'	
8. in Article 16, paragraph 2 is replaced by the following:	
'2. This Chapter shall not apply to activities carried out by public sector bodies, the Commission, the European Central Bank or Union bodies relating to the prevention, investigation, detection or prosecution of criminal or administrative offences or the execution of criminal penalties, or to customs or taxation administration. This Chapter does not affect Union or national law governing such activities.'	
9. Article 17 is amended as follows:	
(a) paragraph 1 is amended as follows:	
(i) the introductory wording is replaced by the following:	
'When requesting data pursuant to Article 15a, a public sector body, the Commission, the European Central Bank or a Union body shall:;'	
(ii) points (b) and (c) are replaced by the following:	
'(b) demonstrate that the conditions **for the** ~~to make a~~ request under Article 15a are met;	
(c) explain the purpose of the request, the intended use of the data requested, including, where applicable, by a third party in accordance with paragraph 4 of this Article, the duration of that use, and, where relevant, how the processing of personal data is to address the public emergency;;'	
(b) paragraph 2 is amended as follows:	
(i) point (c) is replaced by the following:	
'(c) be proportionate to the public emergency and duly justified, regarding the granularity and volume of the data requested and the frequency of access to the data requested;;'	
(ii) point (e) is deleted.;	FI (Comments): FI supports reinstating Article 17(2)(e), in line with the EDPB/EDPS joint opinion. FI states that retaining pseudonymization and the priority of non-personal data is crucial to the current high level of personal data protection.

PUBLIC

Commission proposal	Drafting suggestions and Comments
	However, this is not a redline.
(iii) Point (i) is replaced by the following:	
~~(iib)~~ **'(i)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 body is established or to the EDPS where the request is made by the Commission, the European Central Bank or a Union body.'**	
(ba) paragraph 4 is replaced by the following:	
~~(iid)~~ **'Paragraph 3 of this Article does not preclude a public sector body, the Commission, the European Central Bank or a Union body to exchange data obtained pursuant to this Chapter with another public sector body or the Commission, the European Central Bank or a Union body in view of completing the tasks referred to in Article 15a, as specified in the request in accordance with paragraph 1, point (f), of this Article or to make the data available to a third party where it has delegated, by means of a publicly available agreement, technical inspections or other functions to that third party. The obligations on public sector bodies pursuant to Article 19, in particular safeguards to preserve the confidentiality of trade secrets, shall apply also to such third parties. Where a public sector body, the Commission, the European Central Bank or a Union body transmits or makes data available under this paragraph, it shall notify the data holder from whom the data was received without undue delay.'**	
(c) paragraphs 5 and 6 are deleted;	CZ (Drafting suggestions): (c) paragraph~~s~~ 5 ~~and 6 are~~ **is** deleted; CZ (Comments):

PUBLIC

Commission proposal	Drafting suggestions and Comments
	CZ: CZ cannot agree with the deletion of Article 17(6), which obliges the COM to prepare a model template for requests under Chapter V. CZ believes that such a move is contrary to simplification and that, it might burden businesses more if data requests look different each time. Harmonization of requests at EU level is therefore desirable.
10. Article 18 is amended as follows:	
(a) in paragraph 2, the introductory wording is replaced by the following:	
'2. Without prejudice to specific needs regarding the availability of data defined in Union or national law, a data holder may decline or seek the modification of a request to make data available under this Chapter without undue delay and, in any event, no later than five working days after the receipt of a request pursuant to Article 15a(2) and without undue delay and, in any event, no later than 30 working days after the receipt of a request pursuant to Article 15a(3), on any of the following grounds:;'	
(b) paragraph 5 is deleted;	
11. Article 19 is amended as follows:	
(a) in paragraph 1, the introductory wording is replaced by the following:	
'A public sector body, the Commission, the European Central Bank or a Union body receiving data pursuant to a request made under Article 15a shall:;'	
(aa) point (c) of paragraph 1 is replaced by the following:	
~~(ab)~~ **c) erase the data as soon as they are no longer necessary for the stated purpose and inform the data holder and individuals or organisations that received the data pursuant to Article 21(1) without undue delay that the data have been erased, unless archiving of the data is required in accordance with Union or national law on public access to information in the context of transparency obligations.'**	
(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	

Commission proposal	Drafting suggestions and Comments
person, the trade secret holder shall identify the data which are protected as trade secrets, including in the relevant metadata. The public sector body, the Commission, the European Central Bank or the Union body shall, prior to the disclosure of trade secrets, take all necessary and appropriate technical and organisational measures to preserve the confidentiality of the trade secrets, including, as appropriate, the use of model contractual terms, technical standards and the application of codes of conduct.;'	
12. Article 20 is replaced by the following:	
'Article 20	
Compensation for making data available under Chapter V	
1. Data holders shall make available data necessary to respond to a public emergency pursuant to Article 15a(2) free of charge. The public sector body, the Commission, the European Central Bank or the Union body that has received data shall provide public acknowledgement to the data holder if requested by the data holder.	
2. The data holder shall be entitled to fair compensation for making data available in compliance with a request made pursuant to Article 15a(3). Such compensation shall cover the technical and organisational costs incurred to comply with the request including, where applicable, the costs of anonymisation, pseudonymisation, aggregation and of technical adaptation, and a reasonable margin. Upon request of the public sector body, the Commission, the European Central Bank or the Union body, the data holder shall provide information on the basis for the calculation of the costs and the reasonable margin.	
3. By way of derogation from paragraph 1 of this Article, a data holder that is a microenterprise or small enterprise may claim compensation for making data available in response to a request under Article 15a(2), according to the conditions set in paragraph 2 of this Article.	
4. Data holders shall not be entitled to compensation for making data available in compliance with a request made pursuant to Article 15a(3), where the specific task carried out in the public interest is the production of official statistics and where the purchase of data is not allowed by national	

PUBLIC

Commission proposal	Drafting suggestions and Comments
law. Member States shall notify the Commission where the purchase of data for the production of official statistics is not allowed by national law.';'	
13. Article 21 is amended as follows:	
(a) the heading is replaced by the following:	
'Sharing of data obtained in the context of a public emergency with research organisations or statistical bodies;'	
(b) paragraph 5 is replaced by the following:	
'5. Where a public sector body, the Commission, the European Central Bank or a Union body intends to transmit or make data available under paragraph 1, it shall without undue delay notify the data holder from whom the data was received, stating the following:	
(a) the identity and contact details of the organisation or the individual receiving the data;	
(b) the purpose of the transmission or making available of the data;	
(c) the period for which the data is to be used ~~and the technical protection~~;	
(d) the **technical protection and** organisational measures taken, including where personal data or trade secrets are involved.;'	
14. The following Article 22a is inserted before Chapter VI:	
'Article 22a	
Right to lodge a complaint	
Where a dispute arises concerning a request for data under Article 15a, including its refusal, modification, the level of compensation, or the transmission or making available of data, the data holder, the public sector body, the Commission, the European Central Bank or the Union body may lodge a complaint with the competent authority, designated pursuant to Article 37, of the Member State where the data holder is established.;'	
15. in Article 31, the following paragraphs 1a**, 1b, and 1c** ~~and 1b~~ are inserted:	
'1a. The obligations laid down in Chapter VI, with the exception of Article 29, and in Article 34 shall not apply to data processing services other	SK (Comments):

PUBLIC

Commission proposal	Drafting suggestions and Comments
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.	Slovakia requests that these exemptions remain narrowly defined and time-limited. They should not undermine switching, interoperability, data portability or the removal of switching and egress charges, in particular where public sector customers depend on legacy or customised cloud services. Providers relying on the exemption should be able to substantiate that the relevant service is genuinely customised.
The provider of such data processing services shall not be required to renegotiate or amend a contract for the provision of those services before its expiry if that contract was concluded before or on 12 September 2025. Any contractual provision contained in that contract that is contrary to Article 29(1), (2), or (3) shall be considered null and void.	
~~1b. A provider of a data processing service may include provisions on proportionate early termination penalties in a contract of fixed duration on the provision of data processing services other than those referred to in Article 30(1).~~	
Where the provider of data processing service is a small and medium-sized enterprise or a small mid-cap, the obligations laid down in Chapter VI, with the exception of Article 29, and in Article 34 shall not apply to data processing services other than those referred to in Article 30(1), if the provision of such services is based on a contract concluded before or on 12 September 2025.	
Where the provider of a data processing service is a small and medium-sized enterprise or a small mid-cap, the provider shall not be required to renegotiate or amend a contract for the provision of a data processing service other than those referred to in Article 30(1) before its expiry 1 if that contract was concluded before or on 12 September 2025. Any contractual provision contained in that contract that is contrary to Article 29(1), (2), or (3) shall be considered null and void.~~;~~	
1c. 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.';'	FR (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
	Addition of a 1d. "The Commission shall issue guidelines, in consultation with the European Data Innovation Board (EDIB), on the application of these provisions. FR (Comments): Les guidelines permettraient de répondre aux demande de précisions qui proviendront des acteurs du marché
16. Article 32 is amended as follows:	
(a) paragraph 1 and 2 are replaced by the following:	
'1. Providers of data processing services, the public sector body making available data or documents in accordance with Chapter VIIc Section 3, the natural or legal person to which the right to re-use data or documents in accordance with Chapter VIIc Section 3 was granted, a data intermediation services provider or a recognised data altruism organisation shall take all adequate technical, organisational and legal measures, including contracts, in order to prevent international and third-country governmental access and transfer of non-personal data held in the Union where such transfer or access would create a conflict with Union law or with the national law of the relevant Member State, **including mandatory criminal law provisions of Member States, in particular those protecting their essential security interests within the meaning of Article 4(2) of the Treaty on European Union,** without prejudice to paragraph 2 or 3.	
2. Any decision or judgment of a third-country court or tribunal and any decision of a third-country administrative authority requiring a provider of data processing services, the public sector body making available data or documents in accordance with Chapter VIIc Section 3, the natural or legal person to which the right to re-use data or documents in accordance with Chapter VIIc Section 3 was granted, a data intermediation services provider or a recognised data altruism organisation to transfer or give access to non-personal data falling within the scope of this Regulation held in the Union shall be recognised or enforceable in any manner only if based on an	

PUBLIC

Commission proposal	Drafting suggestions and Comments
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:';'	CZ (Drafting suggestions): **(ba) in paragraph 3, third subparagraph is replaced by the following:** '**By [P.O. insert the date of entry into force of this Regulation plus 6 months] the Commission shall develop guidelines for assessment of whether the conditions laid down in the first subparagraph of this paragraph are met.** The EDIB referred to in Article 42 shall advise and assist the Commission in developing such guidelines ~~**on the assessment of whether the conditions laid down in the first subparagraph of this paragraph are met**~~.' CZ (Comments): CZ: Already within the Data Act, CZ is facing implementation obstacles regarding the assessment of the conditions for third-countries governmental requests in Chapter VII, given that the addressee of the decision or judgment may ask the opinion of the relevant national body or authority. The Omnibus further expands the scope of Chapter VII to include new entities transferred from the DGA (the DGA does not grant these entities the right to request the opinion of national bodies). At the same time, the original third subparagraph already indicates that the Commission should develop guidelines on the assessment of the conditions for third-country governments' requests. The suggested modification clarifies this task. CZ believes that such guidance is

Commission proposal	Drafting suggestions and Comments
	essential for the harmonisation, effective implementation and enforcement of the Data Act.
(c) paragraphs 4 and 5 are replaced by the following:	
'4. If the conditions laid down in paragraph 2 or 3 are met, the provider of data processing services, the public sector body making available data or documents in accordance with Chapter VIIc Section 3, the natural or legal person to which the right to re-use data or documents in accordance with Chapter VIIc Section 3 was granted, the data intermediation services provider or the recognised data altruism organisation shall provide the minimum amount of data permissible in response to a request, on the basis of the reasonable interpretation of that request by the provider or relevant national body or authority referred to in paragraph 3, second subparagraph.	
5. The provider of data processing services, the public sector body making available data or documents in accordance with Chapter VIIc Section 3, the natural or legal person to which the right to re-use data or documents in accordance with Chapter VIIc Section 3 was granted, the data intermediation services provider or the recognised data altruism organisation shall inform the natural or legal person whose rights and interests might be affected about the existence of a request of a third-country authority to access its data before complying with that request, except where the request serves law enforcement purposes and for as long as this is necessary to preserve the effectiveness of the law enforcement activity.;'	
17. Article 36 is deleted.	
18. the following Chapters VIIa, VIIb and VIIc are inserted:	
'CHAPTER VIIa	
Voluntary registration of data intermediation services -and data altruism organisations'	
Article 32a	
Public Union registers **for voluntary data intermediation services and data altruism organisations**	
(1) The Commission shall keep and regularly update public Union registers of:	

Commission proposal	Drafting suggestions and Comments
(a) recognised data intermediation services providers and	EE (Drafting suggestions): (a) **voluntarily registered and** recognised data intermediation services providers and
(b) recognised data altruism organisations.	EE (Drafting suggestions): (b) **voluntarily registered and** recognised data altruism organisations.
(2) Data intermediation services providers registered in the public Union register referred to in paragraph 1 point (a) may use the label 'data intermediation services provider recognised in the Union' in its written and spoken communication, as well as a common logo referred to in paragraph 4.	
(3) Data altruism organisations registered in the public Union register referred to in paragraph 1 point (b) may use the label 'data altruism organisation recognised in the Union' in its written and spoken communication, as well as the common logo referred to in paragraph 4.	
(4) In order to ensure that data intermediation services providers **recognised in the Union and data altruism oganisations** 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).	EE (Drafting suggestions): In order to ensure that data intermediation services providers recognised in the Union and data altruism organisations recognised /…/ EE (Comments): The word "oganisations" is missing r.
Article 32b	
Competent authorities for the registration of data intermediation services providers and data altruism organisations	
(1) Each Member State shall designate one or more competent authorities responsible for the application and enforcement of this Chapter in accordance with Article 37(1).	

PUBLIC

Commission proposal	Drafting suggestions and Comments
(2) The competent authorities shall be set up in a manner so that their independence from any recognised data intermediation services provider or recognised data altruism organisation is guaranteed.	
Article 32c	
General requirements for registration of recognised data intermediation services providers	
In order to qualify for registration in the public Union register referred to in Article 32a paragraph 1 point (a), ~~a~~ data intermediation services **providers**~~provider~~ shall meet all of the following requirements:	SK (Comments): Functional separation may support viable business models, but it must be accompanied by effective conflict-of-interest safeguards, separate access controls, auditable data flows, a prohibition on cross-use of intermediated data and proportionate supervisory powers. Any exemption for micro and small enterprises should not remove the core duties of neutrality and non-misuse of data.
(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**, which may entail the use of data for the detection of fraud or cybersecurity.**~~;~~	
(c) where they offer additional tools and services to data holders**,** ~~or~~ data subjects **or data users** for the specific purpose of facilitating the exchange of data, such as temporary storage, curation, conversion, encryption, anonymisation and pseudonymisation **or other relevant privacy-enhancing technologies**, such tools and services are used only at the explicit request or approval of the data holder or data subject **or data user**;	EE (Comments): Thank you for adding this change of PET´s. We really appreciate it.
(d) where data intermediation service providers ~~which are not micro and small sized enterprises~~ offer ~~value-added~~ services to their clients	

Commission proposal	Drafting suggestions and Comments
other than **data intermediation services and the additional tools and** ~~the~~ services referred to in point (c), they fulfil the following conditions:	
(i) **such other** ~~the value-added~~ services are explicitly requested by the **data holder, data subject or data** user;	
(ii) the data are not used for other purposes than performing the **requested** ~~value-added~~ service;	
(iii) the **data intermediation** ~~value-added~~ services are offered through **an entity** ~~a~~ functionally separate **from entities offering other services** ~~entity~~;	
(iv) the undertaking seeking to offer the **other** ~~value-added~~ services is not designated as a gatekeeper pursuant to Article 3 of Regulation (EU) 2022/1925;	
(v) the commercial terms, including pricing, for the provision of data intermediation services to a data holder or data user are not dependent upon whether the data holder or data user uses **other** ~~value-added~~ services provided by the data intermediation services provider or by a related entity;	
(e) the data intermediation services provider offering services to data subjects acts in the data subjects' best interest where it facilitates the exercise of their rights, in particular by informing and, where appropriate, advising data subjects in a concise, transparent, intelligible and easily accessible manner about intended data uses by data users and standard terms and conditions attached to such uses before data subjects give consent.	
(f) the data intermediation services provider ensures 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) the data intermediation services provider maintains a log record of the data intermediation activity;	EE (Comments): The requirement for maintaining a log record is unclear without an appropriate recital explaining the reasons and context (i.e. a log according to GDPR or for auditing purposes, for competent authorities, how long it should be kept and what is the reasonable level of detail of the log record.) **We**

PUBLIC

Commission proposal	Drafting suggestions and Comments
	would appreciate it if you could add an explanatory recital on the matter in the act.
(h) the data intermediation services provider takes necessary technical or organizational measures to ensure an appropriate level of security for the storage, processing and transmission of non-personal data.	
~~(ed)~~ **Point (d)(iii), of the first sub-paragraph does not apply to micro and small sized enterprises.**	
Article 32d	
General requirements for registration of recognised data altruism organisations	
In order to qualify for registration in the public Union register referred to in Art. 32a paragraph 1 point (b), a data altruism organisation shall meet all of the following requirements:	SK (Comments): Slovakia supports simplification of the data altruism regime, but a common Union minimum for consent and permission records should be retained in an interoperable and machine-readable form.
(a) they carry out data altruism activities;	
(b) they are a legal person established pursuant to national law to meet objectives of general interest as provided for in national law, where applicable;	
(c) they operate on a not-for-profit basis and are legally independent from any entity that operates on a for-profit basis;	
(d) they carry out their data altruism activities through a structure that is functionally separate from their other activities.	
Article 32e	
Registration **in public Union register**	
(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.	FI (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

Commission proposal	Drafting suggestions and Comments
	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. **Registration shall be mandatory where the processing of personal data is likely to result in a high risk to the rights and freedoms of natural persons within the meaning of Article 35 of Regulation (EU) 2016/679.** FI (Comments): FI has supported, like in the EDPB/EDPS Joint Opinion, maintaining a prior registration requirement in certain circumstances, particularly when the processing of personal data is likely to result in a high risk. However, this is not a redline.
A data~~Data~~ altruism organisation which meets the requirements set out in Article 32d may submit an application for registration in the public Union register of recognised data altruism organisations to the competent authority referred to in Article 32b in the Member State in which they have their main establishment.	
(2) Data intermediation services providers and data altruism organisations that have no main establishment in the Union shall designate a legal representative in one of the Member States. The legal representative shall be mandated to be addressed in addition to or instead of the data intermediation services provider or data altruism organisation by competent authorities or data subjects and data holders. The legal representative shall cooperate with and comprehensively demonstrate to the competent authority, upon request, the actions taken and provisions put in place by the data intermediation services provider or the data altruism organisation to ensure compliance with this Regulation. **Article 37(11) and (12) do not apply to data intermediation services providers and data altruism organisations.**	
The data intermediation services provider or data altruism organisation shall be deemed to be under the jurisdiction of the Member State in which the	

Commission proposal	Drafting suggestions and Comments
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.	CZ (Drafting suggestions): (3) **The Commission**~~**Competent authorities**~~ shall establish the necessary application forms. CZ (Comments): CZ: Application forms could be standardized across the Member States to ensure that the same information is required in all applications. A harmonized approach would ensure equal treatment of applicants and provide clarity regarding documentation requirements.
(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 **competent authority requests the applicant to provide additional information necessary to assess compliance with Article 32c, the time limit shall be suspended until the competent authority has received that information. In duly justified cases, where the assessment of compliance requires additional time due to the complexity or novelty of the services, the competent authority may extend the time limit once by a maximum of 12 weeks and shall inform the applicant accordingly, stating reasons. 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.	

PUBLIC

Commission proposal	Drafting suggestions and Comments
The first subparagraph shall also apply where a data altruism organisation has submitted all necessary information pursuant to paragraph **3**~~2~~, and complies with the registration requirements set out in Article 32d.	
The registration in the public Union register shall be valid in all Member States.	
(5) The competent authority may charge fees for the registration in accordance with national law. Such fees shall be proportionate and objective and be based on the administrative costs related to the monitoring of compliance. In the case of small-mid caps, small and medium-sized enterprises, and start-ups, the competent authority may charge a discounted fee or waive the fee.	
(6) Registered entities shall notify **within a reasonable time** the competent authority of any subsequent changes to the information as provided during the application process or where they cease their data intermediation or data altruism activities in the Union.	
(7) The competent authority shall without delay and by electronic means notify the Commission of any notification pursuant to paragraph 6. The Commission shall without undue delay update the public Union register.	
Article 32f	
Duties of recognised data altruism organisations	
(1) Recognised data altruism organisations shall inform data subjects or data holders prior to any processing of their data in a clear and easily comprehensible manner of the following:	
(a) the objectives of general interest and, if applicable, the specified, explicit and legitimate purpose for which personal data is to be processed, and for which it permits the processing of their data by a data user;	
(b) the location of the processing and the objectives of general interest for which it permits any processing carried out in a third country, where the processing is carried out by the recognised data altruism organisation.	
(2) Recognised data altruism organisations shall not use the data for other objectives than the objectives of general interest for which the data subject or	

PUBLIC

Commission proposal	Drafting suggestions and Comments
data holder allows the processing. The recognised data altruism organisation shall not use misleading marketing practices to solicit the provision of data.	
(3) Recognised data altruism organisations shall provide electronic means for obtaining consent from data subjects or permissions to process data made available by data holders as well as for their withdrawal.	
(4) Recognised data altruism organisations shall, without delay, inform data holders in the event of any unauthorised transfer, access or use of the non-personal data that it has shared.	
(5) Where recognised data altruism organisations facilitate data processing by third parties, including by providing tools for obtaining consent from data subjects or permissions to process data made available by data holders, they shall, where relevant, specify the third-country in which the data use is intended to take place.	
Article 32g	
Monitoring of compliance	
(1) The competent authorities referred to in Article 32b shall~~, either on their own initiative or on a request by a natural or legal person, monitor and~~ supervise whether recognised data intermediation services providers and recognised data altruism organisations comply with the requirements laid down in this Chapter, including whether they continue to comply with the requirements for registration laid down therein. **Those competent authorities may also monitor and supervise the compliance of data intermediation services providers and recognised data altruism organisations, on the basis of a request by a natural or legal person.**	
(2) The competent authorities shall have the power to request from recognised data intermediation services providers or recognised data altruism organisations, or their legal representative, all the information that is necessary to verify compliance with the requirements laid down in this Chapter. Any request for information shall be proportionate to the performance of the task and shall be reasoned.	
(3) Where a competent authority finds that a recognised data intermediation services provider or a recognised data altruism organisation	

PUBLIC

PUBLIC

Commission proposal	Drafting suggestions and Comments
does not comply with one or more of the requirements laid down in this Chapter, it shall notify that entity, or its legal representative, of those findings and give it the opportunity to state its views, within 30 days of the receipt of the notification.	
(4) The competent authority shall have the power to require the cessation of the non-compliance referred to in paragraph 3 either immediately or within a reasonable time limit and shall take appropriate and proportionate measures with the aim of ensuring compliance.	
(5) If a recognised data intermediation services provider or a recognised data altruism organisation does not comply with one or more of the requirements laid down in this Chapter even after having been notified in accordance with paragraph 3, that entity shall:	
(a) lose its right to use the label referred to in Article 32a in written and spoken communication;	
(b) be removed from the public Union register referred to in Article 32a.	
Any decision revoking the right to use the label as referred to in the first subparagraph, point (a), shall be made public by the competent authority **and shall be notified to the Commission. The Commission shall remove the entity from the public Union register.** ~~.~~	
CHAPTER VIIb	
Free flow of non-personal data **within** ~~in~~ the Union'	
Article 32h	
Prohibition of localisation requirements for non-personal data within the Union	
(1) Data localisation requirements for non-personal data shall be prohibited, unless they are justified on grounds of public security in compliance with the principle of proportionality or laid down on the basis of Union law.	
(2) Member States shall immediately communicate to the Commission any draft act which introduces a new data localisation requirement or makes changes to an existing data localisation requirement in accordance with the	EE (Comments): Please clarify in the recital how this communication is foreseen.

Commission proposal	Drafting suggestions and Comments
procedures set out in Articles 5, 6 and 7 of Directive (EU) 2015/1535 of the European Parliament and of the Council.'	
Chapter VIIc	EE (Comments): There are several broader issues with Chapter VIIc in terms of the concept of data and documents, for which the following requirements apply. There is no concept of value or evidence in the current act (as in the definition of 'record' usually used in records management and archiving, inclusing cross-borderly. For example in the Estonian Archives Act: "..a record is information recorded on any medium, which is created or received in the course of the activities of an agency or person, and the content, form and structure of which is sufficient to provide evidence of facts or activities"). This means that strictly seen the organisations in scope of this chapter must describe and provide access to any single bit of data and piece of paper they have – including draft documents, content on hard drives etc. In practice we can assume, that all member states will instead develop their own definitions of which kind of information is seen as data and documents and ultimately there will be (as already is the case with the current implementation of DGA and ODD) huge inconsistencies in what kind of information is made available and what not. This will creat further fragmentation in EU law. This omnibus allows to clarify this aspect and harmonise the understanding on the matter. In our understanding, the use of the terms 'data' and 'documents' itself is very inconsistent and should be reviewed consistently throughout the Digital Omnibus. For example, while data is defined as 'digital' and document as strictly 'non-digital', Article 2 (53) provides a definition of 'data [means] data and document'; while there is a definition of 'personal data' there is no definition of 'personal document'; in Chapter VIIc there are still a number of

PUBLIC

Commission proposal	Drafting suggestions and Comments
	paragraphs which require the digital handling of documents (like providing access through a virtual secure environment), the Act itself is called Data Act but applies to 'data and documents' etc. Broadly the above issues highlight that the entire concept of separating data and documents is not useful, instead the Digital Omnibus should be focused on harmonising how public sector information of evidentiary or informational value (i.e. records) should be made findable and accessible despite of their format or media.
Re-use of data and documents held by public sector bodies	EE (Drafting suggestions): Re-use of data ~~and documents~~ held by public sector bodies
Section 1	
General Provisions	
Article 32i	
Subject matter and scope	
(1) This Chapter establishes a set of rules governing the re-use and the practical arrangements for facilitating the re-use of the following:	
(a) existing data and documents held by public sector bodies of the Member States, including certain categories of protected data;	EE (Drafting suggestions): existing data ~~and documents~~ held by public sector bodies of the Member States, including certain categories of protected data;
(b) existing data and documents held by public undertakings that are:	EE (Drafting suggestions): 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;	

Commission proposal	Drafting suggestions and Comments
(iii) acting as air carriers fulfilling public service obligations pursuant to Article 16 of Regulation (EC) No 1008/2008 of the European Parliament and of the Council; or	
(iv) acting as Community shipowners fulfilling public service obligations pursuant to Article 4 of Council Regulation (EEC) No 3577/92 ;	
(c) research data pursuant to the conditions set out in Article 32t.	
(2) This Chapter does not apply to the following:	
(a) data and documents the supply of which is an activity falling outside the scope of the public task of the public sector bodies concerned as defined by law or by other binding rules in the Member State, or, in the absence of such rules, as defined in accordance with common administrative practice in the Member State in question, provided that the scope of the public tasks is transparent and subject to review;	
(b) data and documents held by public undertakings and:	
(i) produced outside the scope of the provision of services in the general interest as defined by law or other binding rules in the Member State;	
(ii) related to activities directly exposed to competition and therefore, pursuant to Article 34 of Directive 2014/25/EU, not subject to procurement rules;	
(c) data and documents, such as sensitive data **or documents**, 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;	

PUBLIC

Commission proposal	Drafting suggestions and Comments
(ii) commercial confidentiality (including business, professional or company secrets);	
(b) data or documents access to which is restricted by virtue of the access regimes in the Member States,	
(i) including cases whereby citizens or legal entities have to prove a particular interest to obtain access to documents;	
(ii) on grounds of protection of personal data, **as well as**~~and~~ parts of data or documents accessible **under**~~by virtue of~~ those regimes which contain personal data the re-use of which has been defined by law as being incompatible with the **legal framework for**~~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 **under**~~in accordance with~~ Union or national law regarding the protection of personal data; ~~logos, crests and insignia;~~	EE (Drafting suggestions): (ii) on grounds of protection of personal data, as well asparts of data ~~or documents~~ accessible under those regimes which contain personal data the re-use of which has been defined by law as being incompatible with the legal framework for 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 under with Union or national law regarding the protection of personal data;
(c) logos, crests and insignia;	
(d)~~(c)~~ data or documents for which third parties hold intellectual **or industrial** property rights;	
(e)~~(d)~~ data or documents held by cultural establishments other than libraries, including university libraries, museums and archives;	
(f)~~(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);	
(g)~~(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;	EE (Drafting suggestions): 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;
(h)~~(g)~~ **data**~~Data~~ or documents access to which is excluded or restricted on grounds of critical entity or critical infrastructure protection related	EE

Commission proposal	Drafting suggestions and Comments
information as defined in points (1) and (4) of Article 2 of Directive (EU) 2022/2557.	(Drafting suggestions): data ~~**or documents**~~ access to which is excluded or restricted on grounds of critical entity or critical infrastructure protection related information as defined in points (1) and (4) of Article 2 of Directive (EU) 2022/2557.
(4) Section 3 of this Chapter does not apply to:	
(a) data and documents that are not certain categories of protected data;	
(b) data or documents held by public undertakings;	
(c) data or documents held by cultural establishments and educational establishments;	LU (Comments): We reiterate our comment that the relevant recitals of the DGA should be included in the DA. In this case, especially recital (12) of the DGA should be included.
(d) data and documents covered by Section 2 of this Chapter.	
~~(da)~~ **Section 3 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.**	
(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 **data or** documents.	
(6) The obligations imposed in accordance with this Chapter shall apply only insofar as they are compatible with the provisions of international agreements on the protection of intellectual property rights, in particular the Berne Convention for the Protection of Literary and Artistic Works (Berne Convention), the Agreement on Trade-related Aspects of Intellectual Property Rights (TRIPS Agreement and the World Intellectual Property Organization Copyright Treaty (WCT).	
(7) The right for the maker of a database provided for in Article 7(1) of Directive 96/9/EC shall not be exercised by public sector bodies in order to	

PUBLIC

Commission proposal	Drafting suggestions and Comments
prevent the re-use of data and documents or to restrict re-use beyond the limits set by this Chapter.	
(8) This Chapter governs the re-use of existing data and documents held by public sector bodies and public undertakings of the Member States, including data and documents to which Directive 2007/2/EC of the European Parliament and of the Council applies.	
(9) This Chapter is without prejudice to Union and national law and international agreements to which the Union or Member States are party on the protection of categories of data or documents referred to in Article 2(**53**~~54~~).	
(10) This Chapter shall enter into application as of [18 months after the publication in the Official Journal of the European Union of this Regulation].	PL (Drafting suggestions): [(10) This Chapter shall enter into application as of [~~18~~ **24** months after the publication in the Official Journal of the European Union of this Regulation.] SK (Comments): The application date should provide sufficient time for Member States to adapt national legislation, designate authorities, establish secure processing environments and connect existing catalogues. Relevant implementing acts, standards and Commission guidance should be available sufficiently in advance. Slovakia requests consideration of a longer or phased implementation period
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	

PUBLIC

PUBLIC

Commission proposal	Drafting suggestions and Comments
equally apply for comparable categories of re-use, including for cross-border re-use.	
(2) If data or documents are re-used by a public sector body as input for its commercial activities which fall outside the scope of its public tasks, the same charges and other conditions shall apply to the supply of the data or documents for those activities as the ones that apply to other re-users.	
Article 32k	
Exclusive arrangements	
(1) The re-use of data or documents shall be open to all potential actors in the market, even if one or more market actors already exploit added-value products based on those data or documents. Agreements or other arrangements or practices pertaining to the re-use of data or documents, which have as their objective or effect to grant exclusive rights or to restrict the availability of data or documents for re-use by entities other than the parties to such agreements, arrangements or practices, shall be prohibited.	LU (Drafting suggestions): The re-use of **public sector open** data or documents shall be open to all potential actors in the market, even if one or more market actors already exploit added-value products based on those data or documents. Agreements or other arrangements or practices pertaining to the re-use of data or documents, which have as their objective or effect to grant exclusive rights or to restrict the availability of data or documents for re-use by entities other than the parties to such agreements, arrangements or practices, shall be prohibited. LU (Comments): The wording of the ODD used here does not work with the regime of the DGA. Luxembourg therefor suggests re-wording the part of the sentence “the re-use of data or documents shall be open” in order to avoid conflicting understanding with Article 32(i)(4) sub-paragraph 2 stating that the Regulation does not create an obligation to allow re-use. We consider this as an important clarification to provide the necessary protection for the DGA regime.
(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	

Commission proposal	Drafting suggestions and Comments
be granted to the extent necessary for the provision of the service or the supply of the product under the following conditions:	
(a) the exclusive right is granted through an administrative act or contractual agreement in accordance with applicable Union and national law and in compliance with the principles of transparency, equal treatment and non-discrimination.	
(b) the agreements **or administrative acts** granting the exclusive right, including the reasons as to why it is necessary to grant such a right, **shall be**~~is~~ transparent and **shall be** made publicly available online, in a form that complies with relevant Union law on public procurement and national law.	
(c) except for exclusive rights related to the digitisation of cultural resources, the validity of the reason for granting exclusive rights concerning data and documents within the scope of Section 2 shall be subject to regular review, and shall in any event, be reviewed every three years.	
(d) exclusive arrangements established on or after 16 July 2019 shall be made publicly available online at least two months before they come into effect. The final terms of such arrangements shall be transparent and shall be made publicly available online.	
(3) By way of derogation of paragraph 1, where an exclusive right relates to the digitisation of cultural resources, the period of exclusivity shall in general not exceed 10 years. Where that period exceeds 10 years, its duration shall be in accordance with applicable Union and national law subject to review during the 11th year and, if applicable, every seven years thereafter.	
(4) In the case of an exclusive right referred to in paragraph 3, the public sector body concerned shall be provided free of charge with a copy of the digitised cultural resources as part of those arrangements. That copy shall be available for re-use at the end of the period of exclusivity.	
(5) For certain categories of protected data, the duration of an exclusive right to re-use data shall not exceed 12 months. Where a contract is concluded **or administrative act is adopted**, the duration of the **arrangement**~~contract~~ shall be the same as the duration of the exclusive right.	

PUBLIC

PUBLIC

Commission proposal	Drafting suggestions and Comments
(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 **arrangements shall**~~arrangementsshall~~ be made publicly available online at least two months before their coming into effect. The effect of such legal or practical arrangements on the availability of data for re-use shall be subject to regular reviews and shall, in any event, be reviewed every three years. The final terms of such arrangements shall be transparent and made publicly available online.	
(7) For existing exclusive arrangements, the following shall apply:	
(a) exclusive arrangements concerning data and documents within the scope of Section **2 existing**~~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;	LU (Drafting suggestions): (b) exclusive arrangements concerning data and documents within the scope of Section **~~2~~3** 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;- LU (Comments): We believe that this provision contains a wrong reference. Shouldn't it refer to Section 3 instead of Section 2?
Article 321	
General principles relating to charging	

PUBLIC

Commission proposal	Drafting suggestions and Comments
(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 **2**~~**1**~~, the factors that are taken into account in the calculation of those charges shall be indicated at the outset. Upon request, the holder of the data or documents in question shall also indicate the way in which such charges have been calculated in relation to a specific re-use request.	
(4) Public sector bodies shall ensure that any charges can also be paid online through widely available cross-border payment services, without discrimination based on the place of establishment of the payment service provider, the place of issue of the payment instrument or the location of the payment account within the Union.	
~~4a.~~ **Article 32la**	
~~4b.~~ **Procedure for re-quests for re-use**	
~~4c.~~ **(1) Public sector bodies shall, through electronic means where possible and appropriate, process requests for re-use and shall make the data or 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.**	
~~4d.~~ **(2) Unless shorter time limits have been established in accordance with national law, public sector bodies and in the case of protected data public sector bodies or the competent bodies referred to in paragraph 1 of Article 32z shall process the request and, in case of a positive decision, 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 principle~~ **within 20 working days of receipt. In case of**	SK (Comments): Slovakia supports clear deadlines for re-use requests. The periods should run from receipt of a complete request and be suspendable where information necessary to assess legal, technical or confidentiality requirements is missing.

PUBLIC

Commission proposal	Drafting suggestions and Comments
particularly complex requests, that period shall not exceed two months of receipt and in case of requests relating to protected data~~, that~~. The period for processing the request shall not exceed three months of receipt~~.~~ whereas this time limit may be extended within reasonable limits in order to deliver the protected data or to provide access for the re-use of the protected data within a secure processing environment.	
~~4e.~~ **(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. Where a negative decision is based on point (d) of paragraph 3 of Article 32i, the public sector body or competent 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.**	PL (Drafting suggestions): (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. **Member States may adopt national provisions laying down the grounds for refusal.** Where a negative decision is based on point (d) of paragraph 3 of Article 32i, the public sector body or competent 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.
~~4f.~~ **(4) Any natural or legal person directly affected by a decision as referred to in paragraph ~~1~~2 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.**	
~~4g.~~ **(5) This Article shall not apply to the following entities:**	LU

Commission proposal	Drafting suggestions and Comments
	(Comments): These exclusions from the procedure foreseen in the present Article create legal uncertainty as to which procedure would apply to them and does not facilitate re-use of existing data of great value. Indeed, whilst those entities fall outside of the scope for the ODD, some of them fall inside of the scope for the DGA. If this paragraph remains as it stands, those entities won't have a clear procedure to follow and they would face legal uncertainty.
~~4h.~~ **(a) public undertakings;**	
~~4i.~~ **(b) educational establishments, research performing organisations and research funding organisations.**	
Article 32m	
Information on means of redress	
Public sector bodies shall ensure that applicants for re-use of data or documents are informed of available means of redress relating to decisions or practices affecting them. **Any decision on re-use shall contain a reference to the means of redress where the applicant wishes to challenge the decision.**	
Section 2	
Re-use of **public sector** open ~~government~~ data	
Subsection 1	
Scope and General Principles	
Article 32n	
General principle for re-use of **public sector** open ~~government~~ data	EE (Comments): **Here are two very important points to us.** Estonia considers that, in the context of the broader Digital Omnibus proposal, the new Data Regulation should clearly define the conditions under which personal data may be made available as open data. In particular, the Regulation shouldensure legal certainty by clarifying that personal data may

Commission proposal	Drafting suggestions and Comments
	only be disclosed as open data where the data subject has given valid consent or where such disclosure is expressly provided for under Union or national law, in full compliance with the applicable data protection framework. Thus we suggest adding additional point 3 as follows: (3) The personal data may only be disclosed as open data where the data subject has given its consent or where such disclosure is expressly provided for under Union or national law, in full compliance with the applicable data protection framework. The disclosure of datasets which would jeopardise Union´s or Member States internal or external security must not be made publicly available. Especially, taking into consideration current geo-political situation. Example of such dataset relates to the energy data. Thus, we suggest another additional prinicple to be added: (4) The disclosure of datasets which would jeopardise Union´s or Member States internal or external security must not be made publicly available.
(1) Data or documents in scope of this Section shall be re-usable for commercial or non-commercial purposes in accordance with Section 1 and Section 2 Subsection 3.	
(2) For data or documents in which libraries, including university libraries, museums and archives hold intellectual property rights and for data or documents held by public undertakings, where the re-use of such data or documents is allowed, those data or documents shall be re-usable for commercial or non-commercial purposes in accordance with Section 1 and Section 2 Subsection 3.	
~~**Subsection 2**~~	
~~**Requests for re-use**~~	
~~**Article 32o**~~	
~~**Processing requests for re-use**~~	
~~**(1) Public sector bodies shall, through electronic means where possible and appropriate, process requests for re-use and shall make the**~~	

Commission proposal	Drafting suggestions and Comments
~~document available for re-use to the applicant or, if a licence is needed, finalise the licence offer to the applicant within a reasonable time that is consistent with the time frames laid down for the processing of requests for access to data or documents.~~	
~~(2) Where no time limits or other rules regulating the timely provision of data or documents have been established, public sector bodies shall process the request and shall deliver the data or documents for re-use to the applicant or, if a licence is needed, finalise the licence offer to the applicant as soon as possible, and in any event within 20 working days of receipt. That time frame may be extended by a further 20 working days in the case of extensive or complex requests. In such cases, the applicant shall be notified as soon as possible, and in any event within three weeks of the initial request, that more time is needed to process the request and the reasons why.~~	
~~(3) In the event of a negative decision, the public sector bodies shall communicate the grounds for refusal to the applicant on the basis of the relevant provisions of the access regime in that Member State or the provisions of this Regulation, in particular points (a) to (c) of paragraph 2 of Article 32i and points (a) to (d) of paragraph 3 of Article 32i or Article 32n (general principle ODD Section). Where a negative decision is based on point (d) of paragraph 3 of Article 32i, the public sector body shall include a reference to the natural or legal person who is the rightsholder, where known, or alternatively to the licensor from which the public sector body has obtained the relevant material. Libraries, including university libraries, museums and archives, shall not be required to include such a reference.~~	
~~(4) The means of redress shall include the possibility of review by an impartial review body with the appropriate expertise, such as the national competition authority, the relevant access to data or documents authority, the supervisory authority established in accordance with Regulation (EU) 2016/679 or a national judicial authority, whose decisions are binding upon the public sector body concerned.~~	

PUBLIC

PUBLIC

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 data or documents. Those arrangements may in particular include the means to supply adequate information on the rights provided for in this Regulation and to offer relevant assistance and guidance.~~	
~~(6) This Article shall not apply to the following entities:~~	
~~(a) public undertakings;~~	
~~(b) educational establishments, research performing organisations and research funding organisations.~~	
Subsection 3	
Conditions for re-use	
Article 32p	
Available formats	
(1) Without prejudice to Subsection 5, public sector bodies and public undertakings shall make their data ~~or documents~~ available in any pre-existing format or language ~~and, where possible and appropriate,~~ by electronic means, in formats that are open, machine-readable, accessible, findable and re-usable, together with their metadata. Both the format and the metadata shall, where possible, comply with formal open standards. **Public sector bodies and public undertakings shall make their documents available in any pre-existing format or language.**	SK (Comments): Slovakia supports the strengthened requirements for open, machine-readable, findable and reusable data, including suitable APIs for dynamic data. Common technical standards and reusable central services should accompany these obligations. The disproportionate-effort safeguard should be interpreted narrowly but should take account of legacy systems and the capacities of small municipalities and public bodies.
(2) **Wherever possible and appropriate,** ~~Member States shall encourage~~ public sector bodies and public undertakings **shall** ~~to~~ produce and make available data or documents falling within the scope of this Section in accordance with the principle of 'open by design and by default'.	
(3) Paragraph 1 shall not imply an obligation for public sector bodies to create or adapt data or documents or provide extracts in order to comply with that paragraph where this would involve disproportionate effort, going beyond a simple operation.	

Commission proposal	Drafting suggestions and Comments
(4) 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.	
(6) Where making dynamic data available for re-use immediately after collection, as referred to in paragraph 5, would exceed the financial and technical capacities of the public sector body, thereby imposing a disproportionate effort, those dynamic data shall be made available for re-use within a time frame or with temporary technical restrictions that do not unduly impair the exploitation of their economic and social potential.	
(7) Paragraphs 1 to 6 shall apply to existing data or documents held by public undertakings which are available for re-use.	
(8) The high-value datasets, as listed in accordance with Article 32v(1) shall be made available for re-use in machine- readable format, via suitable APIs and, where relevant, as a bulk download.'	
Article 32q	
Principles governing charging for **public sector** 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 **or documents** of the marginal costs incurred for the reproduction, provision**, extensive searches** and dissemination of such data or documents as well as for anonymisation of personal data and measures taken to protect commercially confidential information **and other information protected by law** may be allowed.	
(2) Paragraph 1 shall not apply to the following entities:	
(a) public sector bodies that are required to generate revenue to cover a substantial part of their costs relating to the performance of their public tasks;	
(b) libraries, including university libraries, museums and archives;	
(c) public undertakings.	

PUBLIC

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

PUBLIC

PUBLIC

Commission proposal	Drafting suggestions and Comments
confidentiality of the data or documents, together with a reasonable return on investment.	
(7) The re-use of the following shall be free of charge for the **re-user**~~user~~:	
(a) subject to Article 32v paragraph (3), (4) and (5), the high-value datasets, as listed in accordance with paragraph 1 of that Article;	
(b) research data referred to in point (c) of paragraph 1 of Article 32i.	PL (Drafting suggestions): After par. (7) add par. (8): **8. Member States may adopt more detailed or stricter rules as regards principles governing charging allowing for more extensive re-use. In particular Member States may restrict the ability to charge fees higher than those set forth in paragraph 1.**
Article 32r	
Standard licences	
(1) The re-use of data or documents shall not be subject to conditions, unless such conditions are objective, proportionate, non-discriminatory and justified on grounds of a public interest objective.	
(2) When re-use is subject to conditions, those conditions shall not unnecessarily restrict possibilities for re-use and shall not be used to restrict competition.	
(3) In Member States where licences are used, public sector bodies **and public undertakings** shall ensure that the standard licences for the re-use of public sector data or documents, which can be adapted to meet particular licence applications, are available in digital format and able to be processed electronically.	
(4) Public sector bodies **and public undertakings** 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	PL (Drafting suggestions): After par. (4) add par. (5):

Commission proposal	Drafting suggestions and Comments
power, or the ability of the entity to acquire data, including in particular a designation as a gatekeeper under Regulation (EU) 2022/1925.	**(5) Member States may adopt more detailed or stricter rules as regards conditions for re-use allowing for more extensive re-use. In particular Member States may specify a detailed list of conditions for re-use.**
Article 32s	
Practical arrangements	
(1) Member States shall make practical arrangements facilitating the search for data or documents available for re-use, such as asset lists of main data or documents with relevant metadata, accessible where possible and appropriate online and in machine- readable format, and **on data portals** ~~portal sites~~ that are linked to the asset lists. Where possible, Member States shall facilitate the cross-linguistic search for data or documents, in particular by enabling metadata aggregation at Union level.	
Member States shall also encourage public sector bodies to make practical arrangements facilitating the preservation of data or documents available for re-use.	
(2) Member States shall, in cooperation with the Commission, **ensure simple**~~continue efforts to simplify~~ access to datasets, in particular by providing a single point of access and by progressively making available suitable datasets held by public sector bodies with regard to the data or documents to which this Section applies, as well as to data held by Union institutions, in formats that are accessible, readily findable and re-usable by electronic means.	
Subsection 4	
Research data	
Article 32t	
Research data	
(1) Member States shall support the availability of research data by adopting national policies and relevant actions aiming at making publicly funded research data openly available (‘open access policies’), following the principle of ‘open by default’ and compatible with the FAIR principles. In that context, concerns relating to intellectual property rights, personal data	

Commission proposal	Drafting suggestions and Comments
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 **32i**~~32n~~, paragraph 3, point (d), research data shall be re-usable for commercial or non-commercial purposes in accordance with Section 1 and Section 2 Subsection 3, insofar as they are publicly funded and researchers, research performing organisations or research funding organisations have already made them publicly available through an institutional or subject-based repository. In that context, legitimate commercial interests, knowledge transfer activities and pre-existing intellectual property rights shall be taken into account.	
Subsection 5	
High-value datasets	
Article 32u	
Thematic categories of high-value datasets	
(1) The thematic categories of high-value datasets shall be as set out in Annex I.	
(2) The Commission is empowered to adopt delegated acts in accordance with Article **45(2)**~~45(2a)~~ in order to amend Annex I by adding new thematic categories of high-value datasets reflecting technological and market developments.	
Article 32v	
Specific high-value datasets and arrangements for publication and re-use	
(1) The Commission shall adopt implementing acts laying down a list of specific high-value datasets belonging to the categories set out in Annex I and held by public sector bodies and public undertakings among the data or documents to which this Section applies.	SK (Comments): Slovakia supports free access to high-value datasets through APIs and, where relevant, bulk download. The selection of datasets and technical arrangements should be based on a transparent cost-benefit assessment.

PUBLIC

Commission proposal	Drafting suggestions and Comments
	Sustainable financing should be ensured for public bodies whose statutory revenue model currently depends on charges.
Such specific high-value datasets shall be:	
(a) available free of charge, subject to paragraphs 3, 4 and 5;	
(b) machine readable;	
(c) provided via APIs; and	
(d) provided as a bulk download, where relevant.	
Those implementing acts may specify the arrangements for the publication and re-use of high-value datasets. Such arrangements shall be compatible with open standard licences.	
The arrangements may include terms applicable to re-use, formats of data and metadata and technical arrangements for dissemination. Investments made by the Member States in open data approaches, such as investments into the development and roll-out of certain standards, shall be taken into account and balanced against the potential benefits from inclusion in the list.	
Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 46(2).	
(2) The identification of specific high-value datasets pursuant to paragraph 1 shall be based on the assessment of their potential to:	
(a) generate significant socioeconomic or environmental benefits and innovative services;	
(b) benefit a high number of users, in particular SMEs and SMCs;	
(c) assist in generating revenues; and	
(d) be combined with other datasets.	
For the purpose of identifying such specific high-value datasets, the Commission shall carry out appropriate consultations, including at expert level, conduct an impact assessment and ensure complementarity with existing legal acts, such as Directive 2010/40/EU of the European Parliament and of the Council, with respect to the re-use of data or documents. That impact assessment shall include a cost-benefit analysis and an analysis of whether providing high-value datasets free of charge by public sector bodies	

PUBLIC

Commission proposal	Drafting suggestions and Comments
that are required to generate revenue to cover a substantial part of their costs relating to the performance of their public tasks would lead to a substantial impact on the budget of such bodies. With regard to high-value datasets held by public undertakings, the impact assessment shall give special consideration to the role of public undertakings in a competitive economic environment.	
(3) By way of derogation from paragraph 1, second subparagraph, point (a), the implementing acts referred to in that paragraph shall provide that the availability of high-value datasets free of charge is not to apply to specific high-value datasets held by public undertakings where that would lead to a distortion of competition in the relevant markets.	
(4) The requirement to make high-value datasets available free of charge pursuant to point (a) of the second subparagraph of paragraph 1 shall not apply to libraries, including university libraries, museums and archives.	
~~(5) Where making high-value datasets available free of charge by public sector bodies that are required to generate revenue to cover a substantial part of their costs relating to the performance of their public tasks would lead to a substantial impact on the budget of the bodies involved, Member States may exempt those bodies from the requirement to make those high-value datasets available free of charge for a period of no more than two years following the entry into force of the relevant implementing act adopted in accordance with paragraph 1.~~	
Section 3	
Re-use of certain categories of protected data held by public sector bodies	
Article 32w	
Conditions for re-use **of 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	EE (Drafting suggestions): (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

PUBLIC

Commission proposal	Drafting suggestions and Comments
access for re-use, they may be assisted by the competent bodies referred to in Article 32z (1).	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). EE (Comments): It creates confusion that under re-use of protected data, it has rules for documents. If we need rules for documents, they need to be in a separate paragraph to be clearly understood. See comment above on the terms “data” and “document”.
Member States shall ensure that public sector bodies are equipped with the necessary resources to comply with this Article and Article 32x.	SK (Comments): lSlovakia strongly supports the explicit obligation to provide public sector bodies with the necessary resources. Implementation should include common guidance, standard contractual and licensing tools, anonymisation support and shared secure processing environments.
(2) Re-use of data or documents shall not affect the protected nature of those data or documents and shall only be allowed:	EE (Drafting suggestions): Re-use of data ~~**or documents**~~ shall not affect the protected nature of those data ~~**or documents**~~ and shall only be allowed:
(a) in compliance with intellectual property rights.	
(b) if data **or documents that are**~~**that is**~~ considered confidential in accordance with Union or national law on commercial or statistical confidentiality, **are**~~**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.	

Commission proposal	Drafting suggestions and Comments
(3) To ensure the preservation of the protected nature as referred to in paragraph 2, public sector bodies may establish the following requirements:	LU (Comments): The recitals fostering understanding of the DGA regime will disappear once the DGA regulation ceases to exist. Hence, Luxembourg considers it crucial to include all relevant recitals of the DGA into the DA.
(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:	EE (Drafting suggestions): (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: EE (Comments): Please note that the criteria for documents have not been covered in (i) and (iii). Possible solutions: (a) to cover only data (preferred solution) Add (iv) for "redacted, in the case of documents including personal information".
(i) anonymised, in the case of personal data;	
~~(ii)~~ ~~**subject to other forms of preparation of personal data;**~~	FI (Comments): FI supports the suggested removal of "other forms of preparation of personal data". Reuse should be permitted only when personal data is anonymised.

Commission proposal	Drafting suggestions and Comments
(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;	EE (Drafting suggestions): (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.	EE (Drafting suggestions): (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 **public sector** open ~~government~~ data set out in Section 2. This is without prejudice to Article 32y, which prevails in case of conflict.	EE (Drafting suggestions): 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 public sector data set out in Section 2. This is without prejudice to Article 32y, which prevails in case of conflict. LU (Comments): We reiterate our previous comment regarding this provision, and the legal uncertainty that it creates. It remains uncertain which regime is applicable, also because Article 32i(3)(b)(ii) excludes the application of section 2 to certain categories of protected data (section 3) for reasons of data protection. Luxembourg considers this provision as unacceptable if this point is not clarified.

PUBLIC

Commission proposal	Drafting suggestions and Comments
	There is a problem of interaction between the ODD and the DGA. The DGA creates a specific regime for anonymized protected data. This specific regime will, however, never be applicable if this provision remains since it states that anonymized data should always be subject to the ODD regime. This problem needs to be addressed. Both regimes have their merits. The risk to reidentify persons cannot be evaluated in the same way in the DGA regime as in the ODD regime.
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.	LU (Comments): The following sentence of Article 5(5) of the DGA is missing : “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 and to notify any data breach resulting in the re-identification of the data subjects concerned to the public sector body”. We have a strong reservation as long as this paragraph is not included.
(4) The public sector body shall reserve the right to verify the process, the means and any results of processing of data or documents undertaken by the re-user to preserve the integrity of the protection of the data or documents. It shall also reserve the right to prohibit the use of results that contain information jeopardising the rights and interests of third parties. The decision to prohibit the use of the results shall be comprehensible and transparent to the re-user.	EE (Drafting suggestions): The public sector body shall reserve the right to verify the process, the means and any results of processing of data ~~**or documents**~~ undertaken by the re-user to preserve the integrity of the protection of the data ~~**or documents**~~. It shall also reserve the right to prohibit the use of results that contain information jeopardising the rights and interests of third parties. The decision to prohibit the use of the results shall be comprehensible and transparent to the re-user.
Unless national law provides for specific safeguards on applicable confidentiality obligations relating to the re-use of certain categories of protected data, the public sector body shall make the re-use of data or documents provided in accordance with paragraph 3 conditional on the adherence by the re-user to a confidentiality obligation that prohibits the disclosure of any information that jeopardises the rights and interests of third parties and that the re-user may have acquired despite the safeguards put in	EE (Drafting suggestions): 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

Commission proposal	Drafting suggestions and Comments
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.	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. EE (Comments): The re-use of documents should be in a separate paragraph if needed. Currently, it makes confusion according to the terms defined in this act.
(5) Where the re-use of data or documents **that are protected on the grounds of commercial or statistical confidentiality or of intellectual property rights of third parties** cannot be allowed in accordance with paragraphs 3 and 4, re-use shall only be possible:	
~~(a) where there is no legal basis other than consent for transmitting the data under Regulation (EU) 2016/679, with the consent of the data subjects;~~	
~~(b)~~ with the permission from the data holders whose rights and interests may be affected by such re-use.	
The public sector body shall make best efforts, in accordance with Union and national law, to provide assistance to potential re-users in seeking ~~consent of the data subjects or~~ permission from the data holders whose rights and interests may be affected by such re-use, where this is feasible without a disproportionate burden on the public sector body. –	
Where it provides such assistance, the public sector body may be assisted by the competent bodies referred to in Article 32z.	
Article 32x	
Requirements for transfers of non-personal **protected** data to third countries by re-users	

Commission proposal	Drafting suggestions and Comments
(1) Where a re-user intends to transfer certain categories of protected data that are non-personal to a third country, it shall inform the public sector body of its intention to transfer such data and the purpose of such transfer at the time of requesting the re-use ~~**of the data**~~. In the case of re-use based on the data holder's permission the re-user shall, where appropriate with the assistance of the public sector body, inform the natural or legal person whose rights and interests may be affected of that intention, purpose and the appropriate safeguards. The public sector body shall not allow the re-use unless the natural or legal person gives permission for the transfer.	
(2) Public sector bodies shall transmit non-personal confidential data or data protected by intellectual property rights to a re-user which intends to transfer those data to a third country other than a country designated in accordance with paragraph **5**~~7~~ only if the re-user contractually commits to:	
(a) complying with the obligations imposed in accordance with intellectual property rights and Union or national law on commercial or statistical confidentiality even after the data is transferred to the third country;	
(b) accepting the jurisdiction of the courts or tribunals of the Member State of the transmitting public sector body with regard to any dispute related to compliance with intellectual property rights and Union or national law on commercial or statistical confidentiality.	
(3) The Commission may adopt implementing acts establishing model contractual clauses for complying with the obligations referred to in paragraph 2 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 46(2).	
(4) Public sector bodies shall, where relevant and to the extent of their capabilities, provide guidance and assistance to re-users in complying with the obligations referred to in paragraph 2.	
(5) Where justified because of the substantial number of requests across the Union concerning the re-use of non- personal data in specific third countries, the Commission may adopt implementing acts declaring that the legal, supervisory and enforcement arrangements of a third country:	

PUBLIC

Commission proposal	Drafting suggestions and Comments
(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.	LU (Comments): The paragraph previous to this paragraph of Article 5(13) of the DGA is missing : “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.”
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 **for the re-use of certain categories of protected data**	
(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.	

PUBLIC

PUBLIC

Commission proposal	Drafting suggestions and Comments
(2) Where ~~public sector bodies charge~~ fees **are charged, Member States**~~, 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 **may be established**. That list, together with the criteria used to establish it, shall be made public.	
(3) Any fees shall be derived from the costs related to conducting the procedure for requests for the re-use of certain categories of protected data and limited to the necessary costs in relation to:	
(a) the reproduction, provision and dissemination of data;	
(b) the clearance of rights;	
(c) anonymisation ~~or other forms of preparation~~ of personal data and **preparation of** 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.~~	
(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.	
(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.	

Commission proposal	Drafting suggestions and Comments
(5) Public sector bodies may charge higher fees than those allowed in accordance with paragraph 2 and 3 of this Article with respect to very large enterprises, based on objective criteria, taking into account the economic power, or the ability of the entity to acquire data, including in particular a designation as a gatekeeper under Regulation (EU) 2022/1925. Any such calculated fees shall be proportionate. In addition to the elements listed in paragraph 3 of this Article, they can cover the cost of collection and production of the data, together with a reasonable return on investment.	
Article 32z	
Competent bodies	
(1) For the purpose of carrying out the tasks referred to in this Article, each Member State shall designate one or more competent bodies ~~in accordance with Article 37(1)~~, which may be competent for particular sectors, but that collectively need to cover all sectors, to assist the public sector bodies which grant or refuse access for the re-use of certain categories of protected data. Member States may either establish one or more new competent bodies or rely on existing public sector bodies or on internal services of public sector bodies that fulfil the conditions laid down in this Section.	
(2) The competent bodies may be empowered to grant access for the re-use of certain categories of protected data pursuant to Union or national law which provides for such access to be granted. ~~Where they grant or refuse access for re-use, those competent bodies shall be subject to Articles 32k, 32w, 32x, 32y and 32ab.~~	LU (Comments): Luxembourg opposes the deletion of the second sentence. We ask to reintroduce this sentence but to rely on the wording of the DGA, which reads as follows: « Where they grant or refuse access for the re-use, Articles 4, 5, 6 and 9 shall apply to those competent bodies. » Luxembourg considers that the deletion does not contribute to a simplification but rather the opposite. It also creates legal uncertainty regarding these matters since Members States need to decide if and how to address the void caused by the deletion (ex. foresee their own rules). This

Commission proposal	Drafting suggestions and Comments
	will inevitably lead to different regimes and thus complexify the system and at the same time increase administrative burdens for applicants.
~~(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).~~	
(3)~~(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;	EE (Drafting suggestions): (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 **protected** 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~~**, and the** commercially confidential information, including trade secrets or content protected by intellectual property rights;	EE (Drafting suggestions): (c) providing technical support for **the application of** anonymizsation, pseudonymisation and state-of-the-art privacy-preserving methods, **and the preparation for secure re-use of** ~~**and the**~~ commercially confidential information, including trade secrets or content protected by intellectual property rights; LU (Comments): Luxembourg considers merit in the possibility to provide for data sets ready to be reused, including for the means of AI development. This task would logically be incumbent on competent bodies, which shall have the possibility to proceed to data curation, including synthethic data, as well as the

Commission proposal	Drafting suggestions and Comments
	preparation of AI ready data sets, whether on the basis of data sets reused in the secure processing environment or *ex ante*. Considering the ambitions of the European Union to foster innovation, within shorter delays (see reduction to 20 days), such a measure would be key. Therefore, Luxembourg pleads in favor of adding the precision that the assistance includes data curation, including the preparation of data sets for reuse.
(d) assisting the public sector bodies, where relevant, to provide support to re-users in requesting consent for re-use from data subjects or permission from data holders in line with their specific decisions, including on the jurisdiction in which the data processing is intended to take place and assisting the public sector bodies in establishing technical mechanisms that allow the transmission of requests for consent or permission from re-users, where practically feasible;	
(e) providing public sector bodies with assistance in assessing the adequacy of contractual commitments made by a re-user pursuant to Article 32x(2).	
Article 32aa	EE (Comments): We consider it essential to align Article 32aa with Article 32s and move both provisions to Section 1. This is necessary in order to provide for a clear and singular guidance for member states to set up central information points which publish and make searchable the asset lists for both open and certain types of protected data.
Single information point	
(1) Each Member State shall designate a single information point. That point shall make available easily accessible information concerning the	

Commission proposal	Drafting suggestions and Comments
application of Articles 32w, 32x and 32y. **The single information point may be linked to sectoral, regional or local 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.	
(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 **certain** ~~the~~ categories of data referred to in Article 2(~~54~~**53**).	
(4) The single information point shall make available by electronic means a searchable asset list containing an overview of all available **data and** document resources including, where relevant, those document resources that are available at sectoral, regional or local information points~~,~~ with relevant information describing the available data or documents, including at least ~~the data format and size and~~ the conditions for their re-use.	
(5) The Commission shall establish a European single access point offering a searchable electronic register of data or documents available in the national single information points and further information on how to request data or documents via those national single information points.	
~~**Article 32ab**~~	
~~**Procedure for requests for re-use**~~	
~~(1) Unless shorter time limits have been established in accordance with national law, the competent public sector bodies or the competent bodies referred to in paragraph 1 of Article 32z shall adopt a decision on the request for the re-use of certain categories of protected data within two months of the date of receipt of the request.~~	
~~(2) In the case of exceptionally extensive and complex requests for re-use, that two-month period may be extended by up to 30 days. In such cases the competent public sector bodies or the competent bodies referred to in paragraph 1 of Article 32z shall notify the applicant as~~	

PUBLIC

Commission proposal	Drafting suggestions and Comments
~~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.~~	
18aa. Article 33 is amended as follows:	
(a) Point (d) in paragraph 1 is replaced by the following:	
~~3c.~~ **'where applicable, the means to enable the interoperability of tools for automating the execution of data sharing agreements shall be provided.'**	
(b) the second subparagraph of paragraph 2 is replaced as follows:	
~~3e.~~ **'The Commission shall when adopting delegated acts take into account the advice of the EDIB.**	
18a. Article 37 is amended as follows:	
~~3g.~~ **(a) Paragraph (1) is replaced by the following:**	
(1) 'Each Member State shall designate one or more competent authorities to be responsible for the application and enforcement of this Regulation, with exception of Chapters VIIb and VIIc (competent authorities). Member States may establish one or more new authorities or rely on existing authorities.'	
~~3i.~~ **(b) paragraph 3 is deleted.**	FR (Drafting suggestions): ~~**(b) paragraph 3 is deleted.**~~

PUBLIC

Commission proposal	Drafting suggestions and Comments
	FR (Comments): Les dispositions du paragraphe 3 de l'article 37 du règlement en vigueur constituent un point d'équilibre crucial entre les autorités compétentes. Le point f) modifié ci-dessous répond-il à cet objectif ?
~~3e.~~	
~~3f.~~	
~~3g.~~	
~~3m.~~ **(c) paragraph 5 is amended as follows:**	
~~3n.~~ **(-i) point f is replaced by the following:**	
~~3o.~~ **'(f) cooperating with competent authorities of other Member States and, where relevant, with the Commission, or the EDIB, or BEREC, to ensure the consistent and efficient application of this Regulation, including the exchange of all relevant information by electronic means, without undue delay, including regarding paragraph 10 of this Article;'**	
~~3p.~~ **(ii) point g is replaced by the following:**	
~~3q.~~ **'(g) 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 to ensure that this Regulation is enforced consistently with other Union and national law, including the exchange of all relevant information;'**	EE (Drafting suggestions): competent authorities to cooperate with each other to ensure the consistent application and enforcement of this Regulation with other Union and national law, including through the exchange of relevant information.
(d) paragraph 17 is added:	
17. 'BEREC shall facilitate regular exchanges among national competent authorities responsible for the application and enforcement of Articles 23 to 31 and Articles 34 and 35 of this Regulation and shall	

Commission proposal	Drafting suggestions and Comments
collect and disseminate, among those national competent authorities, best practices for the application and enforcement of those articles.'	
19. Article 38 is replaced by the following:	
'(1) Without prejudice to any other administrative or judicial remedy, natural and legal persons shall have the right to lodge a complaint, individually or, where relevant, collectively:	
(a) with the relevant competent authority in the Member State of their habitual residence, place of work or establishment if they consider that their rights under this Regulation have been infringed;	
(b) any matter falling within the scope of this Regulation specifically against a recognised data intermediation services provider or a recognised data altruism organisation, with the relevant competent authority for the registration of data intermediation services or the relevant competent authority for the registration of data altruism organisations.	
(2) The data coordinator shall, upon request, provide all the necessary information to natural and legal persons for the lodging of their complaints with the appropriate competent authority.	
(3) The competent authority with which the complaint has been lodged shall inform the complainant, in accordance with national law, of:	
(a) the progress of the proceedings, of the decision taken; and	
(b) the judicial remedies provided for in Article 39.	
(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. This cooperation shall not affect the cooperation mechanisms provided for by Chapters VI and VII of Regulation (EU) 2016/679 and by Regulation (EU) 2017/2394.	
(5) This Article shall not apply to Chapters VIIb and VIIc.'	
19a. in Article 39, paragraph (4) is inserted:	
'(4) This Article shall not apply to Chapters VIIb and VIIc.''	
20. ~~in~~ Article 40, paragraph **(4) is replaced by the following**~~(6) is inserted~~:	

PUBLIC

Commission proposal	Drafting suggestions and Comments
'(4)~~6.~~ This Article shall not apply to Chapter ~~VIIa,~~ **VIIb and** VIIc.	
(b) paragraph 5 is deleted. '	
21. after Article 41, the following heading is inserted:	
'CHAPTER IXa	
European Data Innovation Board;'	
22. the following Article 41a is inserted:	
'Article 41a	
European Data Innovation Board	
(1) The European Data Innovation Board is established as a means to advising and assisting the Commission in coordinating the enforcement of this Regulation and to serve as a forum of **strategic** discussion for the development of a European data economy and data policies.	
(2) It shall be composed at least of representatives of Member States competent for matters related to data, the competent authorities for enforcement of Chapters II, III, V, VIIa **of this Regulation and representatives' of Member States' authorities overseeing the implementation of Chapter**~~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. **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 participate 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.	LU (Comments): For reasons of legal certainty, Luxembourg insists that the terms "of this Regulation and representatives' of Member States' authorities overseeing the implementation of Chapter" should also refer to "competent bodies" designated in accordance with Chapter VII. Alternatively, Luxembourg could envisage to leave the wording of paragraph 2 untouched, provided that the recitals clearly indicate that the the notion of authorities in this context also includes 'competent authorities' designated in accordance with Chapter VIIc.
(3) The Commission shall decide on the composition of the different configurations in which the Board will fulfil its tasks.	

PUBLIC

Commission proposal	Drafting suggestions and Comments
(4) The Commission shall chair the meetings of the European Data Innovation Board.'	
23. Article 42 is replaced by the following:	
'Article 42	
Role of the EDIB	
(1) The EDIB shall support the consistent application of this Regulation by:	
(a) serving as a forum for strategic discussions on data policies, data governance, international data flows and cross-sectoral developments relevant to the European data economy;	
(b) advising and assisting the Commission with regard to developing consistent practice of competent authorities in the enforcement of Chapters II, III, V, VII, VIIa and VIIc;	
(c) facilitating cooperation between competent authorities through capacity-building and the exchange of information;	
(d) fostering an exchange of experience and good practice between the Member States in the field of re-use of public sector information in collaboration with other relevant governance bodies.;	
(e) advising and assisting the Commission with regard to the implementation of Chapters II, III, V, VII, VIIa and VIIc by suggesting development of guidance for businesses and public organisations;	
(f) advising and assisting the Commission on cross-sector standardisation issues;	
(g) ensuring active cooperation and coordination with other relevant bodies, and expert groups to ensure policy consistency in the digital single market.';'	CZ (Drafting suggestions): New points: **(h) advising and assisting the Commission with regard to:** **(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);**

Commission proposal	Drafting suggestions and Comments
	(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).** CZ (Comments): CZ cannot agree with the proposed limitation of the EDIB's powers to advise and assist the COM in preparing guidelines, harmonized standards, implementing and delegated acts (original Article 42(c) of the Data Act).
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)**, 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)**, 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.'	
(c) paragraph 6 is replaced by the following:	
'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 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	

PUBLIC

Commission proposal	Drafting suggestions and Comments
will not object. That period shall be extended by three months at the initiative of the European Parliament or of the Council.'	
25. Article 46 is amended as follows:	
(a) in paragraph 1, the first sentence is replaced by the following:	
'The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.'	
(b) the following paragraph 1a is inserted:	
'1a. Where reference is made to this paragraph, Article 4 of Regulation (EU) No 182/2011 shall apply.'	
26. Article 49 is amended as follows:	
(a) paragraph 1 is amended as follows:	
(i) the introductory wording is replaced by the following:	
'1. By 12 September 2028, the Commission shall carry out an evaluation of chapters II, III, IV, V, VI, VII, and VIII and submit a report on its main findings to the European Parliament and to the Council, and to the European Economic and Social Committee. That evaluation shall assess, in particular:'	
(ia) point (a) is replaced by the following:	
~~1b.~~ **(a) situations to be considered to be situations of exceptional need for the purpose of Article 15a of this Regulation and the application of Chapter V of this Regulation in practice, in particular the experience in the application of Chapter V of this Regulation by public sector bodies, the Commission, the European Central Bank and Union bodies; the number and outcome of the proceedings brought to the competent authority under Article 18(5) on the application of Chapter V of this Regulation, as reported by the competent authorities; the impact of other obligations laid down in Union or national law for the purposes of complying with requests for access to information; the impact of voluntary data-sharing mechanisms, such as those put in place by data altruism organisations recognised under Regulation (EU) 2022/868, on meeting the objectives of Chapter V of this Regulation, and the role of personal data in the context of Article 15a of this Regulation, including the evolution of privacy-enhancing technologies;'**	CZ (Drafting suggestions): **(a) situations to be considered to be situations of ~~exceptional need~~ public emergency for the purpose of Article 15a of this Regulation and the application of Chapter V of this Regulation in practice, in particular the experience in the application of Chapter V of this Regulation by public sector bodies, the Commission, the European Central Bank and Union bodies; the number and outcome of the proceedings brought to the competent authority under Article 18(5) on the application of Chapter V of this Regulation, as reported by the competent authorities; the impact of other obligations laid down in Union or national law for the purposes of complying with requests for access to information; the impact of voluntary data-sharing mechanisms, such as those put in place by data altruism organisations ~~recognised under Regulation (EU) 2022/868~~, on**

Commission proposal	Drafting suggestions and Comments
	meeting the objectives of Chapter V of this Regulation, and the role of personal data in the context of Article 15a of this Regulation, including the evolution of privacy-enhancing technologies;' CZ (Comments): CZ: For clarity purposes, CZ suggests removing the term 'exceptional need' entirely from the text… Also, the Digital Omnibus repeals the DGA.
(ii) point (m) is replaced by the following:	
'(m) the impact of this Regulation on SMEs and SMCs with regard to their capacity to innovate and to the availability of data processing services for users in the Union and the burden of complying with new obligations'	
(b) the following paragraph 2a is inserted:	
'2a. By [date = entry into force plus 5 years], the Commission shall carry out an evaluation of chapters VIIa, VIIb and VIIc of this Regulation and submit a report on its main findings to the European Parliament and to the Council as well as to the European Economic and Social Committee.	
The report shall assess, in particular:	
(a) the state of registrations of data intermediation services and the type of services they offer;	
(b) the type of data altruism organisations registered and an overview of the objectives of general interests for which data are shared in view of establishing clear criteria in that respect.'	
(c) the scope and social and economic impact of Chapter VIIc Section 2 including	
(d) the extent of the increase in re-use of public sector documents to which Section 2 of Chapter VIIc applies, especially by SMEs and SMCs;	
(ii)~~(e)~~ the impact of the high-value datasets;	
(iii)~~(f)~~ the interaction between data protection rules and re-use possibilities;	
(g) Member States shall provide the Commission with the Information necessary for the preparation of that report.'	
(c) paragraph **4**~~5~~ is replaced by the following:	

PUBLIC

Commission proposal	Drafting suggestions and Comments
'4~~5~~. On the basis of the reports referred to in paragraphs 1, ~~and~~ 2 and 2a, the Commission may, where appropriate, submit a legislative proposal to the European Parliament and to the Council to amend this Regulation.'	
27. Annex I is added as set out in the Annex II to this Regulation.	
Article 2 **Amendments to Regulation (EU) 2018/1724**	
In the table in Annex II to Regulation (EU) 2018/1724, the entry 'Starting, running and closing a business' is replaced by the following:	
[…]	
Article 3 **Amendments to Regulation (EU) 2016/679 (GDPR)**	
Regulation (EU) 2016/679 is amended as follows:	CZ (Drafting suggestions): CZ: New Article 2(4) **2. Article 2(4) is replaced by the following:** **'This Regulation shall be without prejudice to the application of Regulation 2022/2065, in particular the providers of intermediary services shall not be considered controllers when acting within the rules and conditions for limitation of their liability in Articles 4 to 8 of that Regulation.** CZ (Comments): CZ believes that due to recent judgment C-492/23 it is necessary to clarify the relation between DSA and GDPR regulation. CZ prefers to keep the limitations of liability meaningful. If GDPR still applies and creates

Commission proposal	Drafting suggestions and Comments
	obligations for controller, such obligations would effectively void most of the limitations of the requirements that are afforded by DSA to providers of intermediary services. The provisions of Article 4 – 7 of DSA would lose their effet utile in such a case.
1. Article 4 is amended as follows:	
~~(a) in point 1, the following sentences are added:~~	SK (Comments): **SK:** We support deletion of this proposal.
~~'Information relating to a natural person is not necessarily personal data for every other person or entity, merely because another entity can identify that natural person. Information shall not be personal for a given entity where that entity cannot identify the natural person to whom the information relates, taking into account the means reasonably likely to be used by that entity. Such information does not become personal for that entity merely because a potential subsequent recipient has means reasonably likely to be used to identify the natural person to whom the information relates.'~~	EE (Comments): Estonia strongly supports this amendment to the Commission's Proposal. IT (Drafting suggestions): **Replace the proposed additional sentences in Article 4(1) with:** 'Information relating to a natural person shall not constitute personal data in relation to a person or entity which cannot identify that natural person by means reasonably likely to be used by that person or entity. Where personal data have undergone pseudonymisation and are disclosed to a recipient which does not possess, and cannot reasonably and lawfully obtain or use, the additional information or other means necessary to identify the data subject, the information shall be regarded as anonymous information in relation to that recipient. The mere existence of identifying information held by the controller or another person, a theoretical possibility of obtaining such information, or a hypothetical future technological capability shall not constitute a means reasonably likely to be used. Where circumstances subsequently change so that the recipient obtains means reasonably likely to permit identification, the information shall constitute personal data for that recipient from that time.' IT (Comments): This gives operative effect to recipient-relative anonymity. The decisive criterion is whether the relevant entity has reasonably usable means of identification, not whether some other

Commission proposal	Drafting suggestions and Comments
	actor could theoretically re-identify the person. The wording remains temporal: data become personal for the recipient if reasonably usable identifying means are later obtained. AT (Comments): • AT **explicitely welcomes** that the definition of 'personal data' remains unchanged. SI (Comments): The definition of personal data is the foundation of the personal data protection framework in the EU and should remain unchanged. We support the deletion of this paragraph. FI (Comments): FI primarily supports the proposal not to make changes to the definition for personal data. Alternatively, FI can accept possible supplements to the definition of personal data that only codify the relevant CJEU case law. It is important that the supplements do not change the current level of data protection, to which the Commission's original proposal would lead to. This is a redline for FI. FI cannot accept supplements that would go beyond the relevant CJEU case law and would lead to attempts to circumvent the GDPR and would not bring clarity to smaller entities. For instance, FI might be willing to accept the first sentence "Information relating to a natural person is not necessarily personal data for every other person or entity, merely because another entity can identify that natural person" of the COM original proposal, accompanied with clarifying examples in the recital text.
(b) the following points are added:	

PUBLIC

PUBLIC

Commission proposal	Drafting suggestions and Comments
~~‘(32) ‘terminal equipment’ means terminal equipment as set out in Article 1(1) of Directive 2008/63/EC;~~	
~~(33) for ‘electronic communications networks’ the definition of Article 2(1) of Directive (EU) 2018/1972 shall apply;~~	
~~(34) ‘web browser’ means web browser as defined in Article 2(11) of Regulation (EU) 2022/1925;~~	
~~(35) ‘media service’ means a media service as defined in Article 2(1) of Regulation (EU) 2024/1083;~~	
~~(36) ‘media service provider’ means a media service provider as defined in Article 2(2) of Regulation (EU) 2024/1083;’~~	
~~(37) ‘online interface’ means an online interface as defined in Article 3(m) of Regulation (EU) 2022/2065.’~~	
(38) **'**~~“~~scientific research**'**~~”~~ means any research **conducted in an autonomous and independent manner**~~which can also support innovation, such as technological development and demonstration. These actions shall contribute to existing scientific knowledge or apply existing knowledge in novel ways, be carried out~~ with the aim of contributing to the growth of **society's**~~society´s~~ general knowledge and wellbeing**, generating new or complementing existing scientific knowledge, following a methodological and systematic approach consistent with standards of the relevant scientific field, including** ~~and adhere to~~ ethical standards**, and producing verifiable and transparent results** ~~in the relevant research area. This does not exclude that the research may also aim to further a commercial interest~~.’	CZ (Drafting suggestions): ~~“~~scientific research**'**~~”~~ means any research **conducted** ~~**in an autonomous and independent manner**~~~~which can also support innovation, such as technological development and demonstration. These actions shall contribute to existing scientific knowledge or apply existing knowledge in novel ways, be carried out~~ with the aim of contributing to the growth of **society's**~~society´s~~ general knowledge and wellbeing**, generating new or complementing existing scientific knowledge, following a methodological and systematic approach consistent with standards of the relevant scientific field, including** ~~and adhere to~~ ethical standards**, and producing verifiable and transparent results** ~~in the relevant research area.~~ **This does not exclude that the research may also aim to further a commercial interest**. CZ (Comments): CZ: CZ is concerned that it is not explained what is “an autonomous and independent manner”. To ensure, that every kind of entity may conduct

Commission proposal	Drafting suggestions and Comments
	research (even if it is a commercial entity, law enforcement body acting within GDPR or public entity that is not independent, we propose to delete these requirements. However, in line with the simplification agenda, CZ can be flexible as long if the last sentence on furthering a commercial interest is reinstated. CZ wishes to point out that the GDPR is currently more accommodating to scientific research (recitals 33, 157, 159) that this version of the compromise text. EE (Drafting suggestions): '“scientific research”' means any research **conducted in an autonomous and independent manner, which can also support innovation, such as technological development and demonstration,** ~~**These actions shall contribute to existing scientific knowledge or apply existing knowledge in novel ways, be carried out**~~ with the aim of contributing to the growth of **society's**~~**society´s**~~ general knowledge and wellbeing**, generating new or complementing existing scientific knowledge, following a methodological and systematic approach consistent with standards of the relevant scientific field, including** ~~**and adhere to**~~ ethical standards**, and producing verifiable and transparent results** ~~**in the relevant research area. This does not exclude that the research may also aim to further a commercial interest**~~.' EE (Comments): Estonia would prefer referring to the innovation and technological development also in the operative part of the text. AT (Comments):

Commission proposal	Drafting suggestions and Comments
	• AT **continues to reject** the inclusion of a definition for "scientific research" and is concerned about pseudo-scientific research being included in the compromise proposal. • Instead of introducing a new definition, reference should be made to existing definitions in sector-specific Union law. • AT remains open to the **inclusion of explanations** in Recital 29 (see above). In this context we refer to the EDPB Guidelines 1/2026 on processing of personal data for scientific research purposes. • If a definition is in fact included in the text, this would also put into question the proposed changes in Articles **5(1)(b)** and **13(6)** (see below). PL (Drafting suggestions): "scientific research" means research conducted in a methodological and systematic manner, consistent with ethical standards of the relevant scientific field, with the aim of generating new or complementing existing knowledge and contributing to scientific understanding and societal wellbeing. PL (Comments): On definition of scientific research (Article 4(38)), it is crucial to maintain the approach according to which the qualification of a given activity as scientific research is determined by its nature, in particular its autonomy, applied methodology, transparency and contribution to the development of knowledge, rather than by the legal status of the entity conducting the research. SI (Comments):

Commission proposal	Drafting suggestions and Comments
	We recognize this definition as a good compromise. If further changes are made, they should be aimed at a higher convergernce with the EDPB Guidelines 1/2026 on processing of personal data for scientific research purposes. SK (Comments): **SK:** We welcome the proposed changes and we see that they also reflect EDPB Guidelines 1/2026 on scientific research purposes. FI (Comments): FI supports the proposed definition of scientific research as it includes all the necessary elements for scientific research. FI also supports the recitals 28 and 32 which are balanced and take into account both the public and private interests.
2. Article 5 (1)(b) is replaced by the following:	IT (Drafting suggestions): **After point 2, insert a new point 2a:** 2a. In Article 6, the following paragraph 3a is inserted: '3a. For the purposes of paragraph 1, point (e), this Regulation constitutes a basis in Union law for the processing of personal data necessary for the development, training, testing, validation, evaluation, cybersecurity or safety improvement of an AI system or AI model where that system or model is demonstrably intended to serve a substantial public-interest objective. Such objectives shall include, in particular, public health, scientific or technological research, cybersecurity, public safety, accessibility, education, environmental protection, energy sustainability, resilience of essential services, prevention and detection of fraud, improvement of public administration and protection of fundamental rights. Processing under this paragraph may be undertaken by a public authority or by another natural or legal person. The controller shall document the public-interest objective pursued

Commission proposal	Drafting suggestions and Comments
	and shall process only the categories of personal data reasonably necessary for that objective. Processing fulfilling the conditions of this paragraph shall not require an additional assessment under point (f) of paragraph 1 IT (Comments): Article 6(1)(e) requires a Union or Member-State legal basis. The Digital Omnibus can itself supply that basis. This converts a recital-level possibility into a predictable legal ground for AI development serving a substantial public interest, including development performed by private entities.
'collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, **subject to the application of appropriate safeguards** in accordance with Article 89(1), be considered to be compatible with the initial purposes, independent of the conditions of Article 6(4) of this Regulation~~,~~ ('purpose limitation');'	LU (Drafting suggestions): 'collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, ***subject to the application of appropriate safeguards*** in accordance with Article 89(1), be considered to be compatible with the initial purposes, independent of the conditions of Article 6(4) of this Regulation**, and no legal basis separate from that which allowed the collection of the personal data is required**~~,~~ ('purpose limitation');' LU (Comments): We would like to repeat our previous suggestion to partially include recital (50) of the GDPR in Article 5(1)(b). To be more precise, we suggest specifying that in case of compatible further processing, no legal basis - separate from that which allowed the collection of the personal data- is required. This would clarify this provision and help the application of the Regulation for controllers. AT

Commission proposal	Drafting suggestions and Comments
	(Comments): • In principle, AT would be open to this proposal. However, in light of the also proposed very broad definition of "**scientific research**" (see above, comments on Article 4(38)), AT has serious concerns. • Extended possibilities for processing of personal data for (pseudo-)scientific research purposes would increase the volume of personal data processed for this purpose, which would constitute strong interferences with the rights of the data subject and entail a higher risk of data protection infringements. SI (Comments): We support retaining the requirement to ascertain whether processing for another purpose is compatible with the purpose for which the personal data were initially collected, as provided for in the fourth paragraph of Article 6 of the GDPR. SK (Comments): **SK:** We support this proposal. We do not consider it necessary to add the following part "subject to the application of appropriate safeguards". FI (Comments): FI supports this proposal.
3. Article 9 is amended as follows:	
(a) in paragraph 2, the following points are added:	IT (Drafting suggestions): **Add a further point (m) to Article 9(2):** In Article 9(2), add the following point:

Commission proposal	Drafting suggestions and Comments
	‘(m) processing is necessary for the development, training, testing, validation, evaluation or safety improvement of an AI system or AI model serving a substantial public-interest objective referred to in Article 6(3a), where that objective cannot reasonably be achieved to an equivalent standard without processing those categories of personal data and effective technical and organisational safeguards are implemented IT (Comments): The current point (k) addresses only incidental and residual special-category data. It does not cover cases in which special-category data are genuinely necessary to build socially useful AI, for example medical systems or systems designed to detect discrimination. The criterion should be necessity for the substantial public-interest objective, coupled with effective safeguards.
‘(k) **incidental and residual** processing in the context of the development and **technical** operation of an AI system as defined in Article 3, point (1), of Regulation (EU) 2024/1689 or an AI model **as referred to in Regulation (EU) 2024/1689**, subject to the conditions referred to in paragraph 5.	DK (Comments): It is still unclear to us what is meant by “incidental”. We therefore worry that this requirement make the provision very limited in practice and fail to address the challenge. Maybe “unintended” is a better word than incidental? NL (Drafting suggestions): ‘~~**(k) incidental and residual processing in the context of the development and operation of an AI system as defined in Article 3, point (1), of Regulation (EU) 2024/1689 or an AI model as referred to in Regulation (EU) 2024/1689, subject to the conditions referred to in paragraph 5.**~~ NL (Comments): NL remains seriously concerned about the proposed derogation to the prohibition on processing special categories of personal data for “residual” data when training and using AI (Article 9(2)(k) and 9(5) GDPR). This

Commission proposal	Drafting suggestions and Comments
	derogation risks normalising the presence of sensitive data in training, testing, validation, systems and models, which by themselves do not justify the processing of such sensitive data. Operators of AI systems would be allowed to process special categories of personal data if its removal would cause "disproportionate effort". This reverses the protective logic of data protection law and risks creating a perverse incentive: the more data are processed, the easier it becomes to justify the processing of special categories of personal data. NL fears that this exception - specifically for (generative) AI - lends itself to (very) liberal application in practice. Therefore, NL has repeatedly proposed to delete this exception, as it risks broad misuse. However, if a majority of the Member States supports this exception, NL considers it crucial that the conditions should be strictly limited (see below under Article 9(5) and our comments and suggestions regarding Recital 33). AT (Comments): • AT **can support** the proposed changes in Article 9(2)k. PL (Drafting suggestions): '(k) incidental and residual processing, **which is unintended and unavoidable despite the implementation of appropriate technical and organisational measures**, in the context of the development and technical operation of an AI system, as defined in Article 3, point (1), of Regulation (EU) 2024/1689 or an AI model as referred to in Regulation (EU) 2024/1689, subject to the conditions referred to in paragraph 5.

Commission proposal	Drafting suggestions and Comments
	PL (Comments): We acknowledge the clarifications in the recitals and the safeguards on incidental and residual processing of special categories of personal data by AI systems and models, including biometric data for identity verification. We support having legal clarity when it comes to training of AI models and we see a need for further discussions on this topic. Derogations should be interpreted strictly and in line with their purpose, and should not allow intentional processing of special categories of personal data for AI development. SI (Comments): We support this provision as it currently stands. SK (Comments): **SK:** All exemptions in Article 9 GDPR (except for explicit consent and data manifestly made public by data subject) are limited to a specific interest to be pursued by the processing (e.g. preventive or occupational medicine, defence of legal claim, ...). In our view, it is not clear in the proposal what interest justifies such an interference with the right to data protection. We would like to see further clarification of this interest. FI (Comments): FI supports the derogation for AI-processing in Article 9 GDPR, including the proposed text and safeguards. It is important that the derogation applies only to incidental and residual processing of special categories of personal data.

Commission proposal	Drafting suggestions and Comments
(l) processing of biometric data is **strictly** necessary for the purpose of confirming the identity of a data subject (verification), where the biometric data or the means needed for the **one-to-one** verification is under the sole control of the data subject **and, where applicable, subject to appropriate safeguards to protect the fundamental rights and the interests of the data subject, as laid down in Union law or Member State law, in accordance with paragraph 4 of this Article**.'	CZ (Drafting suggestions): CZ: processing of biometric data is ~~**strictly**~~ necessary for the purpose of confirming the identity of a data subject (verification), where the biometric data or the means needed for the **one-to-one** verification is under the sole control of the data subject **and, where applicable, subject to appropriate safeguards to protect the fundamental rights and the interests of the data subject, as laid down in Union law or Member State law, in accordance with paragraph 4 of this Article.** CZ (Comments): CZ: Regarding biometrics verification, CZ is against the addition of "strictly" in Article 9(2)(l), as the derogations already must be interpreted strictly and this exceptional approach, inconsistent with the rest of the Article 9, will make the derogation unpredictably narrow. Given the low-risk nature of biometric authentication, this would not be in line with the simplification agenda. ES (Comments): We support the Commission's proposal as originally drafted. We believe that the reference to national legislation added in the Council's proposal creates fragmentation and is unnecessary, since this exception applies only to biometrics for authentication (one-to-one) and safeguards are already specified in Recital 34; therefore, there is no need to refer to additional safeguards in national legislation. We support to maintain "where applicable"

PUBLIC

Commission proposal	Drafting suggestions and Comments
	AT (Comments): • AT **can support** the proposed changes in Article 9(2)l. PL (Comments): We maintain our previous concerns regarding the notion of "sole control" of the data subject. The current wording assumes that the existence of sole control can serve as a sufficiently clear criterion for permitting the processing of biometric data for verification purposes. However, in practice, the degree of control exercised by a data subject over biometric credentials, templates, devices or verification mechanisms may vary considerably depending on the technological solution used. Without further clarification, there is a risk that the notion of "sole control" could be interpreted differently across Member States and across sectors, leading to divergent implementation of the derogation. This may be particularly relevant in situations involving cloud-based authentication services, identity wallets, delegated credential management solutions or other complex technological environments. We therefore continue to consider it appropriate to clarify in the operative provision that the processing should be strictly limited to what is necessary for verification purposes and should not be used for any other purposes. SI (Comments): We support this provision as it currently stands. SK

PUBLIC

Commission proposal	Drafting suggestions and Comments
	(Comments): **SK:** We propose to delete the word "strictly". The other exceptions in Article 9(2) only use the word "necessary". In our view, there is no reason for such a deviation. We are worried that this could lead to a discussion as to whether the "necessity test" for this exception should be different from the "necessity test" for the other exceptions in Article 9(2) GDPR. The reference to Article 9(4) is not found in any other exception in Article 9(2). We propose to delete this part. In our view, this does not add any value, as Article 9(4) is only an option for Member States and this text merely repeats it. We are in favour of keeping this text only in recital. FI (Comments): Concerning the derogation for biometric verification in Article 9 GDPR [Art 3(3)(a) Digiomnibus], FI would have preferred to harmonise this matter in the GDPR, complemented with additional safeguards. FI can show flexibility in this (not a redline), if the majority of MS support it, although this proposal does not support the aim to simplify. FI supports the new modification under which processing is possible only when it is strictly necessary.
(b) the following paragraph is added:	
'5. For processing referred to in point (k) of paragraph 2, appropriate organisational and technical measures shall be implemented to avoid~~,~~ the collection and otherwise processing of special categories of personal data. Where, despite the implementation of such measures, the controller identifies special categories of personal data **that are incidentally and residually involved** in the datasets used for training, testing or validation or in the AI system or AI model, the controller shall **erase**~~remove~~ such data **without undue delay. If erasure**~~. If removal~~ of those data **proves to be technically impossible or** requires **manifestly** disproportionate effort, the controller	CZ (Drafting suggestions): For processing referred to in point (k) of paragraph 2, appropriate organisational and technical measures shall be implemented to avoid~~,~~ the collection and otherwise processing of special categories of personal data. Where, despite the implementation of such measures, the controller identifies special categories of personal data **that are incidentally and residually involved** in the datasets used for training, testing or validation or in the AI

Commission proposal	Drafting suggestions and Comments
shall**,** ~~**in any event effectively protect**~~ without undue delay **and in any event, effectively protect** such data from being **further processed or processed for other purposes,** used to produce outputs,~~ from being~~ disclosed or otherwise made available to third parties.'	system or AI model, the controller shall **erase**~~remove~~ such data **without undue delay. If erasure**~~. If removal~~ of those data **proves to be technically impossible or** requires ~~**manifestly**~~ disproportionate effort, the controller shall**,** ~~**in any event effectively protect**~~ without undue delay **and in any event, effectively protect** such data from being **further processed** ~~**or processed for**~~ **other purposes,** used to produce outputs,~~ from being~~ disclosed or otherwise made available to third parties. CZ (Comments): CZ: In Article 9(5), the wording "manifestly disproportionate effort" lacks a basis in GDPR terminology and may create interpretative issues. Also, the wording "further processed or processed for other purposes" is too vague and restrictive. To keep GDPR standards, CZ proposes deleting "manifestly" and use the phrase "further processed for other purposes". NL (Drafting suggestions): 5. For processing referred to in point (k) of paragraph 2, **this derogation shall apply only where special categories of personal data appear incidentally and unintentionally, where the processing does not rely on such data, and where the controller has implemented** appropriate organisational and technical measures ~~**shall be implemented**~~ to avoid the collection and otherwise processing of special categories of personal data. Where, despite the implementation of such measures, the controller identifies special categories of personal data that are incidentally and residually involved in the datasets used for training, testing or validation or in the AI system, the controller shall erase such data without undue delay. If erasure of those data proves to be technically impossible ~~**or requires manifestly disproportionate effort**~~, the controller shall, without undue delay and in any event, effectively protect such data from being further processed or processed

Commission proposal	Drafting suggestions and Comments
	for other purposes, used to produce outputs, disclosed or otherwise made available to third parties. The controller shall establish a process of regular verification and assessment of the effectiveness of the measures implemented and shall comprehensively document those measures and the results of the assessments throughout the life cycle of the AI system.' NL (Comments): NL remains seriously concerned about the proposed derogation to the prohibition on processing special categories of personal data for **"residual" data** when training and using AI (Article 9(2)(k) and 9(5) GDPR). NL has repeatedly proposed to delete this because of the risk of abuse and the decrease of the incentive for privacy by design. However, if a majority of the Member States supports this exception, NL considers it crucial that these provisions should be limited more strictly. At least, the reference to **"disproportionate effort"** should be deleted. That means that the exception should not be applicable in case of a 'disproportionate effort' to remove the personal data, but only in case the removal is "technically impossible". The reference to disproportionate effort reverses the protective logic of data protection law: the more data are processed for AI, the easier it becomes to justify that it requires a disproportionate effort to erase the special categories of personal data. Furthermore, the exception should be limited in other ways, for example by defining "incidental and residual" strictly (meaning that the processing may not rely on the special categories of data). Moreover, the "appropriate organisational and technical measures" have to be specified further, for example in Recital 33, including also the obligation to filter out special categories of personal both during data collection and immediately after data collection (cf. EDPB, Report of the work undertaken by the ChatGPT Taskforce, adopted on 23.05.2024, p 7, §19 and §17).

Commission proposal	Drafting suggestions and Comments
	AT (Comments): • AT **can support** the proposed changes in Article 9(5). PL (Comments): While we support the objective of ensuring safeguards in situations involving incidental processing of special categories of personal data, we remain concerned that paragraph 5 continues to introduce a highly detailed and prescriptive compliance framework. The provision goes beyond establishing substantive safeguards and increasingly regulates how controllers must organise and document their compliance activities throughout the lifecycle of an AI system. In particular, the cumulative obligations relating to prevention measures, deletion assessments, protection mechanisms, regular verification, effectiveness assessments and comprehensive documentation create a compliance structure that significantly exceeds what is typically required under the GDPR accountability framework. This raises concerns regarding proportionality and regulatory coherence. Articles 5(2), 24 and 25 GDPR already require controllers to implement appropriate organisational and technical measures and to demonstrate compliance. Additional obligations should therefore be carefully assessed to avoid unnecessary duplication and excessive administrative burden. In its current form, paragraph 5 risks discouraging reliance on Article 9(2)(k) even in situations that the provision is specifically intended to address. Further simplification and closer alignment with the existing GDPR accountability framework is needed.

PUBLIC

Commission proposal	Drafting suggestions and Comments
	While the earlier version raised concerns due to its broad and open-ended character, the current wording risks becoming excessively prescriptive by introducing a highly detailed and cumulative set of operational requirements. In our view, the provision should maintain an appropriate balance between effective safeguards for special categories of personal data and practical implementability. A more balanced approach would better ensure both a high level of data protection and the effective usability of the derogation in situations for which it is intended SI (Comments): We support this provision as it currently stands. FI (Comments): FI supports the derogation for AI-processing in Article 9 GDPR, including the proposed text and safeguards. It is important that the derogation applies only to incidental and residual processing of special categories of personal data.
4. In Article 12, paragraph 5 is replaced by the following:	SK (Comments): **SK:** We support this proposal.
'5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character or ~~[also, for requests under Article 15,]~~ **where an abusive intention on the part of** ~~because~~ the data subject **submitting those requests can be demonstrated** ~~abuses the rights conferred by this regulation for purposes other than the protection of their data~~, the controller may either:	CZ (Comments): CZ: CZ prefers the original Commission proposal based on the reasonable grounds to believe that the request is excessive, otherwise it may be too complicated to prove the abusive intention. CZ could also accept DE proposal. DK

Commission proposal	Drafting suggestions and Comments
	(Comments): The simplification regarding the burden of proof should be incorporated into the text. The original text of the Commission ("has reasonable grounds to believe") would be sufficient for us in this regard. Alternatively we support the previous proposal from GER and POL on an alternative wording. AT (Comments): • AT **can support** the changes in Article 12(5). PL (Comments): We maintain our previous position because the wording of the provision has not been changed and the notion of "abusive intention" still remains insufficiently precise and may lead to divergent interpretations and inconsistent application of the provision across Member States, in particular as regards the controller's ability to demonstrate the grounds for concluding that such intention existed on the part of the data subject. SI (Comments): We support the text as set forth in this proposal. We will not support solutions that would infringe upon an individual's right to access the data being processed about them. The burden of demonstrating that a request is manifestly unfounded or excessive should therefore remain with the controller. It is also key that the formulation "for purposes other than the protection of their data" is not reinserted into the text. FI

PUBLIC

Commission proposal	Drafting suggestions and Comments
	(Comments): FI supports this proposal. FI finds it important to ensure that the proposal would not weaken the current level of protection and would take into account the CJEU case law. The controller should have the burden of demonstrating abusive intentions. For instance, the recent judgement (from March 2026) in case Brillen Rottler (C-526/24) is important. FI does not support changes that go beyond the CJEU case law.
(a) charge a reasonable fee **proportionate to**~~**taking into account**~~ the administrative costs of providing the information or communication or taking the action requested; or	SI (Comments): We support this provision as it currently stands FI (Comments): FI supports this proposal.
(b) refuse to act on the request **and inform the data subject of the reasons thereof**.	SI (Comments): We support this provision as it currently stands FI (Comments): FI supports this proposal.
The controller shall bear the burden of demonstrating**, in the light of all the relevant circumstances of the case,** that the request is manifestly unfounded or **excessive.**	ES (Drafting suggestions): The controller shall bear the burden of demonstrating**, in the light of all the relevant circumstances of the case,** that the request is manifestly unfounded or **excessive.**

Commission proposal	Drafting suggestions and Comments
	The exercise of the rights recognized in Articles 15 to 22 shall not be conditional upon the obligation of the interested party to justify his request. However, the total absence of indication on the purpose of the access may be taken into account together with the other concurrent circumstances to assess the manifestly unfounded or excessive nature of the request. ES (Comments): We recall that we had suggested to add a paragraph: "*The exercise of the rights recognized in Articles 15 to 22 shall not be conditional upon the obligation of the interested party to justify his request. However, the total absence of indication on the purpose of the access may be taken into account together with the other concurrent circumstances to assess the manifestly unfounded or excessive nature of the request."* Not a red line, but we think it could help clarify. PL (Drafting suggestions): „The controller shall bear the burden of demonstrating that the request is manifestly unfounded or that there are reasonable grounds to believe that it is excessive or submitted with an abusive intention, based on objective circumstances related to the request or the conduct of the data subject.” PL (Comments): We maintain our previous wording proposal.

Commission proposal	Drafting suggestions and Comments
	FI (Comments): FI supports this proposal.
5. In Article 13, ~~paragraph 4 is replaced by~~ the following **paragraph 5 is added**:	DK (Comments): Article 13(4) should be formulated in a less complex and more practical manner. We support the previous proposal from GER and POL on an alternative wording.
'4.5 ~~5.~~ Paragraphs 1~~, 2 and 3~~ **and 2** shall not apply where the **following circumstances are met:**	CZ (Comments): CZ: CZ prefers DE proposal, which is simpler and easier for practice to adopt and use. However, since DE proposal refers to para 4 and is not written in the style of EU regulations, CZ is flexible as to the formal changes of wording. PL (Drafting suggestions): (5) Paragraphs 1 and 2 shall not apply if and to the extent that the data subject already has the information or if the provision of such information proves impossible or, provided the processing is to result in a low risk to data subjects, would involve a disproportionate effort, especially in every-day business. Article 14(5)(b) shall apply accordingly." "Sentence 1st, 2nd and 3rd alternative, shall not apply where the processing concerns personal data referred to in Articles 9 or 10 of this Regulation, or where the personal data are further processed for purposes other than those for which the data were originally collected."

PUBLIC

Commission proposal	Drafting suggestions and Comments
	PL (Comments): We acknowledge the Presidency work on this paragraph. We would like this paragraph to bring substantial simplification, in particular for SMEs. We maintain our wording proposal of Article 13(5). FI (Comments): FI supports this proposal.
a)~~**personal data have been collected in the context of a clear and circumscribed relationship between data subjects and a controller exercising an activity that is not data-intensive and**~~ there are reasonable grounds to assume that the data subject already has the information referred to in points (a) and (c) of paragraph 1~~**, unless the**~~ **and the personal data are collected in the context of a direct and clearly circumscribed relationship between data subjects and a** controller**;**	SK (Comments): **SK:** We believe that the relationship between the data subject and the controller will always meet the condition of "direct", since personal data are obtained directly from the data subject. However, we are interested in what the criteria are for “clearly circumscribed relationship” and “there are reasonable grounds to assume that the data subject already has the information”. What should the controller take into account when assessing these two criteria. FI (Comments): FI supports this proposal.
b) ~~**transmits the data to other recipients or categories of recipients, transfers the data to a third country, carries out automated decision-making, including profiling, referred to in Article 22(1), or**~~ the processing **of personal data is not**~~**is**~~ likely to result in a high risk to the rights and freedoms of data subjects within the meaning of Article 35**;**	FI (Comments): FI supports this proposal.

Commission proposal	Drafting suggestions and Comments
c) the processing of personal data does not involve complex processing operations, the processing of large amounts of personal data, special categories of personal data, or personal data relating to criminal convictions and offences;	AT (Drafting suggestions): c) the processing of personal data does not involve complex processing operations, the **large scale** processing ~~**of large amounts**~~ of personal data, special categories of personal data, or personal data relating to criminal convictions and offences; AT (Comments): • AT can **support** the compromise proposal on Article 13(5) and Recital 36 GDPR. The proposed amendments provide important clarifications. • In order to safeguard the consistent terminology of the GDPR, we would suggest that instead of using the term "processing of a large amount of personal data" the term "**large scale processing of personal data**" should be used. A term, that is already used in the GDPR, notably in Article 35 – which the proposed Article 13(5)a itself refers to – as well as Article 37, and covered by relevant EDPB guidelines. • Alternatively, we would ask the Presidency for the reasoning for using the term "processing of large amounts of personal data" instead of "large scale processing of personal data". SI (Comments): We support this provision as it currently stands SK (Comments): **SK:** It is not clear what is covered by "involve complex processing operations" and "the processing of large amounts of personal data". FI (Comments):

Commission proposal	Drafting suggestions and Comments
	FI supports this proposal.
d) the controller does not transmit the data to other recipients or categories of recipients, transfer the data to a third country, nor carry out automated decision-making, including profiling, referred to in Article 22(1).'	SI (Comments): We support this provision as it currently stands SK (Comments): **SK:** We propose to add the term "international organisation" to this provision regarding transfer.We see no reason why it should not be included. FI (Comments): FI supports this proposal.
6. In Article 13, paragraph ~~5~~**6** is added:	
'~~5~~**6**. When the **further** processing takes place for scientific research purposes **by the same controller and where and insofar as**~~and~~ the provision of information referred to under paragraphs 1, 2 and 3 proves impossible or would involve a disproportionate effort ~~subject to the conditions and safeguards referred to in Article 89(1)~~ or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that **further** processing**, subject to the conditions and safeguards referred to in Article 89(1)**, the controller does not need to provide the information referred to under paragraphs 1, 2 and 3. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available.'	AT (Comments): • In principle, AT would be open to this proposal. • However, in light of the also proposed very broad definition of **"scientific research"** (see above, comments on Article 4(38) and Article 5(1)b), AT **cannot support** it. • Extended possibilities for processing of personal data for (pseudo-)scientific research purposes would lead to an increase of the volume of personal data processed for this purpose, which would constitute strong interferences with the rights of the data subject. Paired with a limitation of the data subjects' rights this would increase the risk of data protection infringements. SK (Comments): **SK:** It is not clear to us when providing information to the data subject would require a disproportionate effort, given that the personal data were originally

Commission proposal	Drafting suggestions and Comments
	obtained directly from the data subject, and we therefore believe that the controller has the data subject's contact details, which could be used to provide information about further processing for scientific research purposes. We wish for further clarification of this situation as we are not convinced by the reasoning given in recital 37 "where the controller at the time of collection of the personal data did not know or anticipate that it would process personal data for scientific research purposes at a later stage, in which case it may not have easily available contact details of the data subjects". We see that this proposal is similar to Article 14(5)(b) GDPR, but there is a difference between these scenarios because in the case of Article 14, the personal data were not initially obtained directly from the data subject and there is a possibility that it is not easy for the controller to provide information about the processing *(it proves impossible or would involve a disproportionate effort)*. FI (Comments): FI supports this proposal.
7. ~~In~~ Article 22~~, paragraphs 1 and 2 are~~ **is** replaced by the following:	AT (Drafting suggestions): ~~7. In Article 22, paragraphs 1 and 2 are is replaced by the following:~~ AT (Comments): • In light of the still pending case in front of the CJEU, C-568/25, we would argue for the **deletion of Article 22** from the Digital Omnibus in total. PL (Comments):

Commission proposal	Drafting suggestions and Comments
	As the text does not address our comments, we maintain our previous position. We preferred the COM proposal. We maintain our previously submitted comments regarding Article 22(1), as the wording of this provision remains unchanged. At the same time, we note that paragraphs 2 and 3 reproduce safeguards already contained in the current Article 22(3) and (4) GDPR. As a result, the proposal maintains the existing status quo. The normative effect of the provision remains essentially identical to that of the current Article 22 GDPR. In this context, the added value of reopening Article 22 within the framework of the Omnibus initiative requires clarification. Consideration could be given to whether additional clarification of the key concepts and conditions governing automated decision-making would better contribute to the simplification objectives of the initiative while maintaining the current level of protection of data subjects. SI (Comments): We support this Article as it currently stands SK (Comments): **SK:** We support this proposal.
‘1. **The**~~A decision which produces legal effects for a~~ data subject **shall have the right not to be subject to a decision**~~or similarly significantly affects him or her may be~~ based solely on automated processing, including profiling, **which produces legal effects concerning him or her or similarly significantly affects him or her, unless such processing**~~only where that decision~~:	AT (Drafting suggestions): ~~‘1. The A decision which produces legal effects for a data subject shall have the right not to be subject to a decision or similarly significantly affects him or her may be based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly~~

Commission proposal	Drafting suggestions and Comments
	~~significantly affects him or her, unless such processing~~~~only where that decision~~: FI (Comments): FI support this proposal.
(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller ~~regardless of whether the decision could be taken otherwise than by solely automated means~~;	CZ (Drafting suggestions): is necessary for entering into, or performance of, a contract between the data subject and a data controller **regardless of whether the decision could be taken otherwise than by solely automated means**; CZ (Comments): CZ: CZ believes that this explanatory amendment, while not elegant, is in line with simplification agenda and has real added value by establishing EU-wide consensus and deepening internal market with online services. AT (Drafting suggestions): ~~(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller~~ ~~regardless of whether the decision could be taken otherwise than by solely automated means~~; FI (Comments): FI supports this proposal.
(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or	AT (Drafting suggestions):

PUBLIC

Commission proposal	Drafting suggestions and Comments
	~~(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or~~ FI (Comments): FI supports this proposal.
(c) is based on the data subject's explicit consent.	AT (Drafting suggestions): ~~(c) is based on the data subject's explicit consent.~~
2. In the cases referred to in points (a) and (c) of paragraph 1, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.	AT (Drafting suggestions): ~~**2. In the cases referred to in points (a) and (c) of paragraph 1, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.**~~ FI (Comments): FI supports this proposal.
3. Decisions referred to in paragraph 1 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.'	AT (Drafting suggestions): ~~**3. Decisions referred to in paragraph 1 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.'**~~ FI (Comments):

Commission proposal	Drafting suggestions and Comments
	FI supports this proposal.
(7a) In Article 25, paragraphs 1 and 2 are replaced by the following:	EE (Drafting suggestions): ~~**(7a) In Article 25, paragraphs 1 and 2 are replaced by the following:**~~ EE (Comments): Estonia has concerns about extending the duty of data protection by design and by default to processors. This may create uncertainty in the division of responsibilities between controllers and processors and could run counter to the objective of reducing regulatory burden. By extending the principles of data protection by design and by default directly to processors as well, it blurs the controller's responsibility under Article 5(2) GDPR. In addition, if Article 28 still provides that the controller determines what the processor must do and how, and the processor acts accordingly, then the purpose of this amendment is not clear. Recital 39a states with regard to processors: "to the extent of its own obligations" – we kindly ask to specify what exactly does this mean in practice. Moreover, the current recital 78 already states that "When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations." We are of the opinion that the current text of GDPR already adresses the imbalance in between small controllers and large processors. FR (Drafting suggestions): **7a'. Article 24 is amended as follows:**

Commission proposal	Drafting suggestions and Comments
	(a) paragraph 1 is replaced by the following: '1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, **with particular regard to the lists referred to in Article 35(4) and (5),** the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.' **7c. Article 32 is amended as follows:** **(a) paragraph 1 is replaced by the following:** '1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, **with particular regard to the lists referred to in Article 35(4) and (5),** the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.' **(b) the following paragraph is added:**

Commission proposal	Drafting suggestions and Comments
	‘5. The Board shall publish guidance for the purpose of further specifying the appropriate technical and organisational measures to ensure a level of security appropriate to the level of risk linked to the different types of processings as mentioned in paragraph 1. FR (Comments): Les autorités françaises soutiennent les amendements apportés à l’article 25. Elles rappellent néanmoins qu’elles ont proposé d’autres amendements aux articles 24 et 32, en cohérence avec les amendements apportés à l’article 25 en matière d’approche fondée sur les risques. IT (Drafting suggestions): **Insert Article 24 amendment and revise Article 25:** Insert a new point 7a before the current point (7a), and renumber the current point as 7b: ‘7a. In Article 24, paragraph 1 is replaced by the following: “1. The controller shall implement effective technical and organisational measures to ensure and demonstrate that processing is performed in accordance with this Regulation. Except where this Regulation or other Union law expressly requires a specific measure, the controller shall determine the technical and organisational means by which compliance is achieved. Compliance may be demonstrated by any reliable evidence, including operational records, technical testing, audit results, system logs, certifications or documented controls. The absence of a particular policy, template, methodology or form of documentation shall not in itself constitute an infringement where the controller demonstrates effective compliance with the substantive requirements of this Regulation.”’ Renumber the current point (7a) as point 7b and replace Article 25(1) with: ‘1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing, the controller and the processor shall implement effective technical and organisational measures designed to achieve the data-protection

Commission proposal	Drafting suggestions and Comments
	principles and substantive requirements of this Regulation. Except where a specific measure is prescribed by Union law, the controller and processor shall retain discretion as to the technical and organisational means used to achieve those results.' IT (Comments): Article 24 should become the general expression of outcome-based accountability and freedom of means. Article 25 should then remove "risks of varying likelihood and severity" as the organising legal criterion. Authorities may evaluate whether the required result was achieved, but should not substitute their preferred architecture for another technically effective solution unless Union law prescribes a particular measure AT (Comments): • AT **can support** the proposed changes to Article 25. SI (Comments): We support this Article as it currently stands SK (Comments): **SK:** We support adding processor in this paragraphs. We would propose not to add reference to the lists referred to in Article 35(4) and (5).
'1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, with particular regard to the lists referred to in Article 35(4) and (5), the controller and the processor shall, both at the time of the determination of the means for processing and at the time of the processing itself as applicable, implement, in an effective manner, appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, and to integrate the	CZ (Drafting suggestions): ~~**1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, with particular regard to the lists referred to in Article 35(4) and (5), the controller and the processor shall, both at the time of the determination of the means for processing and at the time of the processing itself as applicable, implement, in an**~~

Commission proposal	Drafting suggestions and Comments
necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.	~~effective manner, appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.~~ CZ (Comments): CZ doubts that these changes solve any essential problem. On the contrary, there will be interpretative problems because there are not corresponding changes to Articles 24 and 32. CZ believes that this proposal is not in the line of simplification agenda, because it is motivated by the effort to influence the setup of services proposed by the processor. EE (Drafting suggestions): ~~'1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, with particular regard to the lists referred to in Article 35(4) and (5), the controller and the processor shall, both at the time of the determination of the means for processing and at the time of the processing itself as applicable, implement, in an effective manner, appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.~~ EE

Commission proposal	Drafting suggestions and Comments
	(Comments): Estonia is also of the opinion that the processor cannot determine the means for processor, this can be only done under the proxy of the controller. PL (Drafting suggestions): We maintain our previously submitted drafting suggestion: "The allocation of responsibilities between the controller and the processor regarding the implementation of these measures shall be clearly defined, in particular in the contract or other legal act referred to in Article 28(3)." PL (Comments): We maintain our previous concerns regarding the practical allocation of responsibilities between controllers and processors under Article 25. While we acknowledge the intention to reflect current technological and market realities by extending data protection by design and by default obligations to processors, the proposed wording does not sufficiently clarify how responsibilities should be allocated in practice between the parties. Given that the controller remains primarily responsible under the GDPR for ensuring compliance with the Regulation, additional clarification would be beneficial in order to avoid legal uncertainty, overlapping obligations and potential inconsistencies in implementation. This issue becomes particularly relevant where technical and organisational measures are designed, developed or maintained by processors on behalf of multiple controllers. In such situations, greater clarity regarding the respective responsibilities of the parties would contribute to legal certainty and facilitate the practical application of the provision.

PUBLIC

Commission proposal	Drafting suggestions and Comments
	FI (Comments): FI has reservations as regards to adding processors in Article 25 without a proper assessment but understands that processors should also have responsibility especially in situations where SMEs use processors that provide services with "take it or leave it" conditions. However, this is not a redline.
2.The controller and the processor shall implement appropriate technical and organisational measures to ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible to an indefinite number of natural persons without the individual's intervention.	CZ (Drafting suggestions): ~~**2.The controller and the processor shall implement appropriate technical and organisational measures to ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible to an indefinite number of natural persons without the individual's intervention.**~~ CZ (Comments): CZ doubts that these changes solve any essential problem. On the contrary, there will be interpretative problems because there are not corresponding changes to Articles 24 and 32. CZ believes that this proposal is not in the line of simplification agenda, because it is motivated by the effort to influence the setup of services proposed by the processor. EE

Commission proposal	Drafting suggestions and Comments
	(Drafting suggestions): ~~**2.The controller and the processor shall implement appropriate technical and organisational measures to ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible to an indefinite number of natural persons without the individual's intervention.**~~
8. Article 33 is amended as follows:	IT (Drafting suggestions): **Insert before point 8:** Before point 8, insert a new point 7c: ‘7c. Article 32 is replaced by the following: “Article 32 Security of processing 1. The controller and processor shall implement and maintain effective technical and organisational measures capable of ensuring: (a) confidentiality of personal data; (b) integrity and authenticity of personal data and processing operations; (c) availability and resilience of processing systems and services; (d) timely restoration of availability following a physical or technical incident; (e) effective access control and authentication; (f) detection, containment and remediation of unauthorised access, disclosure, alteration or loss; and (g) regular testing and verification of the effectiveness of those measures. 2. Compliance with paragraph 1 shall be assessed by reference to the effectiveness of the measures actually implemented and maintained. Completion of a risk assessment or use of a particular risk methodology shall not constitute a condition of compliance.”’ IT

Commission proposal	Drafting suggestions and Comments
	(Comments): Article 32 should be converted from a risk-calibration provision into a security-performance provision. The regulation should define the outcomes that must be achieved while leaving controllers and processors reasonable technical freedom as to how they achieve them. SK (Comments): **SK:** We support this proposal.
(a) paragraph 1 is replaced by the following:	
'1. In the case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall without undue delay and, where feasible, not later than 96 hours after having become aware of it, notify the personal data breach via the **national entry**~~single-entry~~ point established pursuant to Article **23b**~~23a~~ of Directive (EU) 2022/2555 to the supervisory authority competent in accordance with Article 55 and Article 56 **of this Regulation**. Where the notification to the supervisory authority is not made within 96 hours, it shall be accompanied by reasons for the delay.'	EE (Drafting suggestions): 1. In the case of a personal data breach that is likely to result in **an increased risk** ~~a high risk~~ to the rights and freedoms of natural persons, the controller shall without undue delay and, where feasible, not later than 96 hours after having become aware of it, notify the personal data breach via the **national entry**~~single-entry~~ point established pursuant to Article **23b**~~23a~~ of Directive (EU) 2022/2555 to the supervisory authority competent in accordance with Article 55 and Article 56 **of this Regulation**. Where the notification to the supervisory authority is not made within 96 hours, it shall be accompanied by reasons for the delay.' EE (Comments): Estonia supports reducing unnecessary data breach notifications but notes that controllers might underestimate their impact on data subjects. Multiple low-risk breaches, when combined, could pose higher risks to individuals' rights and DPAs should be made aware of those. We recommend using terms like "impactful risks" or "increased risks." ES (Comments):

Commission proposal	Drafting suggestions and Comments
	We prefer 72 hours. In other regulations, this period is even shorter. If we want to harmonize this period, has no sense to increase it here. IT (Drafting suggestions): **Replace the proposed Article 33(1) and revise paragraph 6:** Replace Article 33(1) with: '1. Where a personal data breach satisfies one or more of the objective materiality criteria established pursuant to paragraph 6, the controller shall, without undue delay and, where feasible, not later than 96 hours after becoming aware of it, notify the personal data breach through the single-entry point established pursuant to Directive (EU) 2022/2555 to the competent supervisory authority.' Replace paragraph 6 with: '6. The Commission shall establish, by implementing act, objective and technologically neutral materiality criteria specifying the categories of personal data breaches that require notification. Compliance with those criteria shall replace any obligation to conduct an individual assessment of the likelihood or severity of risk for the purposes of this Article. The Commission may also establish a common notification template. The criteria shall be reviewed periodically in the light of technological and security developments.' IT (Comments): This retains a high notification threshold but makes it objective and harmonised. Controllers should document all breaches and remediation measures, but should notify only when the incident meets defined materiality criteria, rather than conducting a bespoke high-risk analysis for every event. AT (Drafting suggestions): '1. In the case of a personal data breach that is likely to result in **~~a high risk~~an impactful/relevant/increased risk** to the rights and freedoms of natural persons, the controller shall without undue delay and, where feasible, not later than **~~96~~72** hours after having become aware of it, notify the personal

Commission proposal	Drafting suggestions and Comments
	data breach via the national entry~~single-entry~~ point established pursuant to Article 23b~~23a~~ of Directive (EU) 2022/2555 to the supervisory authority competent in accordance with Article 55 and Article 56 of this Regulation. Where the notification to the supervisory authority is not made within **~~96~~72** hours, it shall be accompanied by reasons for the delay.' AT (Comments): • AT **remains very sceptical** about raising the threshold for data breach notifications to the supervisory authority. According to the current legal framework, all data breaches have to be notified to the supervisory authority, those that pose a high risk to the rights and freedoms of data subject additionally have to be notified to the data subject. The proposed changes would eliminate any notification of data breaches that do not meet the requirements of "high risk to the rights and freedoms of data subjects". It would therefore depend solely on the processor to determin, what measures to take to remedy data breaches that pose **a significant but not necessarily high** risk to the rights and freedoms of data subjects. • As a consequence, the EDPB might need to update its guidelines on the assessment of a "high risk" in accordance with Article 70(1)h GDPR. • Furthermore, the raising of the material threshold ("high risk") **in combination** with the extended time limit for data breach notifications ("96h") substantially weakens the protection of the data subjects' rights. • A compromise would be to introduce a threshold between "a risk" and "a high risk", such as "**an impactful/relevant/increased risk**". • AT generally supports the alignment of time-limits in different legal acts • AT supports maintaining the **72h time limit**. PL (Comments):

Commission proposal	Drafting suggestions and Comments
	We strongly support to have the extended deadline for breach notification (96 hours). Extending the notification deadline could also improve the quality and proportionality of breach notifications. In practice, controllers faced with a relatively short notification deadline may be incentivised to notify incidents at a very early stage of the investigation in order to avoid the risk of non-compliance, even where it remains unclear whether the incident meets the threshold for notification. Providing additional time would allow controllers to conduct a more thorough assessment of the incident and its potential impact on the rights and freedoms of natural persons before deciding whether notification is required. This could contribute to reducing precautionary or defensive notifications and enable supervisory authorities to focus their resources on breaches that genuinely meet the notification threshold. Furthermore, the practical challenges associated with assessing incidents within 72 hours may be particularly significant where breaches occur immediately before weekends, public holidays or other periods during which the availability of relevant personnel may be limited. FI (Comments): FI supports this proposal, including the high-risk threshold, and prefers maintaining the current 72 hours.
(b) the following paragraph is added:	
'1a. Until the establishment of the **national entry**~~single-entry~~ point pursuant to Article **23b**~~23a~~ of Directive (EU) 2022/2555, controllers shall continue to notify personal data breaches directly to the competent supervisory authority in accordance with Article 55 and Article 56 **of this Regulation**.'	
(c) the following paragraphs are added:	
'6. The Board shall **establish and make public**~~prepare and transmit to the Commission a proposal for~~ a common template for notifying a personal data breach to the competent supervisory authority referred to in paragraph 1	EE (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
as well as ~~for~~ a list of the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person **and a list of the circumstances in which it is not likely to result in such a high risk. The template and lists**~~. The proposals~~ shall be **available**~~submitted to the Commission~~ within [OP date = nine months of the entry into application of this Regulation]. ~~The Commission~~ ~~may~~~~after due consideration reviews it, as necessary, and is empowered to adopt~~ ~~the template as established by the Board~~**it by way of an implementing act, in accordance with the examination procedure set out in Article 93(2).**	The Board shall **establish and make public**~~prepare and transmit to the Commission a proposal for~~ a common template for notifying a personal data breach to the competent supervisory authority referred to in paragraph 1 as well as ~~for~~ a list of the circumstances in which a personal data breach is likely to result in **an increased risk** ~~a high risk~~ to the rights and freedoms of a natural person **and a list of the circumstances in which it is not likely to result in such a** ~~high~~ **risk. The template and lists**~~. The proposals~~ shall be **available**~~submitted to the Commission~~ within [OP date = nine months of the entry into application of this Regulation]. ~~The Commission~~ ~~may~~~~after due consideration reviews it, as necessary, and is empowered to adopt~~ ~~the template as established by the Board~~**it by way of an implementing act, in accordance with the examination procedure set out in Article 93(2).** EE (Comments): Estonia supports reducing unnecessary data breach notifications but notes that controllers might underestimate their impact on data subjects. Multiple low-risk breaches, when combined, could pose higher risks to individuals' rights and DPAs should be made aware of those. We recommend using terms like "impactful risks" or "increased risks." NL (Drafting suggestions): . The Board shall establish and make public a common template for notifying a personal data breach to the competent supervisory authority referred to in paragraph 1 as well as a list of the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person and a list of the circumstances in which it is not likely to result in such a high risk. The template and lists shall be available within [OP date = nine months of the entry into application of this Regulation]. ~~The Commission may adopt the template as established by~~

Commission proposal	Drafting suggestions and Comments
	~~**the Board by way of an implementing act, in accordance with the examination procedure set out in Article 93(2).**~~ NL (Comments): NL notes that the proposed Article 33(6) suggests that the Commission may only put in an implementing act what the EDPB has established as a template. However, the Commission cannot be required to not make any changes in the template, as the Commission has the final say on the text of the implementing act. NL proposes to give the final say, *regarding both the template and the lists on the notification of data breaches*, to the (independent) EDPB, as this would provide needed legal certainty, while avoiding the risk of more political decision-making. AT (Drafting suggestions): '6. The Board shall **~~establish and make public~~**~~prepare and transmit to the Commission a proposal for~~ **publish** **a)** a common template for notifying a personal data breach to the competent supervisory authority referred to in paragraph 1 **b) ~~as well as~~** ~~for~~ a list of the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person and a list of the circumstances in which it is not likely to result in such a high risk **and** **c) a list of the circumstances in which a personal data breach is likely to result in an impactful/relevant/increased risk to the rights and freedoms of a natural person and a list of the circumstances in which it is not likely to result in such a risk**. The template and lists~~. The proposals~~ shall be available~~submitted to the Commission~~ within [OP date = nine months of the entry into application of this Regulation]. ~~The Commission may~~~~after due consideration reviews it, as necessary, and is empowered to adopt the template as established by the~~

Commission proposal	Drafting suggestions and Comments
	~~Boardit by way of an implementing act, in accordance with the examination procedure set out in Article 93(2).~~ AT (Comments): • AT continues to support the issuing of a common template for data breach notifications and the lists of circumstances relating to the risk threshold by the EDPB. • The task should remain with the EDPB. The wording should be adapted accordingly ("publish"). • The proposed wording regarding the risk threshold is designed to align with the AT proposal for Article 33(1). • A list of circumstances requiring notification under Article 33 as well as under Article 34 should be provided. • For structural reasons, provisions regarding tasks of the EDPB should be moved to Article 70 GDPR, where all tasks of the EDPB are currently regulated. PL (Comments): We think this wording in the combination with the wording of 7a, goes into a good direction. FI (Comments): FI supports the proposal that the common template and lists are established and made public by the EDPB. In case implementing acts were used, it would be important to clarify the status of proposals for updates where the revised legally binding implementing acts have not been adopted yet. Could they be already applied without an implementing act being in force yet? If they could already be

Commission proposal	Drafting suggestions and Comments
	applied, FI can support implementing acts. If not, FI proposes to leave this matter for EDPB and delete the possibility for implementing acts. [Views from the Council Legal Service would also be welcome.]
7. The template and **lists**~~the list~~ referred to in paragraph 6 shall be reviewed **by the Board** at least every three years and updated where necessary. ~~Where the~~ **the Board shall submit its assessment and possible proposals for updates to the Commission** ~~has adopted the previous version~~**in due time. The Commission after due consideration of the** ~~template by way of an implementing act, itshall~~**proposals reviews them and is empowered to adopt any updates** ~~of the template by way of an implementing act~~ **following the procedure** ~~referred to~~ **in paragraph 6.**	
7a. The Commission may adopt the template and any updates referred to in paragraphs 6 and 7, as established by the Board, by way of an implementing act following the examination procedure set out in Article 93(2).'	CZ (Drafting suggestions): ~~**The Commission may adopt the template and any updates referred to in paragraphs 6 and 7, as established by the Board, by way of an implementing act following the examination procedure set out in Article 93(2).**~~ CZ (Comments): CZ believes there are problems with the paragraphs on implementing acts: What if the Commission adopts a template but not its update? We prefer either standard comitology, or leaving these issues fully to EDPB, since these templates are more practical and less impactful. EE (Drafting suggestions): ~~**7a. The Commission may adopt the template and any updates referred to in paragraphs 6 and 7, as established by the Board, by way of an implementing act following the examination procedure set out in Article 93(2).'**~~

Commission proposal	Drafting suggestions and Comments
	EE (Comments): Estonia does not support the amendment as regards the division of competences in between EDPB and the Commission. In a situation where the Board's guidelines can be updated quickly in response to newly emerging possibilities, there is a risk that the guidelines may recommend an updated approach, while the Commission's implementing regulation in force contains outdated information. Amending both the EDPB guidelines and the implementing regulation will be a lengthy process and can result in different outcomes. This could result in a situation where controllers are unable to use up-to-date measures without committing a breach, thereby jeopardising the protection of individuals' personal data. We do understand that the EDPB's guidelines may be challenged in ECJ, but providing that its guidelines must be validated by an implementing regulation will jeopardise the EDPB's autonomy. For this reason, we suggest removing the clauses that permit the Commission to adopt implementing acts. ES (Comments): We had suggested to include a new para 8 with the following wording: *The data breach management should be ready and documented in advance, integrated in the incident management system of the controller, and, when applicable, the DPO should be involved in the process of a data breach* NL (Drafting suggestions): ~~**7a. The Commission may adopt the template and any updates referred to in paragraphs 6 and 7, as established by the Board, by way of an implementing act following the examination procedure set out in Article 93(2).'**~~

Commission proposal	Drafting suggestions and Comments
	NL (Comments): See Article 33(6). AT (Drafting suggestions): ~~7a. The Commission may adopt the template and any updates referred to in paragraphs 6 and 7, as established by the Board, by way of an implementing act following the examination procedure set out in Article 93(2).'~~ AT (Comments): • AT **does not support** the proposed new competence of the EC to adopt implementing decisions regarding data breaches. In our opinion, it is unfit for purpose and appears to run counter to the established system for guidelines, recommendations and best practices. PL (Drafting suggestions): The Commission may adopt the template and any updates referred to in paragraphs 6 and 7, ~~as established by the Board~~, by way of an implementing act following the examination procedure set out in Article 93(2).' PL (Comments): It is not clear what is the impact of the wording "as established by the Board" on the general procedure of adoption of implementing acts, where MS can present comments to the COM proposal. FI (Comments):

Commission proposal	Drafting suggestions and Comments
	FI supports the proposal that the common template and lists are established and made public by the EDPB. See the above comment concerning EDPB templates/lists and implementing acts.
9. Article 35 is amended as follows:	IT (Drafting suggestions): **Replace the proposed amendments to Article 35 with a substantive replacement:** Replace Article 35 with: 'Article 35 Processing assurance and evidence of compliance 1. Controllers shall not be required to carry out a prescribed risk assessment or data protection impact assessment as a condition for commencing processing. 2. For categories of processing identified by the Commission, the controller shall maintain concise evidence sufficient to demonstrate: (a) the purposes of processing; (b) the categories of data processed; (c) applicable retention and access arrangements; (d) technical and organisational safeguards; (e) measures ensuring confidentiality, integrity, availability and resilience; (f) testing performed to verify the effectiveness of those measures; and (g) any known failure to satisfy a mandatory requirement of this Regulation and the corrective action taken. 3. No prescribed template or methodology shall be mandatory. The controller may demonstrate compliance by any reliable technical, organisational or documentary evidence. 4. Failure to prepare documentation in a particular form shall not constitute an infringement where effective compliance with the substantive requirements of this Regulation is demonstrated.' IT

PUBLIC

Commission proposal	Drafting suggestions and Comments
	(Comments): The current compromise harmonises DPIA lists, templates and methodologies but keeps the underlying risk-based bureaucracy. A processing-assurance model preserves evidence for inspection while removing mandatory risk methodology and format. It therefore simplifies compliance without depriving supervisory authorities of verifiable evidence. SK (Comments): **SK:** We support this proposal.
(a) paragraphs 4, 5 and 6 are replaced by the following:	
'4. The Board shall **establish and make public**~~prepare and transmit to the Commission a proposal for~~ a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1.	AT (Drafting suggestions): 4. The Board shall ~~establish and make public~~~~prepare and transmit to the Commission a proposal for~~**publish** a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. AT (Comments): • AT continues to support harmonisation with regard to the data protection impact assessment and welcomes that the respective competences are assigned to the EDPB. • For structural reasons, all respective provisions should be moved to Article 70 GDPR, where all tasks of the EDPB are regulated. FI (Comments): FI supports the proposal that the common template and lists are established and made public by the EDPB. See the above comment concerning EDPB templates/lists and implementing acts.

Commission proposal	Drafting suggestions and Comments
5. The Board shall **establish and make public**~~prepare and transmit to the Commission a proposal for~~ a list of the kind of processing operations for which no data protection impact assessment is required.	AT (Drafting suggestions): 5. The Board shall ~~establish and make public~~~~prepare and transmit to the Commission a proposal for~~**publish** a list of the kind of processing operations for which no data protection impact assessment is required. AT (Comments): • Move to Article 70 (see comment on Article 35(4) above) • The wording should be adapted. FI (Comments): FI supports the proposal that the common template and lists are established and made public by the EDPB. See the above comment concerning EDPB templates/lists and implementing acts.
6. The Board shall **establish and make public**~~prepare and transmit to the Commission a proposal for~~ a common template and a common methodology for conducting data protection impact assessments.'	AT (Drafting suggestions): 6. The Board shall ~~establish and make public~~~~prepare and transmit to the Commission a proposal for~~**publish** a common template and a common methodology for conducting data protection impact assessments.' AT (Comments): • Move to Article 70 (see comment on Article 35(4) above) • The wording should be adapted. FI (Comments):

Commission proposal	Drafting suggestions and Comments
	FI supports the proposal that the common template and lists are established and made public by the EDPB. See the above comment concerning EDPB templates/lists and implementing acts.
(b) the following **paragraph is**~~paragraphs are~~ inserted:	
'6a. ~~The proposals for~~ **The**~~the~~ lists referred to in paragraphs 4 and 5 and ~~for~~ the template and methodology referred to in paragraph 6 shall be **published**~~submitted to the Commission~~ within [OP date = 9 months of the entry into application of this Regulation]. ~~The Commission may~~**after due consideration reviews them, as necessary, and is empowered to adopt** ~~the template as established by the Board~~**them by way of an implementing act, in accordance with the examination procedure set out in Article 93(2).**	AT (Comments): • Move to Article 70 (see comment on Article 35(4) above) FI (Comments): FI supports this proposal.
6b. The lists and the template and methodology referred to in paragraph 6a- shall be reviewed **by the Board** at least every three years and updated where necessary. ~~Where the the~~ **The Board shall submit its assessment and possible proposals for updates to the Commission** ~~has adopted the previous version~~**in due time. The Commission after due consideration of the** ~~template by way of an implementing act, it shall~~**proposals reviews them and is empowered to adopt any updates** ~~of the template by way of an implementing act~~ **following the procedure** ~~referred to~~ **in paragraph 6a.**	AT (Comments): • Move to Article 70 (see comment on Article 35(4) above) FI (Comments): FI supports this proposal.
6ba. The Commission may adopt the template and any updates referred to in paragraphs 6a and 6b, as established by the Board, by way of an implementing act following the examination procedure set out in Article 93(2).	CZ (Drafting suggestions): ~~**The Commission may adopt the template and any updates referred to in paragraphs 6a and 6b, as established by the Board, by way of an implementing act following the examination procedure set out in Article 93(2).**~~ CZ

Commission proposal	Drafting suggestions and Comments
	(Comments): CZ believes there are problems with the paragraphs on implementing acts: What if the Commission adopts a template but not its update? We prefer either standard comitology, or leaving these issues fully to EDPB, since these templates are more practical and less impactful. EE (Drafting suggestions): ~~**The Commission may adopt the template and any updates referred to in paragraphs 6a and 6b, as established by the Board, by way of an implementing act following the examination procedure set out in Article 93(2).**~~ EE (Comments): Estonia does not support the amendment as regards the division of competences in between EDPB and the Commission. In a situation where the Board's guidelines can be updated quickly in response to newly emerging possibilities, there is a risk that the guidelines may recommend an updated approach, while the Commission's implementing regulation in force contains outdated information. Amending both the EDPB guidelines and the implementing regulation will be a lengthy process and can result in different outcomes. This could result in a situation where controllers are unable to use up-to-date measures without committing a breach, thereby jeopardising the protection of individuals' personal data. We do understand that the EDPB's guidelines may be challenged in ECJ, but providing that its guidelines must be validated by an implementing regulation will jeopardise the EDPB's autonomy. For this reason, we suggest removing the clauses that permit the Commission to adopt implementing acts. NL (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
	~~**6ba. The Commission may adopt the template and any updates referred to in paragraphs 6a and 6b, as established by the Board, by way of an implementing act following the examination procedure set out in Article 93(2).**~~ NL (Comments): NL notes that the proposed Article 35(6ba) suggests that the Commission may only put in an implementing act what the EDPB has established as a template. However, the Commission cannot be required to not make any changes in the template, as the Commission has the final say on the text of the implementing act. NL proposes to give the final say, regarding *both the template and the DPIA lists*, to the (independent) EDPB, as this would provide needed legal certainty, while avoiding the risk of more political decision-making AT (Drafting suggestions): ~~6ba. The Commission may adopt the template and any updates referred to in paragraphs 6a and 6b, as established by the Board, by way of an implementing act following the examination procedure set out in Article 93(2).~~ AT (Comments): • AT **does not support** the proposed new competence of the EC to adopt implementing decisions regarding data breaches. In our opinion, it is unfit for purpose and appears to run counter to the established system for guidelines, recommendations and best practices. PL (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
	The Commission may adopt the template and any updates referred to in paragraphs 6a and 6b, ~~as established by the Board,~~ by way of an implementing act following the examination procedure set out in Article 93(2). PL (Comments): It is not clear what is the impact of the wording "as established by the Board" on the general procedure of adoption of implementing acts, where MS can present comments to the COM proposal. FI (Comments): FI supports the proposal that the common template and lists are established and made public by the EDPB. See the above comment concerning EDPB templates/lists and implementing acts.
6c. Lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment and of the kind of processing operations for which no data protection impact assessment is required established and made public by supervisory authorities remain valid until the **Board establishes and makes public the lists**~~Commission adopts the implementing act~~ referred to in paragraph **4 and 5**~~6a~~.'	AT (Drafting suggestions): 6c. Lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment and of the kind of processing operations for which no data protection impact assessment is required **~~established and made public~~published** by supervisory authorities remain valid until the Board **~~establishes and makes public~~publishes** the lists~~Commission adopts the implementing act~~ referred to in paragraph 4 and 5~~6a~~.' AT (Comments): • Move to Article 70 (see comment on Article 35(4) above)

Commission proposal	Drafting suggestions and Comments
	• The wording should be adapted. FI (Comments): FI can support this proposal.
(9a) In Article 37, paragraph 7 is replaced by the following:	EE (Drafting suggestions): ~~**(9a) In Article 37, paragraph 7 is replaced by the following:**~~ EE (Comments): Estonia does not support removing the obligation to notify the contact details of the Data Protection Officer to the national supervisory authority. In our view, this could increase the supervisory authority's workload and make it more difficult to identify organisations that have not appointed a DPO where required. It could also weaken the practical visibility and position of DPOs. NL (Drafting suggestions): ~~**(9a) In Article 37, paragraph 7 is replaced by the following:**~~ SK (Comments): **SK:** We propose that this provision remain unchanged. We believe that it is beneficial for DPA to have of contact details of DPO and also have overview of whether controller/processor has designated DPO. In our view, this obligation contributes to the effective exercise of the powers of the supervisory authority. It allows for immediate and direct communication with the DPO in the supervision and helps to resolve issues related to the protection of personal data more quickly. At the same time, this obligation does not represent a disproportionate administrative burden for controllers or

Commission proposal	Drafting suggestions and Comments
	processors, as it concerns a one-time notification that is updated when contact details change. For the reasons stated, we do not support this change.
'7. The controller or the processor shall publish the contact details of the data protection officer.'	EE (Drafting suggestions): ~~**'7. The controller or the processor shall publish the contact details of the data protection officer.'**~~ ES (Comments): Spain prefers to maintain the requirement to notify the supervisory authority of the DPOs' contact information. This notification is very simple, as the registration process with the authorities is purely declaratory and does not involve any assessment of the DPO's suitability. This registration allows data protection authorities to conduct training and outreach activities for the benefit of DPOs, which are highly valued and in demand by DPOs. Without this registration, it is very difficult to carry out these activities. LU (Comments): Given the tangible benefits provided by notifying Data Protection Authorities of DPO contact details, it is difficult to see what added value would result from removing this obligation - either for the authorities themselves or for data controllers. Removing it would probably weaken transparency and the effectiveness of DPO–DPA communication channels. HU (Comments): HU:

PUBLIC

Commission proposal	Drafting suggestions and Comments
	The fact that the draft would delete the provisions on the mandatory notification of the contact details of Data Protection Officers does not necessary result that Member States could not impose such an obligation on their own – as an official legal obligation. We believe that this could be a step back from a transparency perspective, since the purpose of a common register was precisely to enable data subjects to obtain information about the identity of DPOs from a reliable source. It is questionable whether what is a burden reduction for data controllers (and especially for the authorities) does not cause shortcomings on the part of data subjects. NL (Drafting suggestions): ~~**'7. The controller or the processor shall publish the contact details of the data protection officer.'**~~ NL (Comments): Regarding Article 37 GDPR, NL is concerned about the proposed deletion of the current obligation to notify the contact details of a Data Protection Officer to the Supervisory Authority. This change could undermine the independent position of the Data Protection Officer (DPO) as well as the performance of the tasks of the external supervisory authority. In the event of a data breach or investigation, both must be able to liaise (quickly) with each other. Neither the DPO nor the supervisory should be dependent, in terms of their position or the performance of their duties, on any whims of the organization concerned, caused by whether or not the latter reports the DPO's contact details to the supervisory authority or by (seriously) delaying this process. AT (Comments):

Commission proposal	Drafting suggestions and Comments
	• AT **is open** to an amendment to Article 37(7) but emphasises that any changes must still ensure that data protection authorities are still able to easily find and contact the competent data protection officer without delay or additional administrative burden. PL (Comments): We would like to keep the mechanism enabling supervisory authorities to receive the contact details of the data protection officer. Data protection officer plays a specific role in facilitating cooperation between controllers or processors and supervisory authorities. The proposed amendment may weaken effective and continuous cooperation between supervisory authorities and data protection officers, which constitutes an important element of the supervisory framework established by the GDPR. Supervisory authorities perform a number of tasks that require regular communication with DPOs. The availability of up-to-date DPO contact details may also be particularly relevant in situations requiring prompt interaction, including personal data breaches, ongoing supervisory procedures or other circumstances where timely communication between the supervisory authority and the organisation is important. FI (Comments): FI has doubts about removing the requirement to communicate contact details to DPAs. Would it weaken the efficiency of the work of DPAs and cause, in turn, additional work for them? However, this is not a redline.

Commission proposal	Drafting suggestions and Comments
10. The following article is added:	FR (Drafting suggestions): **10a. Article 40, paragraph 2 is amended as follows:** 2. Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to: (a) fair and transparent processing; (b) the legitimate interests pursued by controllers in specific contexts; (c) the collection of personal data; (d) the pseudonymisation of personal data; (e) the information provided to the public and to data subjects; (f) the exercise of the rights of data subjects; (g) the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained; (h) the measures and procedures referred to in Articles 24 and 25 and the measures to ensure security of processing referred to in Article 32; (i) the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects; (j) the transfer of personal data to third countries or international organisations; or (k) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 77 and 79. **The Commission may also prepare codes of conduct, or amend or extend such codes in relation to point d) of this parahraph.**

Commission proposal	Drafting suggestions and Comments
	Article 40, paragraph 5 is amended as follows: 7. Where a draft code of conduct relates to processing activities in several Member States, the supervisory authority which is competent pursuant to Article 55, ~~**shall**~~ before approving the draft code, amendment or extension, **or the European Commission with regards to a draft code prepared pursuant to paragraph 2 point d) shall** submit it in the procedure referred to in Article 63 to the Board which shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation or, in the situation referred to in paragraph 3 of this Article, provides appropriate safeguards. FR (Comments): Les autorités françaises sont favorables à la proposition d'article 29a qui apparaît comme une solution équilibrée par rapport à la proposition initiale. En outre, la proposition de recourir à un avis du CEPD, qui pourra être rendu contraignant le cas échéant (eu égard au mécanisme prévu à l'article 65 du RGPD) permet de rendre cette procédure plus formelle que l'élaboration de simples lignes directrices. Le délai pour adopter cet avis pourrait même être raccourci dans la mesure où le CEPD a déjà entamé les consultations sur la jurisprudence de la Cour en fin d'année dernière. En complément, les autorités françaises demandent également d'amender les paragraphes 2 et 7 de l'article 40 du RGPD pour permettre à la Commission de proposer des codes de conduites en la matière au CEPD. Suivant l'article 40, paragraphe 9, la Commission pourrait, à la faveur d'un avis favorable du CEPD, rendre ce code contraignant via un acte d'exécution. Les autorités françaises rappellent également leurs propositions d'amendements aux articles 64 et 65 du RGPD afin d'étendre aux

Commission proposal	Drafting suggestions and Comments
	responsables de traitement le mécanisme permettant de saisir pour avis le CEPD sur des sujets les concernant directement. Dans le sillage de l'article 29a, ces amendements permettent de renforcer la gouvernance par le CEPD et la cohérence de l'application du RGPD dans l'Union. Cette mise en cohérence dans l'application du RGPD dans l'Union, qui est une difficulté systématiquement remontée par les opérateurs, constitue l'un des principaux axes qui doit guider les discussions de cet Omnibus numérique.
'Article **29a - Application of pseudonymisation and identification of a natural person** ~~41a~~	CZ (Comments): CZ: These data may be obtained not only by pseudonymisation, but also be the result of linking (combining) such data, without actual identification, e.g. results of search queries from search engines DK (Comments): The incorporation of the SRB-judgement in the operative part of the GDPR is crucial to implement the concept of relative anonymity. Therefore, we support the GER-SWE wording proposal which has previously been put forward. EE (Comments): Estonia would have preferred addressing pseudonymisation only through EDPB guidance (be it in the form of opinion as proposed by Cypriot PRES), which could offer practical and flexible clarification. However, we are open to reflecting it in the GDPR text, provided the wording gives real legal certainty and remains technologically neutral. ES

Commission proposal	Drafting suggestions and Comments
	(Comments): We can accept Article 29a as it currently appears in the compromise text, provided that it refers to EDPB guidelines on anonymization and pseudonymization rather than to Commission implementing acts. FR (Comments): Les autorités françaises sont ouvertes à continuer les discussions sur la question des données pseudonymisées pour parvenir à un compromis permettant de renforcer la sécurité juridique autour de l'utilisation de ce type de données par les responsables de traitement. IT (Drafting suggestions): **Replace Article 29a with:** Replace the proposed Article 29a in its entirety with: 'Article 29a Pseudonymisation, identifiability and anonymous information 1. Whether a natural person is identifiable shall be determined separately in relation to each person or entity processing the information, taking into account only means of identification reasonably likely to be available and used by that person or entity. 2. Personal data which have undergone pseudonymisation shall constitute anonymous information in relation to a recipient where: (a) the recipient does not possess the additional information necessary to attribute the data to a natural person; (b) the recipient does not have reasonable legal, technical or practical means of obtaining or reconstructing that information; and (c) technical, organisational or legally binding measures effectively prevent re-identification. 3. The existence of identifying information in the possession of the controller or another person shall not by itself prevent paragraph 2 from applying. Purely hypothetical, unlawful,

PUBLIC

Commission proposal	Drafting suggestions and Comments
	practically impossible or manifestly disproportionate means of identification shall not be regarded as reasonably likely to be used. 4. Information treated as anonymous pursuant to paragraph 2 shall remain outside the scope of this Regulation in relation to that recipient for as long as the conditions of that paragraph continue to be met. 5. The Commission may establish voluntary technical safe harbours demonstrating compliance with paragraphs 1 to 4. Compliance with such a safe harbour shall create a presumption that the information is anonymous in relation to the recipient. Failure to use a safe harbour shall not prevent a controller or recipient from demonstrating anonymity by other means.' IT (Comments): The decisive change is from the discretionary formulation that pseudonymisation "may" prevent identification to a legal rule that the information is anonymous for a recipient when the statutory conditions are satisfied. Commission safe harbours should be voluntary and evidentiary, not a precondition for anonymity. NL (Comments): Since the opinion of the EDPB in the new compromise text would also pertain to anonymisation, this could also be expressed in the heading of Article 29a. SI (Comments): We support the envisaged approach. The provision should clarify the key elements of pseudonymisation, taking full account of the relevant case law of the Court and the guidance of the EDPB, without altering the definition of personal data. SK (Comments):

PUBLIC

Commission proposal	Drafting suggestions and Comments
	SK: We welcome that the definition of "personal data" in Article 4(1) GDPR remain unchanged. However, we believe that the proposed Article 29a interferes with the concept of "personal data". In particular, the proposed paragraph 2a, which states in which cases the transmission of pseudonymised data to a person other than the controller does not constitute personal data for that other person. We consider this paragraph to be merely a transfer of the proposal from Article 4(1) GDPR to a separate article. At the same time, we do not consider this amendment to be in line with the case law of the CJEU in Case C-413/23 P, on the basis of which the amendment isproposed. In our view, paragraph 1 and 1a are already in GDPR in similar wording - in article 32 paragraph 1 and in recital 26. We are not in favour of paragraph 4, which establishes an obligation for Board to issue an opinion on the application of pseudonymisation and anonymisation pursuant to Article 64(2) of GDPR. The opinion pursuant to Article 64(2) has a deadline for adoption (max 8 + 6 weeks). We believe that the EDPB has more appropriate mechanisms for addressing this issue, which will not be under time pressure and in which the public can also participate. For example, through guidelines, in which the EDPB regularly conducts public consultations and sometimes organises meetings with stakeholders and they are not limited by a deadline for adoption. The issue of pseudonymization and anonymization is important to the public, and adopting hasty solutions would not benefit anyone. We propose to delete this article, article 70(1)(hcb) and recital 27a. FI (Drafting suggestions): **(2a) Where a person other than the controller referred to in paragraph 2 discloses,**

Commission proposal	Drafting suggestions and Comments
	transmits or otherwise makes such data available to a third party and it cannot be ruled out that the third party possesses or can obtain means reasonably likely to enable the data subject to be identified, both the disclosure or transmission of the data ~~to this third party~~ and the subsequent processing of the data by that third party shall be considered as processing of data relating to an identifiable natural person. FI (Comments): FI considers that the CY Presidency's latest compromise proposal on Article 30a and Recital 27a found a balance that clarifies pseudonymisation in accordance with the relevant case law of the CJEU and maintains the current level of protection of personal data. It is important that the proposed para. 2a in Article 30a (ST 10729/26) is included in new Article 29a as it would codify appropriately the rulings of the CJEU in the case EDPS v SRB (see C-413/23 P, para 84). See proposal underlined and bolded. Similarly, the changes proposed in Recital 27a in the previous compromise version (ST 10729) should be included in the text. This would also be in line with the new anonymisation guidelines of the EDPB (see para 21 in guidelines 2/2026 on Anonymisation). "*(2a) Where a person other than the controller referred to in paragraph 2 discloses, transmits or otherwise makes such data available to a third party and it cannot be ruled out that this third party possesses or can obtain means reasonably likely to enable the data subject to be identified, both the*

Commission proposal	Drafting suggestions and Comments
	transmission of the data to this third party and the subsequent processing of the data by this third party is to be considered as processing of data relating to an identifiable natural person. ”
(1) **Controllers and processors may apply pseudonymisation in order to reduce the risks to the data subjects concerned and to comply with their obligations under this Regulation, in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information.~~The Commission may adopt implementing acts to specify means and criteria~~To~~to~~** determine whether **a natural person is identifiable, including through personal data having undergone~~data resulting from~~** pseudonymisation**, account shall be taken of all the means reasonably likely to be used, such as singling out or online identifiers, either by the controller or by another person to identify the natural person directly or indirectly~~ no longer constitutes personal data for certain entities~~**.	EE (Drafting suggestions): (1) **Controllers and processors may apply Privacy Enhancing Tecchnologies, including pseudonymisation in order to reduce the risks to the data subjects concerned and to comply with their obligations under this Regulation, in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information.~~The Commission may adopt implementing acts to specify means and criteria~~To~~to~~** determine whether **a natural person is identifiable, including through personal data having undergone~~data resulting from~~** pseudonymisation**, account shall be taken of all the means reasonably likely to be used, such as singling out or online identifiers, either by the controller or by another person to identify the natural person directly or indirectly~~ no longer constitutes personal data for certain entities~~**. EE (Comments): We should also not focus only on pseudonymisation, but consider other relevant privacy-enhancing technologies (PETs) as well. NL (Drafting suggestions): (1) Controllers and processors may apply pseudonymisation in order to reduce the risks to the data subjects concerned and to comply with their obligations under this Regulation, in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information. To determine whether a natural person is identifiable, including

Commission proposal	Drafting suggestions and Comments
	through personal data having undergone pseudonymisation, account shall be taken of all the means reasonably likely to be used, such as singling out or online identifiers, either by the controller or by another person to identify the natural person directly or indirectly. **Means may not be reasonably likely to be used if the likelihood of identification appears in reality to be insignificant because it would be impossible to do, because it would involve disproportionate effort in terms of time, cost and labour, or because of a legal prohibition. An entity's means may also include taking advantage of means that are only accessible through a third party.** NL (Comments): The first added sentence codifies §82 – 83 of the CJEU EDPS v. SRB-judgment (C-413/23 P), as summarised in §26 of the EDPB Guidelines on Anonymisation (02/2026). The second added sentence codifies the CJEU OC/European Commission judgment (C-479/22), §55-56, as summarised in §28 of the EDPB Guidelines on Anonymisation. To increase legal certainty, in Article 29a(1) should be added that account should also be taken of the means reasonably likely to which the entity processing the data, can obtain access via third parties. An alternative for the first added sentence could be add a new §1a, which is based on §29 of the EDPB Guidelines on Anonymisation (02/2026): **1a. Whether an entity is likely to use certain means to identify an individual should be assessed in light of all objective factors that might influence the availability of such means and the likelihood of their actual use, including:** **a. the properties of the data, such as aggregation, uniqueness, accuracy and precision, and how these affect the data's vulnerability to possible means of identification;**

Commission proposal	Drafting suggestions and Comments
	b. the context of the data processing and whether there are any effective and permanent restrictions on access to the data; **c. any additional information that would allow for the identification of individuals, and how likely it is that such information can be obtained;** **d. the costs and the amount of time that the entity would need to obtain such additional information; and** **e. the available technology**. PL (Comments): We thank the Presidency for the effort of addressing the comments on art. 29a (see par 2 and 3). Current wording still needs more clarifications as it risks divergent interpretations. The findings of the SRB judgement should be clearly incorporated to the GDPR text. We maintain that the relationship between pseudonymisation and the assessment of the identifiability of a natural person should remain clear and provide legal certainty for controllers and processors. To achieve meaningful simplification and legal certainty, we need implementation acts, instead of EDPB guidelines (that are currently delayed). Further clarification is also needed regarding the practical consequences of situations where pseudonymised data may not enable the identification of a natural person from the perspective of a particular recipient, while remaining potentially identifiable for other entities, including entities in third countries, possessing additional information, resources or technical capabilities. In such

Commission proposal	Drafting suggestions and Comments
	circumstances, it is important to ensure that the interpretation of Article 29a does not inadvertently reduce the level of protection applied to pseudonymised data or create incentives to treat such data as posing no meaningful privacy risks. Consideration should be given to the fact that pseudonymised datasets may still be exposed to unauthorised disclosure, further transfers or combination with other datasets, potentially enabling the identification of natural persons by third parties. Further clarification of these aspects would contribute to legal certainty and a more consistent application of the GDPR.
(2) The application of pseudonymisation to personal data may, depending on the circumstances of the case and provided that appropriate technical and organisational measures are put in place and are such as to prevent the data in question from being attributed to the data subject, effectively prevent persons other than the controller from identifying the data subject in such a way that, for them, the data subject is not or is no longer identifiable.	NL (Drafting suggestions): 2) The application of pseudonymisation to personal data may, depending on the circumstances of the case and provided that appropriate technical and organisational measures are put in place and are such as to prevent the data in question from being attributed to the data subject, effectively prevent persons other than the controller from identifying the data subject in such a way that, for them, the data subject is not or is no longer identifiable. **Such technical and organisational measures require, among other things, that the recipient may not be in a position to lift those measures during any processing which is carried out under its control, nor be able to attribute those data to data subjects by recourse to other means of identification such as cross-checking.** **(2a) Where a person other than the controller referred to paragraph 2 transmits such data to a third party who and it cannot be ruled out that this third party possesses or can obtain means reasonably likely to enable the data subject to be identified, both the transmission of the data to this third party and the subsequent processing of the data by the third party is to be considered as processing of data relating to an identifiable natural person.**

Commission proposal	Drafting suggestions and Comments
	NL (Comments): The addition to §2 codifies §77 of the CJEU EDPS v. SRB-judgment (C-413/23 P): "77. *However, that presupposes, first, that Deloitte is not in a position to lift those measures during any processing of the comments which is carried out under its control. Second, those measures must in fact be such as to prevent Deloitte from attributing those comments to the data subject including by recourse to other means of identification such as cross-checking with other factors, in such a way that, for the company, the person concerned is not or is no longer identifiable*." This text proposal serves to align with §85 of the CJEU EDPS v. SRB-judgment (C-413/23 P): "(…) *in so far as it cannot be ruled out that those third parties have means reasonably allowing them to attribute pseudonymised data to the data subject, such as cross-checking with other data at their disposal, the data subject must be regarded as identifiable as regards both that transfer and any subsequent processing of those data by those third parties. In such circumstances, pseudonymised data should be considered to be personal in nature*." PL (Comments): We thank the Presidency for the effort of addressing the comments on art. 29a

Commission proposal	Drafting suggestions and Comments
	At the current stage of the negotiations, it is not clear what the intended normative effect of the proposed Article 29a is. In particular, it is unclear whether the proposed Article 29a is intended to limit the application of certain obligations under the GDPR with regard to an entity that does not possess and cannot reasonably obtain the means enabling the identification of the data subject. Although paragraph 3 provides that Article 29a is without prejudice to other obligations under the GDPR, it does not explain what practical legal consequences are intended to follow from the assessment that, from the perspective of a particular entity, the data subject is not or is no longer identifiable. Consequently, it remains unclear whether the proposed Article 29a is intended merely to codify the existing case law of the Court of Justice of the European Union concerning the assessment of identifiability or whether it is also intended to provide genuine regulatory simplification. If the purpose of the proposal is to introduce such simplification, its scope and legal consequences should be clearly specified. The proposed Article 29a should clearly specify the legal consequences of the assessment referred to in paragraph 2. In particular, it should clarify whether, and to what extent, the fact that, from the perspective of a particular entity, the data subject is not or is no longer identifiable has an effect on the application of obligations under the GDPR. At the same time, it should be made explicit that such assessment does not affect the status of pseudonymised data as personal data under the GDPR or reduce the level of protection afforded to such data.
(3)~~(2)~~ Paragraphs 1 and 2 are without prejudice to other provisions and obligations applicable to the controller ~~and processor~~, including under Chapter IV and V of this Regulation. The provision set out in paragraph 2 shall not apply to processors.	HU (Drafting suggestions): HU: (3) Paragraphs 1 and 2 are without prejudice to other provisions and obligations applicable to **any** controller, **as well as to processors that are**

Commission proposal	Drafting suggestions and Comments
	state-owned or government entities, including under Chapter IV and V of this Regulation. The provision set out in paragraph 2 shall not apply to processors, **unless they are state-owned or government entities**. HU (Comments): HU: Due to the current wording of paragraph 3 of Article 29a introduced by the Omnibus proposal, the possibility of pseudonymisation applies only to controllers, and paragraph 2 shall not apply to any kind of processor. With this in mind, we would propose retaining the reference to processors in paragraphs 2 and 3 of Article 29a, specifically for state-owned and governmental entities. State-owned entities and government bodies acting as processors often handle large amounts of personal data under strict legal mandates, much of which is owned by state ministries or other state bodies. For instance, under Article 5a of Regulation (EU) No 910/2014 of the European Parliament and of the Council (the eIDAS Regulation), each Member State must provide at least one European Digital Identity Wallet (EUDI Wallet) to ensure secure, trusted and seamless cross-border access to public and private services. Due to Article 5a(2) of the eIDAS Regulation, the EUDI Wallet may be operated by a state-owned entity or a public office. Due to the operational nature of the EUDI Wallet, these entities frequently handle personal data controlled by state ministries while processing it within the system as data processors. In these scenarios, allowing state-owned and governmental entities acting as processors on behalf of public authorities to pseudonymise data could ensure consistency across government data processing activities, further enhance e-government operations and safeguard public interest. For example, if government and public sector data processors were permitted to pseudonymise data on their own authority, EUDI Wallet providers could create secure datasets in real time for internal development, testing (Sandbox), and troubleshooting purposes. Pseudonymisation could also

Commission proposal	Drafting suggestions and Comments
	facilitate more efficient data exchange between various government agencies and EU member states, in line with the objectives of the eIDAS Regulation
~~**For the purpose of paragraph 1 the Commission shall:**~~	
~~**(a) assess the state of the art of available techniques;**~~	
~~**(b) develop criteria and or categories for controllers and recipients to assess the risk of re-identification in relation to typical recipients of data.**~~	
(4) The Board shall issue an opinion, in accordance with Article 64(2) of this Regulation, addressing the application of pseudonymisation and anonymisation, including related circumstances and technical and organisational measures referred to paragraph 2.	CZ (Drafting suggestions): ~~**The Board shall issue an opinion, in accordance with Article 64(2) of this Regulation, addressing the application of pseudonymisation and anonymisation, including related circumstances and technical and organisational measures referred to paragraph 2.**~~ CZ (Comments): CZ believes that rules of such significance should be adopted in a binding, formal and predictable way. Mere opinion of EDPB is not acceptable. Standard comitology is much preferred. (red line) In addition, given the importance of defining conditions when personal data cease to be, at least for some controllers, personal in nature, CZ believes that this Article should, at the very least, include the core requirements on the likelihood of preventing identification of a data subject. Means and criteria to determine whether the pseudonymisation effectively prevents identification should be based on costs, amount of time required, available technology, legal powers and restrictions and other relevant objective factors. But CZ is flexible about wording. AT (Comments): • AT is open to further pursuing this proposal.

Commission proposal	Drafting suggestions and Comments
	• However, the provision should be move to Article 70 (see comment on Article 35(4) above).
(5)~~(3)~~ The **Chair**~~implementation~~ of the **Board shall request the opinion referred to in paragraph 4 no later than 6 months after the entry into force of this Regulation. The opinion shall be reviewed and updated where necessary**~~means and criteria outlined in an implementing act may be used as an element to demonstrate that data cannot lead to reidentification of the data subjects~~.	CZ (Drafting suggestions): ~~The **Chair**~~~~implementation~~ of the ~~**Board shall request the opinion referred to in paragraph 4 no later than 6 months after the entry into force of this Regulation. The opinion shall be reviewed and updated where necessary**~~~~means and criteria outlined in an implementing act may be used as an element to demonstrate that data cannot lead to reidentification of the data subjects.~~~~ CZ (Comments): CZ believes that, while this obligation of the EDPB Chair is not contrary to GDPR, it illustrates rather clearly non-systemic nature of the proposal to replace standard comitology with soft law EDPB opinions. This system is does not really create obligations as regards both procedure and the outcome. CZ strongly prefers, in this case, implementing acts to seeking new, non-systemic paths. Proper procedure referred to in Art. 93**(2)** GDPR should be used. Given requirements of the industry and economic actors for legally sound de-personalisation of various data that are, in many contexts, simply not processed to be connected with identified individual, time is of the essence and a deadline of 12 months should be imposed.
~~(4) The Commission shall closely involve the EDPB in the preparations of the implementing acts. The EPDB shall issue an opinion on the draft implementing acts within a deadline of 8 weeks as of the receipt of the draft from the Commission.~~	
~~(5) The Implementing Acts shall be adopted in accordance with the examination procedure referred to in Article 93(3).'~~	
11. ~~In~~ Article **57**~~57(1)~~ is amended as follows:	ES

Commission proposal	Drafting suggestions and Comments
	(Drafting suggestions): ES Drafting suggestions): ***Article 49 Derogations for specific situations*** *1. (...)* *Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.* ***The requirement that the transfer be non-repetitive shall not apply to transfers based on point (d) of the first subparagraph, where such transfers are necessary for important reasons of public interest recognised in Union law or in the law of a Member State, including transfers carried out pursuant to international or administrative agreements on mutual assistance or cooperation.*** ES (Comments): (ES Comments): The purpose of this amendment is to clarify and specify the scope of the derogation for important reasons of public interest laid down in Article 49 of Regulation (EU) 2016/679, in particular as regards international data

Commission proposal	Drafting suggestions and Comments
	transfers carried out in the context of periodic exchanges of information between public authorities. The proposed amendment clarifies that transfers necessary for important reasons of public interest under Article 49(1)(d), including those carried out pursuant to international or administrative cooperation agreements, may in practice take place on a recurring basis. It therefore specifies that the requirement of non-repetitiveness, which applies to the residual ground of compelling legitimate interests, should not be understood as limiting such public interest transfers. This clarification does not affect the exceptional nature of Article 49 derogations, which remain subject to strict necessity, proportionality and appropriate safeguards ensuring a high level of protection of personal data. IT (Drafting suggestions): **Expand point 11 - Article 57:** In Article 57(1), replace point (f) and insert a new point (fa): '(f) receive complaints concerning alleged non-compliance with this Regulation and investigate, to the extent appropriate, whether the controller or processor has complied with this Regulation. A complaint shall constitute a request for regulatory supervision and shall not constitute proceedings for the adjudication of civil liability, damages, compensation, contractual rights or other private-law claims between the complainant and the controller or processor; (fa) conduct effective periodic, sectoral, targeted and sample-based inspections of controllers and processors in order to verify actual compliance with this Regulation, with particular attention to the effectiveness of technical and organisational measures.' IT (Comments): The supervisory authority's primary function should be regulatory: determine GDPR compliance and inspect actual processing. Greater controller freedom should be exchanged for more intensive and technically competent inspection. Complaints remain an enforcement

Commission proposal	Drafting suggestions and Comments
	trigger, but should not convert the supervisory authority into a civil court for damages, contractual rights or compensation. PL (Drafting suggestions): We suggest adding the following wording to **Article 57**: **In performing its tasks, the supervisory authority shall also contribute to supporting innovation and competitiveness of the Union.**
(a) **in paragraph 1,** point (k) is deleted;	SK (Comments): **SK:** We support the proposal because it is only an editorial change resulting from the amendment to Article 35.
(ab) paragraph 4 is replaced by the following; **'4. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character or where an abusive intention on the part of the data subject submitting those request can be demonstrated, the supervisory authority may charge a reasonable fee based on administrative costs, or refuse to act on the request. The supervisory authority shall, in the light of all the relevant circumstances of the case, bear the burden of demonstrating the manifestly unfounded or excessive character of the request.'**	CZ (Drafting suggestions): **(ab) paragraph 4 is replaced by the following;** **'4. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character or because the data subject abuses the rights conferred by this regulation for purposes other tan protection of their rights, ~~an abusive intention on the part of the data subject submitting those request can be demonstrated,~~ the supervisory authority may charge a reasonable fee based on administrative costs, or refuse to act on the request. The supervisory authority shall, ~~in the light of all the relevant circumstances of the case~~, bear the burden of demonstrating that the request is manifestly unfounded or that there are reasonable grounds to believe that is excessive. ~~character of the request~~.'** CZ (Comments):

Commission proposal	Drafting suggestions and Comments
	CZ: Given the excessive and often AI-powered requests to both controllers and DPAs, we would welcome using the Commission's original wording from Art. 12(5) even in Article 57(4) GDPR. CZ is aware of the judgment C-416/23 but believes that simplification efforts could offer alternative solution more suitable to changing circumstances. EE (Comments): Estonia strongly supports this amendment to the Commission's proposal. AT (Comments): • AT **continues to support** the proposed changes to Article 57(4). PL (Comments): As regards Article 57(4), we support the proposed amendment, which may contribute to a more efficient use of supervisory authorities' resources and facilitate the handling of manifestly unfounded, excessive or abusive requests. We think the wording is going in a good direction. SK (Comments): **SK:** We support the proposal, however we are wondering whether this proposal should be limited only to data subject. According to CJEU (C-416/23) the concept of a 'request', according to its usual meaning in everyday language, is particularly broad, since it potentially encompasses any act by which a person or entity asks for something. This means that a request can also be made to DPA by a person or entity other than the data subject, such as body, organisation or association under Article 80 GDPR.

Commission proposal	Drafting suggestions and Comments
	We therefore propose to use the general words 'person or entity' rather than 'data subject'. FI (Comments): FI supports the proposed recital 35a and Article 57(4) GDPR [Art. 3(11) Digiomnibus] concerning data protection authorities' (DPA) possibilities to refuse manifestly unfounded and excessive requests as well.
12. In Article 64(1), point (a) is deleted.	FR (Drafting suggestions): **12a. Article 64 is amended as follows:** **(a) the following paragraph is added:** **'2a. Controllers subject to this Regulation may present a reasoned request that any matter of consistent application directly relevant for them in more than one Member State be examined by the Board with a view to obtaining an opinion on this matter.'** **(b) paragraph 3 and 4 are replaced by the following:** **'3. In the cases referred to in paragraphs 1, 2 and 2a, the Board shall issue an opinion on the matter submitted to it provided that it has not already issued an opinion on the same matter. That opinion shall be adopted within eight weeks by simple majority of the members of the Board. That period may be extended by a further six weeks, taking into account the complexity of the subject matter. Regarding the draft decision referred to in paragraph 1 circulated to the members of the Board in accordance with paragraph 5, a member which has not objected within a reasonable period**

Commission proposal	Drafting suggestions and Comments
	indicated by the Chair, shall be deemed to be in agreement with the draft decision. **12b. In Article 65(1), point (c) is replaced by the following:** **'(c) where a competent supervisory authority does not request the opinion of the Board in the cases referred to in Article 64(1), or does not follow the opinion of the Board issued under Article 64. In that case, any supervisory authority concerned, the Commission or any controller concerned where that opinion was issued on the grounds of a request under Article 64(2a) or of Article 41a may communicate the matter to the Board.'** FR (Comments): Ces modifications visent à étendre aux parties prenantes le mécanisme prévu aux articles 64 et 65, qui permet aux autorités de contrôle nationales de saisir le comité. Elles offrent aux parties prenantes la possibilité de saisir le comité en lui adressant une demande motivée afin d'obtenir un avis ou, en dernier ressort, l'adoption d'une décision contraignante. Les autorités françaises estiment que l'extension de cette possibilité aux parties prenantes soumises au RGPD conduira à une mise en œuvre plus cohérente du RGPD par les autorités nationales de contrôle et garantira l'homogénéité au sein du marché unique. Cela renforcera la sécurité juridique et la prévisibilité pour les acteurs économiques, tout en offrant un mécanisme de recours direct permettant au comité de réagir rapidement et efficacement pour traiter les problèmes liés à l'application cohérente du RGPD dès qu'ils sont identifiés par les parties prenantes.

Commission proposal	Drafting suggestions and Comments
	Les autorités françaises souhaitent que l'accès au Comité soit également ouvert aux responsables de traitements et aux sous-traitants pour leur permettre de le saisir de demandes d'avis sur des sujets les concernant directement. Ces amendements permettraient de renforcer la gouvernance par le CEPD et la cohérence d'application du RGPD dans l'Union, en même temps qu'il permettrait d'ouvrir des dialogues entre le CEPD et les responsables de traitements et sous-traitants à leur initiative sur les sujets le méritant. IT (Drafting suggestions): **Before current point 12, insert Articles 58, 58a, 77 and 79 amendments:** Before current point 12, insert the following new points: '11a. In Article 58, the following paragraph 6 is added: "6. When exercising the powers provided for in this Article, the supervisory authority shall identify the substantive requirement or compliance outcome which has not been satisfied. Except where Union law requires a particular technical or organisational measure, the supervisory authority shall not require the controller or processor to adopt a particular technical design, organisational structure, methodology or compliance instrument where the controller or processor can achieve the required result by another effective means. Supervisory authorities shall have the power to conduct technical and organisational inspections, including inspection of relevant processing systems, security controls, access controls, logs and evidence of operational compliance, subject to applicable safeguards for confidential information, professional secrecy and fundamental rights." 11b. The following Article 58a is inserted: "Article 58a Maximum duration of investigations 1. Any investigation by a supervisory authority concerning an alleged infringement of this Regulation shall be concluded by a final administrative decision or by formal closure no later than 15 months after the earliest of:

Commission proposal	Drafting suggestions and Comments
	(a) receipt by a supervisory authority of a complaint concerning the relevant processing; (b) the first request for information, document, explanation or access addressed to the controller or processor concerning the matter; (c) the first inspection, audit, preservation request or other investigative measure concerning the matter; or (d) in an ex officio case, the date on which the supervisory authority first records or communicates its decision to examine the matter. 2. All preliminary, preparatory, screening, admissibility, competence-determination, pre-investigative, exploratory, informal-supervision, fact-finding or equivalent activities concerning the same material facts shall form part of the investigation for the purposes of paragraph 1. The denomination attributed to such activities under national law or administrative practice shall be irrelevant. 3. The supervisory authority shall not extend, suspend or restart the time limit in paragraph 1 by unilateral administrative act, by reclassification of the procedure or by opening a new file concerning substantially the same controller, processing operations and material facts. 4. Upon expiry of the period in paragraph 1 without a final administrative decision, the investigation shall be closed. It may be reopened in relation to the same controller, processing operations and material facts only on the basis of material evidence which could not reasonably have been known before expiry of that period." 11c. In Article 77, the following paragraph 4 is added: "4. The purpose of a complaint under this Article is to bring an alleged infringement of this Regulation to the attention of the competent supervisory authority for regulatory supervision and enforcement. The supervisory authority shall determine whether the controller or processor has complied with this Regulation but shall not adjudicate claims for compensation, damages, contractual remedies or other civil consequences arising between the data subject and the controller or processor." 11d. In Article 79, the following paragraph 3 is added: "3. Courts shall have jurisdiction to determine contested claims concerning the existence, scope, infringement or civil consequences of individual rights conferred by this Regulation, including claims for compensation under Article 82. Findings made by a supervisory

Commission proposal	Drafting suggestions and Comments
	authority concerning regulatory compliance shall be subject to judicial review and shall not prejudice the court's independent determination of civil liability or compensation."' IT (Comments): Article 58 gives the authority stronger inspection powers while protecting the controller's freedom of technical and organisational means. New Article 58a imposes a single clock beginning with the first substantive investigative event and expressly prevents reliance on an unbounded "pre-investigative" phase. The Article 77/79 distinction is deliberately narrower than stating that supervisory authorities cannot affect rights at all: Article 8(3) of the Charter requires independent supervision and the GDPR necessarily allows corrective orders. The proposal instead reserves adjudication of contested civil rights, damages, compensation and other inter partes consequences to courts, while supervisory authorities determine regulatory compliance. Article 78 judicial review of supervisory decisions remains unaffected. This is a substantive legislative change from the present interpretation in CJEU Case C-132/21, under which Articles 77-79 provide concurrent and independent remedies. The amendment would therefore need clear operative language, not merely a recital. SK (Comments): **SK:** We support the proposal as it is based on the amendment to Article 35.
(12a) In Article 70(1), point (f) is amended as follows:	FR (Drafting suggestions): **13a. In Article 70(1), point (t) is replaced with the following:** **'(c) issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in Article 64(1), on matters submitted pursuant to Article 64(2) and (2a), and to issue binding decisions pursuant to Article 65, including in cases referred to in Article 66;'** FR (Comments):

Commission proposal	Drafting suggestions and Comments
	Cet amendement actualise le point correspondant des missions du Conseil afin de tenir compte des modifications proposées aux articles 64 et 65.
(f) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for further specifying the criteria and conditions for decisions based on profiling pursuant to Article 22(1);	AT (Comments): • AT is **open** to further pursuing this amendment. SK (Comments): **SK:** We support this proposal because it is only an editorial change resulting from the amendment to Article 22. FI (Comments): FI supports this proposal.
13. In Article 70(1), point (h) is deleted.	SK (Comments): **SK:** We support the proposal it is based on the amendment to Article 33.
14. In Article 70(1), the following points are inserted:	IT (Drafting suggestions): **Consequential amendment to Article 70(1):** Consequentially revise point 14 as follows: '(ha) prepare and transmit to the Commission a proposal identifying categories of processing for which the processing-assurance evidence referred to in Article 35(2) should be maintained; (hb) [deleted]; (hc) prepare and transmit to the Commission a proposal for objective and technologically neutral materiality criteria and, where appropriate, a common template for personal data breach notifications pursuant to Article 33;

Commission proposal	Drafting suggestions and Comments
	(hca) issue guidelines, recommendations and best practices concerning effective technical and organisational measures capable of achieving the security outcomes referred to in Article 32, without prescribing a mandatory risk methodology; (hcb) issue guidelines on pseudonymisation, anonymisation and voluntary technical safe harbours referred to in Article 29a IT (Comments): These changes remove references to the discarded DPIA methodology and "security appropriate to risk", while preserving an EDPB advisory role focused on outcomes, objective breach criteria and voluntary pseudonymisation safe harbours. SK (Comments): **SK:** We support the proposals with the exception of the letter (hcb). An explanation is provided in the comments to Article 29a.
'(ha) **establish**~~prepare and transmit to the Commission a proposal for~~ a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment and for which no data protection impact assessment is required, pursuant to Article 35.	FI (Comments): FI supports this proposal.
(hb) **establish**~~prepare and transmit to the Commission a proposal for~~ a common template and a common methodology for conducting data protection impact assessments, pursuant to Article 35.	FI (Comments): FI supports this proposal.
(hc) **establish**~~prepare and transmit to the Commission a proposal for~~ a common template for notifying a personal data breach to the competent supervisory authority as well as for a list of the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person pursuant to Article 33 **and a list of the circumstances in which it is not likely to result in such a high risk.**	EE (Drafting suggestions): **establish**~~prepare and transmit to the Commission a proposal for~~ a common template for notifying a personal data breach to the competent supervisory authority as well as for a list of the circumstances in which a personal data breach is likely to result in an increased risk ~~a high risk~~ to the

Commission proposal	Drafting suggestions and Comments
	rights and freedoms of a natural person ~~pursuant to Article 33~~ **and a list of the circumstances in which it is not likely to result in such a ~~high~~ risk.** EE (Comments): Estonia supports reducing unnecessary data breach notifications but notes that controllers might underestimate their impact on data subjects. Multiple low-risk breaches, when combined, could pose higher risks to individuals' rights and DPAs should be made aware of those. We recommend using terms like "impactful risks" or "increased risks." Relevant amendments should be made here as well. AT (Drafting suggestions): (hc) establish~~prepare and transmit to the Commission a proposal for~~ a common template for notifying a personal data breach to the competent supervisory authority as well as for a list of the circumstances in which a personal data breach is likely to result in **~~a high risk~~an impactful/relevant/increased risk** to the rights and freedoms of a natural person pursuant to Article 33 and a list of the circumstances in which it is not likely to result in such a high risk. AT (Comments): See above, comments on Article 33 and Recital 39. FI (Comments): FI supports this proposal.
(hca) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for the purpose of further specifying the appropriate technical and organisational measures to	CZ (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
ensure a level of security appropriate to the level of risk pursuant to Article 32.	~~**(hca) issue guidelines, recommendations and best practices in accordance with point (c) of this paragraph for the purpose of further specifying the appropriate technical and organisational measures to ensure a level of security appropriate to the level of risk pursuant to Article 32.**~~ CZ (Comments): CZ is concerned that the proposal appears to reinterpret Article 32(1), which was intentionally left open by the legislator, thereby risking over-specification and reduced flexibility. Rather than simplifying compliance, the measure risks increasing complexity and creating further pressure for additional soft law instruments, without a consistent approach across related provisions (e.g. Articles 24 and 25). AT (Comments): • AT **supports** the proposal to issue EDPB guidelines, recommendations and best practices regarding data security measures. FI (Comments): FI supports this proposal.
(hcb) issue the opinion on the application of pseudonymisation and anonymisation referred to in Article 29a.'	CZ (Drafting suggestions): ~~**(hcb) issue the opinion on the application of pseudonymisation and anonymisation referred to in Article 29a.**~~ CZ (Comments):

Commission proposal	Drafting suggestions and Comments
	CZ does not agree with this power of EDPB and believes that comitology is the rational legal solution for developing pseudonymisation under Article 29a- ES (Drafting suggestions): **(hcc) Issue guidelines recommendations and best practices in accordance with point 9.2(l) that establish safeguards on the use of biometric technologies for verification (1 to 1)** ES (Comments): In accordance with our suggestion on recital (34) and 9.2(l), we suggest this new paragraph. AT (Comments): • AT is **open** to pursue this amendment. PL (Drafting suggestions): After point (hcb), we suggest adding the following: **The Board shall, in exercising its tasks, support the consistent application of this Regulation in a manner that also contributes to the, innovation and competitiveness of the Union.** FI (Comments): FI supports this proposal.
~~15.~~ ~~After Article 88, the following articles are added:~~	CZ

Commission proposal	Drafting suggestions and Comments
	(Drafting suggestions): **the new point:** **14a. In Article 77 paragraph 3 is added[A10.1][A10.2]:** **3. Member States may incorporate into their national law rules for prioritisation of complaints based on reviewable and publicly available criteria.** CZ (Comments): CZ: The aim of detailed rules for handling of complaints lies in the possibility of prioritising and planning regulatory action based on the actual impact of complaints and the resources available. Prioritisation shall be based on reviewable and publicly available criteria, without prejudice to the obligation to provide a reasoned effective response and subject to judicial review in every case. The powers of supervisory authorities to adopt planning instruments for the prioritisation and management of complaints should be expressly recognised. This would enable the DPAs more targeted supervisory activities based on evaluation of the level of risk, affects, type of processing, sector etc., while maintaining the capacity for individual assessment of each case. Priority should be given in particular to complaints that demonstrate a clear link to the core right to data protection or a high risk to rights and freedoms, affect many data subjects as well as other criteria. FR (Drafting suggestions): **In Article 70, paragraph 4 is amended as follows:** ‘4. The Board shall, where appropriate, consult interested parties and give them the opportunity to comment within a reasonable period. **This consultation is mandatory before issuing guidelines, recommendations and best practices addressed to these interested parties. The Board duly**

Commission proposal	Drafting suggestions and Comments
	takes these consultations into consideration. The Board shall, without prejudice to Article 76, **make the contributions of interested parties and the results of the consultation procedure publicly available.'** FR (Comments): Les autorités françaises rappellent qu'elles proposent que le CEPD soit aussi obligé de consulter systématiquement les opérateurs en amont de l'élaboration de ses projets de lignes directrices. SK (Comments): **SK:** We support deletion of this proposal.
~~'Article 88a~~	SI (Comments): We support the transfer of the substance of this provision in the e-Privacy Directive.
~~Processing of personal data in the terminal equipment of natural persons~~	NL (Comments): Regarding EC comments during AGS: we are not opposed to a transfer of the current article 5(3) ePrivacy Directive compromise text to the GDPR, which has harmonisation and enforcement benefits. However, the scope of the original Commission proposal was limited to personal data, leaving the ePrivacy Directive applicable to other types of information and data. This would only decrease legal certainty as two separate legal regimes would apply, one of which being a directive subject to member state implementation. In order to achieve true alleviation of administrative burden, a single, harmonised article applicable to all information types could be included here.

Commission proposal	Drafting suggestions and Comments
~~(1) Storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person is only allowed when that person has given his or her consent, in accordance with this Regulation.~~	
~~(2) Paragraph 1 does not preclude storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person, based on Union or Member State law within the meaning of, and subject to the conditions of Article 6, to safeguard the objectives referred to in Article 23(1).~~	
~~(3) Storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person without consent, and subsequent processing, shall be lawful to the extent it is necessary for any of the following:~~	
~~(a) carrying out the transmission of an electronic communication over an electronic communications network;~~	
~~(b) providing a service explicitly requested by the data subject;~~	
~~(c) creating aggregated information about the usage of an online service to measure the audience of such a service, where it is carried out by the controller of that online service solely for its own use;~~	
~~(d) maintaining or restoring the security of a service provided by the controller and requested by the data subject or the terminal equipment used for the provision of such service.~~	
~~(4) Where storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person is based on consent, the following shall apply:~~	
~~(a) the data subject shall be able to refuse requests for consent in an easy and intelligible manner with a single-click button or equivalent means;~~	
~~(b) if the data subject gives consent, the controller shall not make a new request for consent for the same purpose for the period during which the controller can lawfully rely on the consent of the data subject;~~	

PUBLIC

Commission proposal	Drafting suggestions and Comments
~~(c) if the data subject declines a request for consent, the controller shall not make a new request for consent for the same purpose for a period of at least six months.~~	
~~This paragraph also applies to the subsequent processing of personal data based on consent.~~	
~~(5) This Article shall apply from [OP: please insert the date = 6 months following the date of entry into force of this Regulation]~~	
~~Article 88b~~	PL (Comments): We welcome deletion of Article 88b. We would like to keep it deleted. The proposal went beyond a technical simplification exercise and could concentrate user consent and data in the hands of a limited number of major technology providers. We maintain our position presented in the non paper. We propose a two stage approach. • As an interim response to cookie fatigue, we propose to further broaden Article 5(3) exemptions to better reflect functional and low-risk uses of terminal equipment data, as well as certain low-risk advertising models, including contextual advertising. • As step II, in the longer term, we see a need for a structured transition towards Privacy Enhancing Technologies (PETs) as a key enabling layer of the future digital ecosystem. However, PETs require careful assessment, technical standardisation and the development of privacy-preserving alternatives that are compatible with European values, competition objectives and data protection requirements. A dedicated technical discussion is still needed. This should support the development of standards and an effective regulatory framework.

PUBLIC

Commission proposal	Drafting suggestions and Comments
	SI (Comments): We support the deletion. SK (Comments): **SK:** We support deletion of this proposal.
~~**Automated and machine-readable indications of data subject's choices with respect to processing of personal data in the terminal equipment of natural persons**~~	HU (Comments): HU The deletion of this article is not in compliance with Article 5 of GDPR and may cause legal uncertainty, which big tech companies will certainly exploit for unlawful data processing, especially by data controllers outside the EU. We support the concept of automated consent. NL (Comments): In our view, solutions for centralised consent would lead to significant and tangible improvements both in terms of citizens' control over their data and the compliance burdens faced by European companies. NL therefore regrets the deletion of Article 8a (Article 88b) of the GDPR. We therefore urge the Presidency and our fellow Member States to reconsider the removal of this article. FI (Comments): FI considers that excluding Article 88b on centralised and automated consent for cookies is a missed opportunity but would not be a redline, especially if the Commission continues the work on updating the ePrivacy rules and the impact on inter alia the media sector are sufficiently considered.

PUBLIC

Commission proposal	Drafting suggestions and Comments
	On Article 88b, FI supported the CY Presidency's previous compromise proposals and would like to discuss whether a way forward could be a combination thereof (ST 8261/26, ST 9547/26). FI prefers finding a solution to 'cookie fatigue' that enables data subjects to exercise control over the collection and processing of their personal data and where they are provided with adequate information regarding such processing. If the provisions are placed in the GDPR, it should be ensured that non-personal data would not get higher level of protection than personal data (ie. the COM has not proposed to delete Article 5(3) ePD, and therefore the current obligations in ePD would still remain for data other than personal data).
~~(1) Controllers shall ensure that their online interfaces allow data subjects to:~~	
~~(a) Give consent through automated and machine-readable means, provided that the conditions for consent laid down in this Regulation are fulfilled;~~	
~~(b) decline a request for consent and exercise the right to object pursuant to Article 21(2) through automated and machine-readable means.~~	
~~(ba)~~	
~~(2) Controllers shall respect the choices made by data subjects in accordance with paragraph 1.~~	
~~(3) Paragraphs 1 and 2 shall not apply to controllers that are media service providers when providing a media service.~~	FI (Comments): If discussion for the centralised and automated consent for cookies is continued, FI highlights that it considers the exemption for media service

Commission proposal	Drafting suggestions and Comments
	providers to be of utmost importance. The exemption needs to also cover third-party cookies when used in connection with media services.
~~(4) The Commission shall, in accordance with Article 10(1) of Regulation (EU) 1025/2012, request one or more European standardisation organisations to draft standards for the interpretation of machine-readable indications of data subjects' choices.~~	
~~Online interfaces of controllers which are in conformity with harmonised standards or parts thereof the references of which have been published in the Official Journal of the European Union shall be presumed to be in conformity with the requirements covered by those standards or parts thereof, set out in paragraph 1.~~	
~~(5) Paragraphs 1 and 2 shall apply from [OP: please insert the date = 24 months following the date of entry into force of this Regulation].~~	
~~(6) Providers of web browsers, which are not SMEs, shall provide the technical means to allow data subjects to give their consent and to refuse a request for consent and exercise the right to object pursuant to Article 21(2) through the automated and machine-readable means referred to in paragraph 1 of this Article, as applied pursuant to paragraphs 2 to 5 of this Article.~~	
~~(7) Paragraph 6 shall apply from [OP: please insert the date = 48 months following the date of entry into force of this Regulation].~~	
~~7a.~~	
~~Article 88c~~	CZ (Comments): When it comes to AI – CZ believes that Digital Omnibus and changes to GDPR are not ambitious enough, because they do not provide higher level of legal certainty for AI developers and thus do not contribute to much needed simplification to allow AI development and training in the EU. CZ believes that reinstalment of Art. 88c (as proposed by DE or in other form) is essential element prior to closing Council position.

Commission proposal	Drafting suggestions and Comments
	CZ does not insist on keeping the full text of the Commission proposal and is ready to search for compromise wording. DK (Comments): We support the reintroduction of this provision in the operative text. ES (Comments): (See comment to recital 33 a)We would have preferred to keep this article with some amendments (see our comments of 21/05) AT (Comments): AT **can support** the deletion of Article 88c. PL (Comments): We would like to restore Article 88c in the operational part of the text. However, further work is needed to ensure legal certainty. Article 88c is an important element of the package as it provides legal certainty for the development of AI models. Addressing this issue only in a recital is insufficient, in particular, it does not provide legal certainty for companies developing AI systems. Therefore, we support maintaining Article 88c in the operative part of the text, although further work is needed to ensure legal certainty in its application. SI (Comments): We support the deletion of this provision and the inclusion of the corresponding explanation provided in recital 33a.

PUBLIC

Commission proposal	Drafting suggestions and Comments
~~**Processing in the context of the development and operation of AI**~~	CZ (Drafting suggestions): Processing of personal data in the context of the development and operation of AI SK (Comments): **SK:** We support deletion of this proposal.
~~**Where the processing of personal data is necessary for the interests of the controller in the context of the development and operation of an AI system as defined in Article 3, point (1), of Regulation (EU) 2024/1689 or an AI model, such processing may be pursued for legitimate interests within the meaning of Article 6(1)(f) of Regulation (EU) 2016/679, where appropriate, except where other Union or national laws explicitly require consent, and where such interests are overridden by the interests, or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.**~~	CZ (Drafting suggestions): Where the processing of personal data is necessary for the interests of the controller in the context of the development and operation of an AI system as defined in Article 3, point (1), of Regulation (EU) 2024/1689 or an AI model, such processing may be pursued for legitimate interests within the meaning of Article 6(1)(f) of Regulation (EU) 2016/679, where appropriate, except where other Union or national laws explicitly require consent, and where such interests are overridden by the interests, or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. LU (Comments): We observe that only some Data Protection Authorities currently recognize the possibility for the development and operation of AI systems to rely on legitimate interest, and that the risk of fragmentation therefore still does exist. We also recognise the broader strategic implications that this provision may entail for Europe.. We would be willing to continue discussions on this provision and we **would see merit if this part could be kept in the text**.
~~**Any such processing shall be subject to appropriate organisational, technical measures and safeguards for the rights and freedoms of the**~~	CZ (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
~~data subject, such as to ensure respect of data minimisation during the stage of selection of sources and the training and testing of AI an system or AI model, to protect against non-disclosure of residually retained data in the AI system or AI model to ensure enhanced transparency to data subjects and providing data subjects with an unconditional right to object to the processing of their personal data.'~~	Any such processing shall be subject to appropriate organisational, technical measures and safeguards for the rights and freedoms of the data subject, such as to ensure respect of data minimisation during the stage of selection of sources and the training and testing of AI an system or AI model, to protect against non-disclosure of residually retained data in the AI system or AI model to ensure enhanced transparency to data subjects and providing data subjects with an unconditional right to object to the processing of their personal data.'
Article 4 **Amendments to Regulation (EU) 2018/1725 (EUDPR)**	FI (Comments): FI notes that the above considerations on GDPR apply with respect to the EUDPR.
Regulation (EU) 2018/1725 is amended as follows:	
1. Article 3 is amended as follows:	
~~(a) in point 1, the following sentences are added:~~	
~~'Information relating to a natural person is not necessarily personal data for every other person or entity, merely because another entity can identify that natural person. Information shall not be personal for a given entity where that entity cannot identify the natural person to whom the information relates, taking into account the means reasonably likely to be used by that entity. Such information does not become personal for that entity merely because a potential subsequent recipient has means reasonably likely to be used to identify the natural person to whom the information relates.'~~	
~~(b) point 25 is replaced by the following:~~	
~~'(25) for 'electronic communications networks' the definition of Article 2(1) of Directive (EU) 2018/1972 shall apply;'~~	
(c) the following points are added:	
~~'(27) 'mobile application' means a mobile application as defined in Article 3(2) of Directive (EU) 2016/2102;~~	

Commission proposal	Drafting suggestions and Comments
~~(28) 'online interface' means an online interface as defined in Article 3(m) of Regulation (EU) 2022/2065;~~	
(~~29~~**27**) '~~"~~scientific research'~~"~~ means any research **conducted in an autonomous and independent manner**~~which can also support innovation, such as technological development and demonstration. These actions shall contribute to existing scientific knowledge or apply existing knowledge in novel ways, be carried out~~ with the aim of contributing to the growth of **society's**~~society´s~~ general knowledge and wellbeing**, generating new or complementing existing scientific knowledge, following a methodological and systematic approach consistent with standards of the relevant scientific field, including** ~~and adhere to~~ ethical standards**, and producing verifiable and transparent results** ~~in the relevant research area. This does not exclude that the research may also aim to further a commercial interest~~.'	
2. Article 4 (1)(b) is replaced by the following:	
'(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, **subject to the application of appropriate safeguards** in accordance with Article 13, be considered to be compatible with the initial purposes, independent of the conditions of Article 6 of this Regulation, ('purpose limitation');'	
3. Article 10 is amended as follows:	
(a) in paragraph 2, the following points are added:	
'(k) **incidental and residual** processing**,** in the context of the development and **technical** operation of an AI system as defined in Article 3, point (1), of Regulation (EU) 2024/1689 or an AI model **as referred to in Regulation (EU) 2024/1689**, subject to the conditions referred to in paragraph 4.~~.~~	
(l) processing of biometric data is **strictly** necessary for the purpose of confirming the identity of a data subject (verification), where the biometric data or the means needed for the **one-to-one** verification is under the sole	FR (Comments):

Commission proposal	Drafting suggestions and Comments
control of the data subject **and, where applicable, subject to appropriate safeguards to protect the fundamental rights and the interests of the data subject, as laid down in Union law**.'	La France rappelle son attachement aux modifications apportées sur la mention des gardes fous prévus par le droit de l'Union.
(b) the following paragraph 4 is added:	
'4. For processing referred to in point (k) of paragraph 2, appropriate organisational and technical measures shall be implemented to avoid the collection and otherwise processing of special categories of personal data. Where, despite the implementation of such measures, the controller identifies special categories of personal data **that are incidentally and residually involved** in the datasets used for training, testing or validation or in the AI system or AI model, the controller shall **erase**~~remove~~ such data **without undue delay. If erasure**~~. If removal~~ of those data **proves to be technically impossible or** requires **manifestly** disproportionate effort, the controller shall**,**~~ in any event effectively protect~~ without undue delay **and in any event, effectively protect** such data from being **further processed or processed for other purposes,** used to produce outputs,~~ from being~~ disclosed or otherwise made available to third parties.'	
4. in Article 14, paragraph 5 is replaced by the following:	
'5. Information provided under Articles 15 and 16 and any communication and any actions taken under Articles 17 to 24 and 35 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character or **where an abusive intention on the part of**~~also, for requests under Article 17 because~~ the data subject **can be demonstrated**~~abuses the rights conferred by this Regulation for purposes other than the protection of their data~~, the controller may refuse to act on the request **and inform the data subject of the reason thereof**. The controller shall bear the burden of demonstrating**, in light of all the relevant circumstances of the case,** that the request is manifestly unfounded or ~~that there are reasonable grounds to believe that it is~~ excessive.'	
5. in Article 15 the new paragraph 5 is added:	

PUBLIC

Commission proposal	Drafting suggestions and Comments
'5. When the **further** processing takes place for scientific research purposes **by the same controller and where and insofar as** ~~and~~ the provision of information referred to under paragraphs 1, 2 and 3 proves impossible or would involve a disproportionate effort ~~subject to the conditions and safeguards referred to in Article 13~~ or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that **further** processing, **subject to the conditions and safeguards referred to in Article 13,** the controller does not need to provide the information referred to under paragraphs 1, 2 and 3. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available.'	
6. in Article 24 ~~paragraphs 1 and 2 are~~ **is** replaced by the following:	
'1. **The** ~~A decision which produces legal effects for a~~ data subject **shall have the right not to be subject to a decision** ~~or similarly significantly affects him or her may be~~ based solely on automated processing, including profiling, **which produces legal effects concerning him or her or similarly significantly affects him or her, unless such processing** ~~only where that decision~~:	
(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller ~~regardless of whether the decision could be taken otherwise than by solely automated means~~;	
(b) is authorised by Union law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or	
(c) is based on the data subject's explicit consent.	
2. In the cases referred to in points (a) and (c) of paragraph 1, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.	

PUBLIC

Commission proposal	Drafting suggestions and Comments
3. Decisions referred to in paragraph 1 shall not be based on special categories of personal data referred to in Article 10(1), unless point (a) or (g) of Article 10(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.'	
(6a) in Article 27, paragraphs 1 and 2 are replaced by the following:	
1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, with particular regard to the lists referred to in Article 39(4) and (5), the controller and the processor shall, both at the time of the determination of the means for processing and at the time of the processing itself as applicable, implement, in an effective manner, appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.	PL (Drafting suggestions): We maintain our previously submitted drafting suggestion: "The allocation of responsibilities between the controller and the processor regarding the implementation of these measures shall be clearly defined, in particular in the contract or other legal act referred to in Article 28(3)." PL (Comments): We maintain our previous concerns regarding the practical allocation of responsibilities between controllers and processors under Article 25. While we acknowledge the intention to reflect current technological and market realities by extending data protection by design and by default obligations to processors, the proposed wording does not sufficiently clarify how responsibilities should be allocated in practice between the parties. Given that the controller remains primarily responsible under the GDPR for ensuring compliance with the Regulation, additional clarification would be beneficial in order to avoid legal uncertainty, overlapping obligations and potential inconsistencies in implementation. This issue becomes particularly relevant where technical and organisational measures are designed, developed or maintained by processors on behalf of multiple controllers. In such situations, greater clarity regarding the

Commission proposal	Drafting suggestions and Comments
	respective responsibilities of the parties would contribute to legal certainty and facilitate the practical application of the provision.
2.The controller and the processor shall implement appropriate technical and organisational measures to ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible to an indefinite number of natural persons without the individual's intervention.	
(6b) The following Article 30a is added:	
30a - Application of pseudonymisation and identification of a natural person	
(1) Controllers and processors may apply pseudonymisation in order to reduce the risks to the data subjects concerned and to comply with their obligations under this Regulation, in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information. To determine whether a natural person is identifiable, including through personal data having undergone pseudonymisation, account shall be taken of all the means reasonably likely to be used, such as singling out or online identifiers, either by the controller or by another person to identify the natural person directly or indirectly.	
(2) The application of pseudonymisation to personal data may, depending on the circumstances of the case and provided that appropriate technical and organisational measures are put in place and are such as to prevent the data in question from being attributed to the data subject, effectively prevent persons other than the controller from identifying the data subject in such a way that, for them, the data subject is not or is no longer identifiable.	
(3) Paragraphs 1 and 2 are without prejudice to other provisions and obligations applicable to the controller, including under Chapter IV and	

Commission proposal	Drafting suggestions and Comments
V of this Regulation. The provision set out in paragraph 2 shall not apply to processors.	
(4) The European Data Protection Board shall issue an opinion, in accordance with Article 64(2) of the Regulation (EU) 2016/679, addressing the application of pseudonymisation and anonymisation, including the related circumstances and technical and organisational measures referred to paragraph 2.'	
7. in Article 34, paragraph 1 is replaced by the following	
'1. In the case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall without undue delay and, where feasible, not later than 96 hours after having become aware of it, notify the personal data breach to the European Data Protection Supervisor. Where the notification to the European Data Protection Supervisor is not made within 96 hours, it shall be accompanied by reasons for the delay.'	
8. In Article 37 the following paragraphs are added:	LV (Comments): Article 8 should be deleted in order to maintain consistency with Regulation (EU) 2016/679 (GDPR). Given that Article 15 (Article 88, Article 88a) of Regulation (ES) 2016/679 (GDPR) has been deleted, as well as the ongoing discussions that legislation of cookie fatigue may be reviewed outside the Digital Omnibus, it is not supported to leave Article 8 in Regulation (EU) 2018/1725 (EUDPR). Furthermore, this article was deleted in the previous PRES text.
'(2) Storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person is only allowed when that person has given his or her consent, in accordance with this Regulation.	
(3) Paragraph 1 does not preclude storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person, based on Union law within the meaning of, and subject to the	

PUBLIC

Commission proposal	Drafting suggestions and Comments
conditions of Article 5, to safeguard the objectives referred to in Article 25(1).	
(4) Storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person without consent, and subsequent processing **for the same purpose**, shall be lawful to the extent it is **strictly** necessary for any of the following **purposes**:	
(a) carrying out the transmission of an electronic communication over an electronic communications network;	
(b) providing a service**, including its functionality,** explicitly requested by the data subject ~~and ensuring functionality of the requested service~~;	HU (Drafting suggestions): HU: (b) providing a service, ~~**including its functionality,**~~ explicitly requested by the **subscriber or user and ensuring the functionality of the service requested;** HU (Comments): HU: we do not support the amendment in the draft and recommend retaining the previous wording.
(c) ~~Measuring~~**measuring the audience of an online service** ~~in order to create~~**by creating anonymous**~~creating~~ aggregated information about the usage of **that**~~an~~ online ~~service to measure the audience of such a~~ service, where it is carried out by the ~~controller~~**provider** of that online service**,** ~~or by a third party acting together with~~**including jointly with others, or on behalf of** ~~this~~**that provider,** ~~including where the third party is~~**or by an entitled and independent third party performing audience measurement in accordance with Article 24 of Regulation (EU) 2024/1083** ~~solely for its own use~~;	
(d) maintaining or restoring the **technical** security of **the** ~~interface~~**means strictly necessary for the provision of an information society**~~a~~ service	

PUBLIC

Commission proposal	Drafting suggestions and Comments
~~provided by the controller and~~ requested by the **subscriber or user or the technical security of**~~data subject or~~ the terminal equipment used for the provision of such service**;**~~.~~	
~~(e) preventing or detecting fraud provided that such measures do not override the fundamental rights and interests of the data subject.~~	
(5) Where storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person is based on consent, the following shall apply:	
(a) the data subject shall be able to refuse requests for consent in an easy and intelligible manner with a single-click button or equivalent means;	
(b) if the data subject gives consent, the controller shall not make a new request for consent for the same purpose for the period during which the controller can lawfully rely on the consent of the data subject;	
(c) if the data subject ~~declines~~**refuses** a request for consent, the controller shall not make a new request for consent for the same purpose for a period of at least six months.	
This paragraph also applies to the subsequent processing of personal data based on consent.	
(6) This Article shall apply from [OP: please insert the date = 6 months following the date of entry into force of this Regulation]]	
~~(7) Controllers shall ensure that their online interfaces allow data subjects to:~~	
~~(a) give consent through automated and machine-readable means, provided that the conditions for consent laid down in this Regulation are fulfilled;~~	
~~(b) decline a request for consent through automated and machine-readable means.~~	
~~(8) Controllers shall respect the choices made by data subjects in accordance with paragraph 7.~~	
~~(9) Online interfaces of controllers which are in conformity with harmonised standards or parts thereof referred to in paragraph 4 of Article 88b of Regulation (EC) 2016/679 shall be presumed to be in~~	

PUBLIC

Commission proposal	Drafting suggestions and Comments
conformity with the requirements covered by those standards or parts thereof, set out in paragraph 7.	
(10) Paragraphs 7 to 9 shall apply from [OP: please insert the date = 24 months following the date of entry into force of this Regulation].'	
9. **Article 39 is amended as follows:**	
(a) **Paragraph 4 is replaced by the following:**	
'4. **The lists, the template and methodology** ~~established~~**adopted by the** ~~Board~~**Commission and referred to in paragraph 6a of Article 35 of Regulation (EU) 2016/679 should apply to the processing of personal data under this Regulation.'**	
(b) **Paragraphs 5 and 6 are deleted.**	
10. the following article is added:	
'Article 45a	
The common criteria adopted by the Commission and referred to in article 41a of the Regulation (EU) 2016/679 should apply to the processing of personal data under this Regulation.'	

PUBLIC

Commission proposal	Drafting suggestions and Comments
Article 5 **Amendments to and Directive 2002/58/EC (ePrivacy Directive)**	ES (Comments): We consider the expansion of the list of consent exemptions to be essential for simplification and cookie fatigue reduction. However, this reduction should not come at the expense of lowering the level of privacy protection afforded to citizens. Consent exemptions should be limited to low-risk cases and should either be narrowly defined or accompanied by appropriate safeguards to ensure respect for individuals' data protection rights. Expanding this list is not a minor issue. On the contrary, it may have a significant impact on the future design of digital services. It represents an opportunity both for simplification and for fostering more privacy-friendly service designs. For this reason, we believe that the priority should not be the rapid closure of the file. Rather, it is worth taking the time to carefully assess the available alternatives, as well as the impacts and implications of the proposed exemptions.
Directive 2002/58/EC is amended as follows:	FI (Comments): FI can support the amendments to ePrivacy regulation.
1. Article 4 is deleted;	
2. **In**~~After~~ Article **5**~~5(3)~~, **paragraph 3 is replaced by** the following subparagraph ~~is added~~:	NL (Comments): Regarding EC comments during AGS: we are not inherently opposed to a transfer of the current article 5(3) ePrivacy Directive compromise text to the GDPR, which could provide harmonisation and enforcement benefits. However, the scope of the original Commission proposal was limited to personal data, leaving the ePrivacy Directive applicable to other types of information and data. This would only decrease legal certainty as two separate legal regimes would apply, one of which being a directive subject to

Commission proposal	Drafting suggestions and Comments
	member state implementation. In order to achieve true reduction of administrative burden, a single regime should apply, which could also be the GDPR.
'3. Member States~~This paragraph~~ shall **ensure that the storing of information, or gaining of access to information already stored, in the terminal equipment of a~~not apply if the~~** subscriber or user is **only allowed when that person has given his or her consent, in accordance with Regulation (EU) 2016/679.** **Storing of information, or gaining of access to information already stored, in the terminal equipment of** a **~~natural person~~subscriber or user without consent, and subsequent~~, and the information stored or accessed constitutes or leads to the~~** processing of personal data **for the same purpose, shall be lawful to the extent it is solely related to and strictly necessary for~~ any of~~ the following purposes:**	LU (Comments): We remain very sceptical about the proposal to maintain and amend Article 5(3) of the ePrivacy, **instead of keeping all cookie related provisions in the GDPR**, as proposed by the Commission. Simplification also requires **consolidation of legal frameworks**, and our understanding is that keeping this provision within the ePrivacy Directive - rather than integrating it into the GDPR - would ultimately undermine this objective. HU (Comments): HU: We support keeping the list as narrow as possible but also covering necessary and proportionate cybersecurity prevention, detection and response measures. NL (Comments): NL can agree with the wording of the current whitelist. For NL it is important that all whitelisted purposes are clearly delineated to ensure legal certainty for businesses and at the same time prevent unforeseen, unintended or undesirable processing of user information. For NL the expanded whitelist already represents a meaningful improvement to the current regime, and we suggest no additional purposes to be added at this stage.
a) carrying out the transmission of an electronic communication over an electronic communications network;	

PUBLIC

Commission proposal	Drafting suggestions and Comments
b) providing a service, including its functionality, explicitly requested by the subscriber or user ~~and ensuring the functionality of the service requested~~**;**	
c) Measuring the audience of an online service ~~in order to create~~**by creating anonymous aggregated information about the usage of that online service, where it is carried out by the provider of that online service,** ~~or by a third party acting together with~~**including jointly with others, or on behalf of** ~~this~~**that provider,** ~~including where the third party is~~**or by an entitled and independent third party performing audience measurement in accordance with Article 24 of Regulation (EU) 2024/1083;**	ES (Drafting suggestions): (c) ~~Measuring~~**measuring the audience of an online service** ~~in order to create~~**by creating anonymous**~~creating~~ aggregated information about the usage of **that**~~an~~ online ~~service to measure the audience of such a~~ service, where it is carried out by the ~~controller~~**provider** of that online service**,** ~~or by a third party acting together with~~**including jointly with others, or on behalf of** ~~this~~**that provider,** ~~including where the third party is~~**or by an entitled and independent third party performing audience measurement in accordance with Article 24 of Regulation (EU) 2024/1083** ~~solely for its own use~~ **, provided that the personal data initially collected is instantly anonymised, is not further processed for another purpose, combined with data from other services from the provider of the online service or from a third party or shared with third parties, and provided that such processings do not override the fundamental rights and interests of the data subject;** ES (Comments): We share the need to amend the ePrivacy Dirtective in order to expand the whitelist of consent-exempt cases and thereby reduce cookie fatigue. However, it is essential to ensure proportionality and to strike a balance whereby such exemptions help reduce cookie fatigue without leaving citizens exposed to tracking and profiling practices carried out without their consent. In this regard, we agree that a consent-exemption related to audience measurement would be a positive development. However, it should be

PUBLIC

Commission proposal	Drafting suggestions and Comments
	accompanied by appropriate limitations and safeguards to ensure respect for fundamental rights and to protect the interests of citizens. It should be noted that the audience measurement exemption envisaged in this Article would not apply exclusively to media organisations. Rather, it would apply to any online service. FR (Drafting suggestions): c) Measuring the audience of an online service **in order to create** ~~in order to create~~**~~by creating~~** anonymous aggregated information about the usage of that online service, where it is carried out by the provider of that online service, ~~or by a third party acting together with~~including jointly with others, or on behalf of ~~this~~that provider, ~~including where the third party is~~or by an entitled and independent third party performing audience measurement in accordance with Article 24 of Regulation (EU) 2024/1083; FR (Comments): Modification de l'ordre des étapes en matière de mesure d'audience afin de décrire correctement ce processus : les données sont d'abord collectées, puis anonymisées avant d'être agrégées afin de pouvoir mesurer l'audience à l'échelle du site. HU (Comments): HU: This exemption shall apply to all personal data processed from the outset of the measurement process, including pseudonymised data processed during the initial phase, provided the service provider can demonstrate that the data is used solely and specifically for measurement purposes, to generate

Commission proposal	Drafting suggestions and Comments
	anonymous, aggregated usage data for that online service. The proposed amendment to Article 5(3)(c) of the ePrivacy Directive permits providers to bypass cookie consent when "measuring the audience of an online service by creating anonymous aggregated information about the usage of that online service, where it is carried out by the provider of that online service, including jointly with others, or on behalf of that provider, or by an entitled and independent third party…". Accordingly, this definition covers scenarios in which analytical services measure the audience of an online service by creating anonymous, aggregated usage data. However, when using various analytical services (such as Google Analytics), there may be instances at the beginning of the measurement process where the user remains temporarily identifiable. In such cases, the personal data is merely pseudonymised rather than fully anonymised. This could apply to EUDI Wallet service providers, for instance. In line with Articles 5a(1) and (4) of the eIDAS Regulation, these providers are legally required to provide seamless, user-friendly digital interfaces for their EUDI Wallet services. This requires inherently the measurement and monitoring of these services using analytical tools. In this case a stricter data protection authority might rule that, since the user's personal data was temporarily identifiable (i.e. even if for a few seconds), the provider fails to meet the criteria for the exception under Article 5(3)(c). To avoid any potential legal ambiguity in the future interpretation of the proposed Article 5(3)(c) when applied to e-government analytical and measurement services — specifically, where the temporary use of pseudonymised data during the process might otherwise disqualify the service from the exemption — we propose adding a clarification to the current text.
c) maintaining or restoring the technical security of the ~~interface~~means strictly necessary for the provision of an information society service requested by the subscriber or user or the technical security of the terminal equipment used for the provision of such service;	PL (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
	c) maintaining ~~or~~ restoring**, or ensuring** the technical security of the means strictly necessary for the provision of an information society service requested by the subscriber or user or the technical security of the terminal equipment used for the provision of such service, **including in particular cybersecurity, the protection of personal data and privacy of the user and prevention of fraud and unauthorised access provided that such measures do not override the fundamental rights and interests of the subscriber or user;** PL (Comments): We maintain our position presented in the non-paper. We propose a two stage approach to cookies – for reference, please see a comment to Article 88b.
~~d) preventing or detecting fraud provided that such measures do not override the fundamental rights and interests of the subscriber or user.~~	CZ (Drafting suggestions): **e) contextual advertising and related limitation of advertisement display, audience measurement and preventing fraudulent misrepresentation of audience, unless at least one of the following applies:** **(i) the processing could result in a risk to the rights and freedoms of natural persons;** **(ii) the processing involves profiling;** **(iii) personal data are stored at the time when the electronic communication service is not actively used.** **f) other techniques similar to contextual advertising specified by means of implementing act of the Commission, unless at least one of the conditions listed in point (e) applies.** CZ

Commission proposal	Drafting suggestions and Comments
	(Comments): CZ remains convinced that addition of an exemption concerning activities that are **not based on profiling,** and thus constitute a low risk intervention to the limitationof human rights and freedoms, should be added to the whitelist. These activities that are not base don profiling do not involve any retention of personal data beyond the user's active session. CZ wishes to higlight that our suggestion **is inspired by the EDPB/EDPS joint opinion (point 104) which emphasises the need to create incentives to use less intrusive forms of online advertising and aimed to make the rules more proportionate**, i.e. allowing some forms of targeted advertising, which is crucial for European publishers and service providers. As stated in relation to rec. 44, addition of this text is not a red line for Czechia so far but we are convinced that the final text should appropriately balance the data protection and industrial needs. In this regard, we consider this addition as very important. In contrary to our previous comments, we released letter (iv) as it appeared to be incompatible with frequence capping, which from our point of view should remain a valid, non-intrusive option for advertisers, decreasing the "ads fatigue" stemming from a repeated display of an advertisement. To futher work around new and evolving technologies, CZ also suggests that the Commission specifies and elaborates through implementing act techniques that remain low-intrusive, to make the provision future proof and to prevent the long-term legislative deadlock phase. The EDPB should be closely involved in the whole process of drafting the act. Alternatively, CZ can support Poland's proposal to elaborate on the processing where the controller deploys recognized privacy enhancing technologies (PET), at the same time we recommend not adding it as a new letter in paragraph 3, but as a separate paragraph. On the other hand, CZ doesn't support a staggered entry into force – if adopted, the implementing act should be prepared in a way to support the timely application.

Commission proposal	Drafting suggestions and Comments
	While we deem our suggestoins proportionate, we are open to discuss it further. DK (Drafting suggestions): **d) preventing or detecting fraud provided that such measures do not override the fundamental rights and interests of the subscriber or user.** DK (Comments): We would like to reintroduce this exemption to ensure a more proportionate framework for fraud prevention. We are open to introduce further appropriate safeguards. EE (Comments): Estonia prefers to keep this exemption. FR (Drafting suggestions): ***d) measuring the display and performance of advertising made solely on the basis of the immediate content displayed on the user's interface and not based on any type of profiling.*** ***e) preventing or detecting fraud provided that such measures do not override the fundamental rights and interests of the subscriber or user.*** FR (Comments): Réintroduction des exceptions relatives à la publicité contextuelle et à la détection de la fraude conformément à la position française exprimée en réponse à la note de la présidence irlandaise.

Commission proposal	Drafting suggestions and Comments
	PL (Drafting suggestions): In Article 5(3), points (e) and (f) are added: **(e) contextual advertising and related limitation of advertisement display, audience measurement and preventing fraudulent misrepresentation of audience, unless at least one of the following applies:** **(i) the processing is likely to result in a risk to the rights and freedoms of natural persons;** **(ii) the processing involves profiling;** **(iii) personal data are stored at the time when the electronic communication service is not actively used;** **(iv) personal data are connected with past or future activity of the data subject.** **(f) processing where the controller deploys recognised privacy-enhancing technologies (PETs) that effectively mitigate risks to the rights and freedoms of data subjects, in accordance with the technical specifications adopted pursuant to paragraph 4, 5 and 6.** In Article 5, paragraph 4 is added: **(4) For the purpose of Article 5 paragraph (3)(e), the Commission shall:** **(a) assess the state of the art of available technologies;** **(b)develop criteria to assess the effectiveness of risk mitigation in relation to the specific categories of data and processing operations.** In Article 5, paragraph 5 is added:

Commission proposal	Drafting suggestions and Comments
	(5) Article 5(3)(e) enters into force only 6 months after the adoption of relevant implementing acts by the European Commission. The implementing acts shall specify the technical standards and criteria to determine whether a technology qualifies as a recognised Privacy Enhancing Technology (PET) and effectively mitigates risks as referred to in paragraph 3(e). PL (Comments): We propose alternative options for enhancing the privacy of end-users of electronic communications services, for example through solutions collectively referred to as Privacy Enhancing Technologies (PET) – technical solutions, certified by independent bodies, that embed privacy directly into the architecture of data processing. Rather than preventing data use entirely, they can enable organizations to analyze, share and process data while minimizing exposure of personal information and reducing re-identification risks. It is worth analyzing the interoperability and effectiveness of such tools used so far and the potential for their development, while respecting user privacy. To protect user interests, it is worth considering establishing a basis for issuing guidelines on PET by the European Commission in cooperation with European Data Protection Board, specifying the requirements they must meet.
The subscriber or user shall be able to refuse requests for consent in an easy and intelligible manner with a single-click button or equivalent means. If the subscriber or user gives consent, the provider shall not make a new request for consent for the same purpose for the period during which the controller can lawfully rely on the consent of the ~~data subject~~subscriber or user. If the subscriber or user refuses a request for consent, the provider shall not make a new request for consent for the same purpose for a period of at least six months.	FR (Drafting suggestions): The subscriber or user shall be able to refuse requests for consent in an easy and intelligible manner ~~**with a single-click button or equivalent means**~~. If the subscriber or user gives consent, the provider shall not make a new request for consent for the same purpose for the period during which the controller can lawfully rely on the consent of the ~~data subject~~subscriber or user. If the subscriber or user refuses a request for consent, the provider shall

Commission proposal	Drafting suggestions and Comments
	not make a new request for consent for the same purpose for a period of at least **three** ~~**six**~~ months. FR (Comments): Les autorités françaises restent réservées concernant la possibilité de rejeter tous les cookies « par un single clic ou tout moyen équivalent » du fait qu'elle aboutirait à une baisse drastique du taux de consentement des utilisateurs et risque de remettre en cause la pertinence d'une exemption à destination des médias. Elles souhaitent diminuer à 3 mois le délai durant lequel il est interdit de solliciter de nouveau le consentement de l'utilisateur, afin de s'adapter au marché publicitaire valorisant des informations récentes sur les internautes. Elles soulignent que toutes ces modifications supposent de vérifier au préalable l'existence de logiciels permettant de distinguer les différents consentements donnés pour un même site. NL (Comments): For NL it is of utmost importance that the right balance is struck between alleviation of regulatory burden, and the users this article is intended to protect. NL therefore strongly supports the single-click refusal and six-month cooldown and considers it imperative that these remain in the article text. FI (Comments): FI considers that the single-click obligation could be further clarified, particularly with regard to its application to media service providers. Furthermore, the six-month prohibition on re-requesting consent could be revised to allow for a renewed consent request where warranted by service development, changes to the purposes of data processing, or other similarly justified circumstances.

Commission proposal	Drafting suggestions and Comments
Member States shall designate the competent supervisory authority under Regulation (EU) 2016/679 for the supervision and enforcement of the rules under this paragraph.	FI (Drafting suggestions): **In Article 15a, the following paragraph is added:** **5. Member States shall designate the competent supervisory authority under Regulation (EU) 2016/679 for the supervision and enforcement of the rules under ~~this paragraph~~ Article 5(3).** FI (Comments): FI supports this proposal. It should be, however, assessed, if this paragraph could be moved to article 15a, which contains the rules on competent authorities. It is important to ensure that the DPAs have powers to impose administrative fines. FI welcomes the Irish Presidency to look into the EDPB-EDPS JO concerning this.
2a In Article 17, the following paragraph is added:	
3. Member States shall adopt and publish, by [24 months after the adoption of this Regulation] the laws, regulations and administrative provisions necessary to comply with Article 5(3). They shall immediately communicate the text of those measures to the Commission.	
They should apply those measures from [24 months after the adoption of this Regulation].'	
Article 6 **Amendments to Directive (EU) 2022/2555**	
Directive (EU) 2022/2555 is amended as follows:	

PUBLIC

Commission proposal	Drafting suggestions and Comments
1. The following Article 23a is added:	
'Article 23a	
~~Single-entry point for~~ **Incident**~~incident~~ reporting **information point**	
(1) ENISA shall develop and maintain **an incident reporting information**~~a single-entry~~ point to support **the identification and fulfilment of** the obligation to report incidents and related events under the Union legal acts where those Union legal acts provide so ('**incident reporting information**~~single-entry~~ point'). ~~**Without prejudice to Article 16 of Regulation (EU) 2024/2847 of the European Parliament and of the Council, ENISA may ensure that the single-entry point builds on the single reporting platform established under that Regulation.**~~	
~~**(2) ENISA shall take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of the single-entry point and the**~~The incident reporting ~~**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.**~~	
(2) The incident reporting information point shall:	
(a) be designed to allow, on the basis of relevant information provided, the identification of the applicable reporting obligations referred to in paragraph 1 and the direction to the appropriate national entry point referred in Article 23b, and	
(c) make available simplified and documented information on incident notification processes in the different Member States.	
(3) When developing the incident reporting information point, ENISA shall consult the relevant national competent authorities under the relevant Union legal acts, the Cooperation Group, the CSIRT Network and other relevant bodies or groups established at Union level under relevant Union legal acts. ENISA shall establish structured	

Commission proposal	Drafting suggestions and Comments
communication channels to ensure that information available on the incident reporting information point is swiftly and effectively updated. Member States shall communicate to ENISA all relevant and necessary information for the purpose of paragraph 1a.	
(5) After establishing the incident reporting information point and in cooperation with the Cooperation Group, ENISA shall explore the possibility to extend the incident reporting information point by providing a report on:	FR (Drafting suggestions): **(4 ~~5~~) After establishing the incident reporting information point and in cooperation with the Cooperation Group, ENISA shall explore the possibility to extend the incident reporting information point by providing a report on:** FR (Comments): Consistency change
(a) regulatory mapping of relevant EU legal acts imposing cybersecurity risk management measures;	
(b) national measures, including transposition measures, implementing relevant Union legal acts imposing cybersecurity risk management obligations;	
(c) content to support entities in complying with obligations, in particular regarding entity registration, and cybersecurity risk-management.	
(4) The incident reporting 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.	FR (Drafting suggestions): **(5 4) The incident reporting 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.** FR

PUBLIC

Commission proposal	Drafting suggestions and Comments
	(Comments): Consistency change
~~(3) ENISA shall provide and implement the specifications on the technical, operational and organisational measures regarding the establishment, maintenance and secure operation of the single-entry point. ENISA shall develop the specifications in cooperation with the Commission, the CSIRTs network and the competent authorities under the Union legal acts referred to in paragraph (1). The specifications shall ensure that:~~	
~~(a) the necessary capability for interoperability with regard to other relevant reporting obligations referred to in paragraph (1) is ensured;~~	
~~(b) technical arrangements for the relevant entities and authorities under the Union legal acts referred to in paragraph (1) to access, submit , retrieve, transmit or otherwise process information from the single-entry point, are in place and, provide technical protocols and tools that allow the entities and authorities to further process the receive information within their systems;~~	
~~(c) the specificities of the incident reporting requirements set out under the Union legal acts referred to in paragraph (1) are duly taken into account;~~	
~~(d) where relevant, the single-entry point is interoperable and compatible with European Business Wallets referred to in [Proposal for a Regulation: Insert title of the proposal] and that the European Business Wallets can be used at least to identify and authenticate entities using the single-entry point;~~	
~~(e) entities using the single-entry point can retrieve and supplement information that they have previously submitted via the single-entry point;~~	
~~(f) a single notification of information submitted by an entity via the single-entry point can be used to fulfil reporting obligations as set out~~	

Commission proposal	Drafting suggestions and Comments
~~under any of the other Union legal acts which provide for incident reporting to the single-entry point.~~	
~~(4) Unless provided for in the Union legal acts referred to in paragraph (1) of this, ENISA shall not have access to the notifications submitted through the single-entry point.~~	
~~(5) Within [18] months from the entry into force of this Regulation, ENISA shall pilot the functioning of the single-entry point for each added Union legal act, including testing that takes into account the specificities and requirements for the notifications set out by each respective Union legal act, and after consulting the Commission and the relevant competent authorities under the respective Union legal acts. ENISA shall enable the notification of incidents under each Union legal act referred to in paragraph (1) only after piloting the functioning and after the Commission published a notice pursuant to paragraph 6.~~	
~~(6) The Commission shall, in cooperation with ENISA, assess the proper functioning, reliability, integrity and confidentiality of the single-entry point. When the Commission, after consultation of the CSIRTs network and the competent authorities under the Union legal acts referred to in paragraph 1, finds that the single-entry point ensures the proper functioning, reliability, integrity and confidentiality, it shall publish a notice to that effect in the Official Journal of the European Union.~~	
1a. The following Article 23b is added:	LV (Drafting suggestions): **(5) In the event which prevents the submission of single notification through the national entry point, Member States shall ensure that alternative channels are available for reporting of incidents and related events.** LV (Comments):

PUBLIC

Commission proposal	Drafting suggestions and Comments
	LV suggests to include as paragraph 5 the requirement for Member States to have alternative notification channels available in case the national entry point is not available for subjects (corresponding to recital (57)).
'Article 23b	
National entry point for incident reporting	
(1) Member States shall establish and maintain a national entry point for the reporting of incidents and related events under the Union legal acts where those Union legal acts provide so. The national entry point ~~shall allow for at least one of the following tasks~~**may, depending on** ~~national~~**Member States' organisational** ~~arrangements:~~**arrangement, allow for relevant tasks and functionalities in order to support and facilitate the reporting of incidents.**	ES (Drafting suggestions): (1) Member States shall establish and maintain a national entry point for **supporting and facilitating** the reporting of incidents and related events under the Union legal acts where those Union legal acts provide so. ~~The national entry point may, depending on Member States' organisational arrangement, allow for relevant tasks and functionalities in order to support and facilitate the reporting of incidents.~~ ES (Comments): Spain supports the joint proposal to restore the wording of REV5 for Article 23b(1), removing the additional sentence on "relevant tasks and functionalities". That sentence does not identify any concrete task, and its open-ended reference to "functionalities" could be interpreted as supporting a task-based definition of the national entry point. Such an interpretation would be difficult to reconcile with the flexibility Member States need to retain under paragraph 2. FR (Drafting suggestions): **(1) Member States shall establish and maintain a national entry point for supporting and facilitating the reporting of incidents and related events under the Union legal acts where those Union legal acts provide so. ~~The national entry point~~** ~~shall allow for at least one of the following tasks~~**may, depending on** ~~national~~**Member States' organisational**

Commission proposal	Drafting suggestions and Comments
	~~arrangements:~~**~~arrangement, allow for relevant tasks and functionalities in order to support and facilitate the reporting of incidents.~~** FR (Comments): Les autorités françaises estiment que la proposition de compromis utilisée par la présidence irlandaise ne fournit pas les garanties de flexibilité jugées nécessaires pour soutenir le texte. Les autorités françaises soulignent que la dernière proposition de compromis de la présidence chypriote (REV5 du 22/06) offrait en revanche la flexibilité requise pour le volet cybernétique. Elle permettait à chaque État membre d'adapter le point d'entrée national à ses dispositions et besoins nationaux, y compris ceux mis en œuvre pour protéger la sécurité nationale. Par conséquent, les autorités françaises demandent de modifier la rédaction du volet cybernétique, en l'alignant sur la REV5 (22/06) de la présidence chypriote. IT (Drafting suggestions): **(1)** Member States shall establish and maintain a national entry point for **supporting and facilitating** the reporting of incidents and related events under the Union legal acts where those Union legal acts provide so. ~~**The national entry point may, depending on Member States' organisational arrangement, allow for relevant tasks and functionalities in order to support and facilitate the reporting of incidents.**~~ IT (Comments): ACN estimates that the proposed compromise text does not provide the flexibility guarantees required to support the current wording. ACN underlines that the latest compromise proposal of the Cyprus Presidency (REV5 of 22 June) did provide the necessary flexibility for the

Commission proposal	Drafting suggestions and Comments
	cyber-related provisions. In particular, it ensured that each Member State could adapt the national entry point to its own national arrangements and requirements, including those established to safeguard national security. Therefore, ACN suggests amending the wording of the cyber-related provisions by aligning them with the text contained in the Cyprus Presidency's compromise proposal of 22 June. PL (Comments): We have strong concerns regarding the current wording. It is important to have a clear provision on an obligation to establish and maintain a national single entry point. The core functionalities of the point, like for example submission and receiving of notifications, should be listed in the text. The current wording is too vague and risks divergent interpretations. It is not clear what does it mean in practice "to allow for relevant tasks and functionalities in order to support and facilitate the reporting of incidents" To achieve the simplification goal the wording should be precise, otherwise we miss the opportunity to introduce a mechanism providing real burden reduction for entities.
~~enabling the submission of notifications at national level;~~	
~~receiving and processing notifications submitted by entities;~~	
~~ensuring or facilitating access to such notifications for the competent authorities under the relevant Union act;~~	
~~transmitting or making available relevant information to other national authorities, where foreseen under Union or national law;~~	
~~(2) The national entry point may also carry out the following tasks:~~	
~~supporting coordination among competent authorities in relation to reported incidents or information;~~	
~~providing guidance or assistance to entities regarding notification procedures;~~	
~~performing any other function necessary to facilitate the effective management and sharing of notifications at national level.~~	

PUBLIC

Commission proposal	Drafting suggestions and Comments
~~(3)~~**(2) Member States shall retain flexibility to configure their national entry point in accordance with their existing national structures and the allocation of competences among authorities, including by connecting existing systems and enabling the sharing, routing or distribution of relevant information.**	
~~(4)~~**(3) Member States shall** ~~endeavor~~**endeavour to design their national entry point with a view to making the national entry points interoperable with the national entry points of other Member States.**	PL (Comments): Ensuring interoperability of national points is crucial.
(4) ENISA shall, by [12 months from the date of entry into force of this amending Regulation], in consultation with the CSIRTs network, the Cooperation Group and other relevant bodies or groups established at Union level under relevant Union legal acts~~[VH1]~~ **provide non-binding recommendations to support Member States in the establishment, maintenance and secure operation of their respective national entry point. Those recommendations shall address technical, operational and organisational measures, taking into account experiences and lessons learned from existing reporting structures. Those recommendations shall include technical specifications to ensure interoperability between all Member States' national entry points as referred to in paragraph 3 and to facilitate the alignment of incident notifications submitted via their respective national entry point with cross-border reporting obligations.**	LV (Drafting suggestions): **(4) ENISA shall, by** ~~**[12 months from the date of**~~ **entry into force of this amending Regulation], in consultation with the CSIRTs network, the NIS Cooperation Group and other relevant bodies or groups established at Union level under relevant Union legal acts**~~[VH1]~~ **provide non-binding recommendations to support Member States in the establishment, maintenance and secure operation of their respective national entry point. Those recommendations shall address technical, operational and organisational measures, taking into account experiences and lessons learned from existing reporting structures. Those recommendations shall include technical specifications to ensure interoperability between all Member States' national entry points as referred to in paragraph 3 and to facilitate the alignment of incident notifications submitted via their respective national entry point with cross-border reporting obligations.** LV (Comments): Guidelines by ENISA on technical, operational and organisational measures (Article 23b(4)) for national entry points and on harmonization of incident notifications (Article 23c(3)) should be developed before Regulation enters

Commission proposal	Drafting suggestions and Comments
	into force OR the 30 months deadline for the obligation to report via the national entry point should only start after work on these guidelines is concluded. If the development or adaptation of national entry points and work on these guidelines would occur in parallel, that would only create uncertainty for Member States and would hamper the overall process, including meeting the deadline.
(5) ENISA shall, by [18 months from the date of entry into force of this amending Regulation], in cooperation with Member States, develop an open-source solution that may be used by Member States in setting up their national entry point in accordance with paragraph 1, with the objective of strengthening interoperability between national systems and enable faster, more effective cross-border data sharing when a situation requires coordinated action	LV (Comments): Open-source solution that may be used by EU Member States in setting up their national entry points should be kept voluntary and an appropriate deadline for implementation should be envisaged: - the period of 12 months after the availability of such a solution is not sufficient for the creation and implementation of a full-fledged national system; - Such an open-source solution would mean additional technical development work, adaptation of systems to national needs, budget planning and organization of public procurement, security testing, review of procedures, informing of the involved subjects, development/clarification of the relevant regulatory framework for alignment and other measures; - Clarification should be provided on the functionalities to be included in the solution developed by ENISA. It is not clear whether it will cover only the functionality of national entry points for information transmission, or whether it will also include a broader platform through which national competent authorities will be able to receive, process and manage the submitted information. - The development of the open-source solution and the national contact point can also be parallel processes. But in such a case, ENISA should already have a clear vision of the platform's scope, functionality and

Commission proposal	Drafting suggestions and Comments
	what technical solution it is based on, so that it can be planned in advance for its alignment with the national system.
1b. 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 elements and differences in 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 consider concrete steps and a timeline for introducing the unified approach to incident reporting under the Union legal acts.	
(3) Building on the report referred in paragraph (1), ENISA shall, in cooperation with the CSIRTs network, the Cooperation Group and competent authorities under the relevant Union legal acts, and other relevant bodies or groups established at Union level under relevant Union legal acts, develop guidelines for further harmonisation on incident notifications. These guidelines shall, in particular:	
(a) Identify ways to further 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 to the Commission and Council a first draft of these guidelines [by - within 12 months after the entry into force of	LV

Commission proposal	Drafting suggestions and Comments
this Regulation], and a final version within 18 months, and shall update them regularly thereafter.	(Drafting suggestions): **ENISA shall present to the Commission and Council a first draft of these guidelines [by ~~– within 12 months after~~ the entry into force of this Regulation], and a final version within ~~6~~18 months, and shall update them regularly thereafter.** LV (Comments): Guidelines by ENISA on technical, operational and organisational measures (Article 23b(4)) for national entry points and on harmonization of incident notifications (Article 23c(3)) should be developed before Regulation enters into force OR the 30 months deadline for the obligation to report via the national entry point should only start after work on these guidelines is concluded. If the development or adaptation of national entry points and work on these guidelines would occur in parallel, that would only create uncertainty for Member States and would hamper the overall process, including meeting the deadline.
~~(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.~~	
1c. The following article 23d is added :	
‘Article 23d	
Cross-border incident notification	

PUBLIC

Commission proposal	Drafting suggestions and Comments
(1) Member States should aim at facilitating cross-border notifications between national entry points, where incidents have cross-border impacts.	
(2) ENISA shall, in cooperation with the CSIRTs network, the Cooperation Group and competent authorities under the relevant Union legal acts, as well as with other relevant bodies or groups established at Union level under relevant Union legal acts, harmonise its relevant tools with national incident notification templates and facilitate an automatisation process to exchange information about cross-border impacts.	LV (Drafting suggestions): **(2) ENISA shall, in cooperation with the CSIRTs network, the NIS Cooperation Group and competent authorities under the relevant Union legal acts, as well as with other relevant bodies or groups established at Union level under relevant Union legal acts, harmonise its relevant tools with national incident notification templates and ~~facilitate an automatisation process~~ support voluntary automation of information ~~to~~ exchange ~~information~~ about cross-border impacts.** LV (Comments): As there are no guidelines in place, it is unclear what kind of information would be shared through the automated process. Therefore, any automated processes at this point should be voluntary for Member States.
(3) Member States shall retain control over the scope of information shared and any access to such information. '	
2. Article 23 is amended as follows:	
(a) in paragraph 1, the first sentence is replaced by the following:	
'Each Member State shall ensure that essential and important entities notify, without undue delay, its CSIRT or, where applicable, its competent authority in accordance with paragraph 4 of this Article of any incident that has a significant impact on the provision of their services as referred to in paragraph 3 of this Article (significant incident) via the **national entry**~~single-entry~~ point ~~established~~ pursuant to Article **23b**~~23a~~.	
The following paragraph 1b is added:	
(b) ENISA shall, in cooperation with the Cooperation Group, provide a mapping of all the competent authorities and CSIRTs referred to in	LV

Commission proposal	Drafting suggestions and Comments
paragraph 1 in the incident reporting information point established pursuant to Article 23a. '	(Drafting suggestions): **(b) 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 incident reporting information point established pursuant to Article 23a. '**
(b) the following paragraph 12 is added:	
'When a manufacturer notifies a severe incident pursuant to Article 14(3) of Regulation (EU) 2024/2847 and the incident reporting under that Article contains relevant information as required under paragraph 4 of this Article, the reporting of the manufacturer under Article 14(3) of Regulation (EU) 2024/2847 shall constitute reporting of information under paragraph 4 of this Article.;'	
3. in Article 30, paragraph 1 is replaced by the following:	
'1. Member States shall ensure that, in addition to the notification obligation provided for in Article 23, notifications can be submitted to the CSIRTs or, where applicable, the competent authorities, on a voluntary basis via **national entry**~~the single entry~~ point **referred to in**~~established pursuant to~~ Article **23b**~~23a~~, by:	
(a) essential and important entities with regard to incidents, cyber threats and near misses;	
(b) entities other than those referred to in point (a), regardless of whether they fall within the scope of this Directive, with regard to significant incidents, cyber threats and near misses.'	
Article 7 **Amendment of Regulation (EU) 910/2014**	
Regulation (EU) 910/2014 is amended as follows:	
1. in Article 19a, the following paragraph 1a is inserted:	
'1a. Notifications pursuant to paragraph 1, point (b) of this Article to the supervisory body and, where applicable, to other relevant competent	ES (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
authorities, shall be made through the **national entry**~~single-entry~~ point pursuant to Article **23b**~~23a~~ of Directive (EU) 2022/2555.;'	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~~ **supported** through the national entry point pursuant to Article 23b of Directive (EU) 2022/2555.; ES (Comments): Consequential amendment in line with the flexible configuration of the national entry point under Article 23b(1). Anchoring the notification obligation to the competent authority, with the national entry point providing support, keeps compliance tied to the substantive obligation rather than to the availability or configuration of a specific national channel. FR (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 **supported** ~~**made**~~ through the **national entry**~~**single-entry**~~ point pursuant to Article **23b**~~**23a**~~ of Directive (EU) 2022/2555.;' FR (Comments): En cohérence avec les autres propositions relatives au considérant 49 et à l'article 23b, les autorités françaises proposent des modifications visant à assurer une meilleure harmonisation. IT (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 **supported** ~~**made**~~ through the **national entry**~~single-entry~~ point pursuant to Article **23b**~~23a~~ of Directive (EU) 2022/2555.;'

Commission proposal	Drafting suggestions and Comments
	IT (Comments): In line with the other proposals on recital 49 and on article 23b, ACN proposes some consistency changes.
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 **national entry**~~single-entry~~ point pursuant to Article **23b**~~23a~~ of Directive (EU) 2022/2555.;'	FR (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 **supported** ~~**made**~~ through the **national entry**~~**single-entry**~~ point pursuant to Article **23b**~~**23a**~~ of Directive (EU) 2022/2555.;' FR (Comments): En cohérence avec les autres propositions relatives au considérant 49 et à l'article 23b, les autorités françaises proposent des modifications visant à assurer une meilleure harmonisation. IT (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 **supported** ~~**made**~~ through the **national entry**~~single-entry~~ point pursuant to Article **23b**~~23a~~ of Directive (EU) 2022/2555.;' IT (Comments): In line with the other proposals on recital 49 and on article 23b, ACN proposes some consistency changes.
3. in Article 45a the following paragraph 3a is inserted:	

Commission proposal	Drafting suggestions and Comments
'3a. Notifications pursuant to in paragraph 3 to the Commission and to the competent supervisory body, shall be made through the **national entry**~~single-entry~~ point pursuant to Article **23b**~~23a~~ of Directive (EU) 2022/2555.'	FR (Drafting suggestions): '3a. Notifications pursuant to in paragraph 3 to the Commission and to the competent supervisory body, shall be **supported** ~~**made**~~ through the **national entry**~~**single-entry**~~ point pursuant to Article **23b**~~**23a**~~ of Directive (EU) 2022/2555.' FR (Comments): En cohérence avec les autres propositions relatives au considérant 49 et à l'article 23b, les autorités françaises proposent des modifications visant à assurer une meilleure harmonisation. IT (Drafting suggestions): '3a. Notifications pursuant to in paragraph 3 to the Commission and to the competent supervisory body, shall be **supported** ~~**made**~~ through the **national entry**~~single-entry~~ point pursuant to Article **23b**~~23a~~ of Directive (EU) 2022/2555.' IT (Comments): In line with the other proposals on recital 49 and on article 23b, ACN proposes some consistency changes.
Article 8 **Amendments to Regulation (EU) 2022/2554**	
Article 19 of Regulation (EU) 2022/2554 is amended as follows:	
1. in paragraph 1, the first subparagraph is replaced by the following:	
'Financial entities shall report major ICT-related incidents to the relevant competent authority as referred to in Article 46 via the **national entry**~~single-~~	FR

Commission proposal	Drafting suggestions and Comments
~~entry~~ point established pursuant to Article **23b**~~23a~~ of Directive (EU) 2022/2555 in accordance with paragraph 4 of this Article.'	(Drafting suggestions): Financial entities shall report major ICT-related incidents to the relevant competent authority as referred to in Article 46 ~~**via**~~ **with the support of** the **national entry**~~**single-entry**~~ point established pursuant to Article **23b**~~**23a**~~ of Directive (EU) 2022/2555 in accordance with paragraph 4 of this Article.' FR (Comments): En cohérence avec les autres propositions relatives au considérant 49 et à l'article 23b, les autorités françaises proposent des modifications visant à assurer une meilleure harmonisation. IT (Drafting suggestions): Financial entities shall report major ICT-related incidents to the relevant competent authority as referred to in Article 46 ~~**via**~~ **with the support of** the **national entry**~~**single-entry**~~ point established pursuant to Article **23b**~~**23a**~~ of Directive (EU) 2022/2555 in accordance with paragraph 4 of this Article.' IT (Comments): In line with the other proposals on recital 49 and on article 23b, ACN proposes some consistency changes.
2. in paragraph 2, the first subparagraph is replaced by the following:	
'Financial entities may, on a voluntary basis, notify via the **national entry**~~**single-entry**~~ point established pursuant to Article **23b**~~**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.'	FR (Drafting suggestions): 'Financial entities may, on a voluntary basis, notify ~~**via**~~ **with the support of** the **national entry**~~**single-entry**~~ point established pursuant to Article **23b**~~**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

Commission proposal	Drafting suggestions and Comments
	may provide such information to other relevant authorities referred to in paragraph 6.' FR (Comments): En cohérence avec les autres propositions relatives au considérant 49 et à l'article 23b, les autorités françaises proposent des modifications visant à assurer une meilleure harmonisation. IT (Drafting suggestions): 'Financial entities may, on a voluntary basis, notify ~~via~~ **with the support of** the **national entry**~~single-entry~~ point established pursuant to Article **23b**~~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): In line with the other proposals on recital 49 and on article 23b, ACN proposes some consistency changes.
Article 9 **Amendments to Directive (EU) 2022/2557**	
Article 15 of Directive (EU) 2022/2557 is amended as follows:	
1. in paragraph 1, the first sentence is replaced as follows:	
'Member States shall ensure that critical entities notify via the **national entry**~~single-entry~~ point established pursuant to Article **23b**~~23a~~ of Directive (EU) 2022/2555 the competent authority, without undue delay, of incidents	FR (Drafting suggestions):

Commission proposal	Drafting suggestions and Comments
that significantly disrupt or have the potential to significantly disrupt the provision of essential services.;'	'Member States shall ensure that critical entities notify ~~**via**~~ **with the support of** the **national entry**~~**single-entry**~~ point established pursuant to Article **23b**~~**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.;' FR (Comments): En cohérence avec les autres propositions relatives au considérant 49 et à l'article 23b, les autorités françaises proposent des modifications visant à assurer une meilleure harmonisation. IT (Drafting suggestions): 'Member States shall ensure that critical entities notify ~~**via**~~ **with the support of** the **national entry**~~**single-entry**~~ point established pursuant to Article **23b**~~**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): In line with the other proposals on recital 49 and on article 23b, ACN proposes some consistency changes. LV (Comments): Latvia is cautious about CER Directive inclusion in the scope of the Digital Omnibus. The provisions of the Digital Omnibus affecting the CER Directive should first be assessed at expert level within the PROCIV-CER Working Party, where the CER framework was originally examined and negotiated. Expanded position:

Commission proposal	Drafting suggestions and Comments
	• LV has serious concerns regarding the inclusion of the CER Directive within the scope of the Digital Omnibus and cannot support such an approach. LV considers that the critical infrastructure resilience framework should be fully excluded from the envisaged horizontal incident reporting and administrative burden reduction mechanisms. • The CER Directive regulates matters directly linked to national security, the protection of critical infrastructure, civil protection and crisis management, as well as the handling of sensitive information. Integrating these matters into a single horizontal incident reporting system creates risks regarding the protection of critical infrastructure-related information, the separation of responsibilities between competent authorities, and the ability of Member States to apply processes aligned with their national security interests. We further recall that both the CER and NIS2 frameworks are "Directives", which provide Member States with a certain degree of discretion and flexibility in their national transposition and implementation. • Furthermore, the objectives and underlying logic of the CER Directive differ substantially from cyber security and digital incident reporting regimes. Within the CER framework, the assessment of incidents, risks and resilience measures is closely linked to sector-specific and national security considerations. Therefore, subjecting this framework to a single Digital Omnibus approach would not be proportionate. • It would neither be justified nor proportionate to require that non-cyber incidents — such as natural hazards, technical accidents, or physical/human-induced threats (including physical sabotage or terrorism) — be reported through the NIS2 contact point. • Physical incidents, which form the core of the CER Directive, should be reported exclusively to the national competent authorities designated under the CER framework, using the channels established by each Member State in the course of national transposition and implementation of the CER Directive. • The EU framework may promote mechanisms for the establishment of a national entry point with a view to reducing administrative burden;

Commission proposal	Drafting suggestions and Comments
	however, it should not impose a uniform organisational model. Member States must retain the necessary flexibility to organise reporting channels in accordance with their internal administrative structures and specific operational needs. • Consequently, LV does not consider it is appropriate for ENISA to develop a single notification template for incidents unrelated to cyber security or the digital environment (i.e. physical incidents). • The CER Directive has only recently been transposed, or is still in the process of transposition, in several Member States (approximately one third of Member States). Therefore, there is currently insufficient basis to conclude that horizontal amendments aimed at reducing administrative burden are necessary. Before any such amendments are pursued, a comprehensive assessment of the implementation and practical application of the CER framework across Member States would be required. Therefore, LV considers that the CER Directive should be excluded from the scope of the Digital Omnibus in order to preserve Member States' discretion in matters relating to the resilience and protection of critical infrastructure.
2. in paragraph 2, the following sub-paragraph is added:	
'The Commission may adopt implementing acts further specifying the type and format of information notified pursuant to Article 15(1). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 24(2).'	
Article 10 **Amendments, repeals~~Repeals~~ and transitory clauses**	
– 1. Regulation 2019/1150/EU is **amended as follows:~~repealed with effect from [date = entry into application of this Regulation].~~**	

Commission proposal	Drafting suggestions and Comments
– ~~1a.~~ **Articles 2(11), 2(12), 6, 8 to 10, 12 to 14, 16, 17, and 18 paragraphs (2) to (4), are deleted as of [date of entry into force].**	IT (Comments): As regards the individual provisions, the following observations are made: Article 1 must be maintained because it sets out the scope and subject matter of the P2B Regulation, which are necessary elements for the proper application of the other provisions that remain in force. To ensure the legal certainty and coherence of the remaining provisions of the P2B Regulation, it is necessary to maintain certain definitions set out in Article 2. We have identified that the definitions in points (11) and (12) can be repealed, as they are not used in the retained provisions of the P2B Regulation. Article 3 contains material obligations for platforms. Without Article 3.2, business users will no longer be informed before terms and conditions are changed and they will lose the right to terminate the agreement on these grounds. This harms the business user's position in their relation to the platform by weakening contractual transparency and predictability. In addition to the material obligation of Article 3(2), the transparency obligations set out in Article 3 offer considerable protection to business users, particularly since non-compliant terms and conditions are automatically null and void. The repeal of Article 3 would remove an important safeguard for business users against arbitrary enforcement, thereby depriving them of the right to be informed in advance, in a clear and comprehensible manner, of the potential conditions under which the service may be restricted, irrespective of the size of the platform. Article 5 must remain in force because national authorities play a crucial role in addressing ranking-related complaints from business users, and a notable

Commission proposal	Drafting suggestions and Comments
	number of requests based on this article has been received at the national level. Repealing Article 5 would risk reducing the accessibility and effectiveness of redress for SMEs operating on platforms. ITALY also asks to maintain Article 7 as it provides SMEs with insight into the various forms of differentiated treatment they may be subjected to and it enables authorities, including those under the DMA and competition law, to detect and address such practices. Without this provision, platforms are free to put business users at a disadvantage where they compete with the platform's own products and services, or with other business users controlled by the platform, without disclosure. Again, it is important to note that some Member States have received a notable number of Article 7 complaints and tip-offs. Articles 4 and 11 must remain on a permanent basis, and not only until 31 December 2032, or , alternatevely, be repealed only only after a specific review has been carried out in accordance with Article 18 of the current P2B Regulation. Articles 18 and 19 must remain in force to maintain coherence of the Regulation following its partial repeal. We believe its removal will lead to ambiguity and legal uncertainty.
– ~~2. By way of derogation from paragraph 1, the following provisions shall continue to apply until 31 December 2032:~~	
~~(a) Article 2, point (1);~~	
~~(b) Article 2, point (2);~~	
~~(c) Article 2, point (5);~~	
~~(d) Article 4;~~	
~~(e) Article 11;~~	
~~(f) Article 15.~~	

PUBLIC

Commission proposal	Drafting suggestions and Comments
– **2~~3~~**. The following acts are repealed~~, with effect from [Date, aligned with the entry into application of the amendments]~~:	
a) **Chapters III, IV, V, VI, VII of** Regulation (EU) 2022/868;	
b) Regulation (EU) 2018/1807;	
3. Chapter I and II of Regulation (EU) 2022/868 and Directive 2019/1024 are repealed [18 months after the publication in the Official Journal of the European Union].	
~~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**	HU (Comments): HU: Article 11 does not set a later date of application for Article 6(1a) inserting Article 23b. It would also be appropriate to set an explicit deadline for this, aligned with the 30-month date of application. Article 23b does not contain mandatory minimum security requirements specifically to the national entry point; it leaves the technical, operational and organisational measures to non-binding ENISA recommendations. As the entry point is a common national channel for sensitive incident reporting in several regulatory areas, it is worth setting out minimum requirements for secure operation and access in line with the authority's competences.
This Regulation shall enter into force on the third day following that of its publication in the Official Journal of the European Union.	
~~Deviating from paragraph 3,~~ Article 5(2) shall enter into application 6 months after the publication in the Official Journal of the European Union.	

Commission proposal	Drafting suggestions and Comments
By way of derogation from paragraph 1, 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. **By way of derogation**~~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 **national entry**~~single-entry~~ point set out in Article **23b**~~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**~~24~~ months from the entry into force of this Regulation.	IT (Drafting suggestions): **Consequential application rule** Add the amendments concerning Articles 24, 25, 29a, 32, 33, 35, 57, 58, 58a, 77 and 79 GDPR to the provisions applying 18 months after entry into force, unless an earlier application date is agreed for the investigation-duration provisions IT (Comments): A coordinated application date avoids conflicting transitional regimes. LV (Comments): LV sees that it would be valuable to keep reference that deadline for the obligation to report via the national entry point could be extended by 6 months if deemed necessary to keep flexibility as not all Member States have established national entry points that not only will have to be developed but also tested. The guidelines by ENISA on technical, operational and organisational measures (Article 23b(4)) for national entry points and on harmonization of incident notifications (Article 23c(3)) should be developed before Regulation enters into force OR the 30 months deadline for the obligation to report via the national entry point should only start after work on these guidelines is concluded. If the development or adaptation of national entry points and work on these guidelines would occur in parallel, that would only create uncertainty for Member States and would hamper the overall process, including meeting the deadline. HU (Comments):

Commission proposal	Drafting suggestions and Comments
	HU: It is a positive change that application deadline is amended up to 30 months but since but since Commission and ENISA recommendations and guidelines are available in 6, 12 and 18 months this leaves only a maximum of 12 months for adoption.
This Regulation shall be binding in its entirety and directly applicable in all Member States.	
Done at Brussels,	
For the European Parliament *For the Council*	
The President *The President*	
ANNEX I	
Correlation table	
[…]	
[…]	
[…]	
Annex II	

PUBLIC

Commission proposal	Drafting suggestions and Comments
List of thematic categories of high-value datasets, as referred to in Article 32ab(1) of Regulation (EU) 2023/2854	
– 1. Geospatial	
– 2. Earth observation and environment	
– 3. Meteorological	
– 4. Statistics	
– 5. Companies and company ownership	
– 6. Mobility	

PUBLIC