Council of the European Union
General Secretariat

Brussels, 28 November 2025

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

WK 16524/2025 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 26/11)

Following the meeting of the AGS on 21 November 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, FR, HR, IT, LV, LT, HR, NL, AT, PL, SI, SK, FI and SE.

Omnibus VII - Digital Omnibus and Digital Omnibus on AI

MS comments (ddl 26/11/25)

AGS meeting on 21/11/25

Table of Contents

BELGIUM

Digital Omnibus: compilation of technical Questions - BELGIUM

A. AI

Timeline for high-risk AI

Art. 113 is amended with a new §3, point (d) to change the timeline. It says 'Chapter III, sections 1,2 and 3 shall apply following the adoption of a decision of the Commission confirming that adequate measures in support of compliance with Chapter III are available, from the following dates ...'

- Could the Commission clarify why this conditional trigger was chosen instead of a fixed postponement period, which might provide more predictability for authorities and businesses?

- What concrete criteria will the Commission use to determine that ‘adequate support measures’ - such as harmonised standards, templates or guidance - are sufficiently available to activate the High-Risk obligations? Does this relate to the decision qualifying the technical standards as harmonized, or can this also refer to other 'measures'? E.g. common specifications or guidance from the Commission? How will MS be involved in this decision?

- Modifying the date of application of certain provisions brings a level of uncertainty for the implementation period for companies. If we do get to an interim-period, which, if any, safeguards does the Commission foresee to ensure legal certainty and consistency?

AI literacy

- Article 4 has been critizised as vague and horizontal lacking a governance mechanism and guidelines. In this light, how should the Commission and the Member States enforce this obligation? How can they guarantee that providers of HRAIS have or acquire the necessary AI-knowledge?

Article 4

- Scrutiny reservation

- Proposed art. 4a, 1. (a) - How should a controller demonstrate that bias detection “*cannot be effectively fulfilled by processing other data, including synthetic or anonymised data*”, and what evidentiary standards or assessment criteria apply to such justification?

- Proposed art. 4a, 1. (b) - What constitutes “*state-of-the-art privacy-preserving measures*” for AI training (beyond the pseudonymisation already mentioned), and

how will this be updated dynamically in light of new re-identification techniques, model inversion attacks, or advances in secure computation?

- Proposed art. 4a, 1. (d) - How should bias detection and mitigation be handled in collaborative development environments or joint training arrangements, given the strict requirement that special category data must not be "*transmitted, transferred or otherwise accessed by other parties*"?

- Proposed art. 4a, 1. (e) - How must the obligation to erase special category data be fulfilled when such data may already have been "internalised" into model parameters, and does this imply a requirement to retrain or regenerate affected models?

- Should processing of special categories of personal data for bias detection be automatically treated as 'high-risk' under Article 35 GDPR, and what specific DPIA criteria or risk metrics should be applied given the limited derogation under Article 4a?

- It is stated in the explanatory memorandum that an impact assessment was not needed because the proposal made only includes technical changes. Please clarify how changes such as the withdrawal of AI Literacy obligations for deployers and providers of AI systems constitute merely a technical change?

<u>Registration obligation in the EU database for non-high risk ai systems: modification of Article 6, par. 4</u>

- 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?

<u>Amendments to the provisions relating to notifying authorities and notified bodies</u>

- Could the Commission clarify or give examples of the different ways in which 'the establishment, organization, and operation of notifying authorities under the AI Act' can be done to enable the proposed single application and single assessment procedure? Can Member States still designate authorities other than the existing sectoral notifying authorities as AI Act notifying authorities?

- 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?

New Annex XIV

Annex XIV foresees, as subcategories of vertical codes related to Annex III.1, systems intended to be put into service by law enforcement, immigration, or asylum authorities, and systems intended to be put into service by Union institutions, offices, or agencies. Article 43(1) specifies, however, that in such cases, the notified body is actually the market surveillance authority referred to in article 74(8) or (9).

- Does this confirm that in this particular situation, the market surveillance authority acting as a notified body must be listed on NANDO?

- If yes, questions remain as to whether this authority must undergo a full assessment by the corresponding notifying authority, just like a standard notified body (which poses problems in cases where the same authority plays the dual role), and whether each Member State must ensure that the MSA it has designated is also listed as a notified body (should providers automatically address their national MSA acting as a notified body, or may they approach an authority in another MS?) And how will the EDPS itself be monitored as a notified body?

In addition, 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.

- Should the negotiations on the Omnibus act delay its adoption beyond the initial application date of the requirements for HRAIS (August 2026), we would welcome clarification on the interim arrangements. 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?

AI Office

The AI Office shall be exclusively competent for the supervision and enforcement of the obligations under this Regulation in relation to AI systems that are integrated into a designated very large online platform or very large online search engines within the meaning of DSA. How will this enforcement work in practice between the services within the Commission enforcing DSA and

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

Due to overlaps of the AI Act with sectoral (financial services) legislation, many AI Act obligations relating to High Risk AI Systems will be supervised by the market surveillance

authority (MSA) designated under Article 74(6) or (7) AI Act, while the compliance with the (overlapping) requirements under EU financial services law will be supervised in parallel by relevant competent authorities under the EU financial service law (including the European Central Bank).

In the event that they are not the same authorities, the cooperation and information exchange between the MSA and the prudential authorities will therefore be crucial to ensure the enforcement of the AI Act and to enable them to fulfil their respective mandates. However, prudential authorities are subject to professional secrecy obligations under EU law which could prevent information exchange.

- Could the Commission 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?

B. Data Acquis

Notion of very large entreprises – Section 2 Data Act

- How is this notion of 'very large enterprises' legally defined, and in accordance with which legal instrument?

Merging of the ePrivacy Directive with the GDPR

- From a technical point of view, how do you avoid creating loopholes for profiling and cross-site tracking with moving consent to browser settings automated, machine-readable consent signals? Does this depend on the compliance of browsers vendors?

Competent authority for data intermediation services providers – Art. 32b

- Given that the conditions for the appointment of competent authorities in the Data Act and the Data Governance Act were not identical, Does the new art. 32b regarding the competent authorities for data intermediation service providers imply a change of the conditions for such competent authority?

Article 32l

- The new obligation for public bodies to provide easy online payment modalities for fees and charges related both to re-use of open government data and to protected data requires preparations and modifications and additional budgets to organise. What timeline is foreseen for the entry into force of this obligation?

Articles 32q and 32y

- With regards to charges and fees for re-use of open government data or for categories of protected data, why not provide a general definition of “very large enterprises” valid for the whole regulation?

Article 32q

- Why only create the possibility for charging fees for marginal costs of anonymisation of personal data? Why not also for pseudonymisation of personal data? Also considering the modification of the GDPR in the sense that controllers should be able to determine that data resulting from pseudonymization does not constitute personal data with the reformulation of the definition of ‘personal data’…

- And why only having the option of charging costs of measures taken to protect the **commercial** confidentiality of data, why not in a broader sense for all confidentiality measures of data that needs to stay confidential?

- For 32q, 2, a) could there be a clarification on what ‘required’ means? Required by national law? Or any public sector body that decides to cover (a substantial) part of their costs with generated revenue?

Article 32w

- The addition of “documents” to the material scope means that requests for protected data will also concern non-electronic information carriers with protected data. This implies a potential considerable enlargement of the material scope, for which practical preparations and modifications in legal frameworks are needed.

- Redress system now also for non-electronic protected public sector data – requires preparations and modifications and additional budgets to organise redress.

- Where was art. 5.8 integrated? “*8. Where data requested is considered to be confidential, in accordance with Union or national law on commercial or statistical confidentiality, the public sector bodies shall ensure that the confidential data is not disclosed as a result of allowing re-use, unless such re-use is allowed in accordance with paragraph 6.”*

Article 32y

- Would be useful to clarify that a division can be made between charging fees and costs for:

    - 1. the treatment of requests;

    - 2. the prepping of the data ((sub-)sets) for re-use; and

- 3. the potential continuous costs for making and holding protected data available for re-use and providing controlled access to the data;

  in a secure and safe manner that preserves the protected nature, the privacy and the confidentiality of the data and prevents unauthorised re-use of the data and access to the data.

- Why do you not use the term '*pseudonymisation'* instead of "*other forms of preparation of personal data*"?

- With reference to relevant publications of competent authorities, can you elaborate or offer more guidance on the minimum or the 'golden standard' for anonymisation and pseudonymisation?

Article 32aa

- The current text of the DGA article 8 provides that : "*The single information point may be linked to sectoral, regional or local information points*.". This part seems to have disappeared. Why is this?

Free flow of non-personal data

- What will happen to the obligation of organising a single point of contact in the Free Flow of Non-Personal Data regulation? This concerns the rules on data sharing with competent authorities with cross-border aspect. The current regulation contains a specific procedure for cooperation between authorities in article 7.

Risk of increased discrimination based on 'scientific research'

- Concerning the definition of scientific research, the clarification of the compatibility of further processing of personal data for scientific purposes with the initial purpose of processing, and the clarification that scientific research is a legitimate interest : how will it be possible to guarantee that the research, results and data used and produced won't be processed/used/misused/transferred to third parties (who might have particular interest in this) through private funding of scientific research or schemes? For instance (sensitive) health data that can be traced back to specific (groups of) natural persons, that could clearly be commercial quite interesting to a variety of third parties, such as public and private health care organisations, insurance companies, employers, public and private housing organisations, banks providing long term loans to natural persons, public and private fraud detection organisations and so on.

  Especially the phrase " *this does not exclude that the research may also aim to further a commercial interest*" leaves the door open to misuse, that is evidently not intended.

Definition of personal data

- When a controller is of the opinion that the processed data is not considered personal data within the meaning of the 'new' formulation, is it still necessary to conduct a data processing agreement to meet Art 28 GDPR requirements with a processor?

- How about putting in place appropriate safeguards for transfers to non-EU countries when a controller considers it no personal data?

- DPIA obligation when a controller is of the opinion that the large scale processed data is not considered personal data within the meaning of the 'new' formulation

- Is there an information requirement towards the natural persons potentially concerned or a procedure to object for these persons if they do not agree with the analysis of the controller?

- Article 3, amending article 4 of GDPR : CJEU confirmed the existence of the concept of relative personal data in thecase EDPS v. SRB C-413/23) :

    - In light of the CJEU's recognition of the concept of relative personal data in EDPS v. SRB (C-413/23), how should controllers and supervisory authorities assess whether pseudonymised data constitutes personal data for a given entity under the proposed Digital Omnibus Package amendment to Article 4 GDPR? Specifically, what technical and organizational criteria should be applied to determine whether re-identification is "reasonably likely" for that entity, considering indirect means (e.g., data combination, partner access) and the enforcement challenges this creates?

<u>International data transfers</u>

- 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 overlapping between those provisions?

<u>Repealing P2B regulation</u>

- P2B regulation appears to be repealed given the adoption of DSA and DMA. However, the scope of the P2B regulation seems a bit different and focuses more on transparency of contracts from online intermediation services. In this regard could the Commission explain in more detail what are the overlapping provisions in those regulations and how DSA and DMA exhaustively include the provisions, scope and objectives of the P2B regulation?

<u>Single-Entry Point (SEP)</u>

- Article 9 of the Digital Omnibus, modifying art. 23 of the NIS2, states that "Member States shall ensure that critical entities notify **<u>via the single-entry point</u>** established pursuant to Article 23a of Directive (EU) 2022/2555 the competent authority, without

undue delay, of incidents that significantly disrupt or have the potential to significantly disrupt the provision of essential services.". *Do we understand correctly that this means:*

- *reporting via the SEP would be obligatory?*
- *And thereby no longer allowed via national platforms? Not even for purely national incidents?*
- *That Member States would have to amend their national legislations to impose this for NIS2 & CER?*

  - *If so, does this change the nature of the Directive?*

- *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?*

- With regards to the link with the CER (Critical Entitities Resilience) Directive, *the designation as a critical entity is strictly on a need-to-know basis, according to national legislation on the matter. Therefore:*
  - *What kind of information will be asked for when an incident is notified? Can this contain sensitive or even classified information?*
  - *How will the information be treated by the Commission? Is there a common database? Will a contractor be designated to develop the tool?*
  - *There is an obligation on the MS to provide an incident report under the CER Directive as from 2028 on. How does this obligation of reporting on incidents aligns with the idea of developing a common tool?*
  - *What will be shared with who? We understood out of the explanation by DG CNECT that an information flow would be created to the authorities in the MS. But which representatives in the MS will receive the information and how? What if an incident is a CER and NIS2 incident? Or a CER and a GDPR incident? Will sensitive information on the entity be shared?*
  - *What will be the level of security of the platform?*
  - *What if critical entities provide essential services in several EU MS, and the incident that occurs is one of a cross-border nature. Does this not interfere with procedures already in place, for example with the existing Blueprints?*

- *Given that this consists probably mainly national incidents and not necessarily incidents with a cross-border impact, how do you see the principles of sovereignty and subsidiarity in this regard?*

- the AI Office enforcing the AI Act. Will there be a mechanism for cooperation and coordination (for example regarding sequence of events in enforcement)?

- *How does the Commission foresee the interaction between the EU entry point and national CSIRTs and competent authorities, especially for incidents that only have a purely national impact?*

- *The purpose of this proposal is to simplify reporting for entities. What was the methodology used to calculate how much companies would save if they use the SEP?*

- *Similarly, how were the estimated costs for ENISA and for Member States determined with regard to the maintenance and development of the proposed SEP?*

- *Central storage: will incident notifications purely be forwarded to the relevant authorities, or will they also be saved centrally as well?*
    - *Since Art. 6 states that entities using the SEP should be able to retrieve and supplement information that they have previously submitted via the SEP, some form of central storage will be required?*
    - *Would this not be a huge security risk, centralizing an overview of weakest points and dependencies in our digital ecosystem?*

- *Harmonizing timelines. The purpose of the platform is to allow "report once, notify many". Yet timelines for NIS2 (24/74h) and even GDPR (now proposed as 96h) seem to require to report as several moments. Will a SEP then truly allow to report once?*
    - *Will reporting timelines across different EU laws be harmonized to prevent multiple reports of the same incident, and if yes, how?*

- *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?*

***

Digital Omnibus: compilation of technical Questions – BELGIUM (#2)

<u>Single-Entry Point (SEP)</u>

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

- Is it foreseen that incident notifications reported to the single-entry point are further disseminated/dispatched to the relevant competent authorities, or rather that such

competent authorities (more specifically their supervisory staff) consult/analyse the incident notifications in the ENISA platform?

- Does the Commission have detailed numbers/information on the following?
    - Percentage of incident notifications reported under DORA that are also reported by financial entities to other authorities directly. 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.
    - The supposed underreporting as mentioned in the explanatory memorandum.

CZECHIA

CZ Questions for the PRES, Commission regarding the Digital Omnibus

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.

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?

***

CZ Questions for the PRES, Commission regarding the AI Omnibus

Technical questions regarding NANCO codes

1. Draft NANDO codes in Annex IV of the digital omnibus are identical to the draft NANDO codes put forward 5 November 2025 at the online meeting of the AI Board subgroup for Notified Bodies, with the exception of AI technology-specific codes 3.a) Symbolic AI, expert systems and mathematical optimization, their designations differ in the drafts.
   Designations of the codes in the digital omnibus:

   - AIH 0101 Logic- and knowledge-based AI systems that infer from encoded knowledge or symbolic representation, expert systems;
   - AIH 0102 Logic-based AI systems, excluding basic data processing.

   Designations in the draft of the AI Board Subgroup for Notified Bodies differ for the identical AIA codes:

   - AIH 0101 Symbolic AI and expert systems;
   - AIH 0102 Mathematical optimization, excluding basic data processing.

   The question is, which of the designations of NANDO codes AIH 0101 and AIH 0102 are correct?

2. On what basis were these AI technology-specific NANDO codes proposed in Annex XIV of the digital omnibus? What is their difference based on? It is based on an EN or ISO standard?
3. We consider the correct identification of NANDO codes in Annex XIV of the digital omnibus to be crucial not only for notifications under the AI Act, but also for AI system providers, market surveillance and the application of the entire AI Act in practice. Providers of high-risk AI systems will need to easily identify from the NANDO system who to ask for a third-party conformity assessment. Providers will therefore need to identify which AI technology-specific NANDO their AI system falls under. In our view, the development of useful NANDO codes requires a public consultation. For this reason, we propose a public consultation for providers of high-risk AI systems on the topic of NANDO codes.
4. We propose that the nine vertical NANDO codes be reduced to three, i.e. codes AIB 0201, AIB 0202 and AIB 0203 are merged into AIB 0201; codes AIB 0204, AIB 0205 and AIB 0206 are merged into AIB 0202 and codes AIB 0207, AIB 0208 and AIB 0209 are merged into AIB 0203. The reason is that the Czech data protection authority sees no reason to distinguish between Annex III.1.a, Annex III.1.b and Annex III.1.c. There may be remote AI systems used for emotion recognition, etc.
5. We suggest that the NANDO codes be supplemented with guidance, as it is not clear whether each AI technology-specific code is unique, or whether an AI system falls under multiple AI technology-specific codes. It is also not clear what criteria should be used for inclusion in the AI technology-specific NANDO codes: predominant characteristics or determining characteristics?
6. Do the NANDO codes have coherent criteria? For example, the GPAI category is more important than whether the AI system processes only text data, or whether it also includes audio and video.

7. What is the intended connection of the NANDO codes to other related regulations, e.g. harmonisation legislation in Annex I of the AI Act, the Cyber Resilience Act, the GDPR?
8. In relation to point (13) of the digital omnibus (which concerns Article 43, where paragraph 3 is replaced), we would like to ask for clarification of the last sentence of the second subparagraph: “Without prejudice to Article 28, such notified bodies which have been notified under the Union harmonisation legislation in Section A of Annex I, shall apply for designation in accordance with Section 4 at the latest [18 months from the entry into application of this Regulation].” For what reasons can such notified bodies only apply for designation no later than 18 months after the application of this Regulation?

Furthermore, we have a few specific comments on the proposed NANDO codes:

1. Table 3. b) Machine learning, excluding GPAI and single modality generative AI. Line AIH 0203 (AI systems that process text data) is single modality. Therefore, it is confusing why the table title says “excluding single modality”. There is an internal contradiction here.
2. Table 3. b) Machine learning, excluding GPAI and single modality generative AI; specifically, line AIH 0205 AI systems that learn from their environment, excluding agentic AI. In practice, machine learning systems that learn from their environment use an agent to learn. Therefore, the proposed wording of a system that learns from its environment and is not agentic AI is internally contradictory. It is therefore necessary to clarify what exactly is intended by this proposed wording.
3. Table 3. b and 3. d. both mention agentic AI. What are the definitions? Are they two different categories?
4. How will the conformity assessment be carried out in the case where one AI technology can exhibit the characteristics of multiple NANDO codes? Will the AI technology be described by multiple NANDO codes at the same time? Who will then carry out the conformity assessment? Or will the AI technology be divided into individual parts that will be assessed separately (in which case only one NANDO code will always be listed).

GERMANY

Questionary on the Omnibus VII Proposal

I. Digital Omnibus on AI

1. We generally welcome the suggestion to extend and flexibilise the applicability periods for the rules on high-risk AI. Could the COM provide the rationale for giving itself such a decisive role in determining the exact dates? As the question of availability of standards that are adequate, meaningful and sufficiently supportive is crucial for MS, public authorities, notified bodies and national companies subject to the AI Act, we kindly ask: how will the MS will be involved and why aren't they involved more strongly?

2. Against the background of the proposed amendments to Article 113 of the AI Act concerning the extension of the periods for the entry into application for high-risk AI, it must be noted that significant legal uncertainty persists until the formal conclusion of the trilogue on the Digital Omnibus on AI. The periods set out in Article 113 of the AI Act are already binding law and pertain to a particularly sensitive area. The COM is therefore kindly requested to provide clarification on how the proposed extension of these periods in the area of high-risk AI should be addressed from both a business perspective and in administrative enforcement.
   In this context specifically: How does the potential postponement of compliance obligations affect our current procurement projects for high-risk AI? Do we need to adjust contracts because suppliers now have more time for certification?

3. How does COM intend the process, leading to the decision needed for the AI Act high-risk rules & harmonized standards to come into force? In particular, what will be the nature of the guidelines, mentioned, for example, in Article 31 be, will Member States and ESOs/NSBs be involved, and how will that relate to harmonized standards from a legal perspective? How will coherence with European and international standardization be ensured?

4. In our view, the Digital Omnibus package should be used to provide necessary clarifications regarding the definition of an AI system in the AI Act, ensuring that systems primarily based on simple statistical models widely used in the financial sector are clearly excluded. How will the COM address this issue, and what form will the clarification take?

5. The AI Omnibus contains a proposal to add definitions of SMEs and SMCs to Article 3 of the AI Act, but not a definition of start-ups. What is the reason for this? How does the COM intend to deal with the fact that the AI Act, as a consequence, lacks a definition of start-ups?
   - Furthermore, any specialised digital forensic tools come from small niche vendors. Will these suppliers benefit from simplified documentation and quality-management obligations under the amended AI Act, and does this realistically reduce our administrative burden when auditing and validating such tools – or will we need to compensate via stricter contractual audit rights and in-house technical verification?

6. Why does the AI Omnibus not contain the required and urgently needed clarifications of important definitions/concepts and regarding the distribution of responsibilities along the AI value chain (e.g., provider/deployer)?
   - For example in complex public security projects (joint development with IT service providers, shared infrastructures), how should we allocate the roles of „provider“ and „deployer“ under the AI Act, and how does this affect our liability, registration duties, and incident reporting obligations?

7. Why does the Omnibus contain the required and urgently needed clarifications of the research exemptions in Article 2(6) and in Article 2(8) of the AI Act not as legislative measure, but only as a “further measure to facilitate compliance” through guidance on the practical application of these exemptions? In its position paper, DE called for an expanded research exemption. What is the reason for not having introduced this idea in the AI Omnibus?

8. The Omnibus does not offer any solutions (beyond conformity assessment issues) to the central problem of the unclear interaction between the AI Act and sectoral legislation (e.g., Medical Devices Regulation, Machinery Regulation). What is the reason for this? How does the COM intend to resolve these issues in a simplified way not overburdening all relevant players?

9. What changes will the proposed Omnibus bring to the timetable for the COM to issue harmonized standardization requests for GPAI and "Green AI", in accordance with Article 40? By when does the COM plan to publish the corresponding standards? What importance will the current Code of Practice have in the development of harmonized standards in the field of GPAI? In particular, will it contain recommendations or binding requirements for standardization?

10. The AI Omnibus envisages transferring the supervision of certain AI systems based on a general-purpose AI model (gpAIM) or AI systems embedded in very large online platforms or very large search engines to the EU AI Office. Can the COM comment on the figures of use cases involved (how many AI systems in absolute terms, as a percentage)? What is the rationale for excluding Annex I AI systems? Why is the focus of supervision not solely on AI systems based on GPAI models with systemic risk? In this context, please provide more explanation for the new drafting of Art. 75(1) AI Act, as outlined in paragraph 25.

11. Concerning paragraph 25: The competence of the AI Office concerning the market surveillance on general-purpose AI systems seems very broad. How is it delimited from market surveillance activities of other competent authorities when AI general-purpose AI systems are integrated in high-risk AI systems (e.g. in the justice sector)? How would Article 74 (8) AI Act be accounted for?

12. Why did the COM not include additional proposals of the DE position paper in the AI Omnibus, for example the removal of the Fundamental Rights Impact Assessment (FRIA) under Article 27 AI Act or clarification of responsibility after the fine-tuning of a model in different scenarios?

13. Will the Digital Omnibus on AI offer the opportunity for correcting erroneous translations in some non-English versions of the AI Act?

14. In its Explanatory Memorandum, the COM enumerates „further measures to facilitate compliance with the AI Act and address the concerns raised by stakeholders“. The list does not include a revision or update of the already published guideline in the AI Systems definition.

Germany and other stakeholders have repeatedly called for such an update to address inconsistencies in the guideline. Does the COM not agree that greater clarity on what constitutes an AI system would contribute to its aim of a clear, simple and innovation-friendly implementation of the AI Act?

15. With regard to regulatory sandboxes, how will the results of real-world testing that are relevant to AI Act standardization find their way into the future standardization process, also with regard to regulatory learning?

16. Regarding Article 1(6), (14) and (32) of the AI Omnibus: Given that the EU database also serves as an tool for market surveillance, how would national competent authorities maintain adequate oversight of AI systems covered by Article 6(3) if their registration is no longer required? What will be the starting point for a control of the provider's assessment by the market surveillance authority

17. Concerning paragraph 6, 14 and 32: If registration of exceptionally non-high-risk-AI-systems is no longer required, what will be the starting point for a control of the provider's assessment by the market surveillance authority?

18. Concerning paragraph 26 (Article 77 AIA): How is the restriction of information and access rights for authorities protecting fundamental rights justified? How does the restriction relate to information and access rights granted by other legal acts (e.g. GDPR)?

II. Digital Omnibus

19. Concerning the „single-entry point for incident reporting" (Art. 23a of Directive (EU) 2022/2555, NIS2):

    19.1. How would identification of the reporting entities work in practice? Would entities have to register on the national as well as on the European level to use the single-entry point?

    19.2. According to Article 23a(6) the COM shall assess the proper functioning, reliability, integrity and confidentiality of the single-entry point after it is piloted by ENISA. Are there any provisions for re-assessments, for example after updates? What happens if the assessment changes? Would member states need to provide fallback solutions on a national level?

    19.3. The single-entry point would centrally process information that potentially impacts the national security of member states, making it a high value target for foreign adversaries. How does ENISA intend to ensure the required security level, not only to prevent cyber attacks but also other forms of espionage?

20. Germany welcomes the EU COMs undertaking to use the Digital Omnibus as a legislative vehicle, to make data rules simpler, clear and more cost-effective for businesses. Against this backdrop, Germany refers to the demands set out in its Position Paper on the COM's Digital Omnibus (dated 23 October 2025) and the Non-Paper on GDPR reform (dated 23 October 2025) and asks the EU COM to elaborate to what extent the comprehensive compliance requirements under the Data Act (especially information and notification obligations) were critically examined and why no adjustments were made in this regard. The same applies to more far-reaching exemptions for SMEs and volunteer-based organisations, namely regarding Chapter II, and the relationship between GDPR and Data Act.

21. In addition, Germany recommends to critically examine the need for enforcement of the Data Act through public authorities. As far as the Data Act establishes rights between private parties, enforcement of such rights should primarily be in the responsibility of the contracting parties and the civil courts.

22. Consolidating the Data Act:
    22.1. How will the COM ensure that data from EU companies and citizens continue to be processed securely, particularly with regard to cross border data transfers and the application of extraterritorial laws?
    22.2. From a technical perspective, what does the transfer of directives into a regulation (Data Act) mean for the implementation laws across the Member States?

23. Germany recommends streamlining and harmonising EU governance structures – such as the European Data Innovation Board (Art. 29/30 DGA) and the European Data Protection Board (Art. 68/70 GDPR) – so that data related legal acts are applied uniformly across all Member States. How does the COM regard this proposal, how does it evaluate the potential benefits for uniform implementation across Member States, and how does it anticipate the necessary steps to realise such coordination?

24. Regarding the EDIB: The Digital Omnibus introduces more flexible structures to the EDIB. However, there are currently no obligations for deliverables/outputs. Ideally, the EDIB's work will result in transparent and traceable outcomes such as a rulebook for DAOs, binding/non-binding interpretation guidelines, FAQs for certain areas etc. Can the EU COM elaborate on the future structure of the EDIB on working level?

25. Can you please elaborate on how the changes to the requirements DISP have to fulfill (i.e. Art. 12 DGA, now Art. 32c Data Act inter alia) balance the political goals of building trust within the market and especially data sharing services against reducing bureaucracy and regulation for DISPs?

26. Germany welcomes that Article 36 Data Act will be deleted. In this context, what are the EU COMs considerations to keep smart contracts within the scope of Article 11 para 1 sentence 1?

27. Regarding new Chapter VIIc: Please elaborate on the rationale for the new chapter on the re-use of data and documents held by public sector bodies. To what extent are these rules new (and not only merged from former acts), in particular for contracting authorities and contracting entities under the public procurement regimes from directives 2014/24/EU, 2014/25/EU, 2014/23/EU and regulation (EC) 1370/2007, potentially also 2009/81/EC? What is the expected effect on procurement procedures, procurement documents and contract (award) notices? Have the proposed rules been consulted with the procurement experts in DG Grow and the procurement Excellence hub?

28. Under Art. 4 of the Regulation (EU) 2018/1807 tax-related data localisation requirements are justified on the grounds of public security. We assume that this interpretation is still applicable under the new Art. 32h of the Regulation (EU) 2023/2854. Is this correct?

29. Protection of Small and Medium sized enterprises (SMEs) and Small Mid-Cap companies (SMCs): How will the COM monitor and evaluate the impact of these simplifications on the market position of SMEs/SMCs, and what corrective mechanisms will be put in place if data concentration trends emerge?

30. Regarding the integration of (EU) 2019/2024 (Open Data Directive) in the Data Act: What adjustments deems the COM necessary due to the integration of the ODD into the Data Act with regard to the scope of national implementations?

Questions concerning GDPR and GDPR-related provisions in other legal acts

General questions:

31. Which proposals serve the aim of reducing bureaucracy related to data protection law.

32. Which proposals emphasize the risk-based approach?

33. What are the next steps planned by the COM and what is the timeline of possible further GDPR reform, especially with regard to the assessment of possibly necessary adjustments of the GDPR with regards to AI?

Questions concerning Art. 4 point 1 GDPR (page 54-55):

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

35. What is the exact meaning of “entity”?

36. Should the term “entity” be defined separately in the GDPR (as far as can be seen right now this term is only used in Art. 47 GDPR)?

37. Why is the amendment only referred to entities, although it says in the beginning “Information relating to a natural person is not necessarily personal data for every other person or entity”?

38. The use of “other” or “another” is unclear. How does this relate to the controller? Does it refer to persons or entities other than the controller?

39. Why does the proposal not provide for an explicit reference to anonymisation or pseudonymisation (for example to Article 41a)?

40. Which use cases led to the proposal? Are there any examples for use cases in which entity #1 is able to identify a natural person with particular data while entity #2 may not be able to do so?

41. Why did the COM choose the option of changing the definition of “personal data” which would apply to all controllers instead of proposing a risk-based approach?

42. If a processor does not have the means to identify a person, is it then excluded from the GDPR? What if they (unlawfully) make secondary use of the data? In that case, would Art. 28(10) GDPR still apply?

43. Does this definition exclude online tracking or large data brokers who only sell data based on pseudonyms such as device IDs or cookie IDs?

44. What about a person/entity that cannot identify the data subject transmitting the data to a third country without equivalent protection, where it can be identified? Does that also fall under Chapter V of the GDPR on data transfers?

45. If two companies now process data together but one company does not have access or cannot identify it and is then excluded from the GDPR ("joint controllership"), how does that work if one falls under the GDPR and the other does not?

46. How are supervisory authorities supposed to assess the technical means and subjective intention of companies? According to the proposed definition, supervisory authorities would have to do that in order to determine the applicability of the GDPR.

47. Is the proposed definition supposed to apply retroactively? For example, persons who took part in a pharmaceutical study before 2025, believing that their data was protected by a pseudonym, would they now lose their protection (from which they benefitted under the unamended GDPR) retroactively?

48. Will entities that are not able to identify the data subject be allowed to share the data with others, transfer the data to third countries or even publish the data?

49. What is the relationship between the new definition of personal data and the judgement of the European Court of Justice in the Breyer case (C 582/14), where the Court found "that a dynamic IP address registered by an online media services provider when a person accesses a website that the provider makes accessible to the public constitutes personal data within the meaning of that provision, in relation to that provider, where the latter has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person."? Would an IP address still constitute personal data in such a situation?

Questions concerning Article 4 point 38 and Article 5 (1)(b) GDPR (page 55):

50. Could you please describe the adjustments for science and research that the draft contains?

51. Can the COM give examples of when a purpose declared by a company cannot be defined as a research purpose?

52. How are ethical standards determined?

53. What is the exact meaning of "wellbeing"?

54. What is the difference between "wellbeing" and "public interest"?

55. Which kind of research is <u>not</u> meant to fall under the definition?

Question concerning "health data":

56. Why has the COM decided not to define „health data" (Article 9 GDPR)?

57. 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?

<u>Questions concerning AI systems and AI models:</u>

Questions concerning Art. 9 (2)(k) and 9 (5) GDPR (page 55-56):

58. Does the proposed amendment in Article 9(2)(k) GDPR aim to allow Article 9 data to be processed for AI development and operation?

59. Does the COM share the view that the proposed provision in Article 9(5) confirms rather than overrides the prohibition on processing in Article 9(1), since, according to the proposal in Art. 9 (5), the controller must avoid the processing of Article 9 data, remove Article 9 data, and, if removal is disproportionate, protect Article 9 data against use?

60. Article 9 (5) stipulates that the controller shall remove special categories of data, if they are identified in the data sets used for AI-training. Could the COM elaborate, which technical tools or methods are available to remove such data from large language models?

61. Article 9 (5) asks the controller to protect Art. 9 data "without undue delay" from being used to produce outputs. Why did the COM propose a protection "without undue delay" and not "before placing on the market"?

Questions concerning Article 88c GDPR (page 61):

62. To what extent does the proposed provision in Art. 88c reflect the EDPB Opinion 28/2024 of December 2024?

63. Do all other requirements of the GDPR continue to apply when invoking Art. 88c?

64. If so, why does Art. 88c specifically mention the principle of data minimisation, transparency, the right to object, and appropriate technical and organizational measures (TOM)?

65. Should, by explicitly mentioning the principle of data minimisation, transparency, the right to object, and TOM, the validity of the respective GDPR provisions be reinforced, strengthened or modified? If so, what does that mean for the controller that has to fulfil those provisions?

66. Does the COM share the view that, given the emphasis on data minimisation, transparency, the right to object and TOM, the processing of personal data for AI purposes will be made more difficult rather than easier compared to the current legal situation?

Art. 9 (2)(k), 9 (5) and 88c GDPR (pages 55, 56 and 61):

67. Please explain the reason for the inclusion of the "operation of an AI model" in Art. 88c subpara 1 and the "operation of an AI system" in Art. 9 para 2, point k, taking into account that this could lead to a situation where the mere use of an AI system or model for processing personal data would make obsolete the necessity to define a purpose for the processing of personal data.

68. How would Art. 88c and Art. 9 (2)(k) relate to the other legal grounds for processing personal data in Art. 6 (1) and Art. 9 (2)?

69. Why is there no differentiation between the development and the operation of an AI system?

70. Wouldn't it be necessary to also define the term "AI model" and not only the term "AI system"?

71. How does Article 88c relate to Article 32?

Questions concerning Art. 4a AIA (page 21 Digital Omnibus on AI):

72. To what extent does the proposed new Art. 4a AI Act clarify the ability, under GDPR and the Law Enforcement Directive, to use real investigative data – including special categories of personal data – for testing and training analytic AI models specifically for bias detection and error correction?

73. Which additional legal bases or national provisions remain necessary, if any?

74. How should we interpret necessity and substantial public interest for AI model training in the security and law enforcement context, in particular when relying on Art. 4a AI Act and the Law Enforcement Directive?

75. Which concrete safeguards (e.g. pseudonymisation, separate environments for training vs. operations, strict retention schedules, output-filtering) are required in practice to benefit from this derogation?

76. Is the relation between Art. 9 (2)(k) and 9 (5) GDPR and the proposed Art. 4a AI Act clear enough?

Questions concerning Art. 22 GDPR (page 57):

77. Why is it necessary to replace paragraph 1?

78. Does it have any consequence that the provision is no longer formulated as a right not to be subject to certain decisions?

Questions concerning Article 88a GDPR (page 59-60):

79. Since the new provision in Article 88a GDPR contains a new opening clause in para 2 opens up room for MS to set up national laws covering such access, does the COM take a possible fragmentation of the European single market, in particular in the area of commercial online media into consideration? What impact will the transfer of the rules for accessing terminal equipment to the GDPR have on the use of cookies?

80. How does the proposed Art. 88a relate to Art. 6? In particular, must the balancing of interests - required by Art. 6(1)(f) GDPR - still be carried out when “gaining of access to personal data already stored, in the terminal equipment of a natural person” with a view to “maintaining or restoring the security of a service” (Art. 88a(3d)?

Questions concerning Article 88b GDPR (page 60):

81. Could you please briefly describe how the issue of cookie fatigue is to be resolved?

82. Is it correct to assume that, following the amendment to Article 4(1) GDPR, cookies do not fall under 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?

83. Why did the COM not propose a detailed rule for Article 5(3) of the ePrivacy Directive, for example, following the model of what the Council decided regarding Article 8 of the ePrivacy Regulation proposed by the COM but not pursued?

84. The new provision in Article 88b stipulates that decisions made by data subjects regarding access to their end devices (e.g. cookies) must be respected for six months before they can be requested again. Article 88b(3) exempts media companies from this obligation. How does the COM reconcile this special provision for media companies, whose cookie banners account for the majority of those encountered by users on the internet, with the aim of counteracting cookie fatigue, while respecting that the possibility of refinancing through “consent or pay” offers from the media must be guaranteed in order to maintain the diversity and free access to media offerings that are necessary for a democracy?

Question concerning regulatory sandboxes:

85. The leak dated 6 November 2025 contained a provision on regulatory sandboxes in Article 57 concerning the tasks of data protection supervisory authorities. Why has this provision been removed, and does the COM plan to revisit it in a later proposal?

Questions concerning the relation between Data Act and GDPR:

86. Is the relation between the Four to one Data Act and the GDPR or national law on the protection of personal data clear enough?

87. Does Article 1 (5) of the Data Act stay unchanged and apply to all Chapters which apply to personal data?

ESTONIA

Please find below questions from the Estonian delegation, focusing on the cybersecurity incident reporting and the creation of the Single-Entry Point.

- When an entity needs to file a common report via SEP, how is the COM planning to tackle the language aspect of it? E.g. if an entity notifies about an incident to several competent authorities in several Member States (due to requirements from NIS2, GDPR and CER etc), then each Member State may expect that this notification is in their language.
- Is the use of SEP required for every entity or could there be some exceptions? E.g. public sector entities that need to follow NIS2 requirements due to Article (2)(f) of the NIS2 Directive?
- In regards to SEP, the Omnibus has listed NIS2 Directive, DORA Regulation, CER Directive and GDPR and it also mentions e-Privacy Directive, electricity sector requirements (NCCS), EU Digital Identity Regulation and aviation sector regulations. Should (and to what extent) this list also include LED Directive (2016/680) – see Directive's Article 30?
- The Omnibus plans to changes to the notification deadline for the personal data breach notifications (extend it from 72 hours to 96 hours) – how shall this have an effect to SEP?
- How does the COM plan to make a unified reporting template for using the SEP? Or are the entity still expected to fill the common information and the sector-specific information that a competent authority needs for their work and future activities?
- The proposal mentions that SEP is expected to be interoperable with the Business Wallets and that SEP might be one of the use cases of Business Wallets. Could the COM give additional information on what are the plans for Business Wallets regarding the SEP?

IRELAND

IE Comments on Omnibus VII (Digital)

26 November 2025

General comments

- Ireland welcomes the Commission's digital simplification Omnibus package, the seventh simplification Omnibus package proposed by the Commission as part of its broader simplification agenda.
- Ireland has strongly encouraged an ambitious digital simplification package, which supports the EU's strategic positioning as the location of choice for trustworthy digital innovation, while maintaining a central focus on protecting data privacy and fundamental rights of citizens.
- The proposals are a first step, and an important element of the overall approach to improving competitiveness at an EU level, in line with the Draghi Report and related work.
- By reducing barriers to investment and innovation, balanced with clear and predictable protections for citizens, we can unlock growth opportunities from the rapid acceleration of technological developments.
- Ireland recognises the importance of regulation to ensure markets operate efficiently and fairly, and to protect consumers. In this context, it is important that regulations are targeted and proportionate to the policy objective, whether it is to protect consumers and citizens, or to promote competition and innovation.
- Ireland has therefore advocated for a dynamic, ambitious and risk-based approach, focused on removing regulatory overlaps, reducing administrative burdens, and supporting compliance.
- It will also be important to future-proof our EU digital regulatory framework, with the overall aim of increasing the coherence and effectiveness of the EU Digital rulebook.
- This means ensuring that forthcoming digital regulations are developed with the same objectives around simplification, harmonisation and coherence strongly to the fore.
- In this context, Ireland is also very supportive of the broader review of the digital rulebook that will be provided by the Fitness Check of the Digital Acquis.
- Ireland's initial comments and questions on the digital simplification Omnibus package are provided below.

1. Data Act

IE thanks the Commission for these proposals and welcomes many of the ambitions of the proposal which will create a more harmonised landscape for business and Member States.

Amalgamation of the Open Data Directive, the Free Flow of Non-Personal Data Regulation, the Data Governance and the Data Act into a single consolidated Data Act will streamline the data framework providing greater clarity and alignment of the data rulebook.

Strong safeguards regarding the use of personal data should remain in place in alignment with core objectives of the GDPR.

IE notes that essential principles of public trust, transparency, data protection and improved public outcomes and public good are central to any simplification package.

IE welcomes the expansion of the EDIB membership and greater involvement of the EDIB will help to ensure harmonised implementation of the Omnibus data acquis across Member States.

IE welcomes the simplification of the notification procedures in the DGA but notes that we must guard against the risk of the ability to opt-in/opt-out of certain regulatory provisions, thus having unintended consequences such as making the regulation of these emerging sectors more challenging for competent authorities and causing confusion for data users.

IE welcomes the requirement that data intermediation service providers (DISPs) need only be functionally separate entities and not a separate legal person and, allied to the proposal to permit DISPs to provide value-added services, may improve their commercial viability and encourage their establishment in Ireland. In this regard, there are no DISPs or DAOs registered in Ireland currently.

Questions

Does the Commission envisage that the general right to complaint under Article 38 of the Data Act will now apply across all of the consolidated data acquis? Would the role of the Data Coordinator then apply across all of the consolidated data acquis in relation to complaints?

How is the EDIB intending to manage large meetings and deliver on its objectives? The EDIB has a wide mandate, and meetings will have a diverse range of stakeholders, some of whom may have conflicting viewpoints. Will the frequency of meetings be increased?

Comments on specific provisions

Explanatory Text	IE Comment
Paragraph (1) updates the scope of Regulation (EU) 2023/2854 (Data Act) into which new chapters will be inserted as explained further below.	**Welcomes updating of scope to reflect new provisions.**
Paragraph (2) amends definitions and inserts new ones.	**Welcomes updating of definitions for greater alignment across the data acquis and to provide for the new provisions.**

Paragraph (3) creates a new rule under Article 4(8) of Regulation (EU) 2023/2854 (Data Act) that allows data holders to refuse disclosure of trade secrets to a user when there is a high risk of unlawful acquisition, use, or disclosure to third countries, or entities under their control, that are subject to jurisdictions with weaker protections than those available in the Union.	**Welcomes stronger trade secrets protections for data holders.**
Paragraph (5) introduces the same rule for Article 5(11) of Regulation (EU) 2023/2854 (Data Act), concerning data holders disclosing trade secrets to third parties.	**Welcomes stronger trade secrets protections for data holders.**
Paragraphs (5) to (19) narrow the scope of Chapter V from 'exceptional needs' only to 'public emergencies'. It deletes Article 14 and 15, and creates a new Article 15a, which becomes the sole Article for requesting during public emergencies under the B2G regime of Regulation (EU) 2023/2854 (Data Act). The requests can be made when necessary to respond to a public emergency (Article 15a(2)), or to mitigate or support the recovery from a public emergency (Article 15a(3)). Cross-references are adjusted accordingly, language simplified and clarified. Article 1 paragraph (21) creates a new Article 22a that frames the complaints regime under Chapter V, merging previously repeated provisions.	**Preliminary view that this is a welcome change to more accurately define the scope of Chapter V, however still under review.**
Paragraphs (20) to (22) include certain exemptions to Chapter VI of Regulation (EU) 2023/2854 (Data Act) (switching between data processing services): In Article 31, a lighter specific regime is inserted for data processing services that are custom-made, i.e. data processing services that are not off-the-shelf and would not function without prior adaptation to the needs and ecosystem of the user, where these are provided based on contracts concluded before 12 September 2025. Similarly, in Article 31, a new lighter specific regime is inserted for data processing services provided by SMEs and SMCs on the basis of contracts concluded before 12 September 2025, accompanied by a clarification that these providers can include early-	**Welcomes lighter regimes for custom-made services and also the expansion of SME exemptions to small mid-cap companies.**

termination penalties in fixed-term contracts.	
Paragraphs (23) to (25) include modifications to Article 32 of Regulation (EU) 2023/2854 (Data Act) resulting from the integration of bodies currently governed under Regulation (EU) 2022/868 (Data Governance Act) into Regulation (EU) 2023/2854 (Data Act).	**Under review.**
Paragraph (26) removes obligations on providers of smart contracts to comply with essential requirements with an empowerment for the Commission to adopt harmonised standards.	**IE welcomes removal of smart contracts.**
Paragraphs (27) integrates two legal regimes currently in Regulation (EU) 2022/868 (Data Governance Act), a Regulation that shall be repealed once the Omnibus enters into force. This point reforms current rules in chapter III and IV of the Data Governance Act that provide for a compulsory notification regime for data intermediation services providers and for a voluntary registration regime for data altruism organisations. The two regimes shall be inserted as a new Chapter VIIa into Regulation (EU) 2023/2854 (Data Act). In light of the emerging nature of the market for data intermediation services, the obligations of regulation (EU) 2022/868 (Data Governance Act) shall be made more flexible for this market to grow: For one, the regime for data intermediation services providers shall be turned into a voluntary regime. Second, the most critical obligation, the obligation to keep data intermediation services legally separate from any other service a company may want to offer, will be replaced by an obligation to keep services functionally separate paired with an additional set of conditions. Finally, the list of obligations is drastically shortened. As concerns data altruism, reporting and transparency obligations for data altruism organisations are repealed as well as the idea to supplement the rules of Regulation (EU) 2022/868 (Data Governance Act) in a "data altruism Rulebook" with even more detailed rules.	**IE notes the proposal for the simplification of the notification procedures for DISPs and DAOs and the use of official logos as well as the streamlining of the conditions attached to the services. However, to the extent that the regulation of the sector is desirable, we must guard against the risk of an opt-in register and the ability to opt-out of regulatory conditions having unintended consequences that could make the regulation of these emerging sectors more challenging for competent authorities and cause confusion for data users.** **IE welcomes the requirement that data intermediation service providers (DISPs) need only be functionally separate entities and not a separate legal person.**

It introduces a new Chapter VIIb under which the prohibition of localisation requirements for non-personal data withing the Union, formerly contained under the to be repealed Regulation (EU) 2018/1807 (Free Flow of Non-personal Data Regulation) is inserted into Regulation (EU) 2023/2854 (Data Act). The obligation to notify the Commission is maintained but abolishes the national online single information point where Member States should publish applicable data localisation requirements.	**Under review.**
Paragraphs (4), (33) – (58) introduce the merged provisions on the re-use of data and documents held by public sector bodies under Chapter II of Regulation (EU) 2022/868 (Data Governance Act) and Directive (EU) 2019/1024 (Open Data Directive).	**IE notes and welcomes the alignment of the provisions set out in Chapter 2 of the DGA (voluntary sharing of data with protected characteristics held by public sector bodies) with the Open Data Directive given the complementary nature of both.**
Paragraph (57) integrates the basic rules on the European Data Innovation Board (EDIB), a group advising the Commission on the consistent enforcement of the Data Act and serving as a coordination forum for policy-making in the domain of data economy policies. It will integrate the basis rules into the Data Act. The changes will allow the Commission to modify the relevant foundational documents of the EDIB (the Commission decision of 20 February 2023 – C(2023)1074 final) and expand the membership to representatives of national policy-making in addition to competent authorities.	**IE notes the absorption of the EDIB into the Data Act and welcomes the expansion of the EDIB membership.** **Greater involvement of the EDIB will help to ensure harmonised implementation of the Omnibus data acquis across Member States.**
Paragraphs (61) - (65) contain amendments to the provisions of Regulation (EU) 2023/2854 (Data Act) on Committee procedure and the power of delegation, and points (66) on Regulation (EU) 2022/868 (Data Governance Act) necessary to introduce the rules of Regulation (EU) 2022(868 (Data Governance Act) and Directive (EU) 2019/1024 (Open Data Directive) into Regulation (EU) 2023/2854 (Data Act).	**IE notes this.**
Paragraph (68) extends the special focus for SMEs in the context of evaluation to SMCs and point (69) introduces the evaluation of	**IE welcomes the evaluation of the new rules' effect on SMEs and SMCs.**

the newly inserted rules into Regulation (EU) 2023/2854 (Data Act).	
Article 2 introduces in Regulation (EU) 2018/174 the relevant references to data intermediation services and data altruism in the annex related to 'starting, renewing and closing a business'	**Under review.**

2. GDPR

Proposal to amend Article 5(1)(b) GDPR – scientific research

We note that this amendment clarifies that further processing in limited circumstances shall be considered compatible with processing for initial purposes and be independent of the conditions under Article 6(4) GDPR. To provide sufficient guidance and clarity to stakeholders, consideration may be required as to further specifying the type of processing operations/activities which fall within the scope of this provision.

Proposal to amend Article 9 GDPR – special category processing

To better understand the practical impacts of this amendment, we would appreciate further information on the obligations to implement "appropriate organisational and technical measures" to avoid the collection and otherwise processing of special category data.
Is this intended to be entirely subjective, with it being sufficient that each controller is satisfied as to what constitutes 'appropriate measures'.

Proposal to amend Article 13(4) GDPR – information to be provided to data subjects
We would welcome further information on how the Commission sees this working in practice. In particular, where will responsibility lie for determining which type of activities are 'not data-intensive'?

We would also welcome further information on how paragraph 3 would interact with existing transparency obligations.

Proposal for new Article 88c GDPR – Processing for the development and operation of AI
We note that this would be the first time that the GDPR will depart from being a horizontal, technology neutral instrument, with a specific carve out for AI.

We welcome the additional protection afforded to children and note the importance of ensuring and sufficient protection for the fundamental rights and freedom of data subjects.
We also note that provision is made for ensuring "appropriate organisational, technical measures and safeguards for the rights and freedoms of the data subject". Having regard to the choice of legal basis for this processing, we would welcome further information on how in practice the balancing exercise as regards the "the interests, or fundamental rights and freedoms of the data subject" may operate.

Proposal to amend the ePrivacy Directive

We note that with amendment to Article 5(3) of the ePrivacy Directive, the scope of application of the GDPR is being broadened to include matters that would have previously fallen within scope of ePrivacy. We are seeking confirmation of the implications of this change, including as to the intended enforcement model and whether ePrivacy is now in part (in so far as it relates to personal data) being brought under the one stop shop model and remit of the EDPB by virtue of the Article 60 procedure in GDPR.

3. **AI**

Ireland welcomes the Commission's simplification proposal outlined in the Digital Omnibus on AI (2025/0359 (COD).

Ireland would welcome a centralised and clear messaging from the Commission to all stakeholders that the simplification of the AI Act is a deconstruction of the AI Act and it is not deregulation.

Ireland would welcome further clarification from the Commission on a some of the proposed amendments, as outlined below;

- we would welcome further clarification from the Commission on the rationale behind the introduction of the new Article 4a which deletes Article 10.5. Note, we are consulting with our stakeholders on this point as well, and believe it may have impact on the GDPR
- Article 57 Amendments ; we would welcome further clarification on whether this will bring further obligations to the national competent authorities in August 2028.
- Also in relation to Article 77, IE would like to understand the reason for removing the reference to high-risk AI systems in Annex III.

Ireland would like to note that we are currently reviewing the proposal in detail in conjunction with the national stakeholders and experts.
Ireland would like to thank the Commission for its continued support as we progress our national implementation and looks forward to working constructively with the Commission to ensure the AI Act's meets the EU's wider AI policy objectives.

4. **Cyber Security**

- Ireland welcomes the efforts to simplify the reporting of incidents and to link it in with reporting across the digital landscape. However, we do have concerns a single point of entry is also a single point of failure from a cyber security perspective. Regardless of whether ENISA stores the information or not, there will be one main route to report incidents. This in itself can become a vulnerability should there be technical fault, or it becomes a target itself.

- Ireland's National Cyber Security Centre is finalising the development of Ireland's reporting platform to support the implementation of the NIS2 Directive and it has been agreed reporting in relation to the CER Directive will also take place via this one single platform and other National reporting platforms, such as those for GDPR reporting are well established in the State. Ireland would request further clarity regarding the interoperability of the single- point of entry with the range of existing incident reporting mechanisms in Member States without creating conflicts or duplication.

- Furthermore, the Omnibus also does not address some of complexities of incident reporting and handling. For example, ensuring the appropriate National Competent

Authority gets the appropriate information in relation to entities falling into more than one Sector and where there are cross boarder incidents under the NIS2 Directive is a task the National SPOC and CSIRT in cooperation with our National Competent Authority Forum will play a key role in.

- Ireland also has concerns regarding this approach, as it crosses into the national security space, which is the responsibility of the Member State alone. Member States rely on immediate high-fidelity reporting to maintain national threat situation awareness. A centralised single point of entry may cause delays or fragmentation to this vital flow of reporting and undermine key relationships and trust built up over time with our National CSIRT.

- Ireland is of the view that harmonised reporting templates and reporting timeframes would greatly reduce the complexity of reporting requirements. While a single-entry point for reporting is useful, the majority of entities' time and capacity is consumed by the act of reporting itself which the Omnibus does not address in detail. More clarity on what the approach the Commission proposes in this regard would be welcome.

- Ireland also notes that the responsibilities of building the single point of entry platform and maintaining it are being assigned to ENISA. It is imperative that this is adequately resourced and funded and it is factored into their overall mandate which has grown substantially in recent years It will also need to considered in relation to the revision of the Cybersecurity Act in 2026.

SPAIN

ES QUESTIONS TO OMNIBUS VII

AI Questions

Questions about wording or scope of the text:

Article 4: Changes in literacy obligations

The change in the approach to AI literacy, in which literacy is removed as a requirement for providers and instead it is established that the Commission and Member States will encourage providers and deployers to adopt literacy measures:

- Does this constitute an obligation for Member States that could constitute a sanctionable infringement?

- What are considered sufficient measures to consider that a provider is complying with the instructions of the Member States?

Article 11: Reduced technical documentation.

- Does the possibility for SMEs, including startups, to submit technical documentation in a simplified manner also apply to companies whose systems are covered by legislative acts of Annex I?

This question is raised because according to Article 43.3, in the case of high-risk AI systems regulated by legislative acts listed in Annex I, Section A, the provider shall follow the relevant conformity assessment procedure required by those acts. In this regard, clarification is required from the Commission on the applicability of Article 11 since certain harmonized legislation, for example, Regulation 2017/745 on Medical Devices, and Regulation 2017/746 on in vitro diagnostic medical devices, do not contemplate in the context of their conformity assessment the possibility of submitting simplified technical documentation for such companies.

Article 28.8 and Article 29.4: Single designation procedure and possibility of submitting a single designation application for conformity assessment bodies in Annex 1, list A.

- For new applications and in cases where standardized designation application models already exist for their legislative acts, how would the possibility of submitting a single designation application be applied? As an illustrative example, designation under the Medical Devices Regulation and in vitro diagnostic medical devices is cited, where standardized designation application models and scope of application of NANDO codes for their regulations already exist (NBOG F 2017-1, 2017-2, 2017-3, 2017-4 formats).

- In cases where the designation procedure under sectoral legislation, such as in Medical Devices, requires the establishment of joint assessment teams composed of expert representatives from the Commission and experts from Member States other than the one where the applicant conformity assessment body is based, how would the joint assessment procedure of the AIR and the sectoral legislation be integrated? Would additional experts be required to form the joint assessment team? Regarding the Commission representatives and the expert who is part of such teams, should they be from DG CNECT or DG SANTE?

- In the case of bodies already designated under a legislative act, how is this measure applied? Should the bodies wait until their re-designation audit under the sectoral regulations to be able to use the single designation procedure under AIR?

Article 43.3: Role of Notifying Authorities during the period when sectoral Notified Bodies have not made the official designation application under AIR.

Article 43.3 contemplates that, for the purpose of conformity assessment, bodies that have been notified under an act of Annex I shall have the power to assess the conformity of the high-risk system with the requirements of Section 2, provided that in their designation procedure the requirements of Article 31 have been assessed. Given that a period of 18 months is granted to make the official application:

- What role do the sectoral Notifying Authorities play in these cases where the bodies do not yet have the obligation to make an official application? Should they verify compliance with the requirements of Article 31 during the supervision audits of the designation of their harmonized acts?

- Before the official designation application, do Notified Bodies designated under sectoral regulations have the obligation to review in their conformity assessment procedures the requirements of Section 2 of the AIR applicable to high risk?

- In cases where systems have been certified under sectoral legislation and include AI, what happens and what consequences does it have for providers if the sectoral Notified Body does not request designation under AIR or the Notified Body is unable to demonstrate competence for its designation? Is the certificate withdrawn? Is it contemplated that in such cases there will be another body only for the AIR part?

Article 56: Codes of practice: What is the practical effect of not validating codes of practice through implementing acts?

- Does this not create legal uncertainty regarding whether complying with these codes is sufficient to ensure conformity? The legal value of the codes of practice is not clear in this new wording.

Article 57: EU Sandbox

- What is the scope of the EU sandbox?

- Would it only affect systems that are the exclusive competence of the AI Office (GPAI and HRAIS from the same provider based on GPAI) or any system that requests to apply?

Article 58: Governance between Sandboxes

- Timeline for publication of legislative acts for defining sandbox details

- How will this governance be structured?

Article 60a: Real Environment Testing Annex I.B

- The conditions that must be met for providers to conduct testing under real conditions outside controlled spaces are defined in point 60.4. However, in section 60.a which has been introduced to extend the application of these tests to systems in Annex I.B, it is not established that point 60.4 is applicable according to 60.5

What would then be the conditions that providers of Annex I.B systems must meet?

- What would be the requirements of the agreement to establish these testing environments according to Article 60a(2)?

Article 63.1: Simplification of quality system requirements.

- Why has SMC not been included in the simplification in this case as in the rest of the text and only SMEs?

Article 113: Entry into force and sanctions

- No mechanism has been defined in case in December 2027 all harmonized standards cited in the OJEU are not available. What would be the solution, another proposal to amend the Regulation?

Market surveillance, NANDO codes and conformity assessment.

Although Article 74.3 has not been subject to modification by the Digital Omnibus, clarification is required on who has the competence to carry out surveillance of certain systems that have purposes both from Annex I and from Annex III.

According to point 43.3 introduced by the Omnibus, when a high-risk system is covered by both harmonized legislation of Annex I, Section A, and by any of the categories of Annex III, the provider must

follow the conformity assessment procedure according to Annex I. On this basis, it is understood that in these cases the market surveillance authority will also be that of Annex I.

However, it is necessary to clarify what happens in those cases where a system has a duality of purpose and the Annex III category does not apply within the system's purpose according to Annex I.

In the specific case of medical device legislation, when certifying software that has multiple purposes, the manufacturer (provider) has the obligation to identify the modules that have a medical device purpose since they are the only ones that would be certified according to Regulation 2017/745.

For example, in the case of software that has one purpose for appointments and another purpose for diagnosis, the provider should distinguish the two modules before making the conformity assessment application, and only the diagnostic purpose would be certified under Regulation 2017/745. On the contrary, the appointments module would not qualify as a medical device, and therefore would not be subject to market surveillance by medical device market surveillance authorities.

BACKGROUND. FACTS.

Article 57.1 of the regulation establishes: "1. Member States shall ensure that their competent authorities establish at least one AI regulatory sandbox at national level, which shall be operational by 2 August 2026 at the latest."

Additionally, it states in Article 57.7: "The competent authorities shall provide providers and prospective providers participating in the AI regulatory sandbox with guidance on regulatory expectations and on how to comply with the requirements and obligations set out in this Regulation."

It further adds in this same point 57.7, with reference to written evidence of activities carried out in the testing environment: "...Providers may use this documentation to demonstrate their compliance with this Regulation through the conformity assessment process or relevant market surveillance activities."

CONSIDERATIONS.

1. Taking into account that the manner of complying with such requirements and obligations, referred to in Article 57.7, is facilitated and specified through standards.
2. That the publication of standards is not expected before 2 August 2026, the date by which, according to Article 57.1, the regulatory sandbox must be operational.
3. That the Digital Omnibus does not contemplate any moratorium for the establishment of regulatory sandboxes.

CONCLUSIONS.

The following questions arise from the Spanish Agency for AI Supervision:

1. How can competent authorities provide regulatory assurances to participants in regulatory sandboxes in the absence of standards?
2. What legal implications—with regard to conformity assessment—may exist when issuing favorable exit reports from regulatory testing environments in a context of absence of standards, if, when the standards are published, they are not in accordance with what is required in them?

Data Questions + Data Protection (part from MTDFP -- rest must come from MJUS)

Data Act: Article 41a European Data Innovation Board (EDIB)

The changes will allow the Commission to modify the relevant founding documents of the EDIB and expand its composition.

- How does the Commission intend to give EDIB a more relevant role and with greater decision-making capacity?

- How will competent authorities be integrated into EDIB? 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?

The current pace of work (two online meetings per year) and the nature of these meetings (informational without real debates) do not favor exchange among Member States nor allow the EDIB to be given a real strategic function. The EDIB has summoned us to an online meeting on December 10 and we understand that they will give us more details on what they propose. Our objective is for the EDIB to acquire a more relevant role in defining future data policies, with a composition adjusted to its functions and cooperation with other Boards that appear as key elements within the framework of their strategies.

Although the GDPR is not strictly within our competence, we are sharing some questions that we will raise. (We will meet with AEPD soon)

GDPR: Article 4 definition of personal data

The new wording of Article 4.1.a) adds that information will not be considered personal data in the event that the entity does not have means that are reasonably likely to be used to identify the natural person.

- Does this mean that pseudoanonymized data is no longer personal data in a typical scenario? How will they define the boundary between what is reasonably likely and not?

We seek proportionality in the GDPR and therefore we agree that, in this scenario, pseudoanonymized data should not be considered personal data.

GDPR: Article 5 principles relating to the processing of personal data

The new wording of Article 5.1.b) establishes that further processing of personal data for archiving purposes in the public interest, scientific research... will be considered compatible with the initial purposes.

- Within the scope of "archiving purposes in the public interest", could data processing for public data opening be considered compatible? And data processing for the design and evaluation of public policies?

If this is ultimately not contemplated, we would like the scope of this modification of Article 5 to include the processing of personal data with the objective of preserving, organizing, maintaining and publishing information for public interest activities (open data, design and evaluation of public policies), thus assimilating them to research activities. This change would address a current challenge in which the administration itself cannot process data to design public policies as part of its activity unless it is included in a law (which in most cases is not included) while a researcher can access that data.

ON CYBERSECURITY PROPOSED AMENDMENTS

- Can the commission provide more information on the platform model as well as the information flow of cyber incidents?

- Do you want harmonized thresholds for “significant incidents” across regulations?

- What is expected to be the methodology and the agents involved in the process of simplifying and harmonizing incidents?

- How do you avoid a single point of failure (federation, redundancy)?

- How is it expected to generate the trust that will allow for the promotion of voluntary CRA notifications with a centralized model in which the platform moves away from the manufacturer who knows about a vulnerability?

FRANCE

Objet : Questions écrites et commentaires – Omnibus numérique.

Point 1. Questions

France notes that the provisions of the Omnibus do not address the upstream stages of data and metadata production and their cataloguing, in particular in terms of semantic and conceptual interoperability and quality, as well as their updating. These aspects are among the main sources of degradation of data quality for AI. France remains attentive to the preservation of existing European mechanisms that ensure data interoperability, while recognising the need for their simplification.

Could the Commission clarify how it envisages addressing these issues going forward? Should we expect them to be covered in a regulatory instrument beyond the Omnibus, or are they intended to be dealt with primarily within the non-binding framework of the future Data Innovation Board and the Data Union Strategy?

ABOUT AI

Article 4	AI literacy	- What kind of measures would be expected from MS to fulfil requirements of article 4 (i.e. "*Encourage providers and deployers of AI systems to take measures to ensure a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf*") ? - What would be the criteria identified to consider this obligation as fulfilled?
Article 4a	Processing of special categories of personal data for bias detection and mitigation	- How to interpret the shift from Chapter III Section 2 (Article 10) to Chapter I? In particular, do you confirm the article would enter into application as soon as the Omnibus gets adopted? - Insofar as the standardisation request does not include items pertaining to Chapter I, how are the providers and deployers expected to demonstrate that the bias detection and correction cannot be effectively fulfilled by processing other data? Are guidelines/FAQ to be expected? For systems resorting to online learning, when can it be considered that the bias has been corrected?
Article 28	Notifying authorities	- New article 28(8) provides that conformity assessment bodies should be able to apply for designation under both the AIA and the Union harmonisation legislation in a single procedure. Does this obligation is also applicable when notifying authorities under the AIA and the Union harmonisation legislation are different authorities? Are guidelines/FAQ to be expected detailing how to conduct the said "simple assessment procedure"?
Article 30	Notification procedure	- We would appreciate clarification on the choice to empower the Commission to amend Annex XIV through delegated acts, rather than through implementing acts subject to the examination procedure. Given that changes to the list of codes, categories and types of AI systems directly affect the scope of conformity assessment tasks carried out by national notifying authorities and notified bodies, could the Commission explain why Member States are not involved in this process, and how this approach aligns with the governance structure and comitology balance established elsewhere in the AI Act?

Article 43	Conformity assessment	- The AIA does not foresee harmonised standards as providing presumption of conformity with regards to Chapter III, to which Article 17 belongs. Therefore, how is the assessment of the quality management system to be conducted? - Similarly, since Art. 43(3) does not empower notified bodies to assess the conformity of AI systems with regards to Chapter III, how is the quality management system to be assessed? - In our view, particular attention should be paid to the amendment to Article 28, as Regulations (EU) 2017/745 and 2017/746 on MDs and MDIVs do not provide for single designation procedures under several regulations. We note that Article 43 appears to introduce broader requirements than the current version of the IA. Is that correct ?
Article 50	Transparency obligations for providers and deployers of certain AI systems	- We would be grateful for an explanation of the rationale behind the revised wording of paragraph 7, which removes the involvement of the Member States from the approval of the Codes of Practice. In the previous formulation, approval followed the Article 56(6) procedure, ensuring Member State participation in a process directly linked to obligations they are responsible for enforcing. The new wording assigns this assessment exclusively to the Commission. Why does the Commission intend to exclude the Member States from this approval process, and how is this consistent with the broader governance balance of the AI Act? - Moreover, we would be grateful for an explanation on the limitation of the assessment to ensuring compliance with the obligation laid down in paragraph 2 of the article. - France expresses a scrutiny regarding its position on this article pending further clarification
Article 56	Code of practice	- In article 56(6) the assessment of the CoP by both the AI Office and the Board has been replaced by an assessment by the Commission, taking the utmost account of the opinion of the Board. Do we have to understand that the Commission will have to comply with the opinion of the Board?
Article 57	AI regulatory sandboxes	- Is the AI Office sandbox expected to prioritize European providers ? - Is the Omnibus planning to make joint sandboxes mandatory? - We would be grateful 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”. Should this be understood as requiring Member States to participate in cross-border or jointly operated sandboxes, rather than allowing them to organise and operate their own national sandboxes according to their administrative capacities, levels of expertise and available resources? More broadly, how does this wording align with the purpose of the AI Act and with the flexibility afforded to Member States to structure their competent authorities and implement supervisory tools in a manner proportionate to their budgets and levels of AI literacy? - France expresses a scrutiny regarding its position on this article pending further clarification
Article 69	Access to the pool of experts by Member States	- The new wording of article 69 withdraws the Commission's support for access to experts by member states. What is the rationale of the Commission for this withdrawal?

Article 72	Post-market monitoring by providers and post-market monitoring plan for high-risk AI systems	- We would be grateful for clarification on the rationale behind the reformulation of paragraph 3, which now provides that the Commission "shall adopt guidance on the post-market monitoring plan" instead of an implementing act adopted through the examination procedure under Article 98(2). This change appears to remove the involvement of the Member States in defining the structure and mandatory content of post-market monitoring plans, despite the fact that these plans are central both to providers' obligations and to the work of national market surveillance authorities. Could the Commission explain why the role of the Member States has been withdrawn in this area, and how this remains consistent with the governance balance and comitology framework established elsewhere in the AI Act?
Article 75	Market surveillance and control of AI systems and mutual assistance	- In the new wording, the Commission extends the remit of the AI Office to AI systems that constitute or are integrated into a very large platform. What is the reasoning behind such changes? - How should the concept of 'integrated' be understood? Would AI systems having the same providers than VLOPs be considered to fall within the remit of the AI Office? - New paragraph 1c asks the Commission to organise and carry out pre-market conformity assessments and tests of AI systems referred to in paragraph 1 that are classified as high-risk and subject to third-party conformity assessment. In our understanding, it is the job of notified bodies, which are notified by Member States. Does that mean that the Commission would become a notifying authority? Would it resort to bodies notified by Member States? We don't understand, it does not seem useful and it seems to overlap what Member states will already do : market surveillance can be done by the Commission even if a system is pre-market evaluated by a notified body notified by a Member State, can't it ?
Article 77	Powers of authorities protecting fundamental rights and cooperation with market surveillance authorities	- Could the Commission clarify what categories of information may be exchanged under paragraph 1b, and whether such exchanges remain subject to restrictions relating to trade secrets, confidential business information, intellectual property, professional secrecy and secrets protected under national security or law-enforcement rules?
Article 113	Entry into force and application	- The new wording of article 113 extends the application of the obligations concerning high-risk AI systems, which are conditional on the availability of measurements and a decision by the commission. The obligations will come into force 6 months after the Commission's decision, except where this exceeds the set dates (December 2, 2027 and August 2, 2028). - Will the AI Board's validation be necessary for the Commission to decide on whether adequate compliance measures are available? - France expresses a scrutiny regarding its position on this article pending further clarification

Regarding the interplay between the CRA and the AIA, the recitals of the Regulation simplifying the harmonised implementation of the rules on artificial intelligence refer to a proposal for future guidelines on the interactions between AIA and the CRA. However, a frequently asked questions (FAQ) document on the interplay between AIA and the CRA was already being prepared. **France therefore wonders about the relationship between these guidelines and the FAQ already planned, and would like to**

receive more information on the drafting process for these guidelines and the envisaged timelines. France would like to see a more clearly established linkage between the CRA and the RIA in the text of the Regulation simplifying the harmonised implementation of the rules on artificial intelligence. Is the linkage between AIA and CRA also applicable to the elaboration of standards?

ABOUT DATA ACT

Article 32e	Registration	The Data intermediation services providers status (DISP) was created to promote industrial data sharing. This article sets a voluntary registration for the Data intermediation services providers (DISP) who meet the requirements set out in the Data Act. Q : How will voluntary registration guarantee the incentive role of DIS for industrial data-sharing and the development of a DIS market ?

ABOUT CYBER

Regarding the cyber regulatory framework, France notes that several simplification exercises are being proposed separately (the Digital Omnibus, the revision of the CSA and a potential simplification following the Digital Fitness Check). France has questions on the overall coherence of this simplification effort. It would therefore be useful to receive further information on how the simplification measures proposed under the different exercises will interact.

With regard to the single entry point proposed in the Digital Omnibus Regulation on data and cybersecurity, France has questions concerning the introduction, in the recitals, of additional sector-specific incident-notification obligations into the single entry point which do not appear in the operative text (the Network Code on cybersecurity of cross-border electricity flows and the regulatory instruments relating to the aviation sector). On this point, France would like to obtain further details on the timeline envisaged for amending the implementing acts (implementing acts and delegated acts) with a view to integrating these incident notifications into the single entry point.

The recitals of the Digital Omnibus Regulation on data and cybersecurity, as well as recital (54), refer to the proposal for incident-notification templates and the harmonisation of the content of notifiable incidents; however, this is not clearly reflected either in the text or in the annexes. France therefore seeks clarification on how the Commission intends to implement this harmonisation of incident-notification content and these potential templates.

France also has questions regarding the security of the single entry point proposed in the Digital Omnibus Regulation on data and cybersecurity, and in particular about the measures envisaged by ENISA to secure this single entry point. France would like to know how ENISA intends to adapt its platform to incorporate incident notifications, what working method ENISA plans to use to achieve this objective, and how Member States will be involved in the development and security of the platform. France is notesthat Member States are only being consulted on the assessment of the proper functioning of the single entry point prior to its entry into operation.

In view of the possibility for subsequent consultation and modification of the information notified (Article 23a, point (e), inserted into the NIS2 Directive), could the Commission confirm that no additional data storage is envisaged (without prejudice to information-storage requirements already provided for in existing legislation) ? France would like to understand the feasibility of such functionality where applicable?

Recital (52) of the Digital Omnibus Regulation on data and cybersecurity provides for continuity and interoperability between national incident-notification platforms and the single entry point for incident notifications. However, Articles 3, 6, 7, 8 and 9 state that incident notifications under the GDPR, NIS2, eIDAS, DORA and CER will have to be made via the single entry point. How the Commission intends to ensure interoperability between the single entry point and existing national platforms, particularly from a technical perspective.

In relation to the same recital, France also seeks clarification on the meaning the European Commission attributes to the 'integration of notification obligations into business processes'.

Regarding the dissemination of notifications, could the Commission clarify how incident notifications will be shared with other Member States. At national level, once an incident is notified, it is qualified, notably in terms of national security, and this qualification affects how the incident is handled. Does the Commission envisage a mechanism for deferred notifications for reasons of national security?

Regarding the CER Directive, why does the EC want to receive feedback from critical entities when Article 15 initially stated that it should primarily be the Member States that receive this feedback and share the information if necessary, in accordance with both Article 15 of the same directive and Article 1.5? Finally, why does the EC want an implementing act that would tell critical entities what information they must provide, which we believe is not in line with the spirit of the CER Blueprint?

ABOUT E-PRIVACY

In its current wording, the ePrivacy Directive covers both natural persons and legal entities. Article 5(3) ePrivacy therefore states that Member States shall ensure that the use of electronic communications networks to store information or access information stored in the terminal equipment of a subscriber or user is only permitted with their consent (with some exceptions). The new paragraph inserted into this article states that this provision does not apply if (i) the data subject is a natural person and (ii) the information stored on the terminal equipment accessed constitutes or leads to the processing of personal data.

- In our understanding of the facts, these criteria are cumulative. **Is this correct?**
- **What is the scope of this text now? Does it apply only to legal persons and to the storage of and access to information on terminal equipment that does not constitute the processing of personal data?**
- In France, we have the status of individual entrepreneur, which, unlike a company, does not involve the creation of another legal entity. Individual entrepreneurs are therefore considered to be natural persons, which, in our view, creates a difference in treatment between individual entrepreneurs (subject to the GDPR) and legal entities (subject to ePrivacy).

Point 2. Initial comments

ABOUT CYBER

The creation of a single entry point for incident notifications, as provided for in the Digital Omnibus Regulation on data and cybersecurity, constitutes a substantial change to the management of cyber-

incident notifications at European level. France regrets that no comprehensive impact assessment has been carried out to evaluate the feasibility, consequences and costs of such a measure. Furthermore, France would like to know the percentage of the European economy that the European Commission intends to cover with the single entry point, in order to understand whether it is aimed at the entire European economic fabric or primarily at cross-border businesses.

France has concerns about the establishment of the single entry point for incident notifications provided for in the Digital Omnibus Regulation on data and cybersecurity:

- The single entry point covers very different types of notifications, involving very different national arrangements for certain incident notifications, without leaving room for national mechanisms that already exist;
- The single entry point does not address the identified problem of heterogeneity in incident notifications across the various legal instruments;
- The single entry point risks complicating the notification of incidents for entities, since this currently forms part of a victim-assistance pathway and the single entry point would constitute a new and unfamiliar tier. Moreover, this risks affecting the existing relationship of trust between national authorities and their beneficiary ecosystems;
- The single entry point presents significant security risks for the data transmitted and stored within what may constitute a single point of failure;
- The single entry point poses a risk to national security owing to the content or the sender of certain incident notifications, which fall within the scope of national security ;
- The additional delay in processing the report will slow down the activation of support mechanisms, both in terms of cyber security and business operations.

ABOUT GDPR

- Considering the four pillars presented by the France with regard to the simplification of the Digital Rulebook, the Commission’s proposals do not appear to provide adequate responses to the development of new, innovate compliance tools and the operationalisation of existing tools is also missing from the proposal./.

CROATIA

Croatia welcomes the Omnibus VII (Digital) proposals, as other Member States we also have a scrutiny reserve and several initial questions:

Regarding the establishment of the EU sandbox, we would appreciate hearing more details from the Commission regarding:
- management mode and management structure of the EU sandbox;
- CAPEX;
- OPEX;
- eligibility criteria for applicants;
- whether allocations per MS are foreseen or some other criteria will be applied (all this assuming that the sandbox will have a limited number of available allocations for testing that need to be allocated in some way);
- whether it is foreseen to issue reports, certificates etc. on the tests performed, as well as whether they will be applicable throughout the EU;
- whether they intend to test algorithms?

We would appreciate any other information that could clarify this business/use case as a whole.
In general, since regulatory sandboxes for AI are considered to support innovation, it would also be useful to know how they intend to treat beneficiaries, i.e. whether this type of testing will also be considered aid (in the sense of state aid).

We would appreciate to have clarifications/answers in writing and in a form of a document.

ITALY

Please bear in mind – as a disclaimer – that the EN translation is AI generated.

Cyber component

· What are the possible technical solutions that can guarantee the full confidentiality of notifications to ENISA, ensuring that the Agency does not have access to the information and that the single point becomes a "single point of failure"?

· How do you intend to deal with the fact that many Member States have already developed "unified" notification platforms (some limited to CER/NIS, others more extensive) and do not want to abandon the investments made in favour of an EU solution?

· What measures are planned to address the complexity of integrating the EU platform with existing national tools (analysis systems, protocols, ticketing), while avoiding the need to abandon effective national solutions?

· How will the integration of national notification mechanisms, particularly those relating to national security, be ensured?

· Will the notification models provided for in the various regulations be uniform for all Member States or differentiated? Furthermore, will the single point of entry allow for the transmission of a single notification valid for several Member States in relation to a single regulation, or a single notification that simultaneously fulfils the obligations of all regulations in all Member States?

· Does the new single point of contact requirement effectively mean that, in the event of incidents relevant to multiple pieces of legislation, the regulation with the shortest notification deadline (e.g. DORA with a 4-hour obligation) will prevail?

· Is it correct to assume that the notification model developed for DORA will form the basis for extension to other regulatory instruments, such as NIS2, CER and GDPR?

· There is no reference in the text to the Network Code on cybersecurity aspects of cross-border electricity flows (NCCS) or to EASA regulation: will these acts be included at a later stage?

AI component

· What criteria will the Commission use to determine the date of application of the rules on high-risk AI systems in order to increase legal certainty?

· What support tools (e.g. standards, specifications, guidelines) will be considered essential to ensure compliance and reduce the burden on businesses before the rules are applied?

· Why was centralisation at the AI Office chosen for the supervision of large-scale, high-capacity general artificial intelligence models? What role is now envisaged for Member States within this new governance structure?

· Why has the interaction between the AI Act and the Cyber Resilience Act not been explicitly clarified, given the complementarity of the two regulations on the safety and compliance of digital products?

· What are the reasons for removing the literacy requirements? What are the expectations of Member States with regard to promoting AI literacy?

LATVIA

LATVIA DELEGATION QUESTIONS
ON THE DRAFT OF THE DIGITAL OMNIBUS REGULATION (COM (2025) 837)
AND
THE DIGITAL OMNIBUS FOR AI REGULATION (COM (2025) 836)

THE DRAFT OF THE DIGITAL OMNIBUS REGULATION (COM (2025) 837)

Comments:

We support the merging of the GDPR and the e-Privacy Directive into a single regulation. This will reduce ambiguities and fragmentation between different legal norms.

We positively value that the regulation on cookies and Internet of Things (IoT) data will be unified across the EU.

Questions:

1. There is a need for clear and practical guidelines to delineate where the scope of communications confidentiality regulation (EECC/e-Privacy) ends and where the rules on personal data processing under the GDPR and the new Articles 88a/88b begin and ensure consistent application across the EU. This ambiguity is particularly relevant for OTT services such as WhatsApp, Signal and email, which frequently fall under overlapping regulatory regimes.
2. We kindly ask the Commission to clarify how the single EU reporting point fits in with existing communication incident reporting obligations (EECC, NIS2) to avoid double reporting.
3. Will the new exemptions for the minimal processing of special category data in the development of AI systems be sufficiently clear to avoid the risk of non-compliance?
4. Will the subjects be able to report incidents in all Member States, submitting one report? If so, are there plans to ensure that Member States align with each other the requested information? - From the subjects' point of view, this is one of the most pressing issues that despite the same EU legal acts each Member State requires different information and uses different forms.
5. If the single-entry point permits to simultaneously submit reports in several Member States, will that also ensure less administrative burden for multinational companies? - As a general rule, such companies have a separate subsidiary in each Member State where they operate. Then subsidiary is obliged to report an incident where the problem concerns the parent company's central system. This means that the subject would still have to submit several reports to meet the requirements in each Member State. It would be important to understand whether the single-entry point will actually simplify this problem, or whether it will become just another additional reporting channel.
6. Regarding the incident reporting requirements, we kindly request clarification on the categories and specific data fields to be submitted. Whether a standardized reporting

form and formats will be established? Whether recommendations or guidelines are planned/will be available for structuring data and metadata (descriptive attributes) in a unified and consistent format that ensures data quality, interoperability, and usability across different systems?
7. How sensitive information concerning critical infrastructure or (possible) commercial secrets will be handled?
8. What is the envisaged classification categories of the information shared via this new channel?
9. How cybersecurity of this new channel will be ensured?

THE DRAFT OF THE DIGITAL OMNIBUS FOR AI REGULATION (COM (2025) 836)

1. How will the European Commission or national competent authorities ensure this practical “encouragement” for AI literacy?

2. Are targeted training obligations for AI literacy foreseen?
3. Will a minimum measurable AI literacy “outcome” be developed to avoid fragmentation across Member States?
4. What will be the minimum criteria or required format for the “not high-risk” documentation when a provider considers that a system listed in Annex III is not high-risk, to ensure consistent supervision across Member States?
5. What is the legal status of the Annex VI simplified documentation for SMEs/start-ups? Will it be mandatory for SMEs/start-ups, and will it also constitute a sufficient body of evidence?
6. Will the Commission’s guidelines, which will harmonise post-market monitoring, include a concrete template?
7. Will regulatory sandbox “exit assessments” or results be formally usable as evidence of compliance with the AI Act?
8. Will a harmonised EU standard be established for sandbox documentation (testing plans, incident logs, risk-mitigation evidence) to enable reuse?
9. What exactly does the phrase “adequate measures … are available” on page 31 of the EU Omnibus document mean? Does it require a complete set of standards or only a partial set?
10. Will there be a proportionality-based approach in cases where standards are not yet available—e.g., if the provider demonstrably follows available guidelines or alternative approaches, will sanctions be applied proportionally?
11. Does the Commission envisage a unified combined AI Act + GDPR template (a joint DPIA + FRIA)?
12. According to NIS2, definition of security of network and information systems includes authenticity. What measures should be taken to ensure that AI generated data that are basically derivatives of wider data sets can or cannot be considered authentic and therefore trustworthy and fit for use? Shouldn’t we develop quality metrics for it and passing score for authenticity and trustworthiness criteria and implement them in regulation?

LITHUANIA

Lithuania's initial questions regarding the Digital Omnibus:

1. **Regarding Article 49(2) of the AI Act.** If providers are no longer required to register AI systems that they claim are not high-risk due to certain exemptions, does this also mean that other obligations—such as relevant documentation, justification, etc., demonstrating that the exemption applies—no longer apply?
2. **Regarding incidents.** Question is why the unified system for cybersecurity notifications could not also include notifications of serious incidents under the AI Act.

HUNGARY

Suggested clarification questions

(Omnibus package, ‘dedicated’ AI Act amendment)

1. **Paragraph 17(a) (new Article 57(3a) AI Act)**

Is there a deadline for the creation of the AI Office -Sandbox (Member State deadline 2 August 2026)? As a further question, would it not be appropriate to postpone the deadline for the creation of the Member State sandboxes by at least half a year in view of the postponements due to the requirements and the amendment of the provisions concerning the sandbox in general?

2. **Section 25(b), last paragraph (Section 75(1) of the AI Act)**

According to the provision, the (Member State) authorities involved in the implementation of the AI Act must cooperate so that the AI Office can fully act and, where appropriate, take the necessary measures on the territory of the Member States under the exclusive powers granted to it in this amendment. It is not clear how this will work in practice, especially as Member State authorities typically act in accordance with the general administrative procedural law of the Member State. In our view, it is therefore necessary to create a legal basis for this cooperation in some way. Does the Commission plan to initiate further legislation in this regard? Will these rules, aimed at cooperation between the AI Office and the authorities of the Member States, form part of the implementing rule envisaged to be issued under the new Article 75(1a)? Has the Commission examined whether this could be a sufficient legal basis for Member State authorities to ensure the conditions for cooperation and, where appropriate, for action by the AI Office, taking into account the national procedural framework applicable to them?

3. **Paragraph 31 (Amendment to Article 113 of the AI Act)**

What is the timetable for the adoption of the "necessary measures" and the related Commission decision acknowledging this? The Commission is invited to present this timetable, which is relevant for the organisation of the work of the authorities in the Member States.

NETHERLANDS

NL initial written comments and questions on Omnibus VII – Digital Omnibus

- The Netherlands welcomes the effort by the Commission to reduce the administrative burden of the digital acquis. The omnibus should focus on streamlining reporting obligations and definitions, increasing clarity and consistency, and facilitating compliance. In addition, the Netherlands sees an important role for practical tools that make it easier to comply with legislation.
- At the same time, questions and reservations remain about the practical implications of the different proposals. The Netherlands welcomes the Commission to provide written or oral answers to these questions so that we can further develop our position based on this information.

ePrivacy

- How does the Commission view the proposed coexistence of two cookie regimes – one in the ePrivacy Directive for non-personal data and another in the GDPR for personal data – in relation to the goal of reducing regulatory burden?
- Consequently, the newly introduced exemptions (Article 88a(3)) cannot be utilized when no personal data is being processed. Although the main reason for these exemptions is that they apply to 'low-risk' situations, meaning they require no or minimal amounts of personal data, a dual regime would create an incentive to process personal data unnecessarily, solely to benefit from these exemptions.
    - Could the Commission therefore elaborate on its decision to propose exemptions only where personal data is processed, and would the Commission consider including these exemptions in the ePrivacy Directive instead?

Data intermediation services

- The recitals 28 t/m 31 have been very useful in guiding competent authorities regarding the oversight of the provisions regarding data intermediation services.
    - Will the Commission ensure that an amended version of these recitals will find a place in the digital omnibus and/or the new Data Act?

EDIB

- 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?

Cloud provisions

- The Commission proposes to exclude custom-made cloud services from the scope of Chapter VI 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?

P2B

- The need for a repeal of the P2B seems to be largely based on a preliminary 2022 review (published in 2023). Awareness of the P2B has gradually increased since then. While many MS have taken legislative steps since 2023 to strengthen public enforcement of the P2B, the Commission's analysis does not seem to address these efforts nor their impact (e.g. ACM has been receiving increasing numbers of P2B-specific complaints by entrepreneurs: 100 in 2024; ~120 in 2025).
    - Has the Commission included this in its assessment and investigated the impact at MS level, and if so how?
- How does the Commission assess the impact of the proposed P2B repeal on the ability of local entrepreneurs to effectively enforce transparency rules in court or via the national competent authority, given that national enforcement under the P2B uniquely complements the DMA/DSA, particularly when it comes to platforms established elsewhere?
- The Commission concludes that the repeal of the P2B is necessary to eliminate duplications of rules in the DMA and DSA. At the same time, the Commission concludes that some rules remain indispensable thus requiring a transitory phase.
    - How does the P2B-repeal compare to a targeted removal of only those articles without added value? Can the Commission specify how the transitory phase would work and which provisions would fall under this exemption?
- By repealing the P2B, specific and detailed norms for transparency in the P2B will have to be redefined with the risk of differing interpretations of norms within the EU.
    - How does the Commission plan to prevent fragmentation?

Single Reporting Platform

- 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? Which incident notifications processes will at the end be modified on both EU and national level? How will this proposal ensure that the national structures remain at the end intact?
- Member States are in the process of exploring expanding NIS2 notification platforms to notifications in the context of other related legislation. 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?
- Small and medium sized are the most vulnerable to cyberattacks and would be most affected by the administrative burden of multiple notification requirements. Many of these companies, especially SMEs, mainly conduct their operations within a single or a few Member States.
    - How will creation of a European Single Entry Point provide added value for this large group of entities?
- Why is there such a link between the CRA platform and the Single Entry Point if it will at the end have no strong implication with this new structure?
- 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?

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 recital 99 and recitals 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 where this is still the case?
- 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?
- 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.

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?
  - 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?
  - 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?

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?
- 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?
- 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?
- 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?

***

NL initial written comments and questions on Omnibus VII – Digital Omnibus on AI

- Currently, the NL is examining the proposed amendments to the AI Act. All our comments on these proposals are subject to reservation.
- Generally, the Netherlands has a positive stance towards the proposed amendments to the AI act but is critical of a number of changes, particularly the proposal to postpone the deadline of requirements for high-risk AI systems.
- Such a delay creates additional and unnecessary uncertainty and complexity for companies and organizations. The Netherlands prefers adherence to a specific date so that providers and users of high-risk AI know by when they must comply with the requirements.
- The Netherlands also has objections to the removal of the registration requirement for AI systems exempt from high-risk under Article 6, paragraphs 3 and 4, of the AI act.
- This removal reduces transparency regarding the use of AI systems in high-risk contexts, and it is insufficiently clear whether this will lead to a reduction in regulatory pressure rather than increased legal uncertainty. The Netherlands considers the registration requirement to be a relatively light burden that should be retained.

Article 1(31) (Omnibus), amending the application of Chapter 3 of the AI Act

Article 1(31) of the Digital Omnibus introduces a mechanism allowing the European Commission to delay the application of provisions on high-risk AI systems. If the Commission decides that "adequate measures in support of compliance" are available, the provisions apply six months later for annex 3 and 12 months later for annex 1; if not, they apply by December 2027 and August 2028 respectively. While this aims to ease compliance burdens given the current perceived lack of technical standards and guidelines, the proposal does not define what qualifies as "adequate measures" or how the Commission will adopt such a decision. This lack of clarity could create uncertainty for organizations and supervisors, potentially delaying implementation unnecessarily while complicating planning.

1. Can the European Commission clarify what constitutes "adequate measures" and the conditions for adopting such a decision?
2. Why was a maximum delay of 16 months (for annex 3 systems) and 12 months (for annex 1 systems) chosen instead of another timeline?
3. Can the Commission clarify how it will ensure clear and predictable timelines for the implementation of the AI Act for the application of the requirements regarding AI systems**?** ,
4. Did the Commission consider setting a fixed and binding date for the application of the requirements regarding AI systems?

AI Article 1(4), amending AI Act Article 6(4)

Article 1(4) of the Digital Omnibus amends Article 6(4) of the AI Act by removing the obligation for providers to register self-assessments of AI systems classified as non-high risk. Providers must still document their assessment but are no longer required to register for it. While this may reduce the administrative burden for organizations deploying narrow or procedural AI systems under Annex III, it also removes a key transparency mechanism. Companies can now self-assess and declare systems as non-high risk without any public or regulatory disclosure, making oversight more difficult and potentially weakening trust in the risk-based framework of the AI Act.

5. How can policymakers and market surveillance authorities take notice of and verify that a company has self-assessed an application as non-high risk and ensure that this classification is justified in the absence of a registration requirement?
6. What is the European Commission's estimate of the administrative burden or cost savings for companies resulting from this change?

AI Article 1(17), amending AI Act Article 57

The Digital Omnibus allows the AI Office to establish an EU-level regulatory sandbox for AI systems under Article 75(1), implemented in cooperation with relevant authorities and offering priority access to SMEs. While this initiative could foster innovation and support organizations developing high-risk AI systems across borders, concerns remain about its interaction with national sandboxes and the risk of regulatory divergence.

7. How will the European regulatory sandbox coordinate with national sandboxes to avoid duplication or conflicting requirements?
8. What safeguards will prevent market participants from selecting the most lenient market (supervisor) in terms of participation conditions between national and EU-level sandboxes?

Article 4 – AI Literacy

Article 4 has been changed to transform the obligation of providers and deployers with regards to AI literacy into an obligation for the Commission and Member States to foster AI literacy.

9. What can an MSA do when the personnel using a high-risk AI system or performing the human oversight (as required by article 14) are not competent to perform these tasks?
10. Now that the Digital Omnibus has centralized the AI literacy mandate to 'promote and support' by the Commission and Member States, what concrete, budgeted initiatives will be put in place to ensure this new responsibility actively closes the literacy gap?
11. Given the obligation for the Commission and Member States to 'promote and support' AI literacy, what specific, measurable mechanisms or funding initiatives are expected to be established to fulfill this role under the revised Article 4?
12. How does the revised Article 4 legally define the division of responsibility between the European Commission and the national Member States regarding the financing and execution of AI literacy initiatives?
13. Can the Commission elaborate on what measurable promote and support instruments they envisage for this obligation?

Article 1(5) (Omnibus), amending Article 4 – Processing special categories of personal data

Article 4(a) is inserted which broadens the legal basis for processing special categories of personal data for bias detection and mitigation from high risk AI-systems to all AI-systems and –models.

14. 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?

15. Are there concrete examples of non high risk AI-systems for which the commission considers it necessary to broaden the legal basis?

Article 28(8) AI act – Notifying authorities
Article 28 AI act, paragraph 8 states that notified bodies have the possibility to submit a single application and undergo a single assessment procedure to be designated under this Regulation and Union harmonisation legislation listed in Section A of Annex I, where the relevant Union harmonisation legislation provides for such single application and single assessment procedure. A notified body may be designated for several Union legislation listed in Annex I. And there may be different notifying authorities for each of this Union legislation.

16. Is one assessment to be designated under the AI Act valid for all Union harmonisation legislation, or should this assessment be repeated for each of the Union harmonisation legislation?
17. If one assessment is sufficient, how should this be implemented if there are different notifying authorities for these Union harmonisation legislation?

Article 29(4) AI act - Application of a conformity assessment body for notification
The new paragraph (4) of article 29 states that a notified body shall submit the single application for assessment to the notifying authority designated in accordance with that Union harmonisation legislation.

18. Does this imply that the notifying authority that is designated in accordance with that Union harmonisation legislation is also designated as notifying authority under the AI Act?
19. Do Member States still have to designate these notifying authorities, or is this already implicitly done in this Act?

Artikel 43(3) AI act – Conformity Assessment

A notified body which has been notified under Union legislation listed in Section A of Annex I shall have the power to assess conformity of high-risk AI-systems with the requirements set out in Section 2 of Chapter III, if compliance of this notified body with the requirements of article 31 (4), (5), (10) and (11) has been assessed in the context of the notification procedure. Article 31 (10) requires the notified body to be able to carry out all their tasks with professional integrity and the requisite competence in the specific field.

20. Can we assume that when a notified body has the competence to evaluate AI-systems covered by the Union harmonisation legislation listed in Section A of Annex I, this notified body complies with 31 (10) an (11)?
21. Regarding the 'single application and single assessment procedure' mandated by Article 28(8) for Notified Bodies, what specific operational guidelines will the Commission provide to ensure national Notifying Authorities can efficiently execute this merged assessment within the 18-month deadline?
22. What specific, additional information or documentation—beyond existing MDR/IVDR accreditation files—must a Notified Body include in its 'single application' to demonstrably prove compliance with the specialised AI Act requirements concerning competence (Article 31(4), (5), (10), and (11))?
23. Which notifying authority should assess compliance with these requirements?

Article 75 – Market surveillance and control of AI systems and mutual assistance
Under this article the AI Office is exclusively competent for the supervision and enforcement of AI systems under article 75(1) – AI systems that are based on GPAI-models with the same provider for both GPAI-model and AI-system – with the obligations of this Regulation in accordance with the tasks and responsibilities assigned by it to market surveillance authorities.

24. Can the Commission elaborate how this amendment changes the competence of the AI Office with regards to GPAI-models, GPAI-systems and high risk AI-systems by the same provider?
25. Does the Commission expect that the scope of supervision and enforcement will enlarge when the development of general-purpose AI models and systems will be increasingly easier in the future, given the technological possibilities and advancements?
26. Could the Commission elaborate on attribution of roles and (enforcement) competences of the national market surveillance authorities and the AI Office respectively in the supervision of AI systems by GPAI models and clarify how to interpret the following: "the authorities involved in

the application of this Regulation shall cooperate actively in the exercise of these powers, in particular where enforcement actions need to be taken in the territory of a Member State”? Especially where it concerns high risks systems.

27. To which extend is the allocation of powers to the AI Office in Art. 75 compatible with the obligations and limitations as laid out in Art. 74 (8)?

AUSTRIA

Austrian questions and comments regarding Omnibus VII

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

- How will Cion address public concerns regarding fundamental rights (e.g. Art 4a, 77 AI ACT)?
- Please provide clarifications regarding the delayed applicability of provisions related to high-risk-AI is needed in order to adequately safeguard the protection of consumers; would Art 86 AI Act be affected by the *stop the clock* proposal?
  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.*
- Please explain your rationale concerning the removal registration in EU database for AI systems exempted according to the proposed amendment of Art 6 AI Act.
- With regards to personal data, how will the proposal ensure adequate data protection standards?
- Which market surveillance authority would be responsible for supervising the testing under real live conditions?
- Please explain your rationale concerning the amendment of registration of non-high-risk AI.
- Please explain your rationale concerning the provision concerning AI literacy (Art 4). How can you ensure adequate clarity regarding the amendment of the AI literacy obligation?
- Please explain your rationale regarding the amendments on notifications and codes (including quality and conformity assessment)? We do not see merit in changing the current established practice.
- How will the changes in regard to the AI Office interplay with the current structure and competence of the AI Board?
- Could you provide further clarifications on the involvement of national authorities regarding regulatory sand boxes and real-life testing?
- How will ensure the access of members states to the scientific panel?
- Please explain the new structure and competences of the AI Office? Are existing examples (e.g. NCAs) you have modelled this upon?

ad Digital Omnibus

- We would appreciate further clarification regarding the broader context of the Digital Omnibus in relation to the Digital Fitness Check. In particular, we would be interested to understand whether additional adjustments to the data acquis are envisaged in the coming years, and what the current intentions and planning assumptions are in this regard
- The proposed definition of "university" in Art 2(46) as a "public sector body" may unintentionally result in universities of applied sciences ("Fachhochschulen") not being fully covered by the provision. We

would therefore welcome clarification on how these institutions are intended to be addressed within the current definition.

- By deleting Art 14 and 15, the definition of “exceptional need” would be omitted. This would make it unclear what is meant by “exceptional need”, particularly in terms of whether this would include 'public emergency'. Please provide further clarification on this topic.
- Is there no more right to issue a complaint against the (obligatory) request of a public sector body, the EC, the ECB or a Union body to make available data? Moreover, it seems unclear how to determine whether non-personal data are sufficient or insufficient to address a public emergency as no guidelines are set out in the proposed Art 15a para 2. Please provide further clarification on this topic.
- The exclusion of the EDIB from responsibility for Chapters VI and VIII of the new Data Act is viewed with scepticism. Furthermore, it is detrimental that the EDIB is not included in decisions such as whether to request 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).
- Please explain your rationale concerning changing the current established practices in the context of EDPB.
- How will Cion address concerns on the changing of the definition of personal data (incl. pseudonymization)?
- Can you share further details on the amendments regarding automated decision making?
- Can you explain the process of notification of data breaches?
- We do see merit in repealing Regulation 2019/1150 (P2B). However, AT expects clearer information by Cion on where the provisions of the P2B Regulation are to be covered in future, as recital 59 remains very vague. The P2B Regulation addresses specific business issues in the relationship between business users and platforms. The DSA does not address these specific circumstances of business users as it was not taken into account in the negotiations, because we understood the P2B Regulation as *lex specialis* for business users. Business users, especially retailers on online marketplaces who conduct a large part of their sales via these marketplaces, have very different needs than private end users, i.e. consumers on social media platforms.

  Particularly important here are deadlines (Art 3 and Art 4) that are only guaranteed by the P2B Regulation, not the DSA: These concern changes to terms and conditions, but also, in particular, the deadlines for informing business users of the reasons for terminating their access 30 days in advance. This is missing in the DSA, but is essential for businesses.
  - Does the EC plan to incorporate these deadlines into the application of the DSA?
  - Transparency in ranking (Art 5 P2B-Regulation) is also important for business users, as they need to know the relevant parameters for their product listings. To what extent does the EC consider the transparency of ranking (Art 5 P2B) to be covered by the transparency of recommendation systems under Art 27 DSA?
  - Is there a need of an explicit reference to “ranking” in the DSA?
  - To what extent are the EC guidelines issued under Art 5 P2B-Regulation relevant to Art 27 DSA?
  - How is the application of the guidelines ensured in principle, given that they should also facilitate the implementation and enforcement of obligation of Art 6(5) Digital Markets Act (DMA), as stated in recital 52 of DMA?
  - Does Art 14 DSA (terms and conditions) also cover the transparency of restrictions regarding the ability of business users to offer the same goods and services to consumers under different conditions through other means than through those services and the grounds for that restriction (such as Art 10 P2B-Regulation)?
  - Art 11 P2B Regulation regarding internal complaint handling system is broader than Art 20 DSA as Art 20 DSA only covers complaints regarding notices or against the following decisions of platforms and is only available for a certain period of time (six months) after the notice/following decision. According to Art 11 P2B-Regulation the internal complaint handling system also covers other kinds of complaints by business users (e.g. regarding technical problems). How will effective complaint channels that take into account the specific needs of business users be ensured in future?

POLAND

Digital Package – PL questions

Poland welcomes the European Commission's simplification digital package (Digital Omnibus). However, due to limited time available, we submit the **scrutiny reservation**. We would need a reasonable time for in-depth analysis and internal consultations.

Overall, we support the Commission's proposals aimed at strengthening regulatory coherence and transparency. We consider them as fundamental to the proper functioning of the EU single market. In particular, we wish to underline the importance of **reducing unnecessary administrative burdens** and **enhancing legal certainty** for businesses operating in the digital environment.

We also welcome the focus on **deepening the digital single market** and further **harmonizing the relevant legal framework**. We believe this efforts will contribute to the improved conditions for both European businesses and users. At the same time, we emphasize the need for **an impact assessment of the proposed changes**. The aim is to maintain a high level of user protection and to safeguard fair competition in digital markets, as well as maintaining the established regulatory objectives, which primarily include increasing access and facilitating data exchange.

We are pleased that the EU digital law simplification package **incorporates proposals advanced during recent Polish presidency of the Council of the EU**. We will continue to support systemic solutions that make every day regulatory practice more efficient and predictable. In our view, simplification of EU law is not merely about deleting a few redundant articles. It's about building coherent European law in the digital sphere – from regulatory impact assessments, through social dialogue, to consistent implementation.

However, for the EU's digital ecosystem to truly develop, simplifying the digital acquis is important but not sufficient. It needs be accompanied by measures that **improve access to capital**, **expand scale-up opportunities** and **further harmonise the Single Market** (e.g., by addressing the "28-regime" problem).

We believe the simplification mindset should not be limited to the Omnibus packages alone; it should guide all new legislative proposals – particularly the upcoming Digital Networks Act and the Cloud and AI Development Act.

We would like to thank the DK PRES for presenting the plan of discussions until the end of this year. **We would appreciate to receive from the CY PRES information how the works will continue and what are the foreseen deadlines. We believe we should focus on the Omnibus on AI and after finalizing the Council position, move forward with the second one. Knowing the plan would** allow Member States organize internal works and do public consultation.

The proposed time of entry into force of the Digital Omnibus (on the third day after its publication) seems to be unfeasible. We stress the need for introducing longer transitional periods to adapt the existing regulations.

We would also be grateful if the Commission could clarify the following aspects:

I. GENERAL COMMENTS

Comments to proposed digital simplification package (general)

Reference point	PL comment

National-level implementation	From a legislative perspective, once the Digital Omnibus is adopted, does it require Member States to consolidate national provisions implementing the existing legal acts into a single legal instrument? How does the Commission envisage ensuring consistency and avoiding duplication across the national legal framework?

II. DIGITAL OMNIBUS ON AI

Overall, we view the proposed changes positively, as they aim to increase legal certainty and reduce administrative burdens, particularly for SMEs and small mid-caps. However, we would appreciate clarification on the following

Comments to proposed changes of AI Act – Regulation (EU) 2024/1689)

Reference point	PL comment
Art. 4a – Processing of special categories of data	Could the Commission clarify which criteria will guide the assessment of the necessity of processing special categories of personal data ('sensitive data', as per GDPR)? How will it be determined (and by whom) that the intended objective cannot be achieved using synthetic or anonymised data? How does the Commission assess (and intends to address) the risk that providers might invoke the "no alternative" justification inappropriately? What mechanisms are envisaged (1) for reporting to DPA that special categories of data were processed, and (2) for ensuring effective oversight of data deletion once the bias-detection process is completed?
Art. 6(4) – Risk assessment of AI system	Will providers' documentation be subject to systematic review by competent authorities, or only examined upon request? What safeguards are planned to prevent providers from underestimating system risks to avoid obligations under the AI Act? Does the Commission foresee harmonized assessment criteria for authorities across the EU to minimize divergence in evaluations?
Art. 57-58 – Regulatory sandboxes	What measures will ensure that real-world testing does not inadvertently lead to uncontrolled processing of personal data? Could the Commission clarify how will potential overlaps between the AI Act and the GDPR be addressed, for example with respect to consent, legal bases and the protection of data subjects' rights?
Art. 56 – Codes of practice	What is the rationale behind removing the possibility to adopt the positively assessed code of practice by the implementing acts in art. 56(6)? Is that not a step back towards the unified implementation of the AI Act?
Art. 75	In connection with the proposed changes, we would appreciate further information on envisaged principles of cooperation between national market surveillance authorities and the AI Office.
GPAI models	Which body will decide whether an AI system should be considered an AI system that is based on a general-purpose model? If the general-purpose model and the AI system based on the general-purpose model are developed by different providers, does the national market surveillance authority remain competent?

General questions	Could the Commission comment on whether the proposed changes may broaden exceptions for processing sensitive data in a way that affects existing GDPR safeguards? What steps will be taken to promote consistent interpretation among the various authorities involved (the AI Office, the EDPB and national data protection authorities)? How will it be ensured that data subjects have effective means to exercise their rights in cases of breaches occurring in regulatory sandboxes or during bias-detection processes? We note the proposal to postpone entry into force of high-risk AI requirements (Annex III) until December 2027. These additional time is much needed opportunity that the necessary standards and guidance are thoroughly developed and implemented. At the same time, could the Commission clarify the envisaged timeline for preparing these standards and guidance to support effective and timely compliance? Can the EC confirm that not adopting Digital Omnibus on AI before August 2026 would mean the existing high-risk AI requirements apply as originally drafted? In such scenario we are open for retroactive “grace” provisions. What is the rationale for making the postponement of the high-risk AI requirements dependent on the additional decision of the Commission confirming that adequate measures in support of compliance with Chapter III are available (new letter d in art. 113)? Will responses to incidents involving exploitation of AI functionalities or vulnerabilities (including incidents affecting AI-supported tools) be harmonized, for example between the AI Act and other EU legal frameworks such as NIS 2 Directive? If so, how will this harmonization be achieved? If an incident in a GPAI system affects the security of a key or important entity (covered by NIS 2), will the GPAI provider be required to submit dual incident notification (to both the AI Office and the CSIRT)? How will the AI Office's exclusive oversight over GPAI systems under Article 75(1) be coordinated with the responsibilities of national cybersecurity authorities (e.g. CSIRTs or NIS 2 competent authorities) and with national authorities designated under the AI Act? Will the EU AI regulatory sandbox (established under Article 57(3a) by the AI Office), provide an environment for testing resilience to cyberattacks and cyberthreats (e.g., through red-team operations) in alignment with CRA standards?

II. DIGITAL OMNIBUS

Overall, we view the proposed changes positively, as they aim to increase legal certainty and reduce administrative burdens, particularly for SMEs and small mid-caps. However, we would appreciate clarification and further guidance on several aspects mentioned below.

Comments to proposed changes of personal data protection regulation (GDPR and e-privacy)

Reference point	PL comment
1. Impact assessment	How does the Commission plan to ensure that the introduction of relative traceability (Article 4) maintains a consistent standard of data protection across the EU? Additionally, how might situations be reliably assessed where a controller indicates that it "cannot" identify a person, even if identification could be feasible with minimal effort? While the targeted approach is understandable, the absence of a full impact assessment makes it more challenging to anticipate potential effects on the protection of fundamental rights or the associated costs for businesses (e.g., adapting IT systems to accommodate browser signals).
2. Relative anonymisation and re-identification risk	The new approach suggests that data may be considered anonymous for some entities even if identifiable by others, including large platforms. How is a controller expected to demonstrate that it is "not likely" to use means of identification? Would the mere theoretical possibility of identification (e.g., via an external database) affect eligibility for the exemption?
3. Training AI on special categories of data	How should 'residual' presence of data be defined? What would be the boundary between deliberate training on sensitive data and incidental inclusion in AI models?
4. Specific categories of data in AI and 'disproportionate effort'	Which specific technical and organizational measures will the Commission (or EDPB) consider sufficient to prevent inference or disclosure when deletion is not feasible?
5. Burden of proof in abuse of the right of access	What practical guidance will be provided, particularly to SMEs, to apply a "reasonable grounds" threshold effectively without compromising individuals' access rights?
6. Research derogations	How does the Commission envisage ensuring that these exemptions do not create overly broad zones of non-transparency? Could safeguards be put in place to prevent potential circumvention of obligations to inform data subjects?
7. Harmonisation of pseudonymisation standards	How will re-identification risks be assessed in the context of modern AI tools? What safeguards are envisaged to ensure that pseudonymisation does not does not unintentionally reduce the scope of GDPR protections?
8. Signals from browsers (art. 88b GDPR)	Which technical standards are expected to apply? How might this affect advertising-based business models? Can a website block access if a user sends a "refuse all" signal? How will the Commission ensure that major platforms or OS providers do not disproportionate control over consent processes?
9. Exception for media service providers (cookies)	What compliance mechanisms are envisaged to ensure that this exception does not compromise voluntary and informed consent? How will privacy rights be maintained under this exemption?

Comments to proposed changes of GDPR – Regulation (EU) 2016/679)

Reference point	PL comment
Art.4(1)	Could the Commission clarify whether the use of relative terms such as "not necessarily" and "means reasonably likely to be used" might introduce uncertainty for controllers and processors? Is there a possibility that

	processing activities could be divided among separate entities in a way that inadvertently weakens the applicability of GDPR rules? Might this approach also increase the workload for supervisory authorities, who would then need to assess a controller's full range of operations in order to determine which involve personal data? Finally, how does the proposal intend to align with the Court's judgments in cases C-582/14 (Breyer) and C-413/23 P (SRB), which indicate that identifiers do not need to be held by a single entity to qualify as personal data?
Art. 4(38)	Could the Commission clarify how the proposed broadening of the definition of scientific research will interact with national laws in this area? Might the inclusion of commercial interests unintentionally expand the scope for activities that limit data subjects' rights?
Art. 5(1b)	Could the Commission comment on whether the new wording might allow controllers to rely less on Article 6(4), potentially reducing their level of accountability?
Art. 9(2)	Is there a risk that the proposed changes could facilitate the spread of special categories of data within datasets? Are the existing safeguards sufficient to mitigate such risks?
Art. 9(5)	How the "undue delay" timeline corresponds with the general GDPR deadline of 1+2 months for data subjects requests?
Art. 12(5)	What is the rationale behind specifically referring to Article 15 requests? How will controllers determine when a data subject is misusing their rights?
Art. 13(4)	Could the Commission provide examples of processing activities that do not require large amounts of data and explain whether particular challenges were identified in providing information to data subjects in such scenarios?
Art. 13(5)	In which situations does the Commission anticipate that responding to requests could "render impossible or seriously impair the achievement of the objectives of the processing"? How will this safeguard the principle of transparency?
Art. 22(1) and (2)	Could the Commission elaborate on the reasoning behind removing the data subject's right not to be subject to profiling, leaving only obligations for the controller? Is there sufficient evidence indicating that such cases are rare or non-existent?
Art. 33(1)	Is it taken into account that the risk levels reported in data breach notifications may sometimes be underestimated? Could this lead to situations in which data subjects are not notified about breaches affecting them, even following guidance from supervisory authorities?
Art. 35(4–6)	What is the reason behind transferring responsibility for approving the lists from DPAs to the Commission? How does it align with the independence of the European Data Protection Board as an EU authority?
Art. 41a	What is the rationale behind shifting the responsibility for such recommendations from DPAs to the Commission? How does this remain consistent with the independence of the Board and national DPAs? Additionally, how often has the Commission exercised similar powers under the existing legal framework?
Art. 88a	How should "aggregated information" be understood in the context of Article 88a(3)(c)? Should aggregation refer strictly to statistical data at a population level, or does it also include session-level or user-level aggregates?

	What safeguards will be put in place to ensure that controllers do not use the “audience measurement” exception to justify broader behavioural analytics, profiling, personalisation or optimisation activities that exceed the intended narrow scope of audience measurement? Is it permitted to combine telemetry or usage data collected under this exception (article 88a(3)(c) with other datasets or identifiers? Regarding Article 88a(4)(a), has the Commission considered setting precise technical standards for single-click button or “equivalent means” in order to avoid similar doubts to those currently existing regarding the form of consent to data processing (including cookie files processing)? In practice, how should consent to the processing of personal data look like for the end user when starting to use a new device, e.g. a smartphone or personal computer? In accordance with Article 88a(4)(1), will consent to the processing of personal data have to be included in an easy and intelligible manner, which will also mean that it is separate process from the acceptance of the terms and conditions of use of the service or the user regulations?
Art. 88b	Does the Commission anticipate that, in practice, the framework established under this Article will operate in a way that ensures browser-level or software-level choice mechanisms are set to privacy-protective default states, or will the choice of default settings of such automated means be left to the providers?
Art. 88c	How will it be determined when the rights and freedoms of the data subject, particularly in the case of children, override the interests of the controller? Are there harmonized assessment criteria across the EU? How can effective data minimisation be ensured during data selection and model training, given that machine learning typically relies on large and diverse datasets of varying quality? Are there technical standards or certification mechanisms that could enable authorities to assess whether AI systems adequately protect against the disclosure of residual data (e.g., in generative model outputs)? How is the unconditional right to object to the collection of personal data expected to work in practice? Could this mean that individuals may object even before their data is included in training datasets? Finally, are there mechanisms to strengthen transparency towards data subjects, for example through obligations to inform individuals that their data has been used to train an AI model?

Comments to proposed changes of NIS2 Directive (2022/2555)

Reference point	PL comment
Art. 23a – Single Entry Point	Poland, during its Council Presidency, has conducted several discussions regarding this issue and prepared a Presidency Report (10035/25). We see a huge potential of the single entry points for lessening of the administrative burden. We would welcome a presentation by the COM on the high level concept of the SRP, how in practice it will work, what would be the engagement of Member States in the development phase, what would be the flow of

	information and access to information, how will the national solutions be used/integrated in the SRP, who will be responsible to develop templates? Have the Commission evaluated the number of possible incidents and data flows that would be processed by the single entry point? How does the Commission plan to address the security and implementation challenges related to the significant collection of sensitive data? Which entities will have access to the data processed by the single entry platform? Which entity will be responsible for the security of the data proceed there? Could the Commission clarify how it will be ensured that a single notification to multiple authorities does not result in unnecessary dissemination of personal data?
Reference with other EU legislation	How will it be ensured that notifications deemed "equivalent" under different legal acts include only the personal data strictly necessary? How will be ensured that 1) the notifying entities have a simple way to report an incident and that 2) the competent authorities and CSIRTs have enough data to execute their powers (incident handling, audits, penalties)?
Art. 30 (1) – Voluntary notifications	What safeguards are envisaged to ensure that voluntary notifications do not lead to excessive collection of personal data, particularly from entities outside the scope of NIS 2?

Comments to proposed changes of Data Act – Regulation (EU) 2023/2854

Reference point	PL comment
B2G data access	Why the single template for requests for access to private data was deleted (art. 17 par. 6 of Data Act)? This is particularly important given that a single template for such requests is a key element of a coherent B2G data access system. Abandoning the introduction of such a form may lead to new barriers in this area.

Comments to proposed changes of Data Governance Act – Regulation (EU) 2022/868)

Reference point	PL comment
Data altruism & data intermediation services Data altruism consent form	We welcome the efforts to consolidate and streamline the rules for data intermediation services and data altruism organizations. In particular, we appreciate the voluntary nature of the registration regime for data intermediation service providers, which we consider a positive step towards flexibility and proportionality. We would welcome more reasoning on the removal of provisions regarding the development of a unified European data altruism consent form and the proposed 'Data Altruism Rulebook.'
Application forms for data intermediaries and data altruism organisations	What is the reason for allowing the competent authorities to issue application forms while simultaneously removing from the relevant articles provisions on the necessary elements of the application forms? What will prevent Member States from issuing different forms resulting in fragmentation, not simplification? Has the option of preparing the form by the Commission been considered?

Penalties	Could you clarify that art. 40 on penalties is applicable to Chapter VIIa, i.a. Member States are expected to indicate the list of punishable articles in national legislations?
Cross-border enforcement and cooperation	Why has not this opportunity been used to clarify the rules concerning the cross-border cooperation of competent authority in enforcement? It was discussed with the Commission via EDIB and flagged out as problematic. Could you clarify that art. 37.2-15 is applicable to chapter VIIa's competent authorities?
Transitional provisions and transitional period	What is the reason for removing transnational provisions for chapter VIIa? How is the new chapter VIIa to be enforced in the period between its entering into force and the amendment of national legislations implementing the DGA?

Comments to proposed changes of Open Data Directive – Directive (EU) 2019/1024

Reference point	PL comment
Interplay between Section 2 and 3 Scope of Section 3	We would welcome more clarification on the relationship between Section 2 (re-use of open government data) and Section 3 (re-use of certain categories of protected data held by public sector bodies), as we consider this relationship as not entirely clear. Please clarify whether Section 3 covers only data, or both data and documents, as well as clarify the scope of the provisions on the re-use of certain categories of protected data held by public sector bodies?
ODD evaluation	We would welcome to receive reasoning why PL comments and suggestions presented within this year's ODD evaluation process have not been reflected in the proposal? Does the Commission intend to publish a report summarizing this evaluation exercise of the Open Data Directive?
Implementation at the national level	We would also like to highlight the potential implications of implementing the ODD provisions from the Omnibus regulation directly into national law. Unlike a directive, which allows Member States to adapt definitions and limits within their own legal frameworks, a regulation applies directly, requiring significant adjustments to existing national systems. We would appreciate further clarification on the anticipated benefits of this approach, particularly in terms of administrative feasibility and legal consistency.

SLOVENIA

Questions related to Omnibus VII – Slovenia

2025 11 26

GDPR

General question

1. What is the rationale of proposing a change to a regulation implementing a fundamental right, without conducting an impact assessment of the proposed change on fundamental rights and on competent authorities enabling those rights?

Definition of personal data

1. How will the companies assess whether the means reasonably likely to be used allow them to indentify the natural person?
2. Can a company have means to identify a natural person, but chooses not to use those for particular processing and still consider data non-personal?
3. Why does the provision establishing an indeterminate standard of 'reasonably likely to be used' replace the wording and standard set by the Court, which provides that individuals to whom personal data relate remain identifiable unless it can be excluded that the third party(subsequent processor) has means reasonably allowing them to attribute pseudonymised data to the data subject?
4. How will a subsequent processor that already holds certain data and receives data from an entity that considers the transmitted data to be non-personal, while the combination of all data enables the subsequent processor to identify the individual, be able to obtain consent for the processing of personal data?
5. How will the proposal affect the functioning of Chapter V of the GDPR, regarding the transfers of personal data to third countries or international organisations? Will the proposal have an affect on adopted adequacy decisions and the ongoing adequacy procesess?
6. How can an entity which processes data in such a way that they are considered non-personal ensure that an entity in a third country, to which the data are transferred, cannot process those data in a manner that would render them personal again?

Personal data processing for AI development and operation

1. Who will determine whether processing may be pursued for legitimate interest within the meaning of Article 6(1)(f)? Which types of processing/activities quailify as »operation« and »development«?

Personal data processing for scientific research

1. Does the new definition include processing of personal data for the purpose of development of AI and research of markets? What falls into the scope of scientific research and – where is the line drawn?
2. Who will set the ethical standards that the scientific research must adhere to?

Exercise of the right of access

1. How will the controller assess whether the data subject's request for access is made for the purposes other than the protection of personal data?
2. Will this possibly limit individuals right of access for other purposes, such as economic interest, health purposes, and other possible purposes not aimed at abusing the right?
3. Will an individual have to provide additional, possibly senstitive data to prove that their request for access is not abusive?
4. Did the Commission make an assessment on how will this limitation and the possibility to arbitrarily interpret the data subject's intent affect supervisory authorities and national courts?

Cookie rules

1. What is »aggregated information about the usage of an online service« – which information falls into this category? How does article 88a prevent access to communication content when processing is not necessary for the purpose of carrying out transmission of an electronic communication?

Reporting: Single-Entry Point

1. How will the Single Entry Point be connected to national incident-reporting platforms to ensure minimal additional administrative burden for both Member States and reporting entities?
2. Considering the Digital Omnibus is presented as a simplification Act aimed at reducing administrative workload, will incident notifications from obligated entities be channelled through the EU Single Entry Point and automatically forwarded to national competent authorities?
3. Since the obligation for quarterly reporting of significant incidents under NIS 2 through CIRAS appears to remain in place, how will the Omnibus simplify reporting procedures between the Single Entry Point and CIRAS?
4. What safeguards will be implemented to guarantee that ENISA's management of the SEP platform ensures a high level of security for sensitive incident-related data, especially when such data may contain national security–relevant information?
5. Which organization, will be responsible for technical support and which for governance?
6. Who will have access to the data/reports and where will they be stored (in the EU, outside)?
7. Will the platform enable reporting of incidents in all the EU MS languages?
8. Will ENISA provide the solution for the platform or will it outsource it to a certain company? In case of outsourcing it to a company will the principle be followed, that non-EU financed companies cannot participate?
9. How will governance of personal data be handled in order to comply with GDPR when it comes to the Single Entry Point reporting?
10. How does the Commission intend to address concerns that direct reporting of incidents by entities to ENISA through the Single Entry Point could reveal the identity of liable entities? Currently CIRAS allows for anonymised reporting under the control of National Competent Authorities, meaning that this could have the effect of decreased level of reporting from entities, because of national security concerns and sensitive data.
11. How will you ensure direct reporting to ENISA via the Single Entry Point does not bypass national competent authorities, thereby undermining Member States' primary responsibility and legal mandate for national cybersecurity and defence?

SLOVAKIA

Slovak questions on Digital Omnibus:

1. The scope of the changes proposed in the Digital Omnibus in relation to the GDPR is substantial. This is especially the case when it comes to the use of personal data for AI development and training. Could you please explain why an impact assessment has not been prepared for these substantial changes as well as explain in detail how the existing standard of the protection of personal data will be kept?

2. Taking into account the scope of the revision of the data acquis and the readability of the legislative text, why hasn´t the revision been carried out in the form a of RECAST?

3. How should the competent authorities, according to the regulations under the Omnibus framework, prepare for the upcoming changes regarding the enforcement of their responsibilities?

4. How does the EC plan to support Member States in adapting their supervisory structures to the changes?

5. The data package legislative proposal aligns several digital legal instruments and introduces mechanisms such as a single entry point for incident reporting across multiple frameworks. Since the AI Act is in a separate legislative proposal, how does the EC envisage ensuring practical alignment between the proposed data package and the AI act, particularly with regard to supervision, reporting obligations and consistency in definitions?

6. Does the EC plan to use the Digital Omnibus as a platform to promote future interoperability with international partners (e.g., OECD/GPAI, ISO/IEC)?

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.
- We are still analysing the proposals and are looking forward to the discussions.

More detailed comments and questions for the Commission:

1. **The repeal of the P2B Regulation**

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. **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. 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.

2. **GDPR:**

- FI considers that the GDPR has succeeded in its objectives. However, FI has recognized the need to alleviate administrative burden and to ensure a consistent interpretation of the GDPR. Therefore FI has been open to discuss on possible, targeted simplification measures to the GDPR.
- FI 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 FI 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, but we will return with those later on.

Question on the GDPR proposal: 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?

3. **ePrivacy Directive**

Question on the GDPR and ePrivacy proposal: 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?

4. **Data Act**

Question on the Data Act proposal: 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.)

Question on the Data Act proposal: 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?

Question on the Data Act Proposal: 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?

Question on the Data Act Proposal: 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)

Question on the Data Act Proposal: 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))? What would be the future of the PSI Expert Group?

Question on the Data Act Proposal: 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?

SWEDEN

Written questions and initial reactions on Digital Omnibus on AI – COM (2025) 836 (and Digital Omnibus – COM (2025) 837)

- **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?

- Want to have more information on single-entry-point at Enisa and how this will relate to national reporting systems. If possible, could the Commission arrange a separate expert meeting to explain this in more detail.
