Council of the European Union
General Secretariat

Interinstitutional files:
2025/0359 (COD)
2025/0360 (COD)

Brussels, 08 December 2025

WK 17004/2025 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 and Digital Omnibus on AI) - compiled comments (ddl 05/12)

Following the meeting of the AGS on 1 December on the Omnibus VII (Digital Omnibus and Digital Omnibus on AI), delegations will find a compilation of comments as received from: BE, CZ, DE, EE, IE, ES, IT, LU, NL, AT, PT, SI, FI and SE.

Omnibus VII - Digital Omnibus and Digital Omnibus on AI
MS comments (ddl 05/12/25)

AGS meeting on 01/12/25

Table of Contents

BELGIUM

Omnibus VII - BE technical questions – round 2

AI

1. **Single application procedure (art. 28-29)**

- Article 29.4 refers, for the single application procedure existing sectoral notifying authorities.
  - ¬ We therefore would like to reiterate our question if the Member States can still designate a notifying authority other than the existing sectorial notifying authority for the single application procedure?

- Article 43(1) specifies that in such cases, the notified body is actually the market surveillance authority referred to in article 74(8) or (9). In other words, this confirms that in this particular situation, the market surveillance authority acting as a notified body must be listed on NANDO.
  - ¬ Must this authority undergo a full assessment by the corresponding notifying authority, just like a standard notified body? **This may pose potential problems in cases where the same authority plays the dual role.**
  - ¬ Must each Member State ensure that the market surveillance authority it has designated is also listed as a notified body (should providers automatically address their national market surveillance authority acting as a notified body, or may they approach an authority in another Member State)?
  - ¬ How will the EDPS itself be monitored as a Notified body given that no European notifying authority is envisaged?
  - ¬ If this procedure encompasses all different elements of the assessment, does this requirement for a single assessment procedure imply a single accreditation audit, and consequently the use of similar preferred accreditation standards between the sectoral legislation and the AI Act when accreditation is used by the notifying authority for the assessment of candidate notified bodies?

- Can you clarify the applicability of the condition for a hybrid assessment procedure, as no sectoral legislation listed in Annex I(A) refers to the possibility of a joint assessment procedure in connection with another legislation? Would this condition rather imply that a specific procedure needs to be established at the sectoral level to enable a single application and assessment?

2. **EU legal basis to enable exchange of information between prudential authorities and market surveillance authorities**

- Could you please clarify why no specific legal basis is foreseen under the Digital Omnibus Regulation proposal for information exchange between Prudential Authorities and Market Surveillance Authorities – especially considering that (a) it does provide for a specific legal basis for information exchange between other authorities (e.g. Market Surveillance authorities and authorities protecting fundamental rights) and (b) the AI Act provides a specific legal basis as regards information to be exchanged by certain MSAs belonging to the Single Supervisory Mechanism towards the European Central Bank only?

3. **NANDO Codes (Annex XIV)**

The introduction of the NANDO codes is contingent upon the adoption of the Omnibus act. Furthermore, these codes appear to have become a de facto prerequisite for the notification of conformity assessment bodies. As a result, notifications in NANDO are currently on hold for an indeterminate period.

- What would be the interim arrangements should the negotiations on the Omnibus act delay its adoption beyond the initial application date of the requirements for HRAIS (August 2026)? In particular, would it be possible to proceed with notifications in the absence of the codes —potentially on a provisional basis— and subsequently align them once the codes are formally introduced?
  We have pending notification requests and would like to inform the relevant bodies of the upcoming steps to be expected.

4. Processing of special categories of data (Art. 4a)

- When will the Guidelines with EDPB be made available?

5. Registration obligation in the EU database for non-high risk AI systems: modification of Article 6, par. 4

- In the absence of this registration obligation, how can the competent authorities monitor the decisions of such providers and, therefore, how do we prevent companies from circumventing the AI Act without being traceable?

Data

6. Definition of personal data – Article 3(1)

The current proposal of the Commission emphasizes that the application of the GDPR depends on whether the data constitute personal data from the perspective of the controller.

- Would this not create a disruption in the protection of the data?
- How can enforcement of the GDPR be ensured if, during the life cycle of the data, its qualification as personal data will vary depending on the controller processing the data? How could the supervisory authorities assess an 'evolving' qualification of the data?
- In addition to the relevant technical questions raised by the NL in this regard, would a controller still need to respect chapter V of the GDPR (international transfer) if the data is not personal so far as the controller is concerned (while the data could be personal data for the recipient considering the possibility to cross-checking with another set of data).

7. Definition of scientific research – Article 3 (1)

- Could you provide examples of the types of processing activities (or actions?) falling within the scope of this new definition?
- The term 'actions' is used. Could you elaborate what you mean by using the term 'actions'?
- Does the new definition of scientific research encompass AI systems or models?

8. Compatibility of further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes – Article 3(2)

The proposal clarifies that further processing for archiving, scientific, historical or statistical purposes does constitute a compatible further processing. The proposal specifies consequently that Article 6(4) of the GDPR is not applicable.

- If Article 6(4) is not applicable, are the supervisory Authorities still empowered to verify if a 'pseudo-scientific' research is compatible with the initial processing?
- If the new definition of scientific research encompass AI or may encompass AI in certain circumstances, does this mean that AI might be considered as compatible further processing?

- According to the Commission, all other safeguards set out by the GDPR remain applicable. What are those safeguards, if Article 6(4) is no longer applicable and Article 89 only refers to safeguards that may be foreseen in European or National law? (Article 89 only gives the example of pseudonymisation but pseudonymisation may, by virtue of the new proposal, mean that the GDPR is no longer applicable). Could you give examples of safeguards other than pseudonymisation?

9. Processing of special categories of data in the context of AI – Article 3(3)

According to Article 9(1) GDPR, processing of sensitive data is prohibited. Most of the derogations foreseen in Article 9(2) GDPR are based on a legitimate purpose or on consent. AI however is a technical tool, not a purpose in itself.

- Does the new point k) of Article 9(2) means that processing of sensitive data in the context of an AI system or model is allowed no matter for which purpose?
- What is meant by using the word 'remove' in new Article 9(5), could you elaborate? Does this mean that the data should be deleted?
- The way the provision is build gives the false impression of a broad exemption while Article 9(5) restrict it to situation where it is impossible to avoid it, and every efforts should be made to avoid it. What is the objective of the Commission? Can this provision be drafted more clearly?
- How can enforcement of this provision be ensured? How could the supervisory authorities assess the conformity of this provision with the large volume of data on which AI systems rely?

10. Processing on the basis of legitimate interest in the context of AI – Article 3(15) (New Article 88c)

- Does this new provision imply that a controller would be allowed to collect personal data for the sole purpose of development and operation of an AI, based on his legitimate interest, without specifying any other purpose? How do you see the compliance with the purpose principle and the data minimisation principle?
- Recital 47 of the GDPR states that '*At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place'*. Can you you confirm that the reasonable expectations of the data subject at the time and in the context of the collection of the personal data will still be required in view to assess the validity of the legitimate interest in the context of Article 88c?
- What is the right to object qualified as 'unconditional', is it a different from the right to object set out by Article 21 GDPR?

11. International data transfers

- Provisions related to international data transfers as provided in the GDPR, Data Act and Data Governance are formulated in different ways. From the Commission point of view, is there any inconsistency and/or overlap between these provisions?

12. Free-flow of non-personal data

- How would the deletion of the national contact point be organized concretely?

13. <u>Single Entry Point</u>

- The proposal states that "the underlying legal requirements for incident reporting are left unchanged". Do we correctly understand that this proposal <u>does not alter the consolidation level at which institutions are required to report (but also assess) the incident?</u> The DORA regulation for instance requests incident notifications (and assessments) at the level of individual financial entities, not at a consolidated level.

- Do we correctly understand that it will be possible for competent authorities (possibly multiple per member state) to be "integrated" to the single-entry point, so that incident notifications will be automatically shared with such competent authorities? Is it possible to integrate this principle more explicitly in the proposal?
- Would Member States still be allowed to oblige specific incident notification elements that go beyond NIS2?
- Should a request for help to a particular CSIRT be done through the SEP?
- Does the Commission have detailed numbers/information on the proportion of incident notifications directly reported to multiple authorities, e.g. notifications reported by financial entities to their competent authorities under DORA that are also directly reported to other authorities? In our experience, in most member states the reporting is already streamlined to a very high extent in the sense that DORA notifications are further disseminated by DORA competent authorities to NIS2/CER authorities (often in a fully automated manner). The overlap with the GDPR regulation seems fairly limited, and the overlap with the eIDAS Regulation even more so.
- Has the Commission considered other options to further standardize such incident reporting, e.g. one template, taxonomy, set of validation rules, …, applicable to all competent authorities, combined with obligations to (automatically) disseminate the received information to other concerned national/European authorities?

National competences:

Costs

- The proposal aims to reduce compliance costs for entities. What methodology did the Commission use to quantify these expected savings?
- We note that the CRA's Single Vulnerability Platform was budgeted at approximately EUR 11 million, whereas the SEP, which will support reporting across multiple legal acts, is estimated at only EUR 6 million. Could the Commission clarify why the SEP is expected to cost almost half as much as the CRA platform, despite its broader scope and significantly more complex functionality?
- With regard to implementation: on what basis were the estimated costs for ENISA and for Member States calculated, particularly for the development, onboarding, and long-term operation of the Single Entry Point?
- What will be the cost for national authorities to implement the SEP**?** (incl. to assure interoperability of all national authority databases towards the central API; concluding protocols between them)
- Should we first build a portal that integrates all kinds of different complexities (at a higher cost) and then work on common templates to simplify the platform; or should a portal only be built once there is agreement on a minimal set of common templates?

Mandatory nature

- Given the Commission's intention to make the use of the Single Entry Point mandatory, could the Commission clarify whether national reporting platforms will still be used in practice, and if so, in what form? How are Member States expected to integrate their existing national systems with the SEP? Does this imply that Member States must amend their national legislation to impose SEP-based reporting for both NIS2 and CER, including for incidents that are purely national in nature?

Translation of notifications

- Entities will presumably be allowed to notify in their own language, with translation then required. Presumably this can be done via technology. Who should translate: the entity notifying, ENISA, or the member states receiving a notification in a language other than their own?

Divergent timelines

- Given that the Commission has clarified that incident-reporting timelines across EU laws will not be harmonised and that only the reporting process will be streamlined, how will the Single Entry Point ensure that entities are not required to submit multiple notifications at different moments for the same incident due to divergent legal deadlines (e.g., NIS2 24/72h vs. GDPR now 96h)? In practical terms, how will 'report once, notify many' function when timelines remain structurally misaligned?

Space Act

- Would it be the intent of the commission to also include the incident notification requirements under the currently negotiated Space Act into the SEP?

CZECHIA

CZ Questions for the PRES, Commission regarding the Digital (Omnibus VII), 5.12. 2025

CZ questions and comments on the "AI Omnibus"

The Czech Republic welcomes the AI Omnibus presented by the European Commission. The proposal introduces a range of crucial measures that simplify the AI Act. The Czech Republic has been a strong supporter of simplification and, as such, has actively participated on shaping the proposal. We are happy to see that many key improvements from our non-paper were incorporated in the proposal – we specifically welcome postponing the effectiveness of certain high-risk provisions and linking the timeline to the publication of standards, simplifications for SMEs, registration obligations, post-market monitoring, and the notification process for notified bodies.

However, several elements of the proposal would benefit from clarification and could be further improved. The Czech Republic would welcome further explanation from the European Commission on the following points:

- **Alignment of the timeline for Codes of Practice with postponed provisions (e.g., Article 50)**
  How does the Commission envisage aligning the development of the Codes of Practice with the deferred applicability of the relevant provisions of the AI Act?

- **Replacement of deleted obligations through non-legislative instruments (e.g., deletion of Annex III registration obligations)**
  The proposal removes certain obligations, such as the requirement to register Annex III systems. *Does the Commission plan to replace any of the removed obligations with non-legislative tools (e.g., guidance, templates, codes) or allow voluntary compliance mechanisms to maintain transparency where appropriate?*

- **Article 60 – Testing of AI systems in real-world conditions outside sandboxes**
  The Czech Republic welcomes the expanded possibilities for real-world testing. However, clarity is needed on how authorization processes will function in practice. *How will the authorisation of testing in real-world conditions be organised, especially in cases where an AI system is first tested within a sandbox and subsequently outside it? Could the Commission clarify how duplication in authorisation procedures will be avoided?*

- **SME exemptions and possible extension to all enterprises (Article 63)**
  The Czech Republic is assessing whether certain simplifications introduced for SMEs—such as the simplified quality management system (QMS) requirements—could be applied more broadly. Given that the level of protection and conformity assessment requirements remain unchanged, simplified processes may be suitable for all providers regardless of size. *Would the Commission consider applying some of the SME-specific simplifications in Article 63 universally to all enterprises, given that they do not alter the level of compliance or safety?*

- **Clarification of the concept of mutual support and cooperation between national authorities (Article 75)**
  Could the Commission clarify the intended scope of "mutual support and cooperation" among national authorities? In particular, what types of cooperation mechanisms or operational structures are foreseen to ensure effective coordination?

- **Annex XIV – Tools to navigate standards and Codes of Practice**

The Czech Republic considers user-friendly access to applicable standards and Codes of Practice crucial for industry and authorities. *Does the Commission plan to introduce additional support mechanisms—such as an online tool or mapping interface—to help stakeholders navigate the relevant standards and Codes of Practice under Annex XIV?*

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?

Remaining questions we would like to raise again on other topics:

Personal data

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?

P2B

Question on the Digital Omnibus, on the annulment of Regulation (EU) 2019/1150 (P2B) or on Article 10 of the Omnibus itself:

Taking into account that Articles 4, 11 and 15 and certain definitions in Article 2 are to be maintained in force until 2032, it should read as follows:

- Can it effectively maintain the system of enforcement of the retained provisions, has Article 1 P2B (subject matter and scope) been deleted?
- Is it possible for the retained provisions to enter into force, if the Article 19 of the P2B is repealed (Entry into force and effect)?
- Can Article 4 operate without maintaining the definition of 'durable medium' in Article 1 (13)? We see the need to keep in Article 2(13) – definition of durable medium, application of Article 4 P2B.
- Why is Article 3(1)(b) P2B deleted (both published terms as a whole and at the pre-contractual stage)? We know from the practice of the supervisory authority that these are frequently violated provisions.
- Why was the repeal of Article 5(2) to (7) of the P2B Regulation proposed? Is there a plan to incorporate it into the DSA in the future? Article 5 obliges search engines that are not VLOSEs to disclose the parameters used for ranking results. This obligation is not included in the DSA.

Data acquis

CZ is currently assessing the changes proposed by the Digital Omnibus that amends and or/repeals several legislative acts and unifies the data rules under the Data Act. In this regard, we would like to ask the COM about the status of the evaluation reports that were supposed to be carried out, in particular for the DGA, the Free Flow of Non-Personal Data Regulation, Platform-to-Business (P2B) Regulation and the Open Data Directive. Can the COM share them with the MS? We believe that these reports would help us better understand the changes made.

GERMANY

Questionary on the Omnibus VII Proposal

Note: With reference to the written questions submitted by DE on 26th Nov, we furthermore request answers to the following additional questions.

I. Cybersecurity

On the design of the Single Reporting Platform (SRP):

1. What specific data should be collected or stored by the SRP? For this purpose, for example, data centres are hosted by ENISA or are they intended to ensure secure technical storage or transmission to the competent authorities?

2. How should access rights be technically implemented (in particular, the technical interface between SEP and the NCA's existing IT systems)?

3. Sensitive information/security of data:
   - 3.1. Are there any precautions/encryption channels for this?
   - 3.2. Who guarantees these arrangements?
   - 3.3. Who evaluates the platform's CIA criteria?
   - 3.4. Where do COM and ENISA take the competence to assess or are external service providers foreseen for this purpose?

4. Is long-term financing of the platform ensured (cf. situation with the CRA platform where long-term financing is not yet secured)?

5. Are external service providers foreseen for the development of the SRPs?

6. Who is responsible in case of problems with the platform? What happens if the platform becomes the subject of cyberattacks, is unavailable or data is compromised? Are there any back-up solutions (to avoid a single point of failure)?

7. What influence do MS have in case of security problems with the platform?

8. Has COM carried out an impact assessment of the impact of a European reporting platform on the willingness of companies (not only multinationals, but also small and medium-sized enterprises) to report incidents, especially sensitive ones? How should "trust issues" be addressed?
9. How can misunderstandings be prevented that ENISA (as the operator of the platform) is considered as the responsible actor (also for incident handling), e.g. contacted by companies?

Other points:

10. Complexity of technical implementation: Creating interfaces not only at national level, but also at country level is a complex IT venture with a high risk of error vulnerabilities. How does COM wants to solve the problem?

11. We would appreciate clarification regarding the existing platforms? Many public financial resources have already flowed into the creation of national portals. For example, NIS2 is implemented in half of the MS, many others have already built portals, not only for NIS2, but also for the other EU regulations. Would it be an option to use the EU Single-Entry-Point (SEP) as an optional reporting channel alongside the existing national reporting platforms?

12. What is COM's view on streamlining the reporting requirements under the various legal acts on cybersecurity (e.g., DORA, NIS2, CER etc.) or a harmonized template for incident reporting under the respective acts?

II. **GDPR**

13. Regarding Art. 4 Nr. 1: In the opinion of the COM, is the consequence – if an entity cannot identify the natural person to whom the information relates to and thus, the information is not to become personal data for that entity, - the GDPR does not apply and, thus, any processing carried out by that entity in regards to that information does not fall under the GDPR? And does that also apply if the entity openly publishes said information when such information then may be identified by third parties?

14. Regarding Art. 4 Nr. 38: What is meant by "which can also support innovation"? How is "innovation" to be understood and how should it be determined which research can promote innovation?

15. Regarding Art. 5(1)(b): In the opinion of the COM, does further processing require a separate legal basis? If so, does the amendment affect this requirement? Is the proposal to be understood as meaning that further processing for the purposes specified in Art. 89 should ultimately be permissible without any further conditions beyond those specified in Art. 89?

16. Regarding Art. 9(2)(k): To what extent does the proposed text indicate that 9(2)(k) only applies if the controller does not intend to process particularly sensitive data?

17. Regarding Art. 9(2)(l): What scenarios does the provision target? Does it concern access controls, for example? Are these cases not already covered by the other provisions of Art. 9(2)? To what extent is there a need for regulation here?

18. Regarding Art. 12(5): What is meant by data protection purposes within the meaning of the proposal? Can you give examples of data protection purposes and other purposes ("purposes other than the protection of their data")?

19. Regarding Art. 13(4): We would welcome further information on what is considered to a "clear and circumscribed relationship" and "activity that is non data-intensive". In the opinion of the COM, does the exemption in paragraph 4 could also be applied to instances where sensitive data in accordance with Art. 9 is processed (such as doctor-patient relationship in the context of treatment)?

20. We would welcome further information on the intended purpose of the proposal to add a new paragraph 5 to Article 13 GDPR. In particular, what are the reasons for not including processing that takes place for archiving purposes in the public interest, historical research purposes or statistical purposes in the exemption?"

21. Regarding Art. 22: In your understanding, does the new version only involve a clarification or also a change in content, in particular an extension of the processing options?

22. Regarding Art. 88a: In your understanding, does the new version only involve a clarification or also a change in content, in particular an extension of the processing options? According to the wording, other scenarios could be covered in addition to cookies, e.g., access to employees' mobile devices in the context of "bring your own device." Is this intended? If not, how is it ensured that the provision only applies to cookies?

23. Does COM have any forecasts as to what percentage of websites will display cookie banners again due to the exception in Article 88b(3) GDPR?

24. In its presentation on the Digital Omnibus, the Commission emphasized that the changes in the GDPR should not affect "consent or pay" offers for media services. Against this background, we wonder how COM envisages the interaction between Article 88a, which requires a single click "opt-out" button and prohibits a new consent request for six months, and the media exemption in Article 88b (3). Does the exemption also apply to Art. 88a or only to Art.88b?

25. Regarding Art. 88c: What is meant by "where appropriate"? We would also welcome further information on how this Article relates to the legal basis to process data for AI purposes under other (EU)-Regulations, namely the EHDS-Regulation. In the opinion of the COM, how does the "unconditional right to object" in Art. 88c relate to the right to opt-out acc. to Art. 71 of the EHDS Regulation?

III. **Data / Data Act**

26. How exactly is incorporating other legal acts with different subject matters and scopes into the Data Act aid consistency and simplification of the legal acquis?

27. How is consistency with other EU data initiatives being achieved (e.g. with the European Data Union strategy)?

28. How is the structure of national competent authorities being affected by incorporating other legal acts into the Data Act? Does the competent authority for the application and enforcement of the Data Act automatically also become the competent authority for the incorporated acts? Do other nationally designated authorities remain competent authorities

for those other legal acts? Does the existence of more than one competent authority within the scope of the Data Act necessitate the designation of a data coordinator according to article 37 paragraph 2 Data Act?

ESTONIA

EE questions on the Digital Omnibus

We thank the Commission for all the answers and clarifications provided so far.

Here are additional questions we have identified so far:

DATA

- What are the considerations behind making Open Data Directive to a Regulation?
- When the purpose of the omnibus is to simplify, why have the articles regulating single information points and open data publishing not been joined and synchronized? Article 32aa (on DGA single information points) and Article 32s (on Practical arrangements regarding the re-use of open government data) are in combination asking Member States to establish national registers/portals for gathering the descriptions of all the data falling under the mandate of DGA and ODD, and to submit all these descriptions to the European Data Portal. It would be clearer if these articles would be joined into a single generic article, stating clearly that Member States are expected to create an inventory of all their data, describe this data (incl marking which data is open and which restricted) and submit all these description to the European Data Portal.
- Is the Commission going to develop more specific guidelines regarding the higher charges for the re-use of data by very large enterprises (Article 32q (6), 32y (5))? Why have these articles not been joined into a single article to simplify even further?

GDPR

Definition of "personal data"

- Why did the COM propose an amendment to the definition of "personal data" – what was the underlying rationale for this decision? Additionally, could the intended objective have been accomplished by incorporating a recital into the GDPR instead?
- Why did the Commission decided to propose a change to the definition of "personal data" only in GDPR and EUDPR at this stage, leaving the possible change in LED to the future?
- What defines an entity?
- Does the GDPR apply according to the new regime when an entity is of opinion that it cannot identify the natural person to whom the information relates?
- Who is responsible for proving whether an entity has reasonable means to identify the natural person that the information relates – the entity itself or the supervisory authority?

Definition of "media service"

- Does defining "media service" in the GDPR have impact on the art 85.2 (processing for journalistic purposes)?

Processing for scientific research

- The proposal rewords Article 5.1.b to be independent of GDPR Article 6.4. Will future safeguards for scientific research be limited to those listed in Article 89.1 of the GDPR? Alternatively, may a Member State establish additional safeguards under national law pursuant to Article 89?

Processing of biometric data

- What are the actual situations that art 9.2.l will cover?

Data subject's rights
- Why are data subject information requests restricted solely to protecting personal data? How will this be implemented in practice?
- How will the proposals impact the workload of DPAs?

Automated decision-making including profiling
- The provision is no longer formulated as a data subject's right – what was the underlying rationale for this? This issue should be clarified taking into account the Convention 108+, which has already been ratified by several Member States. Article 9.1.a of the Convention grants data subjects the right not to be subject to decisions that significantly affect them based solely on automated data processing, without their views being duly considered.

Position of the EDPB
- What is the reason behind the proposal that the Commission needs approve the EDPB guidance (e.g. art 33, art 35)? How is EDPB's independence maintained with this approach?

Development and operation of AI system
- Why did the COM suggest regulating technical solutions (AI systems and models) in GDPR, given the regulation's current aim of technology neutrality?
- Could the same objectives be achieved by treating AI development as scientific research (technological innovation), and putting in place safeguards for scientific research in GDPR?
- The proposal allows personal data processing based on legitimate interest or, in certain cases, consent. Is this list of legal bases exhaustive, or are other legal bases permitted considering that public authorities usually cannot rely on legitimate interest or consent in their processing.
- Article 9.5 permits a special regime for AI development and operation when processing residual special categories data. Why is this special regime restricted to AI when such data can appear in other processing contexts?

Processing of personal data in the terminal equipment of natural persons
- How will the future relationship between the GDPR and ePrivacy Directive change if certain provisions from the directive are integrated into the GDPR?
- If the controller cannot identify the natural person based on cookies will the rules of proposed art 88a apply?
- How will Articles 88a and 88b be implemented in practice? Particularly given the GDPR's consent validity requirements.

Single entry point for incident reporting
- Does creating a single entry point for incident reporting impact the GDPR's one-stop mechanism?

Question to the Legal Service
- Can recitals in a regulation be amended or added without changing the main text?

IRELAND

Digital Omnibus - Comments and Questions on Proposed Regulation 2025/0359 (COD)

General

We are strongly supportive of aligning the deadline for applying high-risk obligations with the availability of related standards and support tools and welcome the Commission's commitment to providing the necessary guidance to apply the AI Act in parallel with other EU legislation.

Article 4 (Literacy)

- Does introduction of 4a constitute an obligation for Member States that could constitute a sanctionable infringement? How will this be measured, and enforced?
- We would like to see more information on this; new staff resources may not be available (for budgetary or scarcity reasons). How shall the Commission and MS 'encourage' providers and deployers?
- Can the Commission elaborate on what measurable "promote and support" instruments they envisage for this obligation.

Article 50 (Transparency)

Paragraph 7 (Simplified)

The AI Office shall encourage and facilitate the drawing up of codes of practice at Union level to facilitate the effective implementation of the obligations regarding the detection, marking and labelling of artificially generated or manipulated content. The Commission may assess whether adherence to those codes of practice is adequate to ensure compliance with the obligation laid down in paragraph 2, in accordance with the procedure laid down in Article 56(6), first subparagraph. If it deems the code is not adequate, the Commission may adopt an implementing act specifying common rules for the implementation of those obligations in accordance with the examination procedure laid down in Article 98(2).'

- Where there are codes of practice drawn up by the AI Office, are these relevant to the implementation of the Act by the MSAs including prosecution of any breaches of the regulation.

Article 57 (AI Regulatory Sandbox)

- IE would like to ask for clarification on the intention behind the revised wording of paragraph B, which provides that national competent authorities "*shall support the joint establishment and operation of AI regulatory sandboxes, including in different sectors*". IE would welcome further detail on this proposal.
- What is the expected scope of the EU sandbox and how is the relationship with the MS sandboxes and competent authorities expected to work?
- Where the AI Office establishes a sandbox, it shall be with other competent authorities. Who are these authorities? It is not clear as to the reference to other Union legislation other than the AI regulation being examined by the sandbox. What is envisaged here – the AI sandbox surely is aimed at AI only?

- In addition, if the AI office has a sandbox in respect of Art 75(1) – does this mean that there is no requirement for MS to have a sandbox for general purpose AI? Where is the boundary? Can the MSAs rely on the work of the AI office where they are involved in enforcement actions against financial services providers where the AI office cleared a particular AI product.

- IE notes that Paragraph 13 is replaced by the following: *'13. The AI regulatory sandboxes shall be designed and implemented in such a way that they facilitate cross-border cooperation between national competent authorities.'* where 'relevant' is removed. Cross border cooperation is now

mandated in the design and implementation of sandboxes. Does this add to the complexity and cost of national sandboxes? How will this be delivered?

- How will the development of the AI sandbox work to allow for cross border co-operation between national competent authorities. Is it intended there will be MOUs; engagement in the development of sandboxes; specific aspects to be developed in different states. This is a wider question across this entire proposal – in terms of engagement between AI and NCAs and how it will work.

- If cross border cooperation is now mandated in the design and implementation of sandboxes. Does this add to the complexity and cost of national sandboxes?
- Proposed change at Paragraph 14. (old) *National competent authorities shall coordinate their activities and cooperate within the framework of the Board.* New 14. *National competent authorities shall coordinate their activities and cooperate within the framework of the Board. They shall support the joint establishment and operation of AI regulatory sandboxes, including in different sectors.';*
- The joint establishment and operation of AI regulatory sandboxes in different sectors is now mandated. Does this add complication and cost?

Article 58: Detailed Arrangements for, and functioning of, AI Regulatory Sandboxes:

Old 1. In order to avoid fragmentation across the Union, the Commission shall adopt implementing acts specifying the detailed arrangements for the establishment, development, implementation, operation and supervision of the AI regulatory sandboxes. The implementing acts shall include common principles on the following issues:

New 1: In order to avoid fragmentation across the Union, the Commission shall adopt implementing acts specifying the detailed arrangements for the establishment, development, implementation, operation, governance, and supervision of the AI regulatory sandboxes. The implementing acts shall include common principles on the following issues

- We are concerned that this may be adding additional complexity and gold plating.

Article 69 (Access to the Pool of Experts by the Member States):

Old 2. The Member States may be required to pay fees for the advice and support provided by the experts. The structure and the level of fees as well as the scale and structure of recoverable costs shall be set out in the implementing act referred to in Article 68(1), taking into account the objectives of the adequate implementation of this Regulation, cost-effectiveness and the necessity of ensuring effective access to experts for all Member States.

New 2. The Member States may be required to pay fees for the advice and support provided by the experts at a rate equivalent to the remuneration fees applicable to the Commission pursuant to the implementing act referred to in Article 68(1).';

- IE would like if we could consider the implications for costs and fees at this point, and why is this proposal re fees is being proposed.

Article 75 (Mutual Assistance, Market Surveillance and Control of General-Purpose AI Systems)

- The point re: surveillance and enforcement are relevant here. This approach provides exclusive powers for the AI Office to act. Is the boundary between the role of the AI office and the MSA clear – these need to be mapped so that there is clarity of responsibility between national and EU supervision and enforcement. If there are areas where there is disagreement re supervision and enforcement – how is this worked out?

- Will the AI office be required to notify of any actions it is taking re an AI product on the territory of an MS?

- Will this need to be considered by the Courts – do the European courts have exclusive jurisdiction - which courts are involved?
- Why is it proposed that the Commission provide for implementing act to determine the enforcement powers and ability to give penalties. May be better that this is included and considered as part of amendments to the regulation.

Article 77

- The proposal aims to include mutual assistance in this Article including the exchange of information etc where necessary. This does not seem to deal with situations where there is confidential or commercial information or indeed where such provisions are blocked by existing provisions of Union law – especially in financial services. The rules need to make it clear how the Regulation works in particular where there are other similar EU legislation which reduces or blocks flows of information.

Article 113

- IE shares other MS views that it raises practical and operational uncertainties and would welcome further clarification on the practical and operational matters arising from this proposal.

SPAIN

AI Comments

-Article 4.1-Definition of personal data and new Article 4.1a on pseudonymisation

While the search for legal certainty is appreciated, a positive formulation defining when personal data does exist, and not an essentially negative one, may be necessary

It is appropriate to clarify what happens with subsequent communications to entities that do have means of re-identification

It should be clarified whether the regime applicable to "non-personal" data grants any residual rights to the data subject and not only obligations for the controller when the data are personal

The need for minimum traceability mechanisms in the value chain to detect and manage possible re-identifications should also be assessed.

-Article 88.c -New article on legitimate interest in AI

The inclusion of the expression '*where appropriate'*, although it may be a guarantee, introduces a new source of legal uncertainty, since it is not specified, nor are there any lines as to how the existence or otherwise of this 'origin' will be assessed.

The list of purposes of Article 59 of the AIR for the scope of the sandbox may be a starting point for limiting or defining the scope of this legal basis. Aspects such as the definition in recital 38, which could be worded more precisely, should be revised.

It would also be very useful to express the possibility that this legal basis of legitimate interest may be applicable to processing carried out by public authorities, given the limitations that the public administration has (Article 6.1 (f) in fine) to rely on legitimate interest. Specific empowerment may be appropriate.

It would also be appropriate to provide for specific details concerning online scraping, also taking into account the specific prohibition in Article 5 of the AIR.

Issues relating to the exercise of some rights such as information and opposition to processing in practice need to be clarified.

-New Article 4.38-Definition of scientific research

Recital 159 GDPR currently considers that the concept of 'scientific research' should be interpreted broadly. The new definition of 'scientific research' in paragraph 4.38 is even broader, this could be positive, but also create uncertainties. The definition proposed by the Commission is new when widely adopted definitions already exist.

-Article 9.2 (l)-New article on the use of biometrics

The proposal is considered to be positive and consistent with the Opinion issued by the EDPB on airport transit, by regulating the basic elements of the processing on the use for verification and the general rule of sole control held by the data subject.

It would be desirable to delimit the concept of "means of identification" and to introduce certain specifications regarding the phases of identification and the risks, such as requirements necessary at the registration stage or "enrolements".

Consideration should be given to the specific regulation of some requirements with regard to the processing of biometric data for identification (non-authentication), some relationship of the GDPR with high-risk and prohibited AIR systems could be regulated.

-Article 12.5 -Limitation on the exercise of rights

The regulation may incorporate EDPB developments on the right of access.

It can be clarified that there is no need for the data subject to motivate access, but the voluntary explanation of the reasons may help to weigh reasonable limits.

It may also be positive to clarify that under no circumstances does the right imply an obligation on the part of the controller to further process the data at its disposal.

Some regulation and improvement of the law in contexts such as health could be of particular interest.

-Article 13.4 -Exemption from the duty to provide information

The new exemption from reporting in "clear and circumscribed relationships" and "non-data-intensive" activities is ambiguous and creates legal uncertainty, especially for SMEs. See recital (36).

The problem may lie more in 'when' and 'how' it is reported, rather than in the duty itself. For example, it might be useful to allow information on a layered basis or at more flexible times, but to maintain the rights of the data subject.

It would also be necessary to assess the asymmetry that could be created by different regulation between the public and private sectors. It is necessary to start from a stricter duty to provide information for the public sector.

-Articles 22.1 and 22.2-Automated decision-making

Among other improvements, one could follow suit and introduce the application of these guarantees with respect to 'substantially' automated decision-making in line with Article 6 (3) AIR and CJEU case law, i.e. not only to 'only automated' decisions. Improvements on transparency and explainability of the CJEU 2023 and 2025 could be introduced.

It should be assessed whether specific reference should be made to the higher intensity of guarantees regarding the use of technologies as artificial intelligence, especially in AIR high-risk scenarios.

It would also be desirable to explicitly regulate the right to explainability and for data protection to be its special legal basis, to which Article 86 AI Act refers.

With regard to the right to ex-post human supervision, it should include some clarification along the lines of some documents such as those carried out by the Dutch Data Protection Authority or the EDPS.

Clarify the status of subjective rights in Article 22 GDPR and its connection with limits in Article 23 GDPR.

THE GDPR: Art. 33.1 -Security breachs

In relation to the proposed amendment to Article 33, limiting notification to high-risk breachs only has several drawbacks:

First, it restricts general knowledge about the state of digital divides, precisely in a data-driven context. Second, it prevents assessing the impact of non-high risk gaps which, by affecting a multiplicity of controllers, may generate systemic risk. It also makes it difficult to analyse the existence of repeated gaps within the same person.

It should also be noted that setting a notification criterion limited to the controller may be more complex for the controller (especially SME) than making the notification itself. It can also have a deterrent effect by obliging the controller to explicitly state that a gap constitutes a high risk and is more likely to be sanctioned. Finally, communication to data subjects is affected, as the supervisory authority will not be able to order notifications on incidents that it does not know, leading to a loss of control by data subjects over their own data (Recital 7).

With regard to the single definition of 'high risk', there are concerns that specific regional contexts – cultural, social and economic – are not taken into account, and that the decision may lie with actors outside the direct management of the breachs.

As regards the increase of the maximum notification period, it does not align the GDPR requirements with other much shorter notification periods (DORA, NIS2, eIDAS2, CRA, MDR, Critical Infrastructure Directive), thus adding complexity to the controller (especially SME).

Articles 35.4, 35.5 and 35.6 -Processing lists and Data Protection Impact Assessment (DPIA) templates

With regard to Article 35, there are concerns that carrying out the Data Protection Impact Assessment (DPIA) is one of the most important safeguards for enabling processing, even in the same Omnibus proposal.

The DPIA is a continuous and dynamic procedure and the message that it is the Commission that has the final say in the decision to reduce it to a template that can turn it into a mere formalistic checklist would weaken the risk-based approach and effective safeguards for rights and freedoms.

AIR: Article 4a- New article on legal bases for the detection of bias

Positive assessment by extending the exceptional processing of special categories of personal data to ensure bias detection and correction to all AI processing and not only to high-risk AI processing as currently included in the AIR.

ITALY

Component cyber

It would be helpful to clarify why the Commission has not considered including — in parallel to the establishment of an EU single point of access — a significant effort to harmonize/align the definitions, requirements, and timeframes relating to the notification obligations arising from the various regulations affected by the proposal (i.e., NIS2, CER, eIDAS, DORA, GDPR). Regulatory alignment could, in fact, facilitate the full achievement of the objectives underlying the establishment of the aforementioned single portal.

Questions:

1. *How would the Commission ensure a uniform approach to incident notification through the two new proposed delegations that would allow the adoption of **common notification templates for GDPR** (Article 3 point 8 of the proposal) **and CER** (Article 9 point 2 of the proposal) via implementing acts, and in light of the delegations already provided under **NIS2 (Article 23(11)) and DORA (recital (54))**, which already provide for an implementing regulation on harmonized templates?*
2. *Should the exercise of these delegations lead to a **single template for incident notification under the four aforementioned acts**? Why is there no reference to **eIDAS**?*

Component AI

Granting the AI Office exclusive supervisory powers for GPAI and VLOPs would significantly impact Italy's ability to monitor the adoption of AI systems in its domestic market. With reference to the amendments proposed in the Omnibus to Article 75 of the AI Act (point 25 of the proposal), the following questions arise:

1. *When determining the impact and costs of the possible AI Office's exclusive competence for AI systems based on a general-purpose AI model developed by the same provider, on national resources already allocated and investment plans currently being implemented to create similar specific supervisory capacities within national authorities?*
2. *Could you clarify whether, under the revised Article 75 the measures decided by the AI Office should be then enforced by national authorities, thus separating the process of product assessment and definition of the measures from their enforcement?*
3. *Some sectors listed in Annex III (subject to exclusive supervision), although not covered by product legislation under the New Legislative Framework, are supervised by national authorities, with which the AI Act supervisor will need to liaise before deciding on any measures impacting the specific sector. How can these sectoral needs be reconciled with centralized supervision by the AI Office? How would such interaction work?*
4. *Has the Commission considered the possible asymmetry that would arise between supervision for general-purpose AI (GPAI), which would be centralized in the AI Office, and other regulations under the New Legislative Framework, for which product supervision is entirely the responsibility of individual Member States? If so, what circumstances would justify such asymmetry?*
5. *Could the Commission share more information regarding the assistance that national authorities should provide to the AI Office in exercising its exclusive supervisory functions, in particular where enforcement actions need to be taken in the territory of a Member State?*

LUXEMBOURG

Comments and questions on Cybersecurity

ILR (competent authority for NIS2 sectors – except the financial and banking sectors, NCCS competent authority, and AI-market surveillance authority) welcomes the proposition for a European single entry point (SEP) for incident reporting. In fact, we acknowledge the current complexity for incident notifications for several sectors, especially telecom, other digital infrastructure, but also for different types of group settings active in different sectors or based in multiple countries. Therefore, ILR started already years ago with implementing SERIMA (Security Risk Management) , an open source platform, capable to host multi-sectors, multi-regulators and multi-regulations incident notifications. In Luxembourg, SERIMA will be used, once NIS2 has been transposed, for incident notifications under NIS2, CER and GDPR. Currently SERIMA is used for NIS1 and EECC notifications.

We are certain that the SEP will be beneficial for the operators and will foster collaboration among Member-States.

Nevertheless, we believe that clarifications and specifications are needed, legally but also practically. Therefore, our comments/questions will be split into two parts, one concerning the text of the proposal for regulation and one for the practical or technical constraints of the SEP.

Concerning the proposal for regulation:

- Recital 52 states that a continuity and interoperability with existing national solutions should be guaranteed and Recital 57 states that an alternative solution should be available in the case of technical issues, however the proposed amendments to NIS2 (Art6) but also the changes for GDPR as well as CER, do not foresee an alternative solution and does not provide the possibility to use a national platform. Therefore, we would suggest including “at least” in front of “via the single-entry point established pursuant to Article 23a” in article 6. paragraph 2 for the amendment to article 23 of NIS2, and also in paragraph 3 for the amendment to article 30 of NIS2. Same for the amendments of the other Directives or Regulations.
- Recital 49 states that the SEP should also be capable for operators to retrieve information of incident notifications done via SEP. However, this part is not reflected at all in the amendments. We would suggest adding a paragraph for including the bi-directional communication flow of the SEP.
- The SEP is supposed to work for NIS2, GDPR, CER, e-IDAS, DORA, NCCS and aviation. However, incident notification is also part of the AI-ACT, which are currently not foreseen to be integrated in the SEP, we suggest to also include the AI-ACT to guarantee harmonisation EU wide.

Concerning the practical/technical constraints

- It is stated that ENISA is responsible for the security of the platform. We are not sure that this is completely realistic and does not seem to be a risk-based approach due to the interconnection and data transfer towards national platforms. Therefore, we suggest deepening the description of the mode of operation of the platform, to do a risk assessment and define roles and responsibilities depending on the workflow and interconnectivity with national solutions.
- Having experience with SERIMA, we would like to highlight to ENISA the importance to foresee a workflow and risk assessment for the case that the wrong authority has been notified (either due to wrongful information of an entity or due to a misconfiguration).

- Concerning the development and testing of the platform, we are curious to know how member states or authorities are implicated in the process in order to assure interoperability and continuity of national solutions. Furthermore, we see a need for an end-to-end validation of the workflows (from entity to authority (and vice versa)) and thus the implications of member states /authorities would be necessary.
- It is stated that no data is stored on the SEP, thus we are wondering how the retrieval of incident notifications by operators will be feasible. Would it be possible to elaborate on the architecture and workflow?
- It is also written that ENISA shall not have access to the data, also here we are wondering how that would be technically assured, especially as admin of the platform?

***

QUESTIONS ON THE DIGITAL OMNIBUS REGULATION PROPOSAL

Ministry for Digitalisation

General comments

Luxembourg acknowledges that the simplification agenda constitutes a key driver to increase Europe's competitiveness. In general, and preliminary, Luxembourg welcomes the approach and ambition of the European Commission in the context of the Digital Omnibus package. However, given the possible impact of the proposed measures, it is crucial that we thoroughly analyze the package. Luxembourg particularly welcomes the iterative nature of the process, which, through the Digital Fitness Check, allows us to regularly review whether our simplification efforts are still heading in the right direction or whether they need to be stepped up, if necessary.

For Luxembourg, creating a predictable legislative framework that is conducive to innovation through the reduction of the administrative burden should be among the top priorities. At the same time, it is essential that we ensure that we do not dilute the founding principles and the level of protection provided by the GDPR.

In addition, the simplification and streamlining of the legislative landscape in the field of data is an important step in enabling European businesses and citizens to navigate this regulatory framework, which remains complex and fragmented. As a result, we support the European Commission's idea of bringing together the separate texts in the field of data and encourage a thorough analysis to identify and eliminate any overlap, duplication or incoherences arising from the different pieces of legislation. Lastly, we call on the co-legislators to adopt a simplification by default and by design approach at the European level. It is pivotal that we avoid introducing new administrative burdens on the public and private sectors when designing new legislative measures.

Questions and observations regarding the Data Act/Open Data Directive/Data Governance Act and GDPR.

General questions:

- Which proposals in Omnibus serve the aim of reducing bureaucracy related to data protection law?

- What is the timeline for the data proposal of the Omnibus?

Data Act/Open Data Directive/Data Governance Act:

- Over the last years, Luxembourg has invested a lot of resources in implementing Chapter II of the DGA under the system of a centralized data authority that grants permits for reuse of data,

aggregates data and provides for a secure processing environment. According to the Luxembourg national data strategy that procedure shall serve as a model for all data spaces and current preparations for the EHDS regulation, Chapter IV are well advanced in order to harmonize procedures and designations.

- Does the Commission's proposal and the new approach under Chapters VII, a to c (proposed) oblige Luxembourg to change its whole national implementation strategy?

- Why is the adding of new conditions for re(use) of data (currently foreseen by Chapter II DGA) even necessary?

- Why hasn't the Commission proposed the same conditions for reuse of public sector data as currently foreseen in Chapter II DGA? What is the added value?

- Why hasn't the Commission proposed the same conditions for reuse of public sector data as currently foreseen in Chapter IV EHDS? What is the difference between both procedures and systems?

- In what way does the new proposal on reuse of public sector data constitute a lowering of administrative burden in comparison with Chapter II DGA?

- Has the Commission envisaged to largen the scope of 'reuse' under the DGA? If not, why not?

- Is the Commissions intent that all public sector data currently under the Open Data Directive regime may be combined with data currently falling within Chapter II of the DGA within one same procedure?

- May a reuse of data under Chapter II of the DGA (current), fall within the scope of the Data Act in the event more private entities are considering to reuse those data together, in conjunction with their own data?

- Amendment to Article 15 of Regulation (EU) 2023/2854 (Data Act): What is the rationale for introducing such a distinction (paragraphs (2) and (3))? What is the usefulness of paragraph (3), given that it states it must be based on 'Union law or national law'? Could this create legal uncertainty?

- Amendment to Article 21 of Regulation (EU) 2023/2854 (Data Act): It seems there is an error in the way the separation was made: 'the technical protection' (the technical protection measures in point (c)) appear to need to be added to point (d) together with the organizational protection measures. Why so and what is the added value?

- As to the respective scope of Chapter VIIc, Section 2 (current Open Data) and Section 3 (current DGA): Article 2(54) defines 'certain categories of protected data' as data protected for reasons related to the protection of personal data, while adding 'insofar as such data fall outside the scope of Section 2 of Chapter VIIc.' Article 31i(3) specifies which documents Section 2 (Re-use of Open Data) of Chapter VIIc does not apply to it. Article 31i(4) clarifies that Section 3 of Chapter VIIc (current DGA) does not apply to data that are not 'certain categories of protected data. It seems that these additions aim to clarify the respective application of the 'Open Data' provisions and those of Regulation (EU) 2022/868. However, these provisions are complex and do not allow for a straightforward clarification of how these two regimes apply.

- Article 32(i)(3)(b)(iii): If it is necessary to 'define' in a law that the re-use of data is incompatible with data protection. In which way, can this condition be considered a simplification measure?

- Which personal data could fall under Section 2 of Chapter VII of the proposal?

- Article 2(57) introduces a new definition of 're-user' as any natural or legal person who has been granted the right to re-use data or documents held by a public sector body or a public undertaking under Chapter VIIc, or to re-use research data or certain categories of protected data. Chapter VIIc applies to both data and documents. Article 2(48) includes in the definition of 'document' non-digital content. How can this broadening be reconciled with the original objective of providing secure processing environments?

- Article 32w(5) provides that when the re-use of data cannot be authorized in accordance with the requirements of paragraphs 3 and 4 (secure processing environment, anonymization, confidentiality obligation), then re-use will only be possible with the consent of the data subjects (where no other legal basis exists). What added value does this provision bring compared to Article 6 of the General Data Protection Regulation (EU) 2016/679? This could lead to legal uncertainty regarding the application of these two texts. Indeed, could an extensive and a contrario interpretation of this provision lead to the conclusion that there is no need for a legal basis as long as the conditions of paragraphs 3 and 4 are met. Is that correct and, if, what is the reason?

- Could the competent authority under the Data Act (Article 38) be made aware of complaints related to Chapter VIIc (see new Article 38(81)(a), which refers without distinction to 'under this Regulation')? Furthermore, it should be noted that Article 40 provides that 'penalties' (sanctions) do not apply to Chapter VIIc on the re-use of public sector data.

- Luxembourg wants to combine 'secure processing environments' under different data space regulations with the 'AI Regulatory sandboxes'. Would this still be possible with the rules foreseen in the proposal?

GDPR:

- Does the proposal merely codify case law and Recital 26, or does it entail a substantive change?

- In the event of the former, there is no need to codify the recent case law, as this will only create legal uncertainty, as the terms are not one to one the same as in the ECJ case law (which also has a specific character due to the facts related to each case).

  In the latter event, what are the substantive changes?

- The notions of 'controller' and processor already causes discussions on the roles and responsibilities. What is the exact is the scope and meaning of 'entity' and what is its impact on GDPR interpretation?

- Luxembourg is keen to maintain the level of protection offered by the GDPR, would the new definition of 'personal data' allow the transferal of data to a recipient in a third country outside the conditions set forth in Chapter V of the GDPR?

- The proposal foresees that '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'. This is already known and also data protection authorities recognize such processing operations as being part of the legitimate interests of a controller. What is the added value of Article 88c, as it rather seems to establish new concepts/conditions that create legal uncertainty and administrative burden?

- Is an entity processing data on behalf a controller still to be considered as 'processor' within the meaning of the GDPR, if it does not have the means to identify a person?
- Can entities that cannot identify the data subject share the data or even make it public without conditions?
- Has the Commission identified other means to lower the administrative burden, without prejudicing the level of protection?
- Considering the recitals of the GDPR scientific research shall been interpreted broadly. Is the proposal narrowing this purpose? What is the added value of a definition, as it risks to hamper possibilities to re(use) data for research and innovation purposes?
- As regards the notion of scientific research, which kind of research is meant/not meant to fall under the definition?
- How are ethical standards determined? Wouldn't this create even more complexity?
- Why has the Commission decided not to define „health data" in Article 9 GDPR)? Is the mere information "able to do sport" within player licensing procedure considered as falling within Article 9(1) GDPR?
- Does the COM see the necessity to exclude low-risk processing outside the health sector (e.g. data processed for diet-related purchases such as lactose-free milk) from the scope of Article 9 data?

NETHERLANDS

NL Written Comments on Digital Omnibus

General comment

The Netherlands believes that an impact assessment is essential for properly evaluating the effects on regulatory burden and fundamental rights of the proposed measures in the Digital Package. The absence of an impact assessment for these proposals makes it difficult to fully understand the effects on businesses and citizens. The Netherlands urges the Commission to conduct an impact assessment, so that the consequences for regulatory burden and other policy objectives can be carefully considered. This is an important step to ensure that the proposals truly contribute to reducing administrative burdens without undermining the protection of fundamental rights or national competencies.

1. GDPR

On 26 November the Netherlands submitted almost 40 questions and 14 comments about the proposed changes to the GDPR. To date, NL has seen full answers on 3 questions and partial answers on 5 questions. We have not yet seen any answers to the other questions and comments. The Netherlands welcomes the Commission to provide (preferably written) answers to these remaining questions and comments so that we can further develop our position based on this information. We therefore refer to our previous questions and comments, which are included in the appendix. Text boxes in the appendix indicate which questions were fully or partially answered by the Commission at the AGS meeting on 1 December. In addition, we have the following new questions following the presentation by the Commission in this AGS meeting and other questions. In general, a scrutiny reservation applies to the amendments to the GDPR.

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

Questions:

- The Commission emphasises that the proposed Article 4(1) GDPR "definition builds on recital 26 GDPR as clarified in the recent SRB case-law". However, the proposed text and the corresponding recitals do not include the following three elements which reflect the high bar for data no longer being personal data the CJEU sets in its case law and the SRB case. If the purpose of the new definition is to codify the recent SRB case law and Recital 26, has the Commission considered to include the following three elements from the SRB case in Article 4(1) (or the Recitals), and if not, what is the rationale behind this?

  1.) That the recipient of the pseudonymised data is not in a position to lift the technical and organisational measures implementing the pseudonymisation during any processing of the pseudonymised data which is carried out under its control (§77, SRB case).
  2.) That those measures must in fact be as such as to prevent the recipient from attributing those pseudonymised data 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 recipient, the person concerned is not or no longer identifiable (§84, SRB case).
  3.) In the context, inter alia, of a potential subsequent transfer of those data to third parties and 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 (§85, SRB).
- Is there a procedure to object for the natural persons concerned if they disagree with the controller's analysis that the data do not constitute personal data?
- Does the proposed definition exclude online tracking or large data brokers from the scope of the GDPR if they only sell data based on pseudonyms such as device IDs or cookie IDs? What safeguards are envisaged to ensure that pseudonymisation does not unintentionally reduce the scope of GDPR protection? Is there a possibility that processing activities could be divided among separate entities to avoid the applicability of the GDPR?
- Might this definition increase the workload for supervisory authorities? Could controllers easily derail their investigations by simply claiming to not fall under the GDPR, which would easily prolong investigations and would require technical investigations to disproof such a claim?

Processing in the context of AI development and operation (Art. 9(5) and 88c)

Questions:

- The Commission states that the wording of the measures of Article 9(5) are "non-exhaustive", however, this is not being reflected in the wording of the Article nor in Recital 30-31. Has the Commission considered to reflect this in the Article or the recitals?
- The Commission states in its presentation (sheet 29) that Article 88c "reflects EDPB Opinion 28/2024". However, this is not being reflected in the wording of the Article nor in recital 30-31. Has the Commission considered to explicitly add this to the recitals, and if not, what is the reason for this?
- Does Article 88c merely reflect this EDPB opinion, or does it also entail a substantive change?
- The EDPB opinion highlights the elements that must be considered to assess whether data subjects can reasonably expect their personal data to be processed. These include: "whether or not the personal data was 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 was collected, the source from which the data was collected (i.e., the website or service where the personal data was collected and the privacy settings they offer), the potential further uses of the model, and whether data subjects are actually aware that their personal data is online at all." Has the Commission considered to include this elements in Article 88c or the recitals, and if not, what is the reason for this?
- The Commissions states that "the development and operation of AI does not per se qualify as legitimate interest" (sheet 29). However, this is not being reflected in the wording of Article 88c nor in recital 30-31. Has the Commission contemplated about explicitly adding this to Article 88c, and to clarify in this Article the necessity to define a purpose for the processing of personal data as well, and if not, what is the rationale behind this?
- The Commission states that "a controller may rely on Article 6.1.f for pursuing a legitimate interest in the context of AI development and operation, where all conditions of that provision and the other GDPR requirements are met" (sheet 29). If all other requirements of the GDPR continue to apply when invoking Art. 88c, why does this Article specifically refer to some but not all principes of Article 5? Reference is made to only the principle of data minimisation, transparency, the right to object, and appropriate technical and organizational measures.
- Could the Commission clarify the meaning of "beyond controller's obligations" in the following sentence from sheet 29, about Article 88c: "Enhanced transparency and the unconditional right to object are meant as safeguards going beyond the controller's obligations."

Article 33 GDPR (Notification of a personal data breach)

Questions:

- The Commission stated in its presentation in the AGS of 1 December: "The adoption of the list and templates for data breach notifications by way of an implementing act provides more legal certainty to controllers as such act is legally binding." (sheet 36)
    - To what extent will the lists and templates have more legal certainty when they are determined by a Commission's implementing act than when determined by the EDPB?
    - How does the ability of the Commission to reject or amend a proposal for a list or template from the EDPB align with the independence of the EDPB as an EU authority?
    - Could adoption of the lists and templates by the EDPB, without an implementing act of the Commission, not also provide sufficient legal certainty, like EDPB guidelines do?
- Sheet 36 of the presentation by the Commission states: "The extension of the notification period from 72 to 96 hours responds in particular to a request from smaller operators, also addressing the issue of weekends." To what extent does the Commission expect that this could result in data subjects being informed later, that they can only later protect themselves against the consequences of the data breach (such as changing passwords and being alert to phishing messages) and that the risk of damage as a result of the data breach will therefore increase?

- Is it taken into account that the risk levels reported in data breach notifications may be underestimated? The Dutch Data Protection Authority (AP) observes that organizations affected by a data breach often (consciously or unconsciously) underestimate the risk to those involved. This is particularly the case for data breaches resulting from cyberattacks. For example, in 2023, an average of 69% of organizations affected by a serious cyberattack underestimated the risk to those involved. In 54% of cases (a total of 330 data breaches), those affected were not informed after a serious cyberattack, even though they should have been. (Source: AP Data Breach Report 2023, p. 5). The supervisory authority can currently still oblige organisations that have reported a data breach to the supervisory authority, but not to the data subjects, to inform the data subjects as well. Interventions by the data protection supervisor could now result in tens of thousands of data subjects finally being informed. With the proposal the supervisory authority will lose this "corrective" function of the data breach reporting obligation. Could the proposed restriction to high-risk data breaches therefore lead to situations in which data subjects are not notified about breaches affecting them? Could the proposed change make these individuals extra vulnerable to fraud, identity theft and cybercriminals?

Article 35 (Data protection impact assessment)
Sheet 37 of the presentation by the Commission states: "The adoption of the lists by way of an implementing act provides more legal certainty to controllers as such act is legally binding."
Questions: the first three questions (see above) regarding Article 33 apply here accordingly.

Article 41a GDPR (Implementing acts on the definition of 'personal data' and pseudonymisation)
Question: Because the implementing acts would relate to the definition of personal data, this is a core element that does not lend itself to elaboration in implementing acts. Such implementing acts might, after all, affect the scope of the fundamental right to protection of personal data. While fundamental rights can be restricted, this must be carefully considered and should not be done in an implementing act. What is the Commission's view on this?

Cookies (Article 88a GDPR)
Questions:

- Could the Commission clarify what Article 88a(2) implies in comparison to the current ePrivacy Directive regime and if this includes a broadening of the current regime of exemptions? Could the Commission provide examples of such exemptions in practice?

- Could the Commission clarify if the phrase "processing is lawful" (sheet 40 of the presentation) implies that the controller according to Article 88a(3) does not have to comply with Article 5 and 6 GDPR and no balancing test is needed for such processing to be lawful? If so, how can these exemptions still be considered "narrow"?

- Could the phrase "measure the audience" in Article 88a(3)(c) be defined or specified, to exclude that controllers use this exception to justify broader behavioural analytics, profiling, personalisation or optimisation activities that exceed the intended narrow scope of this phrase?

- Could the Commission clarify what "the subsequent processing [...] is lawful" (sheet 40 of the presentation) means for Article 6(4) GDPR? How does the response of the Commission relate to the wording of Article 88a(4) which only seems to apply where consent is being given?

- Are cookies, following the amendment to Article 4(1) GDPR, excluded from the definition of personal data because the controller is unable to determine the identity of a natural person, with the consequence that the requirements for access to terminal equipment are then governed exclusively by Article 5(3) of the ePrivacy Directive? If so, for which specific activities does Article 88a apply?

- The proposal does not indicate which level of GDPR administrative fines would apply to the new articles 88a – 88c proposed to GDPR (eg. regarding cookies and development of AI systems). Should Article 83 be amended to add the threat of administrative fines for Articles 88a - 88c?

Relationship with Article 5(3) ePrivacy Directive
Questions:

- On sheet 39 of the Commission's presentation of 1 December, the Commission stated about the partial removal from the ePD to Article 88a GDPR: "Those cases should be brought under the strong protection framework of the GDPR, creating a single regime" (sheet 39). Could the Commission clarify if by the wording "strong protection framework of the GDPR" it considers this a stronger protection than under Article 5(3) ePD? If so, why?

- Could the Commission clarify what it means to implement Article 5(3) into the GDPR, especially with regard to the confidentiality of communications (Article 7 EU Charter) since the GDPR is based upon Article 8 EU Charter?
- Could the Commission clarify if the sentence "Article 5(3) of the ePrivacy Directive is maintained for connected devices of legal persons and non-personal data" (sheet 39) implies that the exceptions of Article 88a(3)(c)(d) do not apply (accordingly) for such data? Does this mean that the protection for personal data is in fact lower than for connected devices of legal persons and non-personal data?

2. <u>Single Entry Point</u>

- The NIS2, CER, DORA and GDPR are already or will be implemented on a national level. Member States already developed and invested in national entry points and registration tools, taking into account their own national characteristics. Could the Commission clarify how it plans to integrate this solution within the already existing national structures, given the fact that these structures also vary from one Member State to another?
- Which incident notifications processes will at the end be modified on both EU and national level?
- Notifications often include sensitive information and it is therefore important that entities have a strong and trusted relationship with the organization they have to notify to, in this case the national CISRTs. Notifying to an (unknown) EU organization could be experienced as an even higher burden for entities to notify. How will the Commission make sure that this relationship remains unchanged?
- How does the Commission intend to guarantee the national competences with regards to incident reporting, given the fact that entities will report directly and firstly via the EU Single Entry Point?
- How does the Commission envisage interaction / communication and cooperation with national competent authorities in the context of a timely incident response, especially incidents that have only a national impact?
- Many of these companies, especially SMEs, mainly conduct their operations within a single or a few Member States. How will creation of a EU Single Entry Point provide added value for this large group of entities?
- The centralization of all incident notification obligations within one platform, and more specifically the registration 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 have considerable consequences. How will the Commission make sure that the integrity and confidentiality of this information remains unchanged?

3. <u>P2B</u>

- The Commission explained that some provisions from the P2B will be maintained, such as transparency measures on restriction, suspensions and termination and complaint handling. Could the Commission give a list of provisions (and what part of these provisions) that will be maintained and explain in which regulation they will be covered in the future?
- Also the Netherlands would be interested to hear more about how this transitory process will look like?

4. <u>EDIB</u>

- The Digital Omnibus currently does not foresee a formal cooperation mechanism among national authorities concerning cloud switching or cloud interoperability. This is essential, given that the enforcement of the Data Act is based on the country-of-origin principle, and that the concentration of very large cloud operators in two specific Member States necessitates a way to formally organize potential support from the relevant national authorities of European colleagues. The described tasks of the EDIB now specifically do not include coordination of oversight on the provisions regarding data processing services.
- How will the Commission enable coordination of the oversight by the competent authorities for Chapter VI and Chapter VIII of the Data Act?

5. **Cloud provisions**

- The Commission proposes to exclude custom-made cloud services from the scope of ChapterVI of the Data Act, with the exception of the obligation to reduce and ultimately remove switching and egress charges. Assuming this exclusion would take effect, the interpretation of what precisely qualifies as 'custom-made' service generates a lack of clarity and predictability for users especially in relation to the custom-made services already addressed in Article 31(1) of the DA (Recital 17 of the Omnibus).
    - How does the Commission think this will affect the market?
    - Would the exception be applicable also when the customization takes place via third party services provider that operates the changes?
    - In light of these amendments how would the Commission envisage upholding the initial effort to remove the lock-in effect for users?
- Regarding the proposal to exclude SME and SMC providers from some of the provisions in Chapter VI, what is the average contract duration for the designated providers and how does this proposal then affect the market compared to the original Data Act provisions?

***

NL Written Comments on AI timelines

1. **Application date**
   Can the Commission clarify how it will ensure clear and predictable timelines for the implementation of the AI Act in the scenario of the proposed commission decision? Especially when not all harmonised standards are fully available?

2. **Registration of AI systems classified as non-high risk**
   What is the European Commission's estimate of the administrative burden or cost savings for companies resulting from this change?

3. **Processing special categories of personal data**
   Can organisations use this legal basis to collect new special categories of personal data or can they only process data that has been collected earlier for other purposes? Which concrete examples of non-high risk AI-systems are there for which the Commission considers it necessary to broaden the legal basis?

4. **Notified bodies and Notifying authorities**
   Can the Commission confirm that any notified body for products within the scope of Annex I, section A, that is already competent to assess AI in these products, is considered competent as required in article 43.3? Can the Commission confirm that the notifying authorities for products within the scope of Annex I, section A are entitled to designate and notify notified bodies under the AI Act, without the need to be designated as notifying authority under the AI Act?

5. **AI Literacy**
   Can the Commission elaborate on what 'measurable promote and support instruments' they envisage for this obligation for Member States and how the revised Article 4 legally defines the division of responsibility between the European Commission and the national Member States regarding the financing and execution of AI literacy initiatives?

***

Previous (1st round) NL questions about the GDPR, part of the document "NL initial written comments and questions on Omnibus VII – Digital Omnibus", 26 November 2025

Submitted on 26 November 2025

Update 5 December: Text boxes indicate which questions were partially or fully answered by the Commission at the AGS meeting on 1 December. NL has not yet seen any answers to the other questions and comments.

GDPR

In general, a scrutiny reservation applies to the amendments to the GDPR.

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

- Remark: The proposal emphasises that the applicability of the GDPR depends on whether the data constitute personal data from the perspective of the controller. The final sentence of the drafting proposal for Article 4, paragraph 1, makes it no longer relevant whether the data would still constitute personal data if they were provided to a third party. If the data did constitute personal data for that third party, the GDPR would fully apply to that third party, so that protection is maintained.
- Question: However, the explanatory memorandum to the proposal for Article 4, paragraph 1, needs to be tightened up. On page 10 of the Commission proposal it states that "some of the provisions seek to codify interpretations of the Court of Justice of the European Union, such as with regard to pseudonymisation". Recital 27 also gives the impression that it concerns codification. However, the last sentence of the proposal for Article 4, paragraph 1, does not constitute a codification of the case law of the Court of Justice, but rather an amendment to it. Recital 27, in its current wording, does not (yet) indicate that, according to case law, a high threshold applies to the question of whether pseudonymised personal data are not personal data for others. An example is the SRB judgment of 4 September 2025 (C-413/23 P). In it, the CJEU emphasises that "it is settled case-law that (…) it is not required that all the information enabling the identification of the data subject must be in the hands of one person" (see paragraph 99 and paragraphs 83-85). Article 4, paragraph 1, constitutes an amendment to this.
    - For the sake of legal certainty, is it possible to reflect in recital 27 that Article 4, paragraph 1, forms an adjustment to the case law on this point? Could the Council Legal Service and the Legal Service of the Commission reflect on this?
- Question: Can the Commission provide examples of situations in which, according to the amended definition, personal data no longer exist, but in which they still constitute personal data today?
- Technical question: Would a controller still need to put in place a data processing agreement to meet the article 28 GDPR requirements with a processor when the data is not personal so far as the processor is concerned? Would a controller still need to put in place appropriate safeguards with a recipient in a third country under Chapter V of the GDPR, if the data is not personal so far as the recipient is concerned?

***Update**: the first sub-question is answered orally in the AGS of 1 December 2025: Art. 28 GDPR remains applicable for the controller.*

- Technical note: Article 4(1) contains the phrase "that entity cannot identify the natural person to whom the information relates." According to the Advocate General in the EDPS/SRB case, "it is only where the risk of identification is non-existent or insignificant that data can legally escape classification as 'personal data'." (see paragraph 57 of the Advocate General's Opinion and see the Breyer judgment, paragraph 46). This could be referred to in recital 27.

Articles 4(38), 5(1)(b) and 13(5) GDPR (Scientific research)

- Scrutiny reservation: A scrutiny reservation is required to examine the meaning and impact. This is also relevant because a broad "research" definition allows for quick recourse to the exception to the information requirements under the new Article 13(5) GDPR.
- Question: Because scientific research can be "any research," this is a very broad definition. Recital 28 of the proposal refers to "academic, industry, and other settings." Does this definition exclude the possibility that, for example, large tech companies would process personal data under the guise of pseudoscientific research?
- Technical question: It is not yet clear what the relationship is with Recital 159 of the current GDPR, which also concerns scientific research. Can this be clarified?
- Technical question: Recital 32 states that "The processing of personal data for the purpose of scientific research therefore pursues a legitimate interest within the meaning of Article 6(1)(f) of Regulation (EU) 2016/679, provided that such research is not contrary to Union or Member State law." Could a reference to Article 6, paragraph 1(e), of the GDPR be added to this? This is important because Article 6(1)(f) of the GDPR does not apply to processing by public authorities exercising their functions, while public authorities, such as universities belonging to the government, may be responsible for conducting scientific research. Furthermore, it is conceivable that private institutions sometimes have a statutory duty in scientific research.

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

- Remarks: This is a very broad exception to the prohibition on processing special categories of personal data, which is linked to broad terms such as "AI system," "AI model," "training," and "operation." This provision lacks a proportionality or necessity test. According to recital 33, this exception is included "in order to not disproportionately hinder the development and operation of AI and taking into account the capabilities of the controllers (…)". The lack of a proportionality and necessity test conflicts with Article 52 of the EU Charter of Fundamental Rights. According to that article, a restriction of a fundamental right must be necessary for an "objective of general interest" or for the protection of the rights and freedoms of others, and its proportionality must be assessed in the specific case. In addition, it seems hard to explain why AI, that is especially risky, would meet the criteria of Article 52 of the Charter, while any other form of processing (e.g a traditional database or algorithms) would not be allowed under Article 9(2) GDPR.
    - Question: Could the Council Legal Service and the Legal Service of the Commission reflect on this?
- Remark: Article 9(5) is drafted with internal contradictions an is likely leading to more bureaucracy. This provision demands organisational and technical measures to "*avoid v the collection and otherwise processing of special categories of personal data*" as a condition to a clause to lift the prohibition to processing of special categories of personal data, while simultaneously permitting their processing when deletion is impossible. This is a systematic inconsistency. It is illogical to permit an exception that is based on the impossibility of avoiding the thing you require to be avoided.
- Remark: Article 9(5) repeats some principles from Article 5 GDPR, but not all of them, for example, not the legal basis and necessity. This could (wrongly) lead to the a contrario interpretation that not all principles of Article 5 GDPR apply.

Article 9(2)(L) GDPR (Biometric data for confirming the identity)

- Remarks: This is an interesting thought: biometric data processed for the purpose of uniquely identifying a natural person are considered special personal data, but biometric data processed to confirm identity are not special personal data. The ratio of Article 9, paragraph 1, provides no reason to include identity confirmation within its scope. If that had been intended, the words "biometric data" would have sufficed and the further qualification "for the purpose of uniquely identifying a person" could have been omitted. Also, the WP29 differentiated in its 2012 advice between biometric identification (a one-to-many matching process: who are you?) and biometric verification/authentication (a one-to-one matching process: are you who you say you are?). The proposed amendment could therefore be a welcome clarification.
- Question: Is the EC convinced that the proposed text is compatible with recital 51 of the current GDPR, which sets out that "the processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person"? Note that the recital links "identification and authentication" to "processing of special categories of data", appearing in Art. 9.

***Update**: this question is answered in the AGS of 1 December 2025. Page 31 of the presentation by the Commission states: "Proposed amendment does not change the rule that biometric are personal data which undergo processing by a specific technical means. For example, there is no change regarding where photographs are considered processing of special categories of data."*

Article 12(5) GDPR (Requests from data subjects)

- Question: Protection against abuse already exists: the current text already provides the necessary options for refusing manifestly unfounded of excessive requests, including access requests. Couldn't the examples mentioned in Recital 35 already lead to refusal of requests on the basis of the current Article 12(5)? How often does this pose a problem?
- Question: In the case of excessive requests, the burden of proof falls on data subjects to refute that the request is excessive (Recital 35 of the proposal). According to the new Article 12(5) it is sufficient that the controller has "reasonable grounds to believe that it is excessive". However, citizens often lack the information to specify access requests, especially if they are unaware of what authorities do with their data. Doesn't this reduced burden of proof mean that access requests in such cases may be deemed excessive, even if citizens did not have information to specify the request?
- Question: What impact does the Commission expect this proposal to have on the number of complaints to supervisory authorities?
- Question: The limitation to only the "protection of their data" seems too limited and does not seem to correspond with the case law of the Court of Justice. Could the Council Legal Service and the Legal Service of the Commission reflect on this?

Article 13(4) GDPR (Exception to the information obligation)

- Question: Although the rationale behind this provision is supported, it appears to lead to increased complexity. The existing exception to the information obligation in Article 13(4) is now supplemented with three exceptions to exceptions. On balance, the exception to the information obligation hardly seems to apply anymore, because the information obligation revives when the data is, for example, forwarded. The proposal also effectively creates complications due to vague concepts such as "clear and circumscribed relationship". In what way would the proposed Article 13(4) lead to simplification? Can the Commission provide examples of cases in which this leads to simplification?
- Question: The identical exception to the information obligation in Article 14, paragraph 5(a), remains unchanged. However, standardisation of the exceptions in Articles 13 and 14 seems necessary where comparable cases are involved.

Article 22 GDPR (Automated individual decision-making)

- Remarks: In itself, it's useful to have more readable, clearer provision. In the current provision, there is a right for the data subject "not to be subject, unless." In legal practice, this is interpreted as a prohibition for the controller. The new wording reverses this: automated decision-making is not "prohibited unless," but "permitted, unless." As long as nothing material changes, this need not be problematic and may even be clearer than the current, complex wording.
- Questions:
  - What exactly is meant by the addition 'regardless of whether the decision could be taken otherwise than by solely automated means'? This seems to suggest that necessity does not have to be established and seems to undermine point 2(a). This calls for further elaboration. This addition seems to be a reduction of the level of protection, as it also concerns decisions which produce legal effects.
  - How does this addition relate to the phrase "is necessary" at the beginning of point a?
  - Recital 38, final sentence, suggests that if an equivalent alternative is less intrusive, that alternative should be used. Could this be included in Article 22?

Article 33 GDPR (Notification of a personal data breach)

- Remarks: The wording is clearer by making it an 'if' instead of an 'unless' clause. This makes it easier to comprehend and to comply with. The standard extension of the term can be problematic though, as this obligation contributes to maintaining and restoring trust in the handling of personal data. Transparency regarding the nature of the data breach, its likely scope and the nature of the potential damage, the efforts being made to repair the damage, and advice to the public and customers to best understand the consequences for their own interests are necessary measures for maintaining and restoring that trust.
- Questions:
  - Why is it necessary to give the Commission the power to establish the lists and templates? Why was this not left to the EDPB?

    ***Update**: this question seems to be partially answered in the AGS of 1 December 2025. Page 36 of the presentation by the Commission states: "The Commission stated in its presentation in the AGS of 1 December: "The adoption of the list and templates for data breach notifications by way of an implementing act provides more legal certainty to controllers as such act is legally binding." A numbers of questions remain (see additional questions of 5 December).*

  - What benefit is achieved by extending the period from 72 hours to 96 hours? The purpose of the reporting obligation is to prevent data breaches and, if they occur, to minimise the consequences for those involved. The sooner it is reported, the better. The regulation already allows for reporting later than 72 hours, provided a reason is provided. Why isn't this system being maintained?

    ***Update**: this question is partially answered in the AGS of 1 December 2025. Page 36 of the presentation by the Commission states: "The extension of the notification period from 72 to 96 hours responds in particular to a request from smaller operators, also addressing the issue of weekends." The choice for 96 hours is because not every Member State uses the same working days. A numbers of questions remain (see additional questions of 5 December).*

  - Could it also be clarified whether this new threshold and new term also apply to the notification obligation for processors under Article 33(2) GDPR, for example by a reference in Article 33(2) to the conditions of Article 33(1)?

Article 35 GDPR (Data protection impact assessments)

- Scrutiny reservation: It is positive that this proposal makes the black and white lists, which indicate when DPIAs are and are not required, mandatory. However, the proposal removes this power from the national supervisory authorities and gives the EDPB the power to make a proposal, which may or may not be adopted by the Commission. According to recital 40, this can contribute to harmonisation. However, it is questionable whether it is proportionate to remove the power from the national supervisory authorities, as they are close to the practices in their own Member States. If this is proportionate, the question remains why the Commission, rather than the EDPB, needs to be empowered to adopt the lists (and to adopt the DPIA template and methodology). A scrutiny reservation is required to consult the Dutch data protection supervisor and the EDPB on this matter.
- Question: Why is it necessary to grant the Commission the power to adopts the lists and the DPIA template and DPIA methodology? Why was it decided not to leave this to the EDPB?

> ***Update**: this question seems to be partially answered in the AGS of 1 December 2025. Page 37 of the presentation by the Commission states: "he adoption of the lists by way of an implementing act provides more legal certainty to controllers as such act is legally binding." A numbers of questions remain (see additional questions of 5 December).*

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

Remarks:

- With article 41, the Commission claims interpretative authority to decide the borders of personal data, back from the co-legislators, member state supervisory authorities and the CJEU. That can hardly be regarded a simplification. It also may lead to more fragmentation and differences, because the Commission may provide such implementing acts only for certain categories for controllers and recipients. This could lead to different interpretations of the concept of anonymisation between various sectors or, worse, actors within a sector. This introduces uncertainty.
- It is undesirable to further define what constitutes personal data through implementing acts. It is preferable to do this through regular legislation, as this goes to the heart of the matter, or through the EDPB. It would have been more suitable if the Commission would have integrated a more concrete definition – or conditions – in the proposal. Article 41a(1) seems to essentially boil down to this: if you apply these means and criteria, the resulting data no longer qualify as personal data. This effectively suggests a change or restriction of the definition of "personal data." Article 41a links pseudonymisation to the question of whether it still constitutes personal data. This does not seem to be something that can be regulated through implementing acts, as these are elements that touch on a core definition of the GDPR. Implementing acts must prevent deviations from or interference in a definition.
- In practice, there is a need for clarity regarding what is expected in the area of pseudonymisation and what constitutes "good" pseudonymisation. Encouraging pseudonymisation as a protective measure is to be welcomed. If the additional rules pertain to techniques that controllers should use or what constitutes best practices for pseudonymisation, that would be useful. It is preferable to have this done by the EDPB, where this task is now assigned.

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?

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

This article also contains good elements, but requires further clarification in some areas.

Questions:

- As in Article 88a, this article also doesn't mention the option to withdraw consent in paragraphs 1 and 6. How does this relate to Article 7?
- Could paragraph 1, paragraph (b), be split into paragraphs (b) and (c)? The current formulation of paragraph (b) could unintentionally suggest that a refusal of consent must be related to an objection based on Article 21, paragraph 2, of the GDPR (objection to data processing for direct marketing purposes). Incidentally, it is unclear why this paragraph mentions the 'right to object', unlike Article 88a.
- The exception for 'media service providers' in Article 88b(3) is quite broad due to the broad definition in Regulation 2024/1083. Does this exception also apply to Article 88a or only to Article 88b? Do the current cookie rules lead to a change for media service providers?

> ***Update**: this question is answered in the AGS: "Exemption from the obligation to respect a signal transmitted through automated means indicating consent preferences of a user ≠ exemption from asking consent." (page 44, presentation of the Commission)*

- Isn't it necessary for all parts of Article 88b to enter into force at the same time? Paragraph 5 stipulates that paragraphs 1 and 2 apply after 24 months, so there must be appropriate online interfaces at that time that take automated and machine-readable means into account. However, paragraph 6 and 7 stipulate that web browsers are required to provide automated and machine-readable means after 48 months. Are paragraphs 1 and 2 workable if the provision on web browsers and automated and machine-readable means has not yet entered into force?
- Paragraph 6 contains an exception for SME web browser providers. Are they exempt from the obligations under Articles 88a and 88b?

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

Remarks:

- The proposed article 88c aims to create a legal basis for the processing of personal data to develop and operate an AI system under the AI Act. The legal basis will be legitimate interest, "except where [etc]." The EDPB has last year adopted an opinion (https://www.edpb.europa.eu/news/news/2024/edpb-opinion-ai-models-gdpr-principles-support-responsible-ai_en) on the use of personal data in the development and deployment of AI models on 18 December 2024. This opinion concludes that the GDPR allows for the processing of personal data for this purpose, even without the data subject's consent, based on the "legitimate interest" (Article 6, paragraph 1(f) of the GDPR). Whether this basis can be used depends on the circumstances of the case. It must be established that the intended processing is necessary for the purposes of the legitimate interest and that the interests or fundamental rights and freedoms of data subjects affected by the processing of personal data do not outweigh the legitimate interest served by the processing.
- This provision is broad, applying to both "development and operation" and the broad definition of AI systems. The fact that these data processing operations are not necessarily expected by data subjects in all cases is underemphasised. The implications for the data minimisation principle are also underemphasised.
- The generally formulated interests in recitals 30-31 of the proposal do not provide sufficient justification. It must concern a legitimate interest in the specific case.
- It is difficult to explain making such a broad exception for AI, while such an exception does not apply to (less risky) systems outside the context of AI.

Questions:

- By pointing to Article 6(1)(f) as the basis for developing and deploying AI models, this may create the impression that the use of 6(1)(f) is always possible and preferable, even when it is not necessary or proportionate and regardless of the use of safeguards. Combined with the other proposed amendments, such as those to Articles 9 and 88a of the GDPR and Article 4a of the AI Act, even highly sensitive data will soon be able to be used in AI models under 6(1)(f). Could the Commission elaborate whether this is indeed intended?

> ***Update:** this question is answered partially in the AGS: "Proposed amendment clarifies the current GDPR rules: a controller may rely on Article 6.1.f for pursuing a legitimate interest in the context of AI development and operation, where all conditions of that provision and the other GDPR requirements are met." A numbers of questions remain (see additional questions of 5 December).*

- If not, given the already applied EDPB-advice, what is the added value of the proposed Article 88c? Is the goal merely to clarify and confirm what can already been done in practice? Does the Commission, with the second phrase of the proposed Article 88c, agree with the conditions and safeguards formulated by the EDPB in its opinion?

Update: *this question is answered partially in the AGS: "It does not create a new ground for lawful processing; the development and operation of AI does not per se qualify as legitimate interest. It reflects EDPB Opinion 28/2024." A numbers of questions remain (see additional questions of 5 December).*

- What practical effect can be expected if the phrase "except where other Union or national laws explicitly require consent" is implemented, also considering the cross-border aspects of AI?
- The safeguards mentioned in the second paragraph should largely follow from Article 5 of the GDPR. What is the difference between an "unconditional right" and the existing right to object under Article 21 of the GDPR? And how does "enhanced transparency" differ from the existing transparency obligations under Articles 13 and 14 of the GDPR and Article 5, paragraph 1(a), of the GDPR?

Relationship between the GDPR amendments and Directive (EU) 2016/680 (Law Enforcement Directive):

Question: According to recital 43, the necessary amendments to Directive 2016/680 and other EU data processing instruments will be implemented after the Digital Omnibus proposal is adopted, "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." What is the underlying reason why these adjustments only take place at a later stage?

AUSTRIA

Please note that the following comments are of preliminary nature. AT is still analysing the Omnibus VII (e.g. in light of constitutional concerns) and therefore raises a scrutiny reservation.

ad Digital Omnibus on AI

Article 1 (AI Act)

- **Paras 12 and 33**: *How can negative effects on market actors, in particular the public sector, be prevented in case the dates of entry into application do not change as a result of the Omnibus negotiations?*
  - It must be stressed in this context that **notifying authorities cannot notify conformity assessment bodies until NANDO codes are made available to allow registration at EU level**. This means that if the Omnibus negotiations take longer than August 2026, **market actors will not be able to make use of notified bodies for conformity assessment bodies**, whether as part of their regular conformity assessment procedures in the case of Annex I, as required for law enforcement and other sensitive areas in the case of Annex III point 1, or voluntarily in the absence of harmonised standards in the case of other points of Annex III. **It is strongly encouraged to continue developing the implementing act for the NANDO codes as planned while negotiations for the Omnibus are ongoing in order to ensure a modicum of legal certainty for market actors, including law enforcement**.
- **Paras 10, 18, 20 and 26**: *On which legal basis has Cion based its proposed provisions affecting the internal organisation of Member States, their public authorities and infrastructures?*
- **Para 25**:
- *How will the proposed strengthening of the AI Office's responsibilities be matched in terms of the requirements applied to the AI Office as market surveillance authority, in particular independence?*
- *Does the AI Office foresee an imminent evolution into an independent agency?*
- *On which legal basis does the AI Office plan to oversee providers and deployers of high-risk AI systems in the areas of law enforcement, border control, immigration or asylum?*
- **Para 31**:
- *Has the proposal to determine the entry into application of requirements for high-risk AI systems on the basis of a Cion Decision been assessed in terms of its validity as a legal instrument for such a purpose?*
- *If so, which legal basis provides Cion with a mandate to unilaterally specify the entry into application of a broad range of requirements?*
- *Based on which objective criteria does Cion plan to determine that standards are available for an entry into application to be justified?*
- *What effect does the focus on the availability of harmonised standards offering a presumption of conformity have on other valid means of compliance, including conformity assessment by notified bodies?*
- *What are the consequences of postponing the applicability of high-risk AI rules for Art 86 AI Act, which is stated in Section 4: Remedies, but which is only applicable for high-risk AI systems as per Annex III?*

Example: In many sectors (loan applications, electricity, rental, mobile phone contracts) AI systems are used to calculate a person's creditworthiness based on specific characteristics and data. This score is then used to decide whether or not to enter into a contract with that person.

In the case of an unfavourable decision, the consumer currently has no real possibility to challenge it because he/she lacks the necessary information about the AI system used or is even unaware that AI was used in the first place. Consumers need to be informed about the usage of high-risk AI (Art 26 (11 AI Act) and they need an individually enforceable right to explanation (Art 86 AI Act) in order to get specific information about the respective AI system and the decision made. Only then consumers can ascertain further rights, e.g. claims for

damages in case of unfavourable credit terms or a wrongful refusal of a loan application. Postponing high-risk-AI rules would further increase this lack of legal protection for consumers.

Additional questions regarding Art 1 (AI Act)

- **Para 2**: With the proposed extension of the possibilities for testing under real-world conditions to all sectors listed in Annex I Section B, it appears a competence gap has emerged where existing market surveillance authorities for these sectors would not be able to approve testing plans for testing under real-world conditions (due to a lack of mandate provided by the AI Act).
  - *How, in this case, would tests be supervised?*
  - *According to which criteria should testing plans evaluated and how can the protection objectives set out in Art 1 AI Act be met if these products do not need to comply with any other requirements of the AI Act?*
  - It should be noted that it is not clear how these changes affect LEAs.
- **Para 4**: *How does the proposed change improve legal certainty of providers and deployers in terms of AI literacy and how does this change affect existing AI literacy programmes?*
- **Para 5**:
  - *Under which concrete conditions would the proposal to allow the processing of personal data for the detection and correction of bias for all providers and operators of AI systems apply, as the phrasing in the proposal ('may apply', 'where necessary and proportionate') is very vague?*
  - *In addition, as this provision would also have to be monitored by one or more market surveillance authorities, how should these market surveillance authorities proactively and reactively monitor all AI systems and even AI models which are not classified as general purpose AI models?*
  - *Has the impact of this proposal on the regulatory burden of providers and deployers as well as the administrative burden for competent authorities been assessed?*
  - It should be noted that it is not clear if or when LEAs can make use of this provision.
- **Para 6:** Under current Art 6 (4), a provider who considers that an AI system referred to in Annex III is not high-risk shall document its assessment before that system is placed on the market or put into service. The provider is subject to the registration obligation set out in Article 49(2). The question of the applicability of the exemption in Art 6 (3) is initially based on a self-assessment by the provider. *How can you ensure the same level of information for affected stakeholders and public control?*
- **Paras 6, 14, 32**: *How can legal certainty for providers and deployers of AI systems be ensured if the registration of high-risk AI systems which are not deemed to be high-risk by providers of these AI systems is removed, as the powers of market surveillance authorities remain in place and it remains unclear what exactly a preparatory task is?*
- **Para 10**: *Could you explain the legal basis providing Cion with a mandate to propose an integration of the assessment of the requirements for conformity assessment bodies seeking notification for the AI Act into the assessment of requirements for other legislation set out in Annex I Section A, which would result in existing notifying bodies having to assess competence requirements for the AI Act and is therefore a matter of the internal organisation of Member States?*
- **Paras 12 and 33**: *On which scientific basis or using which internationally standardised definitions has Cion developed the technology-specific codes for the notification of conformity assessment bodies (known as NANDO codes)?*

• **Para 13**: *How will the actual assessment of the quality management system be ensured, as the proposed wording of the requirements for integrating the assessment of quality management systems into existing conformity assessment procedures for Annex I does not take into account that some Annex I products do not contain requirements related to quality management?*
• **Para 17**: *How will the involvement of national authorities responsible for the AI Act in the regulatory sandbox for general-purpose AI models and systems be ensured in light of other provisions of the AI Act which call for close cooperation between regulatory sandboxes for the AI Act?*

• **Para 18**: *Could you explain the legal basis which provides Cion with a mandate to propose in paragraph 1 point (d) to determine the cooperation between national competent authorities involved in the regulatory sandbox via a delegated act (which precludes Member State involvement), which is a matter of the internal organisation of Member States?*
• **Para 20**: *Can you explain the legal basis concerning voluntary testing agreements between Cion and certain Member States compel even those Member States who have not entered into this agreement to ensure e.g. access to physical infrastructure for these tests?* E.g. if FR, DE and Cion sign a testing agreement for testing AI systems used within civil aviation, AT would need to ensure that airports will participate in these tests by providing access to their infrastructure; this proposal therefore infringes against the sovereignty of Member States.
• **Paras 21 and 29**: *How will a distortion of competition due to the proposal to not only extend the possibility of applying simplified quality management from micro-enterprises to SMEs and SMCs, but also removing the condition that these companies must not have any partner companies or affiliated companies be prevented?*
• **Para 22**: *How will the right of Member States to access members of the scientific panel, as enshrined in Art 69(1) AI Act be ensured if Cion's obligation to ensure this access is removed?*
• **Para 24**: *How will the proposed guidance instead of an implementing act to specify the post-market monitoring plan improve legal certainty?*
• **Para 25**: *How will the proposed strengthening of the AI Office's responsibilities be matched in terms of the requirements applied to the AI Office as market surveillance authority, in particular independence? Does the AI Office foresee an imminent evolution into an independent agency? On which legal basis does the AI Office plan to oversee providers and deployers of high-risk AI systems in the areas of law enforcement, border control, immigration or asylum?*
• **Para 26**: *Could you further elaborate on legal basis which would provide Cion with a mandate to propose that Art 77 authorities with very strict independence requirements (such as the "Volksanwaltschaft" in AT) would be obliged to inform other authorities about the details of their investigations?*

ad Digital Omnibus
Article 1 (Data Act)

· **On Chapter IXa (European Data Innova□on Board, EDIB):**

· AT supports the development of the EDIB into a genuine strategic innovation body to ensure the implementation of the Omnibus data acquis 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. *Will EDIB have an essential role in this process of reviewing the body of data legislation? How does the EC intend to strengthen the role of the EDIB and enhance its decision-making capacity?*

· **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 the EC 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). Could the EC please explain its rationale concerning this lacking role of the EDIB?

- **On Chapter V (B2G Data Exchange):**

- *Why does the EC deem that clarifications regarding trade secrets in relation to the public sector are necessary?* 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 Art 17(5), there no longer appears to be a right to lodge a complaint against an obligatory request by a public sector body, the EC, the ECB or another Union body to make data available. *In this context, could the EC please explain the rationale for the proposed amendments and deletions in Art 14, 15 and 17?*

- 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 the EC please indicate whether further clarification on this concept will be provided, or whether a commonly accepted interpretation of this wording already exists?* Could Cion list the new elements in the proposal concerning the reuse of data and documents held by public sector bodies and public undertakings (see esp. Art. 32i ff)? What are the differences (if any) to the current regime (especially Directive 2019/1024)?

- 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?*

Additional questions regarding Art 1 (Data Act)

- **On Chapter I (General Provisions) Art 2 (Definitions):**

- The definition of "**document**" is limited to **non-digital content**. At national level, there is a notion of "digital document", 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 the EC please provide the reasons for this major change in the 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 the CIon provide its rationale?*

- **On Chapter VII (unlawful disclosure of non-personal data in a cross-border context) Art 32:** Currently a cooperation mechanism between competent authorities of the MS does not exist. *Does the Cion envisage a cooperation mechanism and a technical instrument for cooperation?*

- **On Chapter VIIa (Data Intermediation and Data Altruism):**

· *Could the 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?*

· *Does the CIon envisage issuing guidelines or other supporting documents for the actors concerned?*

· *Could the Cion elaborate onits rationale behind waiving **reporting and transparency requirements** for data altruism organisations (DAO), and how it intends to ensure that only trustworthy actors operate in the data economy?* Concerning 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.

· On Art 32a and Art 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 the EC envisage a more future-proof **technical system**, if Cion is to assume central responsibility?*

· **On Chapter VIIb (Free flow of data)**

· Concerning **Art 32h (Prohibition of data localisation requirements)**: 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?*

· **On 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 the 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?*

· **On Chapter VIIc High Value Datasets (HVD) and concerning Art 32v (5):** *Could Cion 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.

· **On charging rules and concerning the Articles 32n, 32p, 32q, 32y:** *Could the CIon please explain why there are different articles on charging instead of consolidating them into one article against the backdrop of a general simplification?*

· **On Data Spaces in general:**

· 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. Why has the EC chosen to not include essential horizontal provisions concerning data spaces

and in particular possible links to data intermediaries?

· Furthermore, there are no explicit references to the European Health Data Space (EHDS) Regulation (EU) 2025/327. In relation to data intermediaries and the EHDS, it should be noted that these are not provided for in the EHDS Regulation. Apart from this specific issue, the inclusion of a reference to the EHDS in the Data Act is not considered disadvantageous, although it should be noted that their areas of application (horizontal vs. vertical) differ significantly.

Article 3 (GDPR)

· **Commission implementing decisions (horizontal):**

· Could Cion further explain the rationale behind the shift of tasks and responsibility currently assigned to the national supervisory authorities (such as the "blacklist" and "whitelist" for the data protection impact assessment) to Cion and not to the EDPB?

· **Art 4(1)(a) – definition of "personal data"**

· Could Cion explain how the addition to the definition of personal data ("*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.*") reflects the CJEU case-law described in para 84 of the SRB-judgement ("*Above all, according to the case-law arising from the judgment of 9 November 2023,* Gesamtverband Autoteile-Handel (Access to vehicle information) *(C-319/22, EU:C:2023:837, paragraphs 46 and 49),* ***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 judgment that – where those data are put at their disposal –* ***those data are personal data both for those persons and, indirectly, for the controller***.")?

· *Would the new addition to the definition prevent situations in which a group of companies distributes their pseudonymised data between different daughter-companies while only one company of the group holds the identifier for the pseudonyms (e.g. mapping table or, in case of encryption, the private key)?*

· Where, according to the new definition, the data processed by a person/entity does not constitute personal data for that particular person/entity, the GDPR would not be applicable with regard to that processing by that person/entity. *Could the new definition lead to unintended results, such as*

- *the possibility to transfer such data to a third country without equivalent protection, where the data subject can be identified?*
- *the possibility to publish such data, thus making it available to others who can identify the data subject?*
- *the possibility to sell such data to criminals in the darknet, who can identify data subjects and misuse their personal data?*

· Regarding the element of "likeliness of re-identification":

- *Are there any new measures or resources foreseen for supervisory authorities to mitigate information disadvantages in relation to the new, subjective element "likeliness of reidentification"?*
- *How can the supervisory authority prove a likeliness to re-identify before the reidentification has factually happened? How are disadvantages for the data subjects handled if the likeliness was only constituted after the factual re-identification (and e.g. data has been transferred as non-personal data into a third country, where the identification has occurred and the data now is personal data again, but outside the scope of Union law)?*

· Where the recipient of pseudonymised data is a person/entity processing personal data for a controller and the controller, but not the recipient can identify the data subject:

- *Would that recipient still qualify as "processor" within the meaning of Art 4(7) and be bound by the GDPR?*
- *If not, how could Art 28 GDPR be applied/enforced?*
- *Would the controller still be held responsible for misconduct of that processor?*

- Where there are joint controllers and the data processed is "personal data" for some, but not all of the joint controllers: *How could Art 26 GDPR be applied/enforced?*

- *Why does the addition to the definition first refer to "person or entity" and then only to "entity"? Is there any connection with the use of the term "person or entity" in Art 47(2)(h) and (j)?*

- *Could the amendment of Art 4(1) have unintended, possibly severe effects on other EU legislative acts regulating processing of data, such as the EHDS?* For example:
  - With the amended definition of "personal data", a lot of entities would not be "health data users" pursuant to Art 2(2)(t)(i) EHDS and therefore would not be obliged to provide health data for secondary use. *How will such impacts on the effectiveness of the EHDS be mitigated, especially in situations where the identifier for health data lies with other companies within a group, potentially with micro-enterprises, which are by default exempt from Chapter IV of EHDS?*

- **Art 4(38) – definition of "scientific research"**

- *How does this definition correspond with current understanding of "scientific research" within the meaning of Art 89 (and, possibly, other relevant legislation)?*

- *Who sets the "ethical standards" and assesses adherence to these standards? How is consistent understanding and application of these ethical standards ensured?*

- *Would the proposed definition also cover research by VLOPs (Meta, Google etc.)?*

- **Art 9(2)(k) – processing for AI purposes *[also relating to Digital Omnibus AI]*:**

- There appear to be several varying legal bases for the processing of special categories of personal data across the Digital Omnibus Proposals.
  - *What is the legal relationship between Art 9(2)(k) GDPR, Art 88c GDPR and Art 4a AIA as proposed by the Digital Omnibus AI?*
  - *Why is the processing of special categories of personal data for the purposes of bias control included in the AIA while the legal bases for the processing of personal data for the development and operation of an AI system is included in the GDPR?*

- **Art 9(5) – processing for AI purposes *[also relating to Digital Omnibus AI]*:**

- *Why are the safeguards mentioned in Art 9(5) not included in the Digital Omnibus AI but in the framework of the GDPR?*

- **Art 12(5) – abuse of the right to access:**

- *What is the rationale for limiting the additional form of excessiveness to requests under Art 15, and not applying it to other rights of the data subjects?*

- Art 57(4) includes a clause concerning excessive requests to the supervisory authority which corresponds to Art 12(5). *Are there specific reasons why no corresponding amendment regarding Art 57(4) is proposed?*

- **Art 13(4) – simplification with regard to information in specific situations where personal data are collected from the data subject:**

- Art 13(4) refers to processing activity that is "*not data-intensive*". According to Rec 36, "*[t]he controller's activity is not data-intensive where it collects a low amount of personal data*".
  - *Does "not data-intensive", besides the quantitative component referred to in Rec 36, also entail a qualitative component?*

- *In how far does this reflect the risk-based approach, e.g. with regard to selective processing of special categories of personal data (not amounting to "large-scale processing" under Art 35(3)(b))?*

- **Art 22 – automated decision-making:**

- *Do the amendments regarding automated decision-making extend the currently existing possibilities, in particular by shifting from a general prohibition to a broader permission?*

- *Could Cion give some examples for automated decisions which are currently prohibited, but would be allowed in future?*

- The question whether "necessary for […] a contract" means that it is the automated decision making that is necessary is subject to a preliminary ruling request pending before the CJEU

(C-568/25). According to the proposed Art 22(1)(a), "necessary" would have to be understood "regardless of whether the decision could be taken otherwise than by solely automated means". *Against that backdrop, could Cion explain how it can exclude that the current data protection standard, to be defined by the CJEU, is reduced by the proposed amendment (cf. Rec 27: "preserving the same level of data protection")?*

- **Art 33(1) – data breach notification:**

- *In case the controller underestimates the extent of the risks resulting from a data breach, and therefore does not notify the supervisory authority in line with the new threshold in Art 33(1), are there any instruments to ensure that data subjects are protected from risks incorrectly not identified as "high risks" by the controller?*

- *In how far does the extension of the time-limit for the data breach notification, in line with the plans regarding a single entry point and single reporting, correspond with time-limits in place other reporting obligations in the digital acquis?*

- **Art 33(6) and (7) – data breach notification:**

- *Could you explain the rationale behind empowering Cion, and not the EDPB, to adopt the list and template?*

- **Art 35(4)-(6c) – data protection impact assessment:**

- *Could you explain the rationale behind empowering Cion, and not the EDPB, to adopt the "blacklist" and "whitelist"?*

- **Art 41a – Commission implementing decision in the context of pseudonymisation:**

- *Could you explain the rationale behind empowering Cion to specify, by way of an implementing decision, means and criteria to determine whether data resulting from pseudonymisation no longer constitutes personal data for certain entities, impair the supervisory authorities' independence with regard to the interpretation of the GDPR?*

- *Could harmonisation and clarity with regard to this aspect alternatively be reached by EDPB guidelines and CJEU case-law?*

- **Art 57(1)(k), Art 64(1)(a), Art 70(1)(h)-(hc) – tasks of supervisory authorities/the EDPB:**

- *Could you explain the rationale behind shifting these tasks currently assigned to the supervisory authorities/the EDPB to Cion?*

- **Art 88c – processing for AI purposes *[also relating to Digital Omnibus AI]*:**

- *Under what circumstances is the processing of personal data "necessary for the interests of the controller in the context of the development and operation of an AI system"?*

- *Why does the proposal refer to "the interests of the controller in the context" of the development and operation of an AI system and not simply the necessity "for the development and operation of an AI system"?*

· As we understand it, the processing of personal data for the purposes of developing AI systems is already allowed under Art 6(1)(f) limited by overriding interests of third persons (see EDPB Opinion 28/2024).

- *What is the benefit of including Art 88c in the GDPR?*
- *Could the same be achieved by adding a Recital while safeguarding legal certainty for controllers by not introducing new provisions that call into question the current legal framework?*

· *Why are the safeguards for the processing of personal data for the interest of the controller in the context of the development and operation of an AI system, as mentioned in Art 88c(2), not included in the context of the changes to the AIA, which already includes a variety of regulations and safeguards for controllers in the context of the development and operation of AI systems and therefore, would be the more appropriate place for such regulations?*

Article 4 (EUDPR)

AT still needs to fully analyse the proposed changes concerning the GDPR and therefore upholds its scrutiny reservation.

· *Could Cion explain why Omnibus VII does not cover corresponding amendments of the LED (such as when the GDPR and LED were negotiated)?*

· *How can problems arising from (temporary) divergence of formally universal concepts of data protection (such as "personal data") be dealt with, e.g. where joint controllers under the LED and Ch. IX EUDPR jointly process operative data?*

Article 5 (ePrivacy)

· The proposed amendment to **Art 5 (3) Directive 2002/58/EC (ePrivacy Directive)** seeks to shift the requirements concerning storing of personal data, or gaining of access to personal data stored in the terminal equipment of natural persons, to the GDPR framework. The ePrivacy Directive, however, 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 (see Recital 48). The two regimes will therefore impose different rules and requirements concerning consent, data protection, and related obligations. For example, controllers will be obliged to respect the refusal of a request for consent for at least 6 months with respect to personal data, while no comparable obligation would apply to non-personal information stored in the terminal equipment of natural persons.

In the case of **'cookies'** however, the most relevant use case of Art 5 (3) ePrivacy Directive, controllers store and access not only personal data but also a wide range of non-personal information stored in the terminal equipment of natural persons (e.g. visited pages, search history, browser information, expiring dates and duration, security specifications etc.). In its judgment in case C-673/17 (*Planet49*) the ECJ clarified that any information, including nonpersonal information of natural persons stored in the terminal equipment of users, are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights.

a) In your view, should both the ePrivacy Directive and the GDPR be applicable in cases where the controller simultaneously stores or gains access, within a single automated, technical, or other procedure (e.g. cookies), to both personal data and non-personal information stored in the terminal equipment of a natural person?

b) If so, does that mean that controllers will be required to comply simultaneously with the different rules and requirements of the GDPR and the ePrivacy Directive when accessing or storing both personal data and non-personal information through one single process (e.g. 'cookies')?

· According to the proposed amendment to **Art 5 (3) ePrivacy Directive,** this paragraph should not apply when the information stored or accessed leads to the processing of personal data. This wording suggests that Art 5 (3) does not apply only in cases where the controller stores or gains access to personal data stored in the terminal equipment of natural persons (as covered by the

first part of the sentence: "constitutes"), but also in cases where non-personal information is stored or accessed that may later lead to the processing of personal data.

· According to the proposed amendment to Art 4 GDPR, information shall not be personal for a given entity where the entity cannot identify the natural person to whom the information relates, merely because another entity can identify that natural person. It, therefore, appears possible that a controller may store or gain access to information stored in the terminal equipment of a natural person, without being able to identify the natural person to whom this information relates, thereby rendering the information non-personal and, consequently, outside of the scope of the GDPR. At the same time, however, if another entity can identify the natural person based on this information than this information can lead to the processing of personal data, meaning that the Art 5 (3) ePrivacy Directive would likewise not be applicable. This interpretation would risk creating a regulatory vacuum contrary to the objectives of the EU data protection regime and to the findings of the ECJ in the case C-673/17.
a) In your view, should Art 5 (3) ePrivacy Directive not apply in cases where a controller stores or gains access to information that is non-personal from the controller's point of view but can lead to the processing of personal data by a subsequent entity?
b) If Art 5 (3) ePrivacy Directive is not applicable in these cases, and considering the fact, that the GDPR would also not apply because the information would not be personal, which consent requirements, if any, should be observed by storing or gaining access to these types of information?

· **Additional questions** regarding the addition of the **subparagraph after Article 5(3) ePrivacy Directive** according to which this provision shall not apply if the subscriber or user is a natural person: It appears that the relationship between Art 5 of the ePrivacy Directive (which applies to the placement of cookies or similar technologies to gain information from a user's terminal equipment) and the subsequent processing of personal data subject to the GDPR is still not sufficiently precise:

· Notably, the relationship between the suggested amendment of the ePrivacy Directive and Article 88a GDPR („Processing of personal data in the terminal equipment of natural persons") needs to be specified (ie. which terminal equipment is – under the suggested new regime – covered solely by Art 5 of the ePrivacy Directive?). **In turn, the exact scope of application of Article 88a GDPR should be (further) specified.**

· *Could you perhaps specify as to how the proposed addition can work in practice if a processor does not have the means to identify as a natural person, or more generally: how can it be assured that the exemption can effectively be applied?*

Article 9 (CER)

· Regarding the proposed amendment to **Art 15, para 1 of Directive (EU) 2022/2557 (CER)**:

· The proposed Art 23a in the Directive 2022/2555 (NIS2) requires ENISA to develop and maintain a "single-entry point." *Why was this regulation included in the NIS2-Directive and not in the revision draft of the Cyber Security Act?*

· *Will there be financial support for Member States in connection with the linking of national reporting platforms to the single-entry point?*

· *What will the reporting structure look like in concrete terms? Is an additional step planned between the single-entry point and the national CER authority?*

· Regarding the proposed amendment to **Art 15, para 2 of Directive (EU) 2022/2557 (CER):**

· *The information in the planned Art 15, para 2, subpara 2 will have to be provided by the critical infrastructures, is that correct? When will these exact parameters be determined?*

· *Is a special process/additional information planned for critical infrastructures that operate in various Member States?*

· *How should the technical connection of Member States to the SEP work? Specifically: Can existing reporting platforms be used, or is a separate connection required for this?*

Article 10 (P2B)

General questions:

· On November 18th 2025, one day before the publication of the Omnibus VII (Digital) package, Cion published its report on the review of the Digital Services Act (DSA) and the way that the DSA interacts with other legal acts (COM (2025) 368 final). This report also includes explanations of the DSA interacting with the P2B-Regulation, while the P2B-Regulation is mentioned as a *lex specialis* setting out further requirements of platforms towards business users.

· *Did Cion take into account the findings of the DSA Review report when drafting Omnibus VII and suggesting to repeal the P2B-Regulation?*

· As stated in the last round of questions and comments the DSA does not contain any deadlines – neither for changing the terms and conditions nor, more importantly, for terminating content and accounts of business users (as Art 3 and 4 P2B-Regulation do). Deadlines can be essential for SMEs operating on platforms: Examples include small retailers on online marketplaces (which are sometimes their only sales channel) and hotels on booking platforms, which make a large proportion of their bookings via these platforms. Under the DSA, it would be permissible for platforms to terminate these business users overnight.

· *Has the EC assessed the impact on SMEs when repealing the P2B-Regulation?*

· *Even if Art 4 is to be applicable until 2032, how can legal certainty be ensured for the future? Wouldn't it be necessary to transfer the deadlines into the Digital Services Act?*

Specific questions:

· According to Art 3 (2) P2B Regulation the business user concerned has the **right to terminate the contract** with the provider of online intermediation services when the provider of the online intermediation services changes the terms and conditions. *Does the Digital Services Act also provide such a possibility?*

· *Does the content of the **transparency of terms and conditions under Article 14 DSA also cover:***

· *information on any additional distribution channels and potential affiliate programmes through which providers of online intermediation services might market goods and services offered by business users (such as Art 3 (1) P2B Regulation),*

· *information regarding the effects of the terms and conditions on the ownership and control of intellectual property rights of business users (such as Art 3 (1) P2B-Regulation),*

· *a description of the type of ancillary goods and services offered and a description of whether and under which conditions the business user is also allowed to offer its own ancillary goods and services through the online intermediation services (such as Art 6 P1B-Regulation),*

· *a description of any differentiated treatment which they give, or might give, in relation to goods or services offered to consumers through those online intermediation services by, on the one hand, either that provider itself or any business users which that provider controls and, on the other hand, other business users (such as Art 7 P2B-Regulation),*

· *conditions under which business users can terminate the contractual relationship with the provider of online intermediation services (such as Art 8 (b) P2B-Regulation),*

· *a description of the technical and contractual access, or absence thereof, of business users to any personal data or other data, or both, which business users or consumers provide for the use of the online intermediation services concerned or which are generated through the provision of those services (such as Art 9 P2B-Regulation)?*

· *Does Art 14 DSA allow for providers to **impose retroactive changes** to terms and conditions?*

· Regarding parity clauses: Art 5(3) Digital Markets Act (DMA) prohibits gatekeeper from preventing business users from offering the same products or services to end users through third-party online intermediation services or through their own direct online sales channel at prices or conditions that are different from those offered through the online intermediation services of the gatekeeper. However, the DMA only addresses gatekeepers, and only certain distribution channels. *Wouldn't there be a* ***risk (with the removal of Article 10 P2B Regulation) that platforms could again introduce stricter price parity clauses,*** *forcing retailers to offer the same (or higher) prices everywhere and thus experience reduced margins?*

· *Does Art 27 DSA also cover the parameters of the ranking****, including the possibility of payment to influence the ranking?*** *If not, isn't there the risk that business user will be misled about the implications of any payments?*

· Regarding internal complaint handling: Since Art 20 DSA does not cover complaints beyond decisions taken by the platform on restriction, suspension or termination**:** ***How can other challenges of business users be brought forward to platform providers in future?*** *And how can we get the platforms to respond to these, given that the contact points under the DSA are unlikely to ensure this?*

PORTUGAL

I DIGITAL OMNIBUS

General

1. Does the Commission anticipate any legal, drafting, transposition or implementation challenges arising from the fact that it is proposing a Regulation that amends not only Regulations but also Directives?

2. It appears that at least Regulation (EU) 910/2014 (the eIDAS Regulation) and Regulation (EU) 2022/2554 (DORA) are not mentioned in the title of the proposal. Is this omission intentional for legal reasons, or is it simply an oversight?

3. How will competent authorities be incorporated into the European Data Innovation Board (EDIB), and what level of participation will they have? Will any type of coordination be carried out with other boards such as the AI Board or the European Data Protection Board?

4. Although the Data Acquis means a relevant step to harmonization and simplification, further integration with the Interoperable Europe Act would be welcome (reuse of European solutions to contribute to the Internal Market and governments efficiency).

Single-Entry Point for incident reporting

5. On cybersecurity, we agree on the need for simplification, but we underline that a fully centralised Single-Entry Point at EU level is not the most effective solution and may undermine national trusted models already under development. We therefore advocate a federated, interoperable and cooperative approach among Member States.

In any case:

6. How would effective coordination be ensured between national competent authorities and the different regulations? Is there a risk that companies would still face multiple reporting obligations, even with the creation of a Single-Entry Point?

7. How would the Commission ensure that the implementation of this Single-Entry Point does not create duplication of efforts for companies that are already complying with the obligations under several legal acts?

8. What would be the language regime of this Single-Entry Point?

Integration of definitions and obligations across data regulations

9. How will the Commission ensure that the harmonisation of definitions does not exclude sector-specific nuances that are necessary for regulated areas, such as health, finance, or telecommunications?

10. The alignment between the Data Act and the GDPR may result in overlapping obligations concerning the protection of personal and non-personal data; how will these interactions be managed?

Strengthening legal certainty and simplifying obligations

11. The simplification of obligations may result in a lack of legal protection in highly regulated sectors. How will adequate protection of sensitive data be ensured in sectors such as health and public safety?

12. What specific exceptions or adjustments will be introduced to guarantee that critical sectors (such as finance or health) have appropriate regulations?

Integration of ePrivacy and GDPR in automated consent

13. How will the smooth transition between the current consent rules (cookies) and the new requirements under the Digital Omnibus be ensured?

14. Will it be possible to guarantee that companies do not face excessive costs in aligning their policies with the new regulations, particularly regarding cookies and tracking technologies?

Incorporation of the Open Data Directive, the Data Governance Act (Chapter II), and the Data Act to facilitate interoperability and re-use of public-sector data

15. How can it be ensured that the re-use of public-sector data does not compromise the privacy or security of sensitive data, such as health information?

16. The integration of the Data Act and the Open Data Directive may create regulatory conflicts between general public data and sensitive data; how will the balance between accessibility and security be achieved?

17. What transition regime is foreseen for this adaptation phase?

18. Is the Commission planning to provide harmonised guidance to ensure consistent application across Member States?

Repeal of the Free Flow of Non-Personal Data Regulation and its integration into the Data Act

19. How will the Commission ensure the uniform application of the prohibition on data-localisation requirements and the necessary transparency regarding national exceptions, following the repeal of the FFDR and the elimination of national information points?

20. It is important to clarify what obligations or role will be assigned to public bodies that previously acted as single information points under the former framework, or to ensure that no additional complexity is introduced at this level.

II. DIGITAL OMNIBUS ON AI

AI Literacy

21. Clarification is needed on how alternative, equivalent compliance-guarantee mechanisms will be introduced to ensure that the duty of encouragement is fulfilled by the European Commission and the Member States, and on which specific requirements must be verified for these obligations to be complied with.

Processing of special categories of data for bias mitigation

22. It is recommended that the instrument include a requirement for mandatory consultation of national data protection authorities (and, where relevant, the European Data Protection Board) when developing guidance on the interpretation of Article 4A, thereby ensuring coherence with the GDPR and preventing abusive practices.

Cooperation between AI supervisory authorities and GDPR authorities

23. How will overlapping competences between the AI Office and other regulatory authorities (DSA/DMA) be addressed?

24. What coordination procedures will apply between the AI Office and national authorities when dealing with AI systems involving personal data or privacy-related matters?

Single procedure for conformity assessment bodies

25. It should be emphasised that the applicability of the single procedure is conditional on such a possibility being available in the relevant sectoral legislation, thereby creating asymmetries in implementation and potential competitive inequalities across markets and sectors.

Regulatory Sandboxes

26. Further clarification is needed regarding the governance model between the EU-level sandbox and national sandboxes.

27. How will coordination be ensured across different levels of authority (national and European) so that testing under real-world conditions is consistent and effective?

Strengthening of the AI Office's role

28. We consider that this legislative initiative acknowledges that the new architecture entails a significant reconfiguration of AIA governance, by foreseeing a substantial expansion of the AI Office's competences to meet these new responsibilities, which constitutes an indirect indication of the magnitude of the transformation being introduced. This should be presented at the level of the AI Board.

Extension of deadlines and transitional regime

29. Although we support the introduction of transitional regimes designed to address the practical challenges associated with implementing the AI Act, we have serious legal concerns regarding the newly proposed rules on timelines.

30. For example, we are concerned about the new rules on the timeline for high-risk AI systems, as they would allow the Commission to determine when certain provisions start applying. Such decisions relate to essential elements of the legal act. Moreover, this approach undermines legal certainty for economic operators, who would no longer know when specific obligations will apply, or would only know with limited advance notice.

31. We also have concerns about the Commission's remarks in the last AGS meeting, where it indicated that, if sufficient support tools become available only less than 6 or 12 months before 2 December 2027 or 2 August 2028, respectively, the transitional period would be that one, this means, shorter than the 6 or 12 months foreseen.

32. In any case, six-month periods may prove manifestly insufficient for SMEs, particularly in a context where delays persist in the availability of sufficient support tools.

SLOVENIA

SI QUESTIONS ON DIGITAL OMNIBUS

- What is the relationship (interplay) between the Digital Omnibus Regulation and 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 March 2025)? – Regulation (EU) 2025/327 already overlaps in part with Regulation (EU) 2022/868 (the Data Governance Act – DGA).
- We kindly request examples of entities that are considered "public sector bodies" under the Digital Omnibus Regulation and are, pursuant to the new Article 32w, competent "to grant or refuse access for the re-use of protected data held by public sector bodies." Could national central banks also be regarded as such entities?
- What are the reasons behind for the deletion of Article 4 of the ePrivacy Directive (security of processing)?
- What is the point of retaining the provision of paragraph 3 Article 5 of the ePrivacy Directive due to the fact that »user« under ePrivacy Directive is defined as *»natural person, using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service«*?
- Given that Article 32w(3) of the amended Data Act obliges public-sector bodies to provide or control "secure processing environments" for the re-use of protected data, does the Commission intend to develop an EU-wide reference architecture, minimum security baseline, or technical specification for these environments?
- How does the Commission expect Member States to reconcile the free-flow-of-data principle with situations where secure processing environments under Article 32w may, in practice, necessitate nationally hosted or otherwise domestically controlled infrastructure?
- Given that Article 32w(1)(b) requires public-sector bodies to be equipped with "necessary resources", has the Commission assessed the administrative and financial burden of this obligation?
- Does Article 32z require Member States to establish new competent bodies, or may existing authorities – e.g., data protection authorities – serve as the designated competent bodies for evaluating protected-data re-use requests?
- Does the Commission plan to define EU-level functional, technical, or interoperability requirements for the Single Information Points required under Article 32aa to ensure a consistent approach across Member States?

SI QUESTIONS ON AI OMNIBUS

- How does the European Commission assess the effect of the cumulative regulatory burden on Member States in the period 2025–2027, and is there a plan to introduce a mechanism for evaluating administrative capacity or absorption capability when implementing new horizontal regulations?

- Is the European Commission willing to consider a more gradual or phased approach to the examination of the proposals, which would allow Member States to conduct a more thorough analysis and prepare higher-quality positions, thereby reducing the risk of legal ambiguities in later stages?
- How does the European Commission envisage the timelines for the adoption and implementation of both omnibus regulations, taking into account the fact that many Member States are still heavily engaged in implementing the core horizontal regulations that the omnibus proposals amend or supplement?
- How will the amended provisions of the AI Act affect the Implementing Acts that will already have been adopted by that time, and what will be the deadlines for alignment? The deadline for establishing national AI regulatory sandboxes remains 2 August 2026.

EXPLANATION

Slovenia would like clarification regarding the planned approach to the decision-making procedures, the setting of timelines, and the support to be provided to Member States in implementing the changes introduced by both the AI Omnibus and the Digital Omnibus.

Both proposals amend extremely complex and systemically sensitive legal acts that were adopted relatively recently (e.g., the AI Act, the Data Act, the GDPR, NIS2, and other horizontal acts), many of which are still in an active phase of national implementation.

Since the omnibus proposals intervene simultaneously in several regulatory areas, they require the involvement of a wide circle of stakeholders already during the preparation of national positions. It is necessary to examine their impact on various already-established procedures and structures (e.g., the competences of authorities, market surveillance, incident management, existing IT solutions, registers, and workflows).

This means that, before formulating their positions, Member States must ensure detailed assessments of potential impacts across multiple areas simultaneously, coordination among several ministries and institutions, and the preparation of sector-specific positions, which are then further coordinated at the national level.

This is a process that is extremely demanding both in terms of personnel and expertise, and it cannot be effectively carried out within short timelines.

Member States, including Slovenia, are already facing the challenge that key experts are fully engaged in implementing existing horizontal regulations, which are far from complete. The new omnibus packages therefore represent additional short-term administrative burdens, even though their long-term objective is deregulation and greater proportionality.

In this context, we would also like to highlight that the Digital Omnibus proposal explicitly states that the changes should lead to "negligible, if any, transitional and adaptation costs to businesses and authorities." In Slovenia's assessment, this assumption does not reflect the actual situation, as even the stage of preparing positions and assessing impacts is extensive and requires additional human resources.

Among the proposed amendments to the AI Act is also a proposal to expand the content of the Implementing Act on AI regulatory sandboxes, which would also provide detailed definitions of governance at the national level.

Article 58, paragraph 1, is replaced by the following:

'1. In order to avoid fragmentation across the Union, the Commission shall adopt implementing acts specifying the detailed arrangements for the establishment, development, implementation,

operation, governance, and supervision of the AI regulatory sandboxes. The implementing acts shall include common principles on the following issues:

(a) eligibility and selection criteria for participation in the AI regulatory sandbox;

(b) procedures for the application, participation, monitoring, exiting from and termination of the AI regulatory sandbox, including the sandbox plan and the exit report;

(c) the terms and conditions applicable to the participants;

(d) the detailed rules applicable to the governance of AI regulatory sandboxes covered under Article 57, including as regards the exercise of the tasks of the competent authorities and the coordination and cooperation at national and EU level.';

On 2 December 2025, the European Commission published a draft Implementing Act on AI regulatory sandboxes, which does not contain these provisions, as it is tied to the AI Act currently in force.

FINLAND

General comments

- We welcome the proposal by the Commission as a genuine effort for simplification also in the digital acquis together with the launch of the fitness check.
- In general, we can support the aim to codify and simplify the data legislation.
- We have also recognized the need to alleviate administrative burden and to ensure a consistent interpretation of the GDPR. Therefore, we are open to discuss on possible, targeted simplification measures to the GDPR. The changes to GDPR should be discussed thoroughly in order to ensure that the proposed changes would not lower the level of protection.
- We are still analysing the proposals and are looking forward to the discussions.

More detailed comments and questions for the Commission

1. GDPR

Finland considers that the GDPR has succeeded in its objectives. However, Finland has recognized the need to alleviate administrative burden and to ensure a consistent interpretation of the GDPR. Therefore, Finland has been open to discuss on possible, targeted simplification measures to the GDPR.

Finland welcomes that, in general, the COM proposal respects this and the focus seems to be on targeted amendments to alleviate unnecessary administrative burden and promote competitiveness, whilst safeguarding the current high level of data protection.

Preliminarily Finland can support the aims to alleviate unnecessary administrative burden and the aims to amend and clarify certain aspects, for instance concerning AI development and cookies. However, it is vital to ensure that this does not lead to unwanted outcomes, unclarities or reduced level of data protection. In this regard, it is probably necessary to amend some of the proposals.

Updated questions (5.12):
We would like to ask more details about the proposed amendments to some of the definitions

- **The definition for 'personal data'** is the core of the GDPR and there are fears that this would lead to lower level of data protection in the EU and could be manifestly exploited.
    - We would like to inquire **why the COM has gone further in the definition than what the CJEU has** ruled in case C-413/23 P and **whether the COM has considered the unwanted outcomes of this addition.**
    - In addition, Finland would like to know how this interacts with Convention 108+ for the Protection of Individuals with regard to Automatic Processing of Personal Data. There are also fears that changing the definition for personal data could endanger current adequacy decisions.
    - **Finally, is this the right place and the right way to help controllers and processors with pseudonymization and anonymization? Why isn't the proposed new Article 41 a enough?**
- **The definition for 'scientific research' seems rather wide and seems to include also research that cannot be seen as scientific. How has the COM come up with this definition**, as it seems to differ from the common understanding what is considered 'scientific research'**. Is this the right place to introduce a definition for scientific research?**
    - The definition only mandates to adhering to ethical standards, but **does not include adhering to the methodological and systematic approach nor to structured processes to evaluate data and solve problems in a reliable and valid way.** Maybe this should be added in the definition. **Shouldn't at least the text from recital 28 be added to the definition?**

- And at the same time, **shouldn't the mentioning of supporting innovation, technological development and commercial interest be in the recitals**. It seems to change the definition to something else than scientific research.
- As such, it seems that the **proposed definition would enable derogating from requirements** in the GDPR and weaken the current level of data protection.
- **Why has the COM added a reference to legitimate interest in recitals? Isn't scientific research also for public interest** – at least the public sector relies on this legal basis and there is national legislation concerning scientific research based on Article 6(1)(e) of the GDPR.

- **In Article 9, paragraph 2, there are new derogations proposed concerning AI and biometric verification**
  - Concerning AI, we would like to know **how the COM has considered the proportionality as the recital clearly states that "although the special categories of personal data are not necessary for the purpose of the processing". Is this in line with the Charter**? Wouldn't this de facto mean lower level of data protection, if we accept processing special categories of data, when there is no need for it.
  - Concerning the derogation for biometric verification, what is meant by "held solely by the data subject". Would this include also situations where the service provider requires biometric verification (e.g. iris scanning) to use the service (e.g. cryptocurrency provider), i.e. the provider does not allow any other possibilities for authentication to use the service. **Why aren't there any further safeguards and limitations concerning this derogation?**

- **Concerning Articles 12 and 13**, preliminarily, it seems appropriate to reduce administrative burden in low risk cases and when there are manifestly unfounded requests. However, **we would like to ask the COM whether they actually consider that limiting the rights under Article 15 to only data protection** purposes would not lower the current level of protection. How has the COM taken account the CJEU case law regarding Article 15.

- **Concerning Article 33, Finland preliminarily welcomes changing the data breach notifications to high risk situations**. However, taking account that the data breaches concern high risk situations, **we are cautious whether it would lower the level of protection, if at the same time the deadline for notification is longer**. It seems that the COM has not assessed this proposal appropriately.

- **In Article 35, FI preliminarily welcomes the proposed changes** concerning data protection impact assessments (DPIAs) **and transferring the lists for the EDPB,** as it would promote legal certainty and help controllers assessing whether there is a need for a DPIA. **However, we would like to inquire the COM why there is a need for implementing acts**. Wouldn't this override the powers of the EDPB. **Should the COM at least consult the EDPB, if the COM is going to change the list?** The process would also burden the Article 93 committee.

- 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.

- We have already commented on this, but **we would like to inquire on administrative fines. The proposal does not indicate which level of GDPR administrative fines** (2 % or 10,000,000 eur/ 4 % or 20,000,000 eur) or EUDPR administrative fines (25,000-250,000 eur or 50,000-500,000 eur) **would apply to the new articles proposed to GDPR** (eg. regarding cookies and development of AI systems). **Should there be a threat of administrative fines for these added articles and does the Commission have a proposal, which levels would be appropriate to each proposed new article?**

2. ePrivacy Directive

Question on the GDPR and ePrivacy proposals:

- Why does the proposal split accessing and storing to data on terminal equipment into two different acts?
- How does the Commission assess the impacts on number of consent requests, where the rules in ePrivacy directive remain the same for non-personal data?
- Was a further alignment of the remaining ePrivacy directive art 5(3) with the newly introduced grounds for access for personal data considered?

New additional questions (5.12):

Could the commission further clarify the scope of the proposed art 88a? In Article 5(3) of the ePrivacy Directive it is stated that the said paragraph doesn't apply where the subscriber or user is a natural person, and the information stored or accessed constitutes or **leads** to the processing of personal data. However, the proposed new Article 88a(1) of the GDPR applies to storing of personal data, or gaining of access to personal data already stored in the terminal equipment [..] and Article 88a(3) **to storing of personal data, or gaining of access to personal data already stored in the terminal equipment [...] and subsequent processing.** Furthermore, in recital it is explained that "for the subsequent processing of personal data for other purpose than those defined in the limitative list, Article 6 and, where relevant, Article 9 of Regulation (EU) 2016/679 should be applied".

- Which regime applies **to the storing or access** where the subscriber and the user is a legal person but the information stored or accessed leads to the processing of personal data?

- Does article 88a apply also **to the storing or access** in situations where non-personal data is stored to the terminal if its subsequent processing does lead to the processing of personal data?

- Is the subsequent processing of personal data accessed from the terminal allowed for both the specific conditions in art 88a(3) as well as the legal grounds in Art 6 of the GDPR? Should the conditions in article 88a(3) be interpreted as new additional grounds of processing or does the processor have to always also rely to one of the grounds in Article 6?

We understand that the proposed Art 88a(2) of the GDPR is meant to mirror the existing Art 15(1) of the ePrivacy Directive. Do we understand correctly that Art 88a(2) does not allow restricting the scope of Article 6 of the GDPR? Does Art 88a(2) allow restricting the scope of Art 5(1) of the ePrivacy Directive?

3. Data Act

New additional questions (5.12):

Article 32i (1): The scope covers "existing data and documents". This seems to be adopted from the Open Data Directive, where it is used to refer to the fact that there are no requirement to generate documents or data to fulfil the requirements of the act. Is this the correct reading? The phrase "existing data" is not present in the DGA.

Article 32i (1) (b)(iii) ja (iv): What is the reasoning for extending the scope of the rules on protected public sector data to the public undertakings that are in the scope of the rules on open public sector data?

What is the reasoning for introducing the exclusivity rules on cultural resources and cultural heritage as-is to also cover the re-use of protected public sector data? What is the relationship between Articles 32i(3) and 32i(2)(c)? Is it to be understood that if an exclusivity arrangement is deemed necessary for the digitisation of cultural resources, then article 32i(3) is not applicable? Does the reference to exclusivity arrangements in relation to digitalization of cultural heritage mean that there is a possibility to introduce or prolong the term of protection, where such cultural heritage is not or is no longer protected under copyright law?

Is it a correct interpretation that 32y(2) provides Member States with a broad margin of maneuver to establish the regime applicable on fees, as it says that "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". So it is possible to apply lower fees to other kinds of entities than those mentioned?

Article 32y (2) says that where public sector bodies charge fees, they shall take measures to provide incentives for the re-use of certain categories of protected data for non-commercial purposes, such as scientific research purposes, and by start-ups, SMEs and SMCs in accordance with Union State aid rules. Which rules in Unon State aid legislation is referred to here?

Previous questions:

According to the proposal, Article 37 on competent authorities would apply to Chapter VIIc. Since the legislation being moved into Chapter VIIc was not originally considered to require a competent authority to enforce it, what is the justification for this new requirement that a competent authority be named for enforcing Chapter VIIc?

- (Background: Article 26 of the DGA mandates competent authorities to supervise the rules that apply to data intermediation services and data altruism organisations only, not the re-use of public sector data. The ODD does not mandate the appointment of a supervisory authority at all.)

According the proposal, Article 38 on the right to lodge a complaint would apply to the new Article VIIc on the re-use of public sector data. Chapter II of the DGA and the Open Data Directive do not legislate an independent right to lodge a complaint in them currently; rather, they require that there are means for redress available in the Member State, and this would be the new Article 32o. This appears to create overlapping complaint mechanisms between the Data Act and national law. To clarify, what is the intended interplay between Article 38 and the proposed Article 32o of the Data Act?

How will the continuity of the Implementing Regulation 2023/138 (EU) on high-value datasets be ensured with the revocation of the Open Data Directive?

How would identifying a re-user as a VLOP or VLOSE work in a context where open government data re-use is enabled without user identification, which is a common use case? (cf. Article 32q and 32r)

Questions on the EDIB: Have we understood correctly that the EDIB would serve as the committee for the adoption of implementing acts on high-value datasets? How would the Commission take into account PSI questions in the configuration of the EDIB (Article 41a(3))? Have you considered a mutual obligation to co-ordinate with the Interoperable Europe Board, same way as in Article 15(5)(s) of the Interoperable Europe Act?

Article 36 of Chapter VIII of the Data Act would be repealed. That article imposed obligations to comply with certain requirements in contracts concerning the execution of smart contracts for data sharing. These obligations would be replaced by the Commission's power to introduce standards. In which part of the amendment proposal is the change to Article 35(5) laid down.

Article 32 would be changed to include making data available under Chapter VIIc, Section 3 (currently DGA Chapter II) and obligate public sector bodies accordingly. Can you clarify the relationship between these requirements, that only concern non-personal data, and the requirements in Article 5, DGA (Article 32w, DA), that concern both personal and non-personal data? Can an implementing act per Article 5(12), DGA (Article 32x, DA) remove or reduce the obligations under Article 32, DA? What kind of technical, legal or organizational measures do you envision as being adequate in the context of sharing protected non-personal data?

4. Single Entry Point (SEP) Cyber/NIS2

Updated questions (5.12.):

- Could Commission clarify it's reasoning on why it should be mandatory for companies to report via SEP? If a company finds in certain situation that it would be more effortless and less burdensome to report via existing national portal instead of the SEP, why should law prohibit company from choosing the less burdensome method to fulfill its reporting obligations? Why shouldn't companies be allowed to choose reporting to SEP or national portal based on the situation and use the portal that creates the least administrative burden for them?
- Has Commission evaluated total costs that building and maintaining of SEP will cause to ENISA?
- Does ENISA have sufficient resources in order to bear costs for building the SEP?
- Does ENISA have sufficient resources in order to maintain the SEP 24/7?
- Has Commission evaluated costs that implementing and integrating of SEP to national IT systems will cause to Member States?
- According to Commission presentation on 1 December for the meeting of the Antici Group (Simplification), (ref: WK 16586/2025 INIT), page 5/64, ENISA will bear costs for single entry point (to be secured for ENISA mandate).
  - Has Commission evaluated total costs that SEP will cause to ENISA?
  - Will ENISA also bear costs that SEP implementation and integration to national IT systems will cause in Member States?
- Has Commission estimated total amount of reports and data input to the SEP in annual level?
- 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.
- Recently Member States have invested to set up functional national platforms for incident reporting. Member States are also investing for development of platforms on on-going basis. What is expected from Member States in respect to national platforms during the transitional period? Should these platforms close when the SEP is functional?
- SEP must be fully functional and secure at the moment of application especially if SEP is the only allowed platform for incident reporting. If SEP has functionality issues even after "18 months + max 6 months delay in case of functionality issues", how shall additional development time for SEP be granted and how incident reporting shall take place during that time?
- There will be major security risks related to upkeep and data flows in the SEP. How the risks will be addressed and managed?
- As the SEP will not provide substantive changes to current requirements under the respective acts in regards reporting or recipients, SEP would need to be able to deal with various thresholds for incident reporting, various contents of data and various recipients. Thresholds, datasets and recipients vary not only based on the respective act in question but also based on the Member States' national transposition of the act (for example, NIS 2 Directive only harmonizes the minimum level of scope and obligations). Therefore, it will be very complex in technical level to achieve fully functional SEP, especially if the goal is to make reporting easy and transparent.

- How does the Commission view these challenges?
- Has Commission evaluated that EU-level SEP is technically possible despite high-level complexity of data flows and variations not only between respective acts but also national aspects related to transposition of the acts?

- 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. How is this aspect (SEP's link to Member States' national security and EU competence) taken into consideration in regards to mandatory use of SEP in all reporting situations under the respective legislation?
- How will the risks of the SEP be evaluated – especially in regard to data flows and possible downtime? How will reporting take place if the SEP is down? What would be the alternative back-up way of receiving incident reports?
- 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?

5. P2B Regulation

Updated questions (5.12.):

The P2B focuses on contractual relationships between online platforms of all sizes and their business users. We agree that DSA and DMA have partly the same rules as P2B. However, provisions especially in DMA only apply to very large online platforms. It is important that the Omnibus proposals do not weaken the position of SMEs in the Single Market, as many business users also use online platforms that are smaller than those designated as gatekeepers.

- **Could the Commission elaborate, would it not be necessary for online platforms smaller than gatekeeper companies to comply with all P2B-related rules in the future?** For example, a provision on self-preferencing can also be found in the DMA but the prohibition would then only apply to gatekeepers. Business users operate on several online platforms that are smaller than gatekeeper platforms.
- **How would Union law safeguard the rules on the legal protection of business users in contractual relationships with online platform companies in the future?**
- **Could the Commission specify how and to what extent the repeal of the P2B Regulation would reduce the costs of regulation for companies - both online platform companies and companies using online platforms?**

6. Artificial Intelligence Act

Updated questions (5.12.):

The COM is introducing a new Article 4a, replacing Article 10(5) AI Act, which provides a legal basis for providers and deployers of high risk AI systems and AI models to exceptionally process special categories of personal data for the purpose of ensuring bias detection and correction under certain conditions. **We would like to inquire why the COM has changed the requirement "strictly necessary" to "necessary". There is no assessment concerning this, but taking account that this Article concerns high risk AI systems, it seems that this would also lower the current level of protection and should have been evaluated properly – especially when the derogation would now apply to more entities.**

Concerning **Article 3 and definitions, why hasn't the COM proposed to streamline some of the definitions with the GDPR/LED**. Different definitions cause unnecessary administrative burden and unclarities to

entities. It could also jeopardize the level of personal data protection. For instance, **biometric data (see Article 3, points 34 to 36) should be streamlined with GDPR/LED**. It is also unclear whether law enforcement authorities in Article 3, point 45 is in line with the LED and how the definition should be interpreted with the LED.

SWEDEN

Swedish comments on Omnibus VII Digital

Single-entry-point (SEP)

- Does the proposal imply that the SEP should link to national reporting systems, with the actual reporting still taking place within the national platforms, or that reporting would occur directly in a common SEP (with the content subsequently forwarded to the national platforms)?
- Would the use of a common SEP be mandatory?
- An SEP as proposed would require high availability. How would the necessary redundancy be ensured? What would happen in the event of a service outage?
- How would an SEP operate in relation to individual Member States' national regulations on reporting thresholds (for example, within the framework of NIS2)?
- What possibilities exist for national customisation? Would there be possibilities for national adaptations (for example, regarding the content of questionnaires) also in the longer term?
- How would the need for adjustments over time be addressed? What influence would Member States have over these changes?
- How is the SEP intended to be managed in the longer term, and what influence will Member States have in the longer term from a governance perspective?

Digital Omnibus – COM (2025) 837

Please refer to the written comments submitted by Sweden on 26 November in relation to the Digital Omnibus – COM (2025) 837.

- We would like to get clarity on the interplay between the platform work directive and the proposal of Omnibus VII Digital. Especially P2B Regulation and how the derogation related to the Platform Work Directive is to be understood.

Digital Omnibus on AI - COM (2025) 836

Please refer to the written comments submitted by Sweden on 26 November.

- What are the possible fall backs if harmonised standards are not ready before the requirements enter into force by 2 December 2027?
- How should grace period for transparency requirements be designed to be practicable for both providers and deployers?

***

- **Entry into force:** 6 months for Annex III, 12 months for Annex I, by 2 Dec 2027 or 2 August 2028, depending on the decision from the Commission. The decision from the Commission is dependent on adequate standards and guidelines. Not specifying a clear date for entry into force may result in ambiguity for the actors as it requires, among other things, that the information about the date is clearly disseminated to the actors concerned. Why has the Commission opted for this arrangement instead of indicating 2 August 2027 or 2 December 2027 and then Annex I 12 months later?
- **Clarification regarding interplay between different legislative acts:** Clarifications have been introduced concerning the relationship between the Digital Services Act and the AI Act, as well as between the GDPR and the AI Act. In addition, the Commission will develop guidelines for other relevant interplay between legislative acts. While this is a positive step, greater legal certainty would arguably have been achieved had these interactions been specified in binding provisions rather than addressed through non-binding guidance. What is the purpose of initiating guidelines for clarifications regarding interplay between legislative acts, instead of legal provisions?
- **Transference of Article 10(5) to Article 4(a):** The provision concerning the processing of sensitive personal data will be placed under a separate heading and its scope of application will be relaxed (the requirement of being "strictly necessary" will be reduced to "necessary"). Moreover, the exemption is afforded greater prominence within the AI Act. Considering that this approach may broaden the circumstances under which personal data may be processed, we would like to ask the Commission to elaborate on the practical implications of the said provision?
- With reference to the above, in the Commission's proposal in the Digital **Omnibus – COM (2025) 837**, whereas the Commission proposes to expressly exempt processing in the context of the development and operation of an AI system from the general prohibition of processing special categories of personal data set out in Article 9.1 of the General Data Protection Regulation (GDPR), we would like to ask the Commission to further elaborate on the interplay between the amendments in the GDPR and in the AI Act in this regard. In addition, does the Commission envision increased processing of personal data due to the proposed amendment in this regard and if so, would it be possible to further elaborate on the practical implications of this amendment?

- **The exclusive competence for market surveillance on General Purpose AI (GPAI)**: Given that we are still examining the proposal, we can see some advantages in giving the Commission exclusive competence for market surveillance of AI systems based on GPAI when it is the same provider. This clarification should simplify the work of market surveillance authorities on national level.
- **Centralising oversight with the AI Office:** What additional resources will the AI Office need to handle its increased responsibilities?
- **AI-literacy**: Article 4 of the proposal provides that "the Commission and Member States shall encourage providers and deployers of AI systems to take measures to ensure a sufficient level of AI literacy […]". This raises questions regarding compliance. What is the precise meaning of "encourage" in this context, and what obligations, if any, does this impose on Member States? What practical requirements must be met to comply with such an encouragement? While it is positive that the provision does not impose an obligation framed as "ensure", the use of a concept that is inherently difficult to operationalise may create uncertainty as to its implementation. Also, what measures does the Commission envisage to guarantee a consistent interpretation of "AI literacy" across Member States, given its non-binding nature and the challenges of practical enforcement?
- **Expanded scope of application concerning small mid-cap companies (SMCs):** In principle, extending simplified rules to a broader range of companies is a positive development. However, the proposal foresees the provision of guidance and related support measures for these entities. What measures does the Commission envisage to ensure that the provision of guidance and support for small mid-cap companies will be applicable in time? What other concrete measurements will the Commission take to enable innovation and growth of AI- startups and scaleups in Europe?
