Council of the European Union
General Secretariat

Brussels, 23 December 2025

WK 17677/2025 INIT

LIMITE

SIMPL
ANTICI
DATAPROTECT
CYBER
TELECOM
CODEC
PROCIV

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

WORKING DOCUMENT

From:	General Secretariat of the Council
To:	Antici Group (Simplification)
Subject:	Omnibus VII (Digital Omnibus) - compiled comments (ddl 18/12)

Following the meeting of the AGS on 12 December on the Omnibus VII (Digital Omnibus), delegations will find a compilation of additional questions and comments as received from: BE, CZ, DE, HU, NL, AT, PT, SI, FI and SE.

Omnibus VII - Digital Omnibus

(ddl 18/12/25)

AGS meeting on 12/12/25

Table of Contents

BELGIUM

DATA

- **Entry into force & transitional period :**
    - ***Slide 71*** : "Q *Are non-digitised data or non-digitised documents now in scope?" to which the answer provided for by the COM is : "Before they were in scope of the ODD but not Ch II DGA. Now they are in scope of the ODD and Ch II DGA. & No additional burden as public sector bodies do not need to share any data under Chapter II DGA (now Section 3 of Chapter VIIc).*".

This is a **new element** in the legislative package --and not merely a 'copy paste' of the existing texts and obligations—and thus requires modification of national legislation and the necessary preparation time (means, budgets, infrastructure) to be able to implement these novelties. Entry into force three days after the publication seems unrealistic. Besides, we would welcome a reassessment of the budgetary impact of the creation of more possibilities to allow re-use of protected public sector data. We wonder whether the fact that it is not compulsory really means that there is no budgetary impact.

- ***Slide 75****, under the second point : "Ch II DGA and ODD scope and obligations remain the same. However inter alia: Ch II DGA now: includes non-digitised content, has info on means of redress & possibility for online payment"*

The online electronic payment system that should be provided on the website by each public sector body requiring the payment of fees for re-use of their data is also a **new element**. This requires necessary preparation time (means, budgets, infrastructure) to be able to implement these novelties. Entry into force three days after the publication seems unrealistic.

- ***Slide 82*** : Q "*What is the rationale of the amendments to the single information point (Chapter II DGA)?" COM answer : "Deleted "may" provision to link the information point to sectoral, regional or local information points." & "Simplification & streamlining*".

Does this mean that there still will be the requirement of only one single information point per member state (that can be linked to sectoral, regional or local information points) ? or can there now be several single information points per region for example?

- **Slide 83 :** Q "Could the Articles on single information points and open data publishing not be joined and synchronised?" COM answer : "*The proposal aimed at joining and synchronising Articles that were virtually the same (or very similar), bearing in mind not to cause too much burdens on Member States for the implementation." & "This is why the two regimes were kept separately*."

If Member States where that use one and the same 'infrastructure' for both single information point and open data publishing, would this be conform the new provisions of the Data Act?

- **Slide 86 :** Q "*In the context of High value data sets, what does "substantial part of their costs relating to the performance of their public tasks" mean? Is there a definition?*"

We would like to receive a further clarification. Does this mean, under the current and the new framework, that it concerns only public sector bodies that are by law obligated to cover a substantial part of their costs of their public tasks by their own revenues?

CZECHIA

CZ Questions regarding the Omnibus VII (deadline 18. 12.)

GENERAL DIGITAL OMNIBUS

Data acquis

- Do we understand correctly that the exemption from data sharing under proposed Art. 4(8) and 5(11) of the Data Act can be used on the basis of demonstrable serious harm resulting also from the mere sharing (lawful disclosure) of trade secrets with European users or third parties?
- In this regard, can the EC confirm that there is no risk of abuse of the data sharing exemption in case of data access requests (lawful disclosure) on the grounds of a possibility of disclosure of trade secrets to non-European entities?
- How should the phrase "*unlawful acquisition, use, or disclosure to third-country entities*" in Articles 4(8) and 5(11) be interpreted? Does "*unlawful*" also apply to "*disclosure*"? If so, what makes the acquisition, use, or disclosure unlawful? Does this mean that the user or third party cannot share the data with another third party outside the EU without the explicit consent of the data holder?
- Do we understand correctly that the new exception in Article 31(1a) of the Data Act only applies to systems other than IaaS that are highly customized but not custom-built based on Art. 31(1))?
- Why is the Art. 38(3) of the Data Act obliging competent authorities to cooperate (also in cross-border context) in resolving complaints proposed to be deleted?
- What is the intended role of the EDIB within the Digital omnibus? Is it still a COM expert group focused on implementation, or is it being expanded to include the political level? Do we understand correctly that the EDIB will now include representatives of all competent authorities (not only the data coordinator) as well as representatives of the MS responsible for data policy? In what formations will the EDIB meet?

Single-entry point

- Will the Commission and/or ENISA conduct case studies and issue a formal written report to assess the added value and benefits of SEP for national authorities and reporting entities?
- Will the Commission finance or co-finance the integration of existing national platforms with SEP (connectors, API work, access control alignment, testing), and how will previously made Member State investments be recognised (e.g., eligibility under EU programmes, co-funding rates, or cost offsets)?
- Given that the proposal requires Member States to provide alternative reporting channels in case of incidents or SEP non-functionality, how will the setup and ongoing

operational costs for these channels be mitigated or supported to ensure they do not undermine SEP's objectives?

- The draft foresees that ENISA shall not have access to notifications submitted through SEP; could you specify whether ENISA will see any type of information reported? The same question applies for any potential private-sector provider responsible for the SEP.
- How will SEP comply with the language requirements for incident reporting—ensuring that entities have the option to submit in their national language?

We would also like to raise again some questions that were not answered during the last two Q&As

Questions regarding the proposed Digital Omnibus Regulation - Amendments to Regulation (EU) 2023/2854 Data Act

To clarify or make sure that the proposal does not change the existing regulation of statistical data (adjustment of so-called open data and re-use of data) collected by the central bank.

- Can the Commission confirm that confidential statistical data collected by central banks under ESCB regulations remain fully outside the scope of Section 2 (open data) and Section 3 (re-use of protected data) of the proposed Regulation?
- Can the Commission confirm that the proposed Regulation does not oblige central banks to modify or replace their existing dissemination frameworks as long as they comply with ESCB statistical rules?
- Can the Commission confirm that proposed Regulation allows Member States explicitly exclude their national central banks from national implementation measures on public sector data governance, in view of their specific EU-law mandates?
- Can the Commission confirm that proposed Regulation allows confidential datasets held by central banks not to be included in the national single information point or asset lists unless already publicly accessible?

CZ shares NL questions from the previous round regarding Article 88a GDPR (Access to terminal equipment)

This article contains several good elements, but some elements require further clarification:

- The exception in paragraph 2 with regard to "member state law" can lead to fragmentation and divergent rules. Paragraph 2 appears to go further than the existing Article 5(3) of the e-Privacy Directive and seems to go beyond just cookies. What specifically does paragraph 2 cover, and why is it necessary?
- Is a legal basis within the meaning of Article 6 GDPR still required in addition to Article 88a(3)?
- Paragraph 4 does not mention the option to withdraw consent. Shouldn't a section on consent withdrawal be added? In other words: how does Article 88a(4) relate to Article 7 GDPR, which stipulates that consent must always be withdrawable?
- If a website no longer works after rejecting cookies, is Article 88a fulfilled?
- The last sentence of paragraph 4 also applies to "subsequent processing." This is a significant expansion. Therefore, no proportionality test applies here. How does this relate to Article 6 of the GDPR and necessity and proportionality?

We would also like to raise again some questions that were not answered during the last Q&A on Single-entry point:

Governance and National Integration

- The Staff Working Document (SWD) concludes that SEP is the best possible solution. Could you elaborate **on the key factors behind this assessment?**
- How does SEP **concretely reduce administrative burden for national authorities**, given the diversity of reporting obligations under NIS2, DORA, GDPR, and other legal frameworks? Could you provide concrete examples of expected simplifications?
- In the financial analysis, cost savings are projected from implementing SEP across multiple frameworks. How were these savings calculated, and how did the Commission account for **investments already made by Member States** in building national reporting systems? What specific efficiencies or reductions in costs does SEP deliver?
- Will the Commission **finance or co-finance integration costs for national platforms**, given that Member States remain responsible for alternative means of reporting and the significant investments already made by Member States?
- Could the Commission provide **an overview of the proposed technical solution** for SEP, including how it might integrate with existing national platforms?
- Will there be a **formal mechanism for Member States to influence SEP design** beyond CSIRTs Network consultations (e.g., a dedicated technical working group including GDPR, CER, DORA authorities)?
- What does "alternative means" for reporting entail in practice, and how will the associated costs for Member States be mitigated?

Access Management and Visibility

- The draft regulation mentions ENISA shall not have access to the notifications submitted through the SEP. **Is there any type of information that ENISA will be able to see in the reporting process?**
- How will the governance be structured to ensure national PoC manage access rights and visibility for all relevant national authorities? What national PoC should have admin access if any?
- The regulation mentions technical arrangements for authorities to access and process information. Will **multiple national authorities be able to view the same incident report**, and what restrictions will apply to prevent unnecessary data exposure (e.g., cybersecurity data)? How will the confidentiality of information be ensured between authorities of a single Member State?
- Will there be role-based access controls to prevent **unnecessary exposure of sensitive data** across sectors?
- How will **requests for additional information from different authorities be coordinated to avoid overwhelming reporting entities?**

Technical Standards and Interoperability

- The proposal requires ENISA to consider APIs and machine-readable standards for integration with national systems. At what stage of the preparation process **will Member States receive the technical specifications**, so they can assess the adaptability of SEP to their existing national solutions?
- Will ENISA or the Commission have ability to edit data?

- Will the submitted data be encrypted? What are the encryption standards expectations?
- What are the considerations regarding backups and storages of data? Are these to be handled centrally or nationally?
- What access or visibility should have the provider of SEP in case the provider is from private sector?

Practical Functioning

- The regulation mentions entities can retrieve and supplement previous submissions. Will SEP also **support structured workflows for follow-up actions** (e.g., status updates, additional data requests)?
- The proposal allows entities to retain the information they previously submitted via SEP. Will national authorities be informed when an entity requests such information?
- How will the Commission ensure that this mechanism **does not bypass national authorities' oversight**? Should information requests be routed exclusively through national authorities?
- The reporting templates for NIS2 and DORA differ significantly, and the information required under DORA is often insufficient for an effective CSIRT response under NIS2. How does the Commission plan to address these discrepancies to avoid duplication and ensure that **reports remain actionable for cybersecurity authorities**?
- How will SEP **handle language requirements for incident reporting**? Will entities be allowed to submit reports in their national language, and if so, who will be responsible for translation—ENISA, Member States, or the reporting entity?

Scope and Timeline

- How will the Commission ensure readiness for the 18-month deadline, and what criteria will trigger the optional extension to 24 months?
- How **will delays be managed if technical or security requirements** are not met within the set timeframe? Would the Commission consider a flexible approach, e.g., starting the application period 6 months after the Commission confirms SEP readiness, rather than a fixed date?
- Is the Commission **considering any transitional provisions** for cases where it is not technically feasible to migrate reporting from existing national platforms to SEP within the set deadline?

<u>*Personal data*</u>

Systemic links to other data protection instruments

Amended definition of "personal data" in GDPR is clearly important for other EU data protection instruments. While the EUDPR (regulation 2018/1725) is being modified in the same way, there is not a corresponding amendment to LED (directive 2016/680). Is the Commission proposing to establish two definitions of "personal data" or will the LED and other rules be amended later in line with recital 43?

Legal bases for AI systems

Given the recital 30 and Article 88c, the legitimate interest in Article 6(1)(f) GDPR appears to be a default legal basis for both the development and the use of AI systems – at least in private sector. Consent could be required by EU or Member State law as well. Could the Commission confirm that EU or Member State law could also use a legal obligation as a legal basis for processing by AI system?

Special categories and AI systems

We understand that specific legal ground for processing in Article 10(2) AI Act is separate from the new amendments to Article 9 GDPR - there may be overlaps but those rules are mutually independent. Could the Commission confirm?

Pseudonymisation

Since means and criteria for qualified pseudonymisation will be formally adopted by the Commission, why is the benefit for controller in Article 41a(3) so unremarkable? If the means and criteria were implemented correctly, should not the controller deserve a stronger legal position?

GERMANY

Questionary on the Omnibus VII Proposal

Preliminary note: The questions already submitted by GER have not been fully answered yet. We assume that the Commission will answer them. Therefore, we have refrained from resubmitting the same questions. Thus, the following questions should be understood as additional questions.

III. GDPR

1. How does the Commission assess the impact of Article 88c GDPR on creative artists such as singers, actors, or voice actors whose data - such as their appearance or voice - is published in their works and is therefore particularly accessible to AI?

2. Controllers' information requirements
   „In Article 13, paragraph 4 is replaced by the following:
   '4. Paragraphs 1, 2 and 3 shall not apply where the personal data have been collected in the context of a clear and circumscribed relationship between data subjects and a controller exercising an activity that is not data-intensive and there are reasonable grounds to assume that the data subject already has the information referred to in points (a) and (c) of paragraph 1, unless the controller transmits the data to other recipients or categories of recipients, transfers the data to a third country, carries out automated decision-making, including profiling, referred to in Article 22(1), or the processing is likely to result in a high risk to the rights and freedoms of data subjects within the meaning of Article 35."

   - This change in law may be a benefit for small operators, but may have a detrimental effect on data processing by public bodies such as the tax administration. Up to now, it has been possible to inform the persons concerned by means of a general, publicly available information letter. This simplification is essential for public bodies.

   - Would a supplementary exemption for public sector bodies be conceivable, as it is currently planned for private processors with non-extensive data processing?

   - Would the concern to relieve controllers of administrative obligations related to data protection not be better taken into account if the previous regime is maintained and paragraph 4 is only supplemented by the proposed regime/simplification?

3. General question on Art. 88a GDPR (especially (3)): the provision only uses the term "service", whereas Art. 5 (3) ePrivacy Directive uses the term "information society service". Is the term „service" in Art. 88a GDPR meant to be broader than in Art. 5 (3) ePrivacy

Directive? Please explain in further detail the operational simplifications brought about by the proposed Art. 88a GDPR.

4. Slide 94: Is it intended that all provisions on cookies will be part of the One Stop Shop mechanism in the future? A separate enforcement by national data protection or other authorities under ePrivacy Directive would thus not be possible anymore.

   Slide 94 states: „Where the new articles provide for new elements, we will reflect." What does this mean in concrete terms?

5. Slide 95 reads: „It is difficult to estimate how many more cookie banners will be displayed because of the media exemption from central cookie settings"→ Is an exemption for media service providers thus really necessary, especially against the background of the "cookie fatigue"?

6. Slide 98: „The proposed amendments to Art 4(1) GDPR do not change our understanding on what is personal data, but builds on recital 26 and case-law." → We kindly ask COM to explain this point in more detail. In our understanding the new definition of personal data in Art. 4 (1) GDPR leads to narrowing down the scope of personal data and goes beyond the CJEU judgment in EDPS ./. SRB.

7. Slide 100: Why is an additional legal basis under Art. 6 not required, even though two additional new exemptions to the consent requirement are added? How do these two new exemptions fit into the regulatory framework of the GDPR, which stipulates that all legal bases for processing must be included in Art. 6 GDPR (cf. EuGH, Schufa, C 634/21 und Digi, C-77/21)

8. Slide 101 explicitly emphasizes that aggregated information about the usage of an online service to measure the audience of such a service can only be created, where it is carried out by the controller of that online service solely for its own use. Slide 102 emphasizes, that „[the] Exemption only applies where aggregated information are used to measure the audience. This would exclude broader behavioral analytics for individuals by definition." Do we understand it correctly that, as a result, only anonymous first party cookies would be permitted under Art. 88a Abs. 3 c) GDPR?

9. What practical example is there for the regulatory alternative in Art. 88a (3) (d) GDPR regarding the request only by the terminal equipment? (Art. 88a (3) *(d) reads: „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.")?*

IV. Data / Data Act

10. Incorporating four different legal acts with different subject matters and scopes into the Data Act will pose complex challenges to member states' implementation legislations, e.g. in designating competent authorities. Will this complexity be taken into account in determining the date of application of the revised Data Act legislation and will member states be allowed sufficient time to implement the changes into their national laws?

V. Other

11. With regard to Article 10(2) of the Digital Omnibus Regulation, is the European Commission's proposal to be understood as meaning that the P2B rules applicable until 31 December 2032 (including Articles 4 and 15 of the P2B Regulation) can continue to be enforced until that date by the national P2B authorities in the event of original P2B factual conduct, or is the continued application of those specific P2B rules limited exclusively to situations in other EU legal acts which contain cross-references to the P2B Regulation?

12. Contrary to the repeal of the P2B Regulation with the entry into force of the Digital Omnibus Regulation currently provided for in Article 10(1) of the Digital Omnibus Regulation, does the European Commission intend to provide for transitional periods for the enforcement of the P2B Regulation?

13. Is it planned to transfer the provisions of the P2B Regulation in addition to the DSA in favour of business users as symmetrical provisions in the future to the DSA in order to close the resulting delta to the respective substantive regulations and obligated addressees of the DSA and DMA when the P2B Regulation is repealed and to ensure a comparable level of protection for business users in the future?

14. In its assessment, to what extent has the European Commission taken into account or intends to take into account developments since the publication of the report on the preliminary assessment of the P2B Regulation in 2023, such as the establishment of national P2B enforcement authorities in several EU Member States (such as NL and DEU), a significant increase in the number of complaints by business users and nationally led enforcement procedures for the P2B Regulation?

HUNGARY

Hungarian questions on Digital Omnibus

Questions on data regulation and ePrivacy:

1. There are other definitions that were included in the DGA but were not incorporated into the Data Act. Is it possible to take them over or what will happen to them? (e.g. access, data sharing, main establishment, legal representative)

2. Would it not be necessary for the text to address the continuity of the existing registers of data intermediation and data altruism organisations, and how these will be transformed in the future into a register under the Data Act? Presumably, the intention is to avoid any interruption, meaning that entities already registered should be able to continue using the label without having to re-register.

3. The conditions have been simplified for the provision of data intermediation services. Do we understand that, in the new approach, even statistical offices can provide such a service? Or Article 32c para b) constitutes an obstacle to that (the data they collect are used only for the development of that data intermediation service)?

4. Do we understand correctly that the tasks of the data coordinator will also cover cooperation on the new types of procedures introduced in the Regulation?

5. Could we consider further amendments to the ePrivacy Directive, in line with last December's amendment to Regulation (EC) No 223/2009 on European statistics or it is not needed?

Text proposal for a new article:

A national statistical institution or the Commission (Eurostat) may request a provider of a publicly available electronic communications service to make data processed under this Directive and the relevant metadata available free of charge where the data requested are strictly necessary for the development, production and dissemination of European statistics and cannot be obtained by other means or their reuse will result in a considerable reduction in the response burden according to the rules and procedure specified in Article 17b-17e. of regulation (EC) No 223/2009 of the European Parliament and the Council of 11 March 2009 on European statistics and repealing Regulation (EC, Euratom) No 1101/2008 of the European Parliament and of the Council on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities, Council Regulation (EC) No 322/97 on Community Statistics, and Council Decision 89/382/EEC, Euratom establishing a Committee on the Statistical Programmes of the European Communities. Such data access shall concern in principle non-personal data and, only in specific circumstances, personal data processed under this Directive.

Justification: Regulation (EC) No 223/2009 allows mobile operators' data to be used for statistical purposes. However, the ePrivacy Directive does not allow this, so there is now a conflict between the two pieces of legislation. This causes confusion in the application of the law. Based on the above, ePrivacy would refer back to Regulation 223/2009.

Position and questions on "Single entry point":

1. Will the single entry point, even temporarily, store data submitted via reporting and how can it be ensured that it won't store any data?

2. How does ENISA plan to guarantee that information reported via the system stay safe, with particular regard to the fact that the system is planned to handle all reported incidents, including incidents of critical entities, in all MS?

3. Was the proposal on the development of SEP preceded by or accompanied by a preliminary impact assessment that examined and evaluated, the potential (including national security or defence) risks of a platform where all incidents of all MSs are reported? Wouldn't the establishment of such a complex system, especially in the current geopolitical situation, increase the risk of cyber attacks and the danger that sensitive

information is obtained by criminals? Was it examined and evaluated by the Commission that these potential security risks are in line with the aim to be achieved?

4. In order to meet the security, national security concerns, instead of the authorization to develop the platform laid down in the legislation, wouldn't it be more forward-looking if the regulation determined a date for the examination of the precise technical background and feasibility of security requirements, with the involvement of experts from the Member States, ENISA and the Commission?

5. What guarantees do Member States and notifiers receive that information and data shared via the "single entry point" are shared only with competent authorities entitled?

6. In case the Single Reporting Platform (SRP) is planned to be used, or further developed as single entry point, we would like to ask further clarification how ENISA or the Commission plan to schedule the planning, the elaboration of the specifications and the development of the system? According to our information, the development of SRP is planned to end by next summer (2026). It is questionable whether the modifications are still feasible at this stage of the SRP system's development. When do you plan to make the decision on the usage of Single Reporting Platform, and based on what criteria?

7. How much would it cost to design and develop such a system, and where could the funding come from? Does the application of single entry point entail any costs for Member States?

8. According to the Commission, simplifying reporting by introducing SEP will reduce the administrative burden and lead to significant cost savings. Could the Commission please explain what calculations it has based this conclusion on? Based on our current understanding of the SEP, it would serve solely as a reporting interface, and further clarifications and consultations between the authority/CSIRT and the reporter wouldn't take place through it. Furthermore, for those not covered by the relevant EU legislation, a separate system would still need to be maintained for reporting. This means that the existing channels would have to be maintained and operated in the same way, but in the future in parallel with the SEP.
9. In its calculations relating to the development of the SEP, the Commission stated that, according to its estimates, the introduction of the SEP would result in annual savings of EUR 41.5 million. To arrive at this figure, it took the average number of incidents per year and multiplied it by the average cost of incident handling. Why does the Commission believe that the average costs associated with handling incidents would disappear or decrease? To our knowledge the reporting interface would only serve to report incidents in one place, the other tasks would remain unchanged.

10. Based on the workshop on SEP, the interface will only be able to receive and transmit reports. Accordingly, all relevant authorities and CSIRTs will be able to send comments or questions regarding the report through their own data reporting solution.
Does the Commission's assessment also cover this aspect, i.e. whether the central reporting interface can still achieve its objective of reducing the administrative burden?

11. Authorities/CSIRTs receive a lot of questions from institutions about the reporting interface and filling out incident reports. If the reporting interface is not operated by the competent authority/CSIRT, the question arises as to how ENISA will be able to provide customer service. Does the Commission's concept and cost estimate include customer service available in all EU member state languages?

12. Did the Commission examine whether reviewing the different requirements and deadlines to be met under the reporting obligations laid down in individual EU standards would be a more effective way of reducing the administrative burden on businesses?

13. Was the proposal on the development of SEP preceded by or accompanied by a preliminary impact assessment that examined and evaluated, with regard to institutions subject to DORA, the benefits and risks in terms of administrative burden reduction and harmonization, supervisory response time, financial stability, legal liability, and the accuracy of DORA-specific details?

14. According to DORA Regulation, authorities must forward incident reports to the European Supervisory Authorities. Would you please let us know whether it will be possible to submit these reports via SEP or whether authorities will need to use their own channels in the future as well.

15. The DORA Regulation allows an institution to outsource its incident reporting tasks. How will the central interface be able to ensure this, and how will authorities/CSIRTs be able to verify that only the representative of the authorized company can report incidents on behalf of the institution?

16. In the case of incident reports under the DORA Regulation, it is up to the Member State authority to decide whether, for example, an incident caused by a service provider must be reported individually by each institution concerned or whether they can receive a comprehensive report on the incident. If a single reporting interface is introduced, this detailed rule will need to be clarified so that, in the event of an incident affecting a group within the EU, the report is sent in the appropriate manner to the interface and, through it, to all competent authorities and CSIRTs. What is the Commission's position on the applicability of this detailed rule in the case of the platform included in the proposal?

NETHERLANDS

NL comments on Digital Omnibus

General

The Netherlands emphasizes the importance of stakeholder consultation for all significant legislative proposals. In the context of the Digital Omnibus, can the Commission ensure that the impacts on both businesses and citizens are better assessed through consultation, including SMEs and stakeholders from the digital sector? Does the Commission agree that for the ultimate success of the Digital Omnibus, it is important to not only organize public consultations, but also engage in discussions with entrepreneurs and enforcement organizations to understand the practical impacts and effects on regulatory burden, ensuring these are properly reflected in the decision-making process?

Platform-to-Business Directive

- Our national authority informs us that they regularly receive signals and complaints from business users about the P2B regulation (about 100 signals each year in 2024 and 2025). These signals are mainly about articles 4, 5, 7 and 11. Given that the Commission proposes to keep articles 4 and 11, but not articles 5 and 7, how does the Commission ensure that business users do not lose protection? For instance, for differentiated treatment, the DMA only covers gatekeepers. Furthermore, article 5 in the P2B is more specific on how certain criteria impact ranking compared to the DSA, also according to the DSA report. How do business users still keep the necessary level of protection with the repeal of articles 5 and 7?

- The DSA uses the country-of-origin principle for the delineation of competences between national authorities, whereas article 15 of the P2B gives member states flexibility to organize national enforcement. We are aware that certain case law relates to the question of the enforcement possibilities of the P2B regulation. However, these cases are not specifically about the delineation of competences between national authorities, but about the competence of member states to introduce national rules regarding information society services under the directive on electronic commerce. In the Netherlands we have used the flexibility of article 15 and have made ACM the competent authority for P2B, where the scope is determined by the place of establishment of the business user of the intermediation service and the location of the consumers to whom the goods and services are offered. An advantage of this is that the distance between the authority and the user that is protected is smaller and the workload of enforcement is shared among authorities. Moving the P2B provisions to other regulation means that ACM could no longer supervise in certain cases and that business users or consumers in the Netherlands would have to file the complaints elsewhere.
    - Has the Commission taken this into consideration?
    - How does this work when article 15 on enforcement remains?

Data acquis

- We welcome the initiative to streamline data regulation and many of the proposed changes. In particular, we support the added safeguards to protect trade secrets from disclosure to third-country entities.
- Nonetheless, we see the cloud provisions in the Data Act as a key element in improving competition in the cloud market and thereby enabling European cloud providers to compete on a level playing field. We believe the created exemptions for existing cloud service contracts, and particularly the proposed article 31, sub 1a, would create uncertainty regarding the cloud provisions and unnecessarily delay or reduce the effectiveness of the cloud switching provisions.
- Furthermore, we welcome that the rules for data altruistic organizations and chapter 5 of the Data Act have been simplified. Nonetheless, the Netherlands sees that these rules remain unclear and possibly redundant and disproportionate. The Netherlands would support removing these provisions entirely.
- Additionally, we see no reason to create the possibility for government agencies to impose different conditions and higher rates on very large companies (proposed article 32q sub 6 of the Data Act). Open data should be free of charges and conditions.
- We welcome that the rules for data intermediaries have been simplified. However, we do believe that keeping the certification of data intermediaries obligatory would benefit the development of a

market for trusted data intermediaries. There are few incentives for companies to voluntarily apply for certification.

- Lastly, the Netherlands would welcome more clarity on the organization of regulatory coordination of the competent authorities for the Data Act provisions on cloud. Although we do see the merits of organizing this regulatory coordination through BEREC instead of the EDIB, we question whether the upcoming Digital Networks Act is the right legislative file to pursue this through.

Cybersecurity (Single Reporting Platform)

- The Netherlands supports the Commission's initiative to work on simplification. The effects with regards to the proposal of an EU Single Entry Point are however not properly evaluated and identified, while this is essential to evaluate and ensure that the proposal effectively contributes to reducing administrative burden and other policy objectives. The Netherlands therefore explores and supports alternative solutions to simplify and harmonize cybersecurity legislation and reduce administrative burdens for businesses.
- To this day and after the first Q&A's and discussions within the Antici Group on Simplification, the serious concerns of the Netherlands with regards to an EU Single Entry Point remain. The proposal itself does not address the below concerns sufficiently nor do possible technical details/solutions on how an EU Single Entry Point *could* look like provide the necessary (legal) reassurances.
- First, the Netherlands underlines that notifications often include sensitive information. It is therefore important that entities have a strong and trusted relationship with the organization they have to notify to. Moreover, this sensitive information may contain information related to a Member State's essential and national security interests. Member States should therefore remain the direct recipient of incident reports, and all processes related to reporting obligations should remain the sole responsibility of the Member States. This includes the processing, redirecting or storage of all data related to the reporting or registration of incidents.
- Second, the Netherlands has concerns regarding the impact of this proposal on existing national structures. The NIS2, CER, DORA and GDPR are already or will be implemented on a national level. Member States have already developed and invested in national entry points and registration tools, taking into account their own national characteristics and the varying types of information that will be shared. According to the Netherlands, the proposal for a Single Reporting Platform does not sufficiently take existing national structures into account, as well as that these existing structures are a national competency of the Member States, under the Regulations and Directive, which are essential to fully implement EU legislation, such as the NIS2, CER etc. Moreover it does not clarify how a single entry point at EU-level would be adjusted to and integrated with national structures and its preferences, as well as who has access to the sensitive information that will be shared through these national structures. The Netherlands emphasizes that national entry points and registration tools should remain unchanged and intact.
- Third, small and medium sized are the most vulnerable to cyberattacks and would be most affected by the administrative burden of multiple notification requirements. Many of these companies, especially SMEs, mainly conduct their operations within a single or a few Member States. It remains unclear what the advantages for an entry point at EU-level would be for this large group of entities that have no cross-border operations.
- Lastly, the centralization of all incident notification obligations within one Single Entry Point, and more specifically the registration and/or processing of sensitive information of all Member States, could make the EU more vulnerable for malicious actors. This centralization also creates dependencies with regards to the continuity of services, since potential failure or downfall of this critical (notification) processes may have considerable consequences.

GDPR

- The NL is concerned that some of the proposed changes to the GDPR might undermine the protection of fundamental rights. Such potentially far-reaching changes demand a proper impact assessment, substantive discussion, and the EDPB-EDPS Joint Opinion that is expected in mid-February next year.
    - However necessary, this would undoubtedly risk delaying the negotiations about the digital omnibus as a whole. For the sake of speed, it is important that we treat the right themes in the right trajectory. We propose only treating the proposed changes that

simplify, clarify, and streamline legislation as a part of this omnibus. In that way, we keep the omnibus trajectory "clean", and mitigate the risk of delaying the negotiations.

Most amendments and changes that are proposed to the GDPR will not only have their effect on companies and businesses, but on society as a whole. Because of these potentially far-reaching changes we would like to request an appropriate impact assessment. If follows from point 13 of the Interinstitutional Agreement on better law-making that an impact assessment is needed to adequately assess the effects of the proposed changes on data protection and on reducing the regulatory burden, because of the estimated significant economic and social impacts. This was also emphasized in the European Council's conclusions of the 23rd of October.

Article 4(1) GDPR (Definition of personal data)

Questions following the presentation of the Commission of 12 December:

- Is it correct that according to the proposal the following principles will (continue to) apply to determine whether data are personal data?
    - The assessment of identifiability is context-dependent and must be made for each party separately, based on the means that party can reasonably use to enable identification. The relevant perspective for assessing identifiability is that of the controller, namely at the time of its data collection.
    - Pseudonymised data qualify as personal data for the controller if it has means that reasonable likely enable the controller to identify data subjects, even if the controller only via third parties can access to information enabling identification.
    - Reasonable means for identification of the data subject are present when they are allowed by law and practically possible, depending on objective factors, such as the costs of and the amount of time required for identification and the available technology, so that the risk of identification is present and not insignificant.
    - For a recipient, pseudonymised data qualify as personal data if it has means that reasonable likely enable the recipient to identify data subjects, especially if it is able to attribute those data to data subjects by recourse to other means of identification such as cross-checking, or is able to lift the technical and organisational measures implementing the pseudonymisation.
- Has the Commission considered a positive phrasing of Article 4(1), instead of negative formulas like "not necessarily personal data" or "not become personal (…) merely because"?
- Slide 111 states there is "*no intention to re-define what data are personal and what are not"*. Slide 112 reads: "*The proposed definition does not change the notion of personal data. It aims to address issues which are raised under the current wording.*" Could the Commission reflect on why the proposal is necessary while no redefinition is intended?
- Slide 112 states that the proposal "builds on recital 26 and case-law". How does the last sentence of Article 4(1) relate to the following sentence of the SRB judgment, §84: *"It is apparent, in particular, (…) that – where those data are put at their disposal – those data are personal data both for those persons and, indirectly, for the controller."*? And how does it relate to the following sentence in §85: "(…) *Accordingly, 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, (…) , the data subject must be regarded as identifiable as regards both that transfer and any subsequent processing of those data by those third parties.*"
- Slide 112: Could the following clarifications (from slide 112) about the definition of personal data be included in Article 4(1) or in the Recitals: "*The GDPR applies to all entities who have "the means" reasonable likely to be used to identify the individual, even if they receive the data from an entity for which the data is not personal. The test of not having the "means" is very high: the risk of identification must be non-existent or insignificant*"?
- Slide 113: Could the clarifications regarding Chapter V and Art 28 GDPR be included in the corresponding Recital?
- Slide 114: Could the following clarification be included in the corresponding Recital(s): "*The proposed definition does not impact the fact that the "information enabling identification" must not be in the hands of the same entity. As long as a recipient has lawfully and realistically (SRB §82, Breyer §46) access to such additional information, the data is personal for this entity."*?

Articles 4(38) and 5(1)(b) (Scientific research)

Questions:

- To what extent does the proposed definition of scientific research differ from the definitions used by the EDPS and EDPB? The definition in the opinion of the EDPS on data protection and scientific research of 6 Januari 2020, §3.5, requires that "*relevant sectoral standards of methodology and ethics apply, including the notion of informed consent, accountability and oversight" and that "the research is carried out with the aim of growing society's collective knowledge and wellbeing, as opposed to serving primarily one or several private interests"*. The definition in the EDPB Guidelines 05/2020, §7.2, reads: "*a research project set up in accordance with relevant sector-related methodological and ethical standards, in conformity with good practice".*
- Has the Commission considered to include in the definition the adherence to "the relevant sectoral standards of methodology", like in the definitions of the EDPS and EDBP? The EDPS notes that "*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 conduct of research must allow testing of hypotheses, with both the conclusion and the reasoning transparent and open to criticism. Openness and transparency help distinguish between science and pseudo-science*".
- Could the following clarification from slide 117 of the Commission presentation of 12 December be included in Recital 32: "*Public sector can rely on Art 6(1)(e) for scientific research*" ?

Art. 9(2)(k) and 9(5) GDPR (Processing of special categories of data for AI-systems)

Questions following the presentation of the Commission of 12 December:

- Slide 121: Could the clarification: "The derogation respects the proportionality principle", be included by adding the proportionality test to the wording of Article 9(2)(k) or of Recital 33?
- Slide 127: The Commission states "it does not lower the level of protection". Since there is no impact assessment conducted, where is this statement based upon?

Article 41a GDPR (Implementing acts on the definition of 'personal data' and pseudonymisation)

Questions:

- Article 41a does not seem suitable for an implementing act. It explains core concepts of the GDPR. However, delegated and implementing acts may not concern 'essential elements', as these should be regulated through the procedure for a regulation/directive (including the Council and the European Parliament). The Court of Justice of the European Union has ruled, among other things, that an element is essential if it requires a political assessment. A provision is also essential if it allows for a significant interference with fundamental rights. This follows from the judgment of the EU Court of Justice of 5 September 2012 in case C-355/10. Could the Council Legal Service and the Legal Service of the Commission reflect on this?
- According to Article 41a(4), the Commission shall "closely involve the EDPB in the preparations of the implementing acts", and the EDPB will be asked for an opinion. The provision does not specify what happens if the EDPB has serious objections (during the drafting process and in its subsequent opinion). Can the implementing act still be adopted in the event of a negative opinion from the EDPB? And what is its legal status in that case?

Questions about Article 41a following the presentation of the Commission of 12 December:

- The Commission states in her presentation (sheet 111) that the implementing acts will contain an "*Assessment of techniques against the requirements of the GDPR and its interpretation by the courts and the data protection authorities*". On the same sheet, the Commission states: "*Fully respects powers of DPAs and the courts*". If the interpretation by the Courts and the data protection authorities is leading and if the intention is to fully respect the existing powers, what is the reason to not leave this to the DPAs (EDPB) and the Court?
- The Commission states on the same sheet that there is "*no intention to re-define what data are personal and what are not*." However, according to the proposed Article 41a(1), the Commission will have the power to make rules to "*(…) determine whether data resulting from pseudonymisation no longer constitutes personal data for certain entities*". If the Commission does not want to re-define what personal data are, has the Commission considered to limit the proposed implementing acts to techniques that controllers should use for pseudonymisation *as a protective measure* and to disconnect this from the definition of personal data?
- The Commission also states on the same sheet that the aim is to reduce legal uncertainty. Could adoption of guidelines by the EDPB not also provide sufficient legal certainty?

Article 88a GDPR (Access to terminal equipment)

Questions following the presentation of the Commission of 12 December:

- Slide 100: Could the Commission clarify how all GDPR principes are applicable if there is no additional legal basis under Article 6 and no balancing or necessity test needed for the whitelisted grounds for processing without consent? How does this comply with Article 5 GDPR?
- Slide 102: The Commission states it "would in principle not see greater risks for the rights on individuals". Since there is no impact assessment conducted, where is this statement based upon?
- Slide 102: The Commissions states: "General principles apply and protect against abuse", but how does this relate to the fact that no necessity or proportionality test is needed to conduct these processing activities? (cf. slide 100)
- Slide 103: Could the Commission include the right to withdraw explicitly in the wording of Article 88a(4) and could the fact that Article 7 fully applies be included explicitly in the wording of the corresponding Recitals?
- Slide 104: How does the sentence: "It is important to note that the GDPR's principles and all other requirements continue to apply fully, this includes the compatibility test of Article 6(4) GDPR" relate to the sentence: "Subsequent processing addresses the processing after the storage or gaining access as mentioned in the first sentence of Article 88a(1) ≠ "further compatible processing" in the sense of Article 6(4)."? These sentences seem to be contradict each other?

Article 88b GDPR (Automated and machine-readable choice)

Question following the presentation of the Commission of 12 December:

- Slide 107: Could the fact that Article 88a(4) applies "where no central choice has been made" be included explicitly in the wording of Article 88a(4) (or the corresponding Recital)? Could the fact that both the 6 month obligation and the single click obligation also "apply where preferences were set centrally" be included explicitly in the wording of Article 88(4) (or the corresponding Recital)?

Article 88c GDPR (Processing in the context of the development and operation of AI)

Questions following the presentation of the Commission of 12 December:

- Slide 120: The Commission compares the "unconditional right to object" in Article 88c to Article 21 (2). Does the reference to only Article 21(2) mean that the Commission is of the opinion Article 21(3) does not fall within the scope of the "unconditional right to object" in Article 88c? And if so, for what reasons?Could the clarification regarding "unconditional right to object" be included as such in the wording of Article 88c, including an explicit reference to Article 21(2) and Article 21(3)? Or otherwise, could "or in the context of the development and operation of AI" be added to Article 21(2) and Article 21(3)?
- How can be avoided that this unconditional right to object only will exist on paper? Because Article 88c does not require the consent, individuals whose personal data ends up in an AI dataset through scraping will generally be unaware of this scraping. Organisations will be obliged to "enhanced transparency", but it seems not likely that someone will proactively consult this information, if the data subject remains unaware of the data processing.
- Slide 120: Could the clarifications regarding the meaning of "enhanced transparency": *"Enhanced transparency is the transparency going beyond what is required under Art 13 and 14 GDPR, such as for example, additional information about the data collection criteria, alternative forms of informing data subjects, e.g. media campaigns, FAQs, model cards (see EDPB Opinion 28/2024, para. 98 et. seq)."* be included in the corresponding Recital?

AUSTRIA

Austrian questions and comments regarding the Omnibus VII
18 December 2025

Please note that the following comments are of preliminary nature. AT is still analysing the Digital Omnibus and the Digital Omnibus on AI and therefore raises a scrutiny reservation.

ad Digital Omnibus – COM(2025) 837 final

Art 1 (Data Act)

Art 1 (2): Definitions

- The definition of "**document**" is limited to **non-digital content**. At national level, the concept of a "digital document" exists, with digital documents being e.g. official public sector publications. Thus, at national level, the definition of document is understood in a digital context as well.
  - Could Cion provide the rationale for this change in definitions?
  - In addition, it is unclear why *"sound, visual or audiovisual recordings"* are included in the definition of "document", as these mostly constitute digital (audio) recordings and would therefore also need to be defined separately. Particular care must be taken to ensure coherence with the **historically evolved provisions** of the Member States on "documents". Do the MS have to amend their existing national legislation so that references to "documents" are extended to "data and documents"?
- General point: "**synthetic data**" is not defined, even though it is one of the focal points of the forthcoming Data Union Strategy. Could Cion please provide a definition or the reasons for omitting that?
- The definition of **university** as a „public sector body" might lead to the problem that in Austria technical colleges, ie. universities of applied sciences („Fachhochschulen") will not be addressed by the definition. Could Cion please provide a reasoning for this definition?

Art 1 (7): B2G Data Exchange

- The **newly proposed Art 15a(2)** states that "*where the provision of non-personal data is insufficient to address the public emergency, personal data may also be requested […]*". Considering that such data are required in situations of public emergency, which by their nature do not allow for lengthy discussions, it is essential to **clearly define the term "insufficient**". In this regard, could Cion please indicate whether further clarification on this concept will be provided, or whether a commonly accepted interpretation of this wording already exists?

Art 1 (11): B2G Data Exchange

- Why does Cion deem that clarifications regarding trade secrets in relation to the public sector are necessary (see amendments to Art 19)? To our knowledge, there have been no negative precedents.
- Why are **Art 14 and 15 Data Act** (DA) omitted? By this, the definition of "exceptional need" is lacking. However, the term is still used in the newly proposed Art 15a(1).
- Furthermore, with the deletion of Article 17(5), there no longer appears to be a **right to lodge a complaint** against an obligatory request by a public sector body, Cion, the ECB or another Union body to make data available. In this context, could Cion please explain the rationale for the proposed amendments and deletions in Articles 14, 15 and 17?

Art 1 (16): Unlawful disclosure of non-personal data in a cross-border context

- Currently no cooperation mechanism between competent authorities of the MS exists. Does Cion envisage a cooperation mechanism and a technical instrument for cooperation?

Art 1 (18): Chapter VIIa – Data Intermediation and Data Altruism

- Regarding the newly proposed **Articles 32a et seq.**: Could Cion please explain as to why a **switch to a voluntary regime** is now envisaged, especially given that Member States made substantial investments in notification frameworks and new administrative structures? We see the registration of data intermediaries and data altruism organisations as a **hallmark of quality** that strengthens the position of actors in the data economy and trustworthiness in those actors. We should prevent a race to the bottom as regards compliance standards. Does Cion envisage issuing guidelines or other supporting documents for the actors concerned?

- Could Cion please explain why **reporting and transparency requirements** for data altruism organisations (DAO) are further waived, and how it intends to ensure that only trustworthy actors operate in the data economy?

- Regarding the newly proposed **Art 32a and 32e**: The technical specifications for transmitting Member States' registry entries to Cion are missing. Work is still being conducted on the basis of Word documents. Does Cion envisage a more future-proof **technical system**, if Cion is to assume central responsibility?

- Concerning the newly proposed **Art 32c** and the provision *d. (iii) "the value-added services are offered through a functionally separate entity"*: Are data intermediaries only allowed to offer additional services through a **functionally separate entity**? Are data intermediaries permitted to offer additional services only through a functionally separate entity? Are there any exemptions from this provision for SMEs and SMCs?

  - From an innovation enabling and data facilitation perspective, data intermediaries should be allowed to assist data users in particular in the maintenance and curation of data. Furthermore, as essential actors in the data economy, data intermediaries merit a more prominent anchoring in the Data Act, in particular as regards their function in data transfers, curation and the potential improvement of data quality.

Art 1 (18): Chapter VIIb (Free flow of data)

- Art 32h of the proposal prohibits "data localisation requirements". Would a general policy or a specific provision in certain **procurement procedures** requiring the processing of data and/or the localisation of servers within the EU fall under this prohibition and would therefore only be permissible, if contracting authorities can justify this requirement on grounds of public security?

Art 1 (18): Chapter VIIc (Open Data, Re-Use of Public Sector Data)

- Concerning the inclusion of the provisions of the Open Data Directive (ODD): Do the Member States remain free **to go beyond the minimum requirements** laid down in Union law, for example with regard to national provisions concerning the appointment of open data officers (previous Recital 19 ODD) or concerning the ad hoc establishment of arbitration bodies?

- Could Cion outline the new elements in the proposal concerning the reuse of data and documents held by public sector bodies and public undertakings (in particular **Articles 32i et seq.**), and explain how these differ, if at all, from the current framework under Directive (EU) 2019/1024?

- Regarding the proposed **Art 32v (5)** on specific high-value datasets (HVD): Could Cion please provide a legal clarification in writing on the definition of a "**substantial part of their costs** relating to the performance of their public tasks"? This reference has not yet been clarified.

- Concerning **Articles 32n, 32p, 32q, 32y**: Could Cion please explain why there are different articles on charging instead of consolidating them into one article against the backdrop of a general simplification?

Art 1 (21 et seq.): Chapter IXa (European Data Innovation Board, EDIB)

- Regarding **Articles 41a et seq.**: Will EDIB have an essential role in this process of reviewing the body of data legislation? How does Cion intend to strengthen the role of the EDIB and enhance its decision-making capacity?
  - AT supports the development of the EDIB into a genuine strategic innovation body to ensure the implementation of the Omnibus across Member States and to promote a forward-looking strategic exchange and the further development of the European data economy. Within the context of the

Digital Fitness Check, our stance would be that EDIB should serve as a key body for discussions among Member States, together with selected scientific experts and essential stakeholders.

- Regarding **Article 41a et seq. in conjunction with Chapter VI (Cloud-Switching)**: Concerning the omission of the responsibility of EDIB for Chapters VI and VIII of the Data Act, could Cion please provide an explanation for this exclusion and confirm intentions to assign this to bodies to be created under the upcoming Digital Networks Act (DNA)?
  - If no alternative channel is available to convey the positions of the MS, it would be problematic if EDIB was not appropriately involved in the decision-making process concerning the drafting of harmonised standards, the preparation of implementing and delegated acts, and the adoption of guidelines for interoperable frameworks and common standards and practices for the functioning of European data spaces (currently Art 42(c) of the Data Act).

ad Data Spaces in general

- Why has Cion chosen to not include essential horizontal provisions concerning data spaces and in particular possible links to data intermediaries?

  - At present, the legal text lacks explicit horizontal provisions on the availability of data within the framework of data spaces, particularly since the Union is investing significant financial and political resources in the design and further development of common European data spaces. Furthermore, there are no explicit references to the European Health Data Space (EHDS) Regulation (EU) 2025/327.

<u>Art 6-9 (Cyber security)</u>

- Will it be mandatory to report incidents without cross-border implications via the single-entry point (SEP), or is a submission to the relevant national reporting platform sufficient in such cases?
- Will the voluntary notifications also be made via the SEP or exclusively via the national platform or can the entities choose in such cases?
- What specific set of data is considered “common data”, beyond the name of the reporting institution?
- Even with a harmonized reporting form, the specific information to be provided may vary depending on the reporting regime or Member State (e.g., time of the incident, thresholds). How will this challenge be accommodated?
- Which authority is responsible at national level for the organizational setup, technical operation and financing of a common reporting platform and/or the national connection to the SEP?
- Which parts of the SEP will be funded by ENISA/EU budget and which parts have to be financed by the Member States themselves?
- Will the Member States be involved in the development process or in the collection of SEP requirements by ENISA?

PORTUGAL

PT questions on Omnibus VII
18.12.2025

I. DIGITAL OMNIBUS

Article 4(1) amendment – pseudonymised data

1. Regarding the amendment to Article 4(1): even if pseudonymised information is no longer considered personal data for a specific controller under the proposed wording, was the need considered for that controller, when transmitting such data to a third party, to assess whether, for that third party, the data could constitute personal data? And were any limitations on such transmissions considered?

Article 12(5) amendment – justification of purpose

2. On the amendment to Article 12(5): under the new wording, do you consider that data subjects must always justify the purpose for which they request access under Article 15? Could you clarify what you mean by a "purpose other than the protection of their data"? And how does this concept align with the principle that personal data belong to the data subject, if their access is limited to certain circumstances?

Article 22(1) and (2) amendment – removal of explicit data-subject reference

3. Concerning the amendment to Article 22(1) and (2): why was it considered necessary to remove the explicit reference to the data subject's rights? In other words, why not simply amend point (a) as now proposed, instead of substantially modifying the wording of the whole article?

Articles 33(6) and 34(1) – high-risk criteria list

4. On the list of circumstances in which personal data breaches are likely to result in a high risk to individuals, which the Committee must prepare and send to the Commission under Article 33(6): will this same list also apply to the assessment of high risk under Article 34(1)? Given the proposed deletion of Article 70(1)(h), aren't we facing a potential gap here?

New Article 41a – placement within Chapter IV

5. Regarding the new Article 41a: what is the rationale for inserting this article, without a heading, into Section 5 of Chapter IV, between the provisions on codes of conduct and certification?

SLOVENIA

Definition of personal data:

The proposed amendment to the definition permits controllers who, due to the manner of processing, no longer regard certain data as personal data to transfer such data to a recipient in a third country, regardless wheter this recipient has means reasonably likely to be used to identify the individual. How will data subjects retain control over their personal data (access, withdrawal of consent, etc.) in cases where the recipient in a third country, has the means reasonably likely to be used to indentify those data subjects?

Access to personal data:

Why is the amendment concerning the right of access not targeted and does not explicitly address the objective of preventing abusive practices, but instead leaves a broad margin for interpreting »purposes other than the protection of the data subject's personal data«? What will the controller take into account when assessing the purpose of the request, and on the basis of which information will this assessment be carried out? Will the data subject requesting access be required to specify their purpose in the request, even if doing so would necessitate the disclosure of additional personal data?

FINLAND

Updated FI written comments and questions on Digital Omnibus (updated on 18.12.2025)

Contents

Finland's questions on the Digital Omnibus proposal

Finland would like to thank the Commission for its detailed answers and the Presidency for the swift management of the process. Finland supports measures to reduce the burden on companies and simplify regulation. Some things still need clarification and below are more specific comments and questions on which we would welcome further clarification.

1. Data Act

Our national data coordinator has expressed concern that competent authorities currently lack a reliable common IT system for cooperation between authorities in handling complaints under the Data Act (or the Data Governance Act), or otherwise for exchanging information between authorities, the Commission, and the Board, similar to the cooperation mechanisms under the DSA. Is the Commission aware of the practical challenges related to information exchange, and does the Commission have plans to address this situation?

1.1 Competent authorities

- Article 32z states that Member States must designate competent bodies under Article 37(1) to support public sector bodies. To what extent do these bodies fall under the rest of Article 37, such as the obligations in section 5?
- What investigative and sanctioning powers must Member States grant competent authorities under Article 37(5), particularly in relation to Chapter VIIc? Should these powers include verifying whether: (i) research organisations are making publicly funded research data accessible under Article 32t, and (ii) public sector bodies are making data accessible as required by Chapter VIIc, Section 2?
- The proposal would apply Article 37 on competent authorities to Chapter VIIc, even though the rules being moved into Chapter VIIc did not previously require such authorities. What is the justification for introducing this new supervisory requirement?
  (Background: Article 26 DGA requires supervision only for data intermediation services and data altruism organisations; the ODD requires no supervisory authority at all.)

1.2 Exclusivity of cultural resources and heritage

What is the rationale for extending the exclusivity rules for cultural resources and cultural heritage to the reuse of protected public sector data? How should the relationship between Articles 32i(3) and 32i(2)(c) be understood? If an exclusivity arrangement is necessary for digitising cultural resources, does that mean Article 32i(3) no longer applies? Does the reference to exclusivity in the context of digitising cultural heritage imply that a protection period may be introduced or extended even when the material is no longer protected by copyright?

1.3 Making data available

Article 32 would be amended to include obligations for making data available under Chapter VIIc, Section 3 (currently DGA Chapter II), and would impose duties on public sector bodies. How do these obligations, which concern only non-personal data, relate to Article 5 DGA (Article 32w DA), which covers both personal and non-personal data? Can an implementing act under Article 5(12) DGA (Article 32x DA) limit or reduce the obligations set out in Article 32 DA? What kinds of technical, legal or organisational measures are considered adequate when sharing protected non-personal data?

2. GDPR

Finland thanks the COM for the responses and clarifications, but welcomes further information on the following:

- **Definition for personal data:** The COM noted that the proposal "builds on recital 26 GDPR and the standing case-law of the CJEU (Breyer, OC v European Commission, SRB). Could the COM explain why it considers appropriate to include the final sentence, as it seems not to be in line with the CJEU Judgement (C 413/23 P, see paras 84 and 85) and may also contradict with other case law from the CJEU as well. The proposal seems to go further than the CJEU case law and as such would lower the current level of data protection.
- **Administrative fines for AI and cookies: We would welcome a more comprehensive answer on administrative fines** and 1) how the current provisions of Article 83 would apply to the new Articles 88a, 88b, 88c and/or 2) how should Article 83 be supplemented (should the level of administrative fines be 10 000 000 / 2% or 20 000 000 / 4 %). Effective sanctions play an important role in assessing the proportionality and effectiveness of the proposal and whether the current level of data protection remains.
- **Concerning AI development and operation, how has the COM evaluated public sector, as legitimate interest or consent are not, in principle, considered possible legal basis for authorities** whilst processing personal data for the performance of a task carried out in the public interest or in the exercise of a official authority. The proposed Article 88c only mentions legitimate interest and consent. Can the Member States regulate on public sector AI development and operation in compliance with Article 6(3) GDPR or are public sector controllers able to rely on legitimate interest as well?
- Regarding the definition "scientific research", could the COM further clarify why the proposal includes commercial interest. There was no answer for this. Why isn't there any references to the competence of the researcher? Why has the COM chosen to leave important matters in the recitals?
- Article 9(2)(l): The COM has clarified what 'held solely by the data subject' and stated that '**any other use or further processing is not possible without the active involvement of the data subject'.** Why isn't there specific safeguard and paragraph concerning this? **Shouldn't there also be safeguards** (e.g. requirement to delete such data?) **if in any event the controller gains knowledge for the limited time of the verification process?**
- Exercise of the data subjects' rights: The COM has clarified what 'data protection purposes' mean and has stated that for 'right of access requests, excessive requests include the abuse of this right for purposes other than the protection of a data subject's personal data. The limitation must be read in light of the intention of abusing this right'. **Why isn't this appropriately clarified in the recitals and/or formulated in more detail in the Article proposal?**
- **Concerning Article 33**, we would welcome the COM the share the analysis on **how is it possible to extend the time limit whilst at the same time safeguarding the current level of protection, if the threshold is raised to high risk?**
- **Concerning Article 35, we would still welcome the COM to answer why the COM would not be obliged to ask at least an opinion from the EDPB before changing the list**? This Article seems to give the COM a lot of power. Does the COM think that Article 93 committee can replace the opinion of the EDPB and independent data protection authorities?

3. ePrivacy Directive

We have some concerns whether the differences in art 5(3) of ePrivacy directive and the proposed art. 88a grounds for access for data stored in terminal equipment will provide clarity to the rules. Was a further alignment of the remaining ePrivacy-directive art. 5(3) with the newly introduced grounds considered? Why does the proposed white-listing allow for more grounds of processing of personal data than non-personal data?

How should one-click principle be interpreted in cases where media service providers rely on their exemption in art. 88b, in particular where pay or consent -models are used? Commission has indicated that the proposal does not change the approach to pay or consent -models. Does the requirement of one-click lead to limiting the use of pay or consent -models in practice?

4. Single Entry Point (SEP)

Disclamer: following comments are preliminary as FI does not have official position yet for the SEP or Digital Omnibus proposal. We are still scrutinizing the proposal.
Preliminary FI comments on the SEP:

- FI supports aims to reduce administrative burden of entities subject to reporting obligations.

- FI supports Member States' obligation to receive and accept reports via SEP.

- Preliminary we see that introducing obligation for reporting entities to submit all reports to SEP is a change to substance of reporting obligations in respected legal acts.

- Decision on how to report (SEP or national platform) should be solely up to the reporting entity. This allows an entity to report with least burdensome way in a single event.

- Decision on whether to rely solely on SEP or also maintain a national platform should be up to the Member State.

- In order not to affect trust building efforts between authorities and reporting entities the SEP would need to be very explicit and transparent about which authorities and Member States will receive the submitted information at the time of submission of the information.

- At the moment a high level of trust exists in Finland between private sector and cybersecurity authorities. Therefore, private sector and authorities receive and exchange cybersecurity-related information on voluntary basis. We are concerned that forcing entities to report only through EU-level SEP would harm existing practices and exchange of voluntary information. This would therefore de facto harm our situational awareness of the level of cybersecurity in Finland even though it has opposite purpose for EU-level.

- ENISA's capability to create SEP as well as concerns related to risks and security of SEP should be addressed before obligating ENISA to create it. This is highly important especially if respected acts would allow no other way than SEP to report incidents.

Preliminary FI comments on data and information related to national security:

- It is difficult to unambiguously determine whether data and information is linked to national security.

o Each authority assesses the grounds for confidentiality and, consequently, the impact on national security from the perspective of its own field of responsibility.

- Some entities themselves might recognise the direct link to national security. For example, their services are related to national security.
- Competent authorities are able to recognize the link to national security, for example, through national CSIRT's technical investigation.
- It is also common for the nature and extent of an incident to be determined much later than the incident is reported. The link to national security may become evident when there is more information on the incident.

- Many of the incident reports may contain data or information that is linked to questions that are related to national security. This will be the case especially for NIS 2 and CER reports.
- Even though information might or might not be linked to national security at the time of reporting it, it might become relevant later or when combined with other information or incident reports.

- Information of reportable incidents under NIS 2 or CER directives might be under certain circumstances as such information that is contrary to the essential interests of Member States' national security, public security or defense.

As regards to our previous questions, Finland thanks the COM for the responses and clarifications, but welcomes further information on the following:

- Could the commission explain more in detail how the SEP proposal meets the principles of subsidiarity and proportionality, in particular the obligation for the providers to notify incidents only via the SEP?
- There will be major security risks related to upkeep and data flows in the SEP. How the risks will be addressed and managed?
- What will be the language of the portal and required language of the report?
- Finland would like to emphasize that the transition to a Single Entry Point should not weaken national authorities' rights or their practical ability to obtain and process data that is essential for carrying out their tasks. How has this been taken into account?
- How will reporter of information to SEP know, which authorities and Member States will receive reported information? Will the reporter of information be able to report – on voluntary basis – additional information to only authorities it chooses to? This is vital to remain trust between the reporter and recipient of information.
- FI is open to bilateral technical meeting with the COM in regard to SEP.

5. P2B Regulation

We thank the Commission for its presentation and answers to the Member States questions on the repeal of the P2B Regulation in the AGS working party meeting on 12 December. On the basis of the Commission presentation and our preliminary analysis, we consider that after the repeal of the P2B Regulation, **the key changes in the Union law from the perspective of business users would be:**

- **the service provider is not obliged to notify in advance of any changes or restriction, suspension and termination of the service (Articles 3 and 4 of the P2B Regulation)**
- **the right of business users to access data would be regulated only in relation to platform companies with gatekeepers status – not in relationships between smaller online platforms and business users. [P2B Article 9 / DMA Article 6(10)]**

Could the Commission provide an evaluation of the competitiveness and cost impacts on business users of online platforms if these provisions will be repealed?

SWEDEN

Pleas find attached a comment/question from on the incident reporting.

The proposal for a Single Entry Point (SEP) for incident reporting
Sweden, while maintaining a scrutiny reservation, has a generally positive view of the proposal to simplify incident reporting. However, we note that certain sectors, such as the financial sector, already have well-functioning national reporting systems under DORA, with minimal risk of duplicate reporting. For these actors, questions arise regarding the added value of using an EU-level entry point to transmit information to their national authority. It is unclear whether this approach truly simplifies reporting when the process would involve routing through the EU before reaching the competent national authority.

Therefore, it should be considered whether reporting via the SEP could be voluntary rather than mandatory. If incident reporting is to be carried out through the SEP, it is essential to ensure that the correct information reaches the appropriate recipients without delays or unnecessary complexity.