Council of the European Union
General Secretariat

PUBLIC

Interinstitutional files:
2025/0360 (COD)

Brussels, 19 June 2026

WK 8978/2026 INIT

LIMITE

SIMPL
ANTICI
DATAPROTECT
CYBER
TELECOM
PROCIV
COMPET
MI
CODEC

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 rules) - MS comments: follow-up of the AGS of 15 June 2026

Delegations will find enclosed comments as received from CZ, DK, DE, EE, EL, ES, FR, IT, LU, NL, AT, PL, PT, FI, on Omnibus VII (Digital rules).

Omnibus VII – Digital rules
Regulation on Simplification of the digital legislative framework

– MS comments –

AGS 15/06/2026

PUBLIC

Table of Contents

CZECHIA

ČESKO

CZ comments on Digital Omnibus (follow up to AGS meeting on 15. 6.)

Data acquis

- **Trade secrets** – CZ believes the current text shifts the balance established in the Data Act, making the exemptions from sharing of trade secrets in Art. 4(8) & 5(11) widely applicable, thus undermining the main principles of the Data Act. Similarly, as NL, BE, MT, EL, **we prefer the previous compromise text from May 29 without additional changes on trade secrets.**
- CZ also proposes to **return of the deleted Article 17(**6), which obliges the Commission to prepare a model template for requests under Chapter V to allow better harmonization across the EU.
- CZ proposes that the COM prepares **guidelines on Chapter VII and the conditions for third-country governments' requests** which are essential for the harmonization, effective implementation and enforcement of the Data Act.
- **CZ supports further work on EDIB structure,** notably proposes **the return of deleted competencies of EDIB in relation to Chapters VI and VIII of the Data Act.**
- To ensure harmonized implementation **– individual definition of 'very large enterprises' at MS levels should be avoided.** Additionally we would welcome further information justifying this change in Recital 25.
- **The term 'data user',** which is defined under the DGA, **should be maintained** (since the DGA is to be repealed, CZ considers it important to maintain this definition in the Digital Omnibus).
- **In Art. 32e CZ proposes standardized application forms on data intermediation services providers** to ensure that the same information is required in all applications.
- CZ also supports the input by Luxembourg on the Data Act Part from 15th June 2026.

Cybersecurity incident reporting

- **CZ particularly appreciates more detailed definition of the national entry** point and its functions, which provides greater clarity, but also ensures that this remains sufficiently flexible and does not impose new rigid requirements on national systems.
- The current proposal guarantees that each Member State can establish its national entry point flexibly according to its own needs. It may take different forms, including by connecting existing systems and enabling the sharing, routing or distribution of relevant information. This flexibility, and the possibility to fully use already existing systems is key for CZ.
- In this respect, CZ underlines the necessity to further align and clarify all relevant provisions of the proposal, including recital in a way that allows the flexibility declared in the proposal to be effectively applied at the national level in practice. Further clarification is needed also in terms of practical functioning of the cross-border notification system. This relates to provisions in art. 6(1a) and 6(1c).
- **Additionally, we would appreciate clarifying recital 50** by using a consistent term for ENISA outputs. The current wording refers both to "non-binding recommendations" and "guidelines", which creates ambiguity as to whether these are separate instruments or the same output described inconsistently.

Drafting suggestions related to the incident reporting:

Rec. 50

To ensure the security of national entry points in particular and with a view to designing interoperable national entry points, ENISA should develop non-binding **guidelines ~~recommendations~~** addressing the appropriate and proportionate technical, operational and organisational measures for Member

States to develop, maintain and securely operate their respective national entry point. ENISA should establish a cross-sector working group to develop **these** guidelines in cooperation with **CSIRTs and** competent authorities ~~**and CSIRTs**~~ under the relevant Union legal acts**.** ~~**when drafting the technical, operational and organisational measures necessary to establish, maintain and securely operate the national entry point by**~~ **ENISA should make use** ~~**making use of**~~ existing cooperation groups and networks **when establishing this working group.** ~~**of Member States established under these acts.**~~

CZ comment:

CZ suggests clarifying recital 50 by using a single, consistent term for ENISA outputs. The current wording refers both to "non-binding recommendations" and "guidelines", which creates ambiguity as to whether these are separate instruments or the same output described inconsistently. We would prefer the use of "guidelines" since it's also used in rec. 51. CZ would favour aligning the text to one term only and overall clarify the wording of this recital.

Rec. 54:

CZ comment:

CZ would like to note that besides DORA templates, at the end of May, the NIS Cooperation Group adopted the templates for incident reporting according to NIS2 that could be also reflected.

Art. 6 (1a) (new art. 23b on National entry point for incident reporting):

CZ comment:

CZ believes that the NEP should be capable of the full range of core functions necessary to make the system operationally effective, as stated in art. 23b para 1, and provide added value for Member States or reporting entities.

Art. 6 (1c) (new art. 23d on Cross-border incident notification)

(2) ENISA shall, in cooperation with the CSIRTs network, the Cooperation Group and competent authorities under the relevant Union legal acts, as well as with other relevant bodies or groups established at Union level under relevant Union legal acts, ~~**harmonise its relevant tools with national incident notification templates and**~~ facilitate an automatisation process to exchange information about cross-border impacts.

CZ comment:

The reference to specific "tools" appears to be a legacy from earlier versions and is no longer relevant in the current context.

GDPR related suggestions

Pseudonymization

- Regarding the application of pseudonymisation under Article 29a, CZ would like to briefly reiterate that it continues to consider this issue **a red line**. **Rules of such significance should be adopted in a binding, formal and predictable manner.**
- While we acknowledge that EDPB opinion is more certain than guidelines, the significance of this issue is why we continue to strongly prefer standard legally binding comitology.
- Regarding art. 29a paragraph 2, CZ considers the proposed wording as containing inherent risks and therefore being prone to potential misuse. An example could be artificial chains of controllers or subsequent indirect linking of data. But we understand that Presidency believes such risks could be mitigated by comitology (as we prefer) or EDPB opinion?

Scientific research

- Regarding scientific research, in Recital 28 CZ proposes **deleting** from the first sentence the words "**the purpose of the research**" (as any research that is scientific should benefit from the relevant exemptions) and "**reliability, accountability, oversight**" (as these are neither included in the definition nor explained, and it is unclear what, in the context of inherently uncertain research, for example "reliability" is meant to signify).
- Additionally, CZ will support the revised wording of the third sentence of Recital 28. Although it still uses the unclear terms "**autonomously and independently**", it at least states

that such requirements are not incompatible with the commissioning of research in both the private and public sectors.

AI

- **CZ believes that Digital Omnibus and changes to GDPR are not ambitious enough and do not contribute to much needed simplification to allow AI development and training in the EU**.
- CZ believes that **reinstalment of Art. 88c** (as proposed by DE or in other form) is essential element prior to closing Council position, it is being seen as a practical measure by the academia and industry.
- CZ is against the addition of "**strictly**" in Article 9(2)(l), as all the derogations in paragraph 2 already must be interpreted strictly and this exceptionally "strict" approach, inconsistent with the rest of the Article 9, will make the derogation unpredictably narrow and therefore the opposite of simplified.
- CZ **does not support the unclear sentence on artists** in Recital 33a. Under the GDPR, artists are addressed only within the freedom of expression exemption. It is unclear why their legitimate interest is highlighted here or what additional obligations this would create in the AI context. Recitals 105, 134 AIA are already there. CZ therefore calls on CY PRES to either clearly explain this sentence or **delete it.**
- CZ **does not support the wording "manifestly disproportionate effort",** which lacks a basis in GDPR terminology and may create interpretative issues. It may propose deleting "manifestly" and "further processed" as unclear and overly restrictive, or, as a compromise, aligning the wording with the GDPR by **using "further processed for other purposes"**.

Right of access and exemption from information obligations

- In relation to Article 12(5) CZ prefers abuse of rights to apply across all rights and therefore **opposes the square brackets limiting** it to Article 15. Given the difficulty of proving intent, it favors the Commission's approach based on reasonable grounds to presume abuse, with a clear preference order led by the Commission text (without limitation to Art. 15). In the spirit of compromise, we can also accept the **new wording on "reasonable grounds"** as proposed by Presidency and German delegation.
- In relation to Article 13 on low-risk processing CZ strongly **supports the German proposal**, which is more practical and streamlined and better corresponds to the simplification objective.
- On the other hand, CZ supports amending Art. 57(4) GDPR with words "or where an abusive intervention on the part of the data subject submitting those requests can be demonstrated" and "in the light of all the relevant circumstances of the case" since this provides further clarification.

Cookies

- CZ supports deletion of art. 8a of the GDPR, following the Coreper discussion last Monday.
- Concerning the ePrivacy part of the proposal, CZ supports further in-depth discussion on possible solutions to the "cookies fatigue" phenomenon.
- We note that an IA has been prepared for the ePrivacy Regulation proposed in 2017; **at the same time, it should be recognised that since then, the technological development has been quite significant.**
- We remain convinced that **extending the whitelist reasonably and in a proportionate manner is a right approach,** and in this regard, we see a space to accommodate the low-risk purposes further.
- We remain convinced that for the purposes of Article 5 of the ePrivacy part of the proposal, the text
    - should be further complemented by the **contextual advertising** and

- **Clarify that collection of anonymised vehicle data for road safety and accident prevention is clearly recognised under the letter b).**

- Particularly the second point concerning the road safety is very important for Czechia, **given that research and development in the automotive sector are based in the EU**, and in this regard, it constitutes a **red line** for us, as flagged in our written comments sent prior to the AGS meeting held on 27 May 2026.
- **Czechia remains open to further discussion and bilateral exchange.**

Drafting suggestions to the ePrivacy Directive part of the proposal (new text highlighted; similar suggestion was shared to the previous compromise text)**:**

Recital 44b

(44b) ... This could include memorising the user's choices and selected elements such as, among others, the user's language settings, configuration choices, items placed in shopping baskets or memorising information to facilitate filling in of online forms. **Another example is the storing of or access to information in terminal equipment for the purposes of road safety, transport safety, and accident prevention, including the operation, maintenance, and improvement of connected vehicles and mobility systems.**

CZ Comment:

The narrow exemptions of Article 5 of the ePrivacy Directive (2002/58/EC) creates significant difficulties for vehicle manufacturers seeking to transfer data out of vehicles; any time the onboard telematics unit or sensors send data externally, it may qualify as "accessing/storing information" under Article 5(3). This challenge is compounded by the fact that a vehicle is rarely used by a single individual; it may be driven by the owner, a family member, an employee, or a short-term renter, with passengers also potentially implicated. In this regard and given the importance of automotive sector for the EU, including the R&D based in the EU, we suggest adding an example of data processing, which would in our opinion fall under art. 5(3)(b) of the proposal – providing a service explicitly requested by the subscriber or user. ***Reflecting this particular change in the omnibus is a red line for CZ.***

Article 5 (3)

(f) contextual advertising and related limitation of advertisement display, audience measurement and preventing fraudulent misrepresentation of audience, unless at least one of the following applies:

(i) the processing is likely to result in a risk to the rights and freedoms of natural persons;

(ii) the processing involves profiling;

(iii) personal data are stored at the time when the electronic communication service is not actively used;

(iv) personal data are connected with past or future activity of the data subject.

Recital 44b (to be added to the very end of the recital)

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

CZ Comment:

CZ suggests adding new exemptions concerning activities that are not based on profiling, i.e. covering low-risk to the rights and freedoms, non-profiling activities that do not involve any retention of personal data beyond the user's active session nor any link to past or future behaviour. This suggestion is inspired by the EDPB/EDPS joint opinion (point 104) which emphasises the need to create incentives to use less-intrusive forms of online advertising and aimed to make the rules more proportionate, i.e. allowing some forms of targeted advertising, which is crucial for European publishers and service providers. Czechia remains convinced that with this addition, the text would

appropriately balance the data protection and industrial needs. In this regard, we consider this addition as proportionate.

***

PUBLIC

DENMARK

DANMARK

Comments from DK regarding Omnibus VII (Digital rules):

Comments regarding the Data Act

DK is supportive of many of the other changes to the Data Act. We are in particular supportive of the addition of "where possible and appropriate" in Article 321a on the re-use of public sector data and the addition in Article 33 that the Commission should consult EDIB before adopting delegated acts.

Comments regarding ePrivacy

DK is very supportive of the deletion of Article 88b of the GDPR on central consent.

- We are very supportive of the changes to Article 5, para 3 and related changes to preamble 44.
- We are particularly supportive of the deletion of "instantly" and "solely for their own use" in the preamble, as well as with the added text regarding how anonymous aggregated information can be shared with third parties, which is essential for media services' ability to attract advertisers.
- We further find that the new introductory text in the Article and the preamble better reflects the reality in which audience measurement is performed (that is, that the first step is to collect information and the second step to process it).
- We can support the new para (e) regarding an exemption for prevention and detection of fraud.

Like other Member States, we believe that it would be prudent to expand the whitelist for low-risk and strictly necessary purposes, while we would have preferred to see the exemption for contextual advertising reintroduced

***

PUBLIC

GERMANY

DEUTSCHLAND

15 June 2026: DE comments on Omnibus VII (Digital)

PUBLIC

General remarks

- We thank the CYP Pres for preparing a new proposal. However, we still cannot accept the text without further changes that take into account our key concerns. Thus, Chancellor Merz might address the lack of ambition of the Council negotiations on the Digital Omnibus during the European Council meeting this week.
- While the current proposal is addressing some of the concerns DE has voiced in the process, the current proposal is still not sufficient to achieve the desired simplifications and relief. DE has stated in CRP and AGS that key priorities should be implemented in the text.
- DE key priorities remain unaddressed, particularly:
    - Regarding cookies, Germany demands an impact assessment as was asked for by a large majority of MS in COREPER and which must also include the issue of the six months waiting period in draft article 5 of ePrivacy Directive. This impact assessment shall cover all relevant parameters, such as the effects on consumer protection, the digital economy, and the media sector.
    - With regard to the GDPR, the proposed simplifications concerning data subject rights have still not been implemented in a practical manner.
    - It is crucial for us, that in Art. 29a the concept of relative anonymity is reflected more clearly. We refer to the respective GER and SWE proposal.
    - We thank the Presidency for including our proposals on Recital 33a. However, the recital only works in combination with the legal basis in Article 88c.
      Therefore, we still urge the Presidency to additionally reintroduce Article 88c of the Commission's proposal, subject to the deletion of the last clause (as proposed in the last GER written comments).
    - Regarding single-entry-points, the necessary flexibility to account for diverse national circumstances is still lacking.
- We share the assessment of several other Member States that more time might be needed to collaboratively work on further enhancements to the text. The objective should be to adopt an ambitious Council position on the Digital Omnibus which significantly improves the competitiveness of the EU and eliminates existing legal uncertainty.
- [For Germany, a PGA would, in principle, be conceivable.]

On the Presidency Note

Round 1: Data Act

- DE acknowledges that the Presidency has submitted a new proposal on trade secrets protection ("handbrake mechanism", Art. 4 (8), Art. 5 (11) Data Act) in its new draft compromise text, taking into account DE proposals.
- DE keeps advocating especially for improving data access and data use to develop, train, test and validate AI Systems (Art. 4 (13) Data Act) as well as for reducing bureaucracy by striking disproportionate information and notification obligations.
- In addition, DE refers to the proposed amendments regarding the Data Act, the Open Data Directive and the Data Governance Act, which are included in the comments previously submitted.

- DE Non-paper positions have previously been submitted in documents and are therefore not new. The DE Non-paper proposals are in line with political objectives on simplifying the Digital Acquis.

PUBLIC

Round 2: P2B

- We are still examining the proposal.

Round 3: Cyber and Single-Entry-Points

- We thank the CYP Presidency for developing a new proposal. Unfortunately, we have not yet been able to examine the proposal in the short time since its publication. We therefore place a scrutiny reservation and refer to our statement from CRP, briefly:
- "A national single entry-point for incident reporting as proposed for the European level is not acceptable for us."

GDPR:

Round 4: Application of pseudonymisation and identification of a natural person

Art. 3(1), Art. 3(10) – Proposed Art. 29a GDPR, Recital 27a, Recital 27b

- The incorporation of the SRB-judgement in the enacting terms of the GDPR is crucial for GER. Our goal is to implement the concept of relative anonymity to achieve greater legal clarity. In the spirit of compromise, we are also open to locate the proposal in Art. 29a GDPR to keep the definition of personal data in Art. 4 (1) untouched.
- We thank the Presidency for **adding a new paragraph 2** which now contains some provisions on relative anonymity.
- But in our view Art. 29a (2) still needs **some modifications and clarifications** to truly achieve the goal of **greater legal clarity**.
  The **SWE-GER proposal** (supported by DNK) can serve as a basis for these necessary modifications.
- We believe the SWE-GER proposal is well-balanced as it also sets clear and concrete boundaries, for example by **excluding data processors from the scope of application.**

Round 5: Other GDPR provisions

Personal data processing for purposes of AI Training

Article 3(15) - Article 88c, Recital 33a

- For future European competitiveness—a core objective of the Digital Omnibus—it is crucial that European companies are able to develop and operate AI in compliance with the GDPR. For GER, it is essential that the **necessary adjustments to the legal framework are addressed in the Digital Omnibus**.
- We thank the Presidency for including our proposals on **Recital 33a**. However, the recital only works in combination with the legal basis in Article 88c.
- Therefore, we still urge the Presidency to additionally **reintroduce Article 88c** of the Commission's proposal, subject to the **deletion of the last clause** (as proposed in the last GER written comments).

Data Breach Notifications

Article 8 – Recital 39

- We **thank the Presidency** for altering the threshold to **96 hours.**

Information obligations

Articles 3(4) and 3(5) - Recitals 35, 35a, 36

- We still cannot fully agree to the current text proposals of the Presidency for Art. 12 (5) and Art. 13 (4).
- We thank the presidency for including in Art. 12 (5) the GER**-POL proposal** (supported by DNK) as an alternative text-option with respect to the burden of proof. Of course, we strongly **support this text suggestion**, thereby lowering the threshold for the controller. Moreover, in the case of an abusive intention, the alleviation in Art. 12(5) should be limited to Art. 15, as suggested in the PCY text in square brackets.
- With respect to Art. 13 (5), we thank the Presidency for attempting to create a more comprehensive structure of the exemption for information obligations. However, we consider the possible scope of this exemption too narrow and the proposal too complex. **We thus again refer to our GER-POL proposal** (supported by DNK).
- In order to solve existing problems of blocking effective communication, GER reiterates the importance of the suggested addition in Art. 32, to adjust the level of security to an appropriate extent.
- Regarding scientific research the regulatory text does not yet sufficiently address the inclusion of commercial research.
- GER sees a further need to ease the burden on DPAs in handling complaints, which have increased massively – partly due to AI. We refer to our proposal for an amendment to Article 57(1)(f) GDPR (possibility to discontinue proceedings on grounds of expediency).
- Art. 49 GDPR: GER is of the view that the automatic exchange of information (AEOI) in tax matters with third countries must be ensured under the GDPR. We support the Commission's endeavors to clarify the matter outside of the amendments of legislation in the context of the Digital Omnibus.

<u>Round 6: Cookies and ePrivacy provisions</u>

- We thank the presidency for its work on Articles 8a GDPR (Article 88b in the Commission proposal and Article 5 Paragraph 3 ePrivacy-Directive (Article 88a in the Commission proposal).
- Germany can support the deletion of Article 8 a (Article 88b in the Commission proposal), which corresponds to the need of an impact assessment, that Germany strongly demanded for.
- Regarding Article 5 Paragraph 3 ePrivacy-Directive (and the corresponding recitals as well as the provisions in the amendments proposed for Article 37 Regulation (EU) 2018/1725 (EUDPR) (Article 4 Number 8 of the Digital Omnibus)):
    a. We support the demands of the POL Non-paper.
    b. We demanded for an impact assessment on multiple aspects, particularly
        i. regarding a general review of the proposed time period of 6 months for which service providers – in particular media services financed through advertising based on consented cookies – shall be prohibited to demand a user for consent again,
        ii. the white list and the general impacts of the provisions on the digital economy, audience measurement, the IoT sector, machine-to-machine communication and new technologies in general – particularly in the automotive sector.

PUBLIC

c. We refer to our position (dated 8 June) submitted to the council and Member States on 9th June.

DEU/SWE Proposal on Pseudonymisation

In our view, Art. 29a does not seem as ideal place of regulation to this end. Still, in the spirit of compromise, we are also open to locate the proposal in Art. 29a GDPR to keep Art. 4 (1) untouched.

Drafted suggestion in the operative text:

(xx) Data shall not be considered personal for an entity if that entity is unable to identify the natural person to whom the data relates.
To determine whether the natural person is identifiable, account should be taken of only the means the entity possesses or can obtain and are reasonably likely to be used to identify the natural person directly or indirectly.
The provision set out in (xx) shall not apply where the entity concerned puts data at the disposal of other persons who possess or can obtain means reasonably likely to be used to identify the data subject.
In such a case, both the transfer of data by this entity and the subsequent processing of those data by the recipient will be considered as processing of personal data.
The provision set out in (xx) shall not apply if the entity is a processor.

In the recital:

Regarding pseudonymised data, the existence of additional information enabling the data subject to be identified does not, in itself, mean that pseudonymised data must be regarded as constituting, in all cases and for every person, personal data. Pseudonymisation may, depending on the circumstances of the case, effectively prevent persons other than the controller from identifying the data subject in such a way that, for them, the data subject is not or is no longer identifiable.
Data which are in themselves impersonal may become 'personal' in nature where they are put at the disposal of other persons who have means reasonably likely to enable the data subject to be identified. In so far as it cannot be ruled out that those third parties have means reasonably allowing them to attribute pseudonymised data to the data subject, such as cross-checking with other data at their disposal, the data subject must be regarded as identifiable as regards both that transfer and any subsequent processing of those data by those other persons.
A means of identifying the data subject is not reasonably likely to be used where the risk of identification appears in reality to be insignificant, in that the identification of that data subject is prohibited by law or impossible in practice, for example because it would involve a disproportionate effort in terms of time, cost and labour. Means reasonably likely to be used by an entity to identify a natural person directly or indirectly include inter alia legal means of obtaining additional information from another person making it possible to identify the data subject as well as the singling out and cross-checking with other data at their disposal.

DEU/POL Proposal on Article 12(5) and 13(IV)

Article 12(5)(b) - proposed adjusted wording:

The controller shall bear the burden of demonstrating that the request is manifestly unfounded or that there are reasonable grounds to believe that it is excessive or submitted with an abusive intention, based on objective circumstances related to the request or the conduct of the data subject.

Argument: Without lowering the burden of proof for the controller, the provision will not have the desired simplification effect.

Article 13(4) – proposed adjusted wording:

4. Paragraphs 1, 2 and 3 shall not apply if and to the extent that the data subject already has the information or if the provision of such information proves impossible or, provided the processing is to result in a low risk to data subjects, would involve a disproportionate effort, especially in every-day business. Article 14(5)(b) shall apply accordingly. Sentence 1, 2nd and 3rd alternative shall not apply where the processing concerns personal data referred to in Articles 9 or 10 of this Regulation, or where the personal data are further processed for purposes other than those for which the data were originally collected.

Argument: The current proposal is too complex and will cause practical difficulties in its application. The compromise text still lacks practicability. In addition, the exceptions to the general rule introduced by the EC are too far reaching to have an actual simplification effect.

Digital Omnibus – Position of Germany on the Impact Assessment of Article 8a GDPR and Article 5 Paragraph 3 ePrivacy Directive

As announced during the Permanent Representatives Committee meeting on 8 June 2026, Germany supports Poland's non-paper and the proposed approach regarding Article 8a GDPR, the enrichment of the white list in Article 5 Paragraph 3 ePrivacy Directive and the demand for an impact assessment that must also fundamentally review the 6-month-period proposed in Article 5 Paragraph 3 ePrivacy Directive. The impact assessment should include all relevant parameters such as the effects on consumer protection, the digital economy, and the media sector, and address the following aspects and questions:

1. What requirements on integrity and competition exist in other legal areas that regulate time periods within which consumers may not be contacted again for business reasons, and what are the experiences that were made with these regulations?
2. What time periods do supervisory authorities currently apply in the area of cookie banners regarding the blocking effect of a previously refused consent, how do companies comply with these existing time periods and what enforcement measures are known in this regard?
3. How would the proposed 6-month time period affect the ability of users to review and change their consent decision during the duration of the time period?
4. Depending on the duration of the time period not to demand again for consent, to what extent does the number of interactions by consumers with cookie consent banners decrease?
5. What proportion of the dissemination of cookie banners is attributable to different online services, particularly media services, and what impact would the proposed six-month period have on the business models of different types of media services?
6. To what extent does a short period for not re-asking reduce consumers' willingness to read cookie banners attentively and make conscious settings?
7. To what extent do the proposed regulations affect the financing of services with journalistic content and the economic viability of digital business models of press publishers and other media providers, including advertising-funded, paid, and mixed-funded services?
8. What would be the impact of the proposed regulations on media pluralism, media diversity and access to journalistic content in the European Union?
9. What impact would the proposed regulations have on the competitiveness and innovation capability of the European media, advertising and digital economy in international competition?
10. How do the proposed regulations affect competition and market structure in the digital ecosystem, particularly with regard to media companies, small and medium-sized enterprises, advertising companies, technology providers and large digital platforms?
11. What effects do the proposed regulations have on the availability of objective and comparable audience and reach data, on independent audience measurement systems and regarding transparency, comparability, and verifiability of audience measurement?

12. Through the implementation of the proposed regulations, what are the administrative, technical and organisational costs to companies, press publishers and providers of journalistic media services, and are these burdens in an appropriate proportion to the intended goals?
13. How far does the scope of application (use cases) of the regulations extend?
14. What impacts are to be expected on

- the end-users and consumers,
- the service providers,
- the job market and employment effects,
- the digital services and media services that finance their services through advertising, which is based on tracking cookies for advertising purposes,
- the audience measurement (will the use of independent measurements by third parties to verify reach and advertising effectiveness remain possible?),
- the digital economy, the IoT sector, machine-to-machine communication and new technologies in general – particularly in the automotive sector

and

- the controllers whose storage of personal data or access to personal data stored on a terminal equipment of a natural person falls outside the scope of the ePrivacy Directive and does not affect its regulatory purpose.

PUBLIC

DE Non-paper
concerning Digital Omnibus provisions on Data Act

I. Introduction

DE appreciates and would like to thank the Council Presidency for the work it has done so far on negotiating the Data Act part of the Digital Omnibus. Germany has participated constructively in the discussions from the very beginning. For us, it has been and remains crucial that the Digital Omnibus achieves tangible improvements, particularly for SMEs, midcaps, startups, science and research, public bodies, and the voluntary sector – while maintaining the level of protection provided by the GDPR and the AI Act. Germany also supports the goal of swiftly concluding negotiation on all Omnibus packages. At the same time, it is clear to us that this must not come at the expense of quality or ambition.
Based on the most recent compromise text and the deletions and amendments of provisions, we fear that the Digital Omnibus will not achieve the intended effect of simplification and reducing bureaucratic burdens. Therefore we ask the Presidency, the Commission and colleagues from Member States to consider the following amendments which DE considers crucial for the Digital Omnibus' success.

II. Trade secret handbrake

To strengthen the protection of trade secrets that are of strategic importance to EU companies, we call for an adjustment to the "trade secret handbrake".

Art. 4 Para. 8 und Art. 5 Para 11:

~~In exceptional circumstances, w~~**W**here the data holder who is a trade secret holder is able to demonstrate that, despite the technical and organisational measures taken by the user pursuant to paragraph 6 of this Article, it is ~~highly~~ likely to suffer ~~serious economic damage~~ **disproportionate harm** from the disclosure of trade secrets or that the disclosure of trade secrets to the user poses a high risk of unlawful acquisition, use, or disclosure to third country entities, or entities established in the Union under the direct or indirect control of such entities, which are subject to jurisdictions offering weaker or non-equivalent protection compared to that under Union law, that data holder may refuse ~~on a case-by-case basis~~ a request for access to the specific data in question. That demonstration ~~shall~~ **may** be duly substantiated on the basis of objective elements, such as the enforceability of trade secrets protection in third countries, the nature and level of confidentiality of the data requested, and the uniqueness and novelty of the connected product.

This proposed amendment sets appropriate limitations regarding the substantive requirements and the burden of proof on data holders. It also improves the practical usability of the data, and at the same time upholds the central objective of the Data Act: to make data more accessible for innovation, research and new business models, particularly for startups and SMEs.

III. Reduction and simplification of information and notification obligations under the Data Act

DE continuously advocates for less bureaucratic information and notification obligations in the Digital Omnibus. DE repeatedly submitted draft proposals for reduced information and notification obligations to further reduce bureaucratic burdens for affected companies while maintaining the Data Act‘s regulatory goals and main obligations.

Remove information obligations under Art. 3 para 2 and 3; Art. 28:

Art. 3

2. Before concluding a contract for the purchase, rent or lease of a connected product, the **relevant** seller, rentor or lessor, which may be the manufacturer, shall provide at least the following information to the user, in a clear and comprehensible manner:

~~(c) whether the connected product is capable of storing data on-device or on a remote server, including, where applicable, the intended duration of retention;~~

(d) how the user may access, retrieve or, where relevant, erase the data~~, including the technical means to do so, as well as their terms of use and quality of service~~.

3. Before concluding a contract for the provision of a related service, the provider of such related service shall provide at least the following information to the user, in a clear and comprehensible manner:

~~(c) whether the prospective data holder expects to use readily available data itself and the purposes for which those data are to be used, and whether it intends to allow one or more third parties to use the data for purposes agreed upon with the user;~~

~~(e) the means of communication which make it possible to contact the prospective data holder quickly and communicate with that data holder efficiently;~~

~~(g) the user's right to lodge a complaint alleging an infringement of any of the provisions of this Chapter with the competent authority designated pursuant to Article 37;~~

~~Article 28~~

~~1. Providers of data processing services shall make the following information available on their websites, and keep that information up to date:~~

~~(a) the jurisdiction to which the ICT infrastructure deployed for data processing of their individual services is subject;~~

~~(b) a general description of the technical, organisational and contractual measures adopted by the provider of data processing services in order to prevent international governmental access to or transfer of non-personal data held in the Union where such access or transfer would create a conflict with Union law or the national law of the relevant Member State.~~

~~2. The websites referred to in paragraph 1 shall be listed in contracts for all data processing services offered by providers of data processing services.~~

PUBLIC

Remove notification obligations for data holders under Art. 4 para. 2 sentence 3, para. 7 sentence 3 and para. 8 sentence 3, under Art. 5 para. 10 sentence 3 and para. 11 sentence 3 and Art. 32 para 5.

Art. 4

2. [...] ~~Where the data holder refuses to share data pursuant to this Article, it shall notify the competent authority designated pursuant to Article 37.~~

7. [...] ~~In such cases, the data holder shall notify the competent authority designated pursuant to Article 37 that it has withheld or suspended data sharing and identify which measures have not been agreed or implemented and, where relevant, which trade secrets have had their confidentiality undermined.~~

8. […] ~~Where the data holder refuses to share data pursuant to this paragraph, it shall notify the competent authority designated pursuant to Article 37~~.

Art. 5

10. [...] ~~In such cases, the data holder shall notify the competent authority designated pursuant to Article 37 that it has withheld or suspended data sharing and identify which measures have not been agreed or implemented and, where relevant, which trade secrets have had their confidentiality undermined.~~

11. […] ~~Where the data holder refuses to share data pursuant to this paragraph, it shall notify the competent authority designated pursuant to Article 37.~~

Article 32

~~5. The provider of data processing services, the public sector body making available data or documents in accordance with Chapter VIIc Section 3, the natural or legal person to which the right to re-use data or documents in accordance with Chapter VIIc Section 3 was granted, the data intermediation services provider or the recognised data altruism organisation shall inform the natural or legal person whose rights and interests might be affected about the existence of a request of a third-country authority to access its data before complying with that request, except where the request serves law enforcement purposes and for as long as this is necessary to preserve the effectiveness of the law enforcement activity.~~

PUBLIC

Simplify information obligations of providers of data processing services under Art. 29 para. 5 and 6 to the extent that providers should be generally required to inform about circumstances that hinder switching:

Art. 29
5. Where relevant, providers of data processing services shall provide information to a customer on **circumstances that hinder the switching of** data processing services ~~that involve highly complex or costly switching or for which it is impossible to switch without significant interference in the data, digital assets or service architecture.~~
~~6. Where applicable, providers of data processing services shall make the information referred to in paragraphs 4 and 5 publicly available to customers via a dedicated section of their website or in any other easily accessible way.~~

PUBLIC

IV. Use of non-personal data for AI training

DE proposes to exempt the use of non-personal data for the development and training of AI models within the company of the data holder from the contractual requirements solely for the purposes of Art. 4 para. 13 sentence 1, and without prejudice to Art. 4 para. 14.

Art. 4
13. A data holder shall only use any readily available data that is non-personal data on the basis of a contract with the user**, unless such data are used solely and to the extent necessary by the data holder or by undertakings within the same group for the development, training, testing and validation of AI systems or AI models**. […]

V. Provisions concerning Member States' designation of supervisory authorities

In its current Digital Omnibus draft the Presidency proposes to strike Article 37 Paragraph 3 and Article 40 Paragraph 4 and 5 on the competence of supervising authorities for data protection and on data protection sanctions. DE proposes not to strike these provisions and to keep them as applicable law. It should be the exclusive right of member states to designate competent authorities and their sanctioning powers. The Data Act provisions, that the Presidency proposes to strike, have been the legal basis for only recently adopted national implementation laws for the application and the enforcement of the Data Act. To strike these provisions at this point will create legal uncertainties for the designation of competent authorities and will make it necessary for member states to unnecessarily revise their national implementation laws.

Art. 37

3. The supervisory authorities responsible for monitoring the application of Regulation (EU) 2016/679 shall be responsible for monitoring the application of this Regulation insofar as the protection of personal data is concerned. Chapters VI and VII of Regulation (EU) 2016/679 shall apply *mutatis mutandis*.

The European Data Protection Supervisor shall be responsible for monitoring the application of this Regulation insofar as it concerns the Commission, the European Central Bank or Union bodies. Where relevant, Article 62 of Regulation (EU) 2018/1725 shall apply *mutatis mutandis*.

The tasks and powers of the supervisory authorities referred to in this paragraph shall be exercised with regard to the processing of personal data.

Art. 40

4. For infringements of the obligations laid down in Chapter II, III and V of this Regulation, the supervisory authorities responsible for monitoring the application of Regulation (EU) 2016/679 may within their scope of competence impose administrative fines in accordance with Article 83 of Regulation (EU) 2016/679 and up to the amount referred to in Article 83(5) of that Regulation.

5. For infringements of the obligations laid down in Chapter V of this Regulation, the European Data Protection Supervisor may impose within its scope of competence administrative fines in accordance with Article 66 of Regulation (EU) 2018/1725 up to the amount referred to in Article 66(3) of that Regulation.

VI. Guidelines for clarification

From the beginning of the legislative process, stakeholders have called for more guidance concerning the Data Act. Legal uncertainty especially impacts SMEs, particularly those without specialized legal departments, preventing them from making use of the Data Act. Due to its horizontal scope and its limited number of regulations, the Data Act is especially abstract. This means that waiting for CJEU rulings to provide legal certainty would be far too time-consuming.

To create greater legal certainty and thus trust at EU level and to promote the uniform interpretation of the Data Act within the EU, DE calls for appropriate guidance to be issued by the Commission and the EDIB.

Art. 24 guidelines on cloud switching and data processing services

[…] **Within six months after [Digital Omnibus Regulation] has entered into force the Commission shall adopt guidelines on the scope of the technical obligations concerning switching between data processing services, taking into account the advice of the European Data Innovation Board (EDIB) referred to in Article 42, inter alia on the definition and classification of data processing services. The guidelines shall be updated at least annually.**

Art. 32 para. 3 subpara. 2 guidelines addressing international data flows

[…] **Within six months after [Digital Omnibus Regulation] has entered into force the Commission shall adopt guidelines [for international data flows] on the assessment of whether the conditions laid down in the first subparagraph of this paragraph are met. The guidelines shall be updated at least annually.**

Art. 33 para. 11 guidelines for the interplay of Data Act and data spaces

[…] **Within six months after [Digital Omnibus Regulation] has entered into force the Commission shall adopt guidelines laying down frameworks for common standards and practices for the functioning of common EU data spaces, taking into account existing standards. The guidelines shall be updated at least annually.**

VII. Open Data & Data Governance Act

1. Procedure for requests for re-use

The new insertion of Article 32la results in the abolition of the original option, for the authority to set its own time limits, which is crucial to prevent public bodies from refusing to disclose data on the grounds that the time limits are too short. We therefore advocate retaining the original system of deadlines and continuing to allow the granting authorities to set their own deadlines.

Art. 32la

2. ~~**Unless shorter time limits have been established in accordance with national law,**~~ **In cases where public sector bodies –** and, in the case of protected data, public sector bodies or the competent bodies referred to in paragraph 1 of Article 32z **didn't set their own reasonable time limit for the timely provision of data or documents, those public sector bodies or the competent bodies** shall process the request and shall deliver the data or documents for re-use to the applicant or, if a licence is needed, finalise the licence offer to the applicant as soon as possible and in principle within 20 working days of receipt. […]

2. EU Data Portal

DE proposes to add a provision in Section 1 ("General Provisions") of Chapter VIIc requiring the Commission to make practical arrangements at EU Level facilitating the search for data or documents

available for re-use, thus combining respective provisions of the current Open Data and Data Governance Act. An EU-wide access point like the EU Data Portal is of fundamental importance for easy cross border access, exchange and usage of open data throughout the Union. It would furthermore secure the succession of the INSPIRE geo-portal for spatial data which will be merged with the EU data portal in the context of the revision of the Directive 2007/2/EC as the requirement to establish and operate an INSPIRE geo-portal at EU level in Article 15 Paragraph 1 is proposed to be deleted.

Art. 32lb Open Data Portal

1. Member States shall ensure an easy access to data, in cooperation with the Commission.

2. To ensure an easy access to data, the Commission is required to set up a European single access point. This single access point shall enable users to locate suitable data falling within special categories as referred to in Art. 2 paragraph 53, held by public sector bodies and EU institutions, and, where data does not fall within the scope ofArt. 2 paragraph 53, to make such data available.

This single access point shall

a) **make data not covered by Article 2 paragraph 53 available via electronic means in accessible, readily findable and re-usable formats**
b) **offer a searchable electronic register of data available in the national single information points as referred to in Article 32aa,**
c) **offer further information on how to request data via those national single information points as referred to in Art. 32aa.**

VIII. Open Data / High Value Datasets

In light of the proposed revision of Directive 2007/2/EC (INSPIRE) as part of the Environmental Omnibus it should be clarified that complementarity with the INSPIRE Directive is to be ensured when identifying specific high-value datasets. The proposed revision of the INSPIRE Directive will lead to the applicability of key provisions of the ODD/HVD part of the Data Regulation, which makes coherence even more important than before. It should also be noted that Recital 68 corresponding to Article 14 Paragraph 2 ODD (i.e. Art. 32v) explicitly mentions Directive 2007/2/EC in addition to Directive 2010/40/EU. Directive 2007/2/EC seems therefore in retrospect to have been accidentally omitted in Article 14 Paragraph 2 ODD.

Art. 32v para. 2 subpara. 2

For the purpose of identifying such specific high-value datasets, the Commission shall carry out appropriate consultations, including at expert level, conduct an impact assessment and ensure complementarity with existing legal acts, such as **Directive 2007/2/EC and** Directive 2010/40/EU of the European Parliament and of the Council, with respect to the re-use of data or documents. That impact assessment shall include a cost-benefit analysis and an analysis of whether providing high-value datasets free of charge by public sector bodies that are required to generate revenue to cover a substantial part of their costs relating to the performance of their public tasks would lead to a substantial impact on the budget of such bodies. With regard to high-value datasets held by public undertakings, the impact assessment shall give special consideration to the role of public undertakings in a competitive economic environment.

PUBLIC

IX. Data Governance Act / Sanctions

The Presidency proposes to exclude Chapter VIIa (Data Governance Act) from the Data Act sanctions regime (Article 40). DE would like to maintain the possibility to sanction data intermediation services in cases of misuse. With the current version of Article 40, taking the label away and deleting the service from the EU register is the only punishment in case of data misuse. This is – in our view – not enough to generate more public trust in the service providers.

Art. 40

(6) This Article shall not apply to Chapter ~~VIIa,~~ **VIIb and** VIIc.

3. Open Data / Standard licences

The proposed changes for the setting of conditions for the re-use of data and documents applies to Articles 32q, 32r, 32k, and the associated Recital 25. We have concerns that the changes depart from the current practice of standard licences and will make it more difficult to reuse public sector data in open-source projects. Furthermore, the combination of data from other sources can be hindered by different licensing models. Greater consideration for particularly large enterprises can already be achieved through a differentiated fee structure. In this way, the standard licences can be retained. Retaining standard licences helps to prevent fragmentation, reduces legal uncertainty, and ensured interoperability within the EU open data ecosystem.
We therefore advocate for the deletion of Art. 32r Para. 4 and an adjustment of Art. 32r Para. 3 as follows:

Art. 32r

3. In Member States where licences are used, **Member States shall encourage the use of standard licenses for the re-use of public sector data or documents**. Public sector bodies ~~and public undertakings~~ shall ensure that **such** ~~the~~ standard licences ~~for the re-use of public sector data or documents~~, which can be adapted to meet particular licence applications, are available in digital format and able to be processed electronically.

~~4. Public sector bodies may establish special conditions for the re-use of data and documents by very large enterprises. Such conditions shall be proportionate and should be based on objective criteria. They shall be established taking into consideration the economic power, or the ability of the entity to acquire data, including in particular a designation as a gatekeeper under Regulation (EU) 2022/1925.~~

Art. 32q Para. 6 should be amended as follows:

6. ~~Public sector bodies may set out~~ **Without prejudice to Article 32r,** charges higher **than the charges provided for in paragraphs 1, 4 and 5** may be set out for the re-use of data and documents by very large enterprises ~~than the charges provided for in paragraphs 1, 4 and 5~~. […]

***

PUBLIC

ESTONIA

EESTI

Comments of Estonia on Presidency revised compromise text.

PUBLIC

Recital 39 and Article 8

Estonia supports reducing unnecessary data breach notifications but notes that controllers might underestimate their impact on data subjects. Multiple low-risk breaches, when combined, could pose higher risks to individuals' rights and DPAs should be made aware of those. We recommend using terms like "impactful risks" or "increased risks."

Recital 39, 40 and Article 3(8) and 3(9)

Estonia does not support the amendment as regards the division of competences in between EDPB and the Commission. In a situation where the Board's guidelines can be updated quickly in response to newly emerging possibilities, there is a risk that the guidelines may recommend an updated approach, while the Commission's implementing regulation in force contains outdated information. Amending both the EDPB guidelines and the implementing regulation will be a lengthy process and can result in different outcomes. This could result in a situation where controllers are unable to use up-to-date measures without committing a breach, thereby jeopardising the protection of individuals' personal data. We do understand that the EDPB's guidelines may be challenged in ECJ, but providing that its guidelines must be validated by an implementing regulation will jeopardise the EDPB's autonomy. For this reason, we suggest removing the clauses that permit the Commission to adopt implementing acts.

Recital 39a

By extending the principles of data protection by design and by default directly to processors as well, it blurs the controller's responsibility under Article 5(2) GDPR. In addition, if Article 28 still provides that the controller determines what the processor must do and how, and the processor acts accordingly, then the purpose of this amendment is not clear. Recital 39a states with regard to processors: "to the extent of its own obligations" — we kindly ask to specify what exactly does this mean in light of the fact that the processor's obligations stem from the contract, while the controller determines the purposes and means of processing?

Article 3(9a)

Estonia does not support the amendment, as it would significantly increase the workload of the supervisory authority, which would then have to verify all public authorities and businesses subject to the obligation to appoint a data protection officer, rather than contacting only those that have failed to appoint one. Also, this can weaken the position of DPOs.

15.06 AGS

Cyber

- **We welcome the update text that gives further flexibility. We are still analysing said text and its implications, but it could be one way forward regarding national entry points.**
- **We also welcome the amendment regarding open-source solution that is developed by ENISA, in cooperation with Member States.**

- **We also welcome that the text mentions other relevant bodies and groups established at Union level under relevant Union legal acts.**

Remarks:
ART 23a
Article 23a(2)(c) – Guidance should also **explain** what to do if the national entry point is not (yet) functioning; this **should be added to recital 49a for example**.
Article 23a(5) –

- The introductory sentence differs from paragraph 3; clarification is needed.
- **Points (a)–(c)** concern risk management and registration, which **are not clearly linked to the incident reporting information poin**t (IRIP). **If** incident reporting information pointis **intended to cover broader tasks in the future**, **this is a new concept and its name (and recital 49a) should be adjusted accordingly.**

ART 23b
Article 23b(2)(b) –national entry point (NEP) may also carry out the task of "providing guidance or assistance to entities regarding notification procedures". **Does this task correlate to the task related to incident reporting information point** that is managed by ENISA according to Article 23a (2) (c)? **If both (the IRIP and NEP) have such tasks, then duplication should be avoided.**

ART 23c
We find that there is the need to harmonize the notification timelines across all relevant Union legal acts. Otherwise, there **might be** a situation where **the entity is expected to use the NEP several times for notifying one incident**.

Art 23c **Paragraph (3) should also have the same amendment that was made to Article 23a (3) and Article 23b (4**) **- mentioning** also cooperation with "**other relevant bodies or groups established at Union level under relevant Union legal acts**".
- Paragraph (3) point (b) mentions an analysis – does this also entail an incident classification taxonomy?

Article 8
- We still find that there is a need to add a new paragraph to Article 30 regarding those entities that are subject to NIS2 *(as they are MSP or MSSP)* **and DORA. There is no provision that foresees that if the same entity has fulfilled NIS2 Article 21 requirements, then said entity is in compliance with requirements deriving from Article 30 of DORA.**
We provided the wording and reasoning in writing –input on 02.06.2026.

Longer:
Article 23a
- Article 23a (2) (c) - should these guides also entail information on what to do if national entry point is not (yet) functioning? This aspect should be added to a relevant recital – like recital 49a.
- Article 23a (3) – we welcome the amendment at the end of first sentence ("and other bodies or groups established at Union level under relevant Union legal acts").
- Article 23a (5):

- We note that the introductory sentence does not entail the same kind of reference as it is the same Article's paragraph 3. Is this intentional?
- The proposed points a to c are about cybersecurity risk management measures and about entity registration. In what way could the incident reporting information point (IRIP) be connected to said topics? If in the future, it is expected that IRIP is meant for more matters other than incident reporting details/matters, then this is a new concept that requires that the

IRIP's name needs to be changed – since IRIP's name does not entail such new topics. This should also be reflected in recital 49a that might need an amendment.

Article 23b

- Paragraph (2) point (b) mentions that national entry point (NEP) may also carry out the task of "providing guidance or assistance to entities regarding notification procedures".

We are not against such task, but how much does this correlates to the task related to incident reporting information point (IRIP) that is managed by ENISA – see proposed Article 23a (2) (c)? If both (the IRIP and NEP) have such tasks, then clarification is needed.

- Paragraph (4) - we welcome the amendment at the first sentence ("and other relevant bodies or groups established at Union level under relevant Union legal acts").
- Paragraph (5) - we welcome this new paragraph as it provides an opportunity for Member States to use said open-source solution that shall be developed by ENISA, in cooperation with Member States.

Article 23c

- Paragraph (1) tasks the Commission to submit a report about common elements and differences in definitions, thresholds, deadlines, formats and procedures applying to notifications that are done due to relevant obligations in NIS2, eIDAS, GDPR, DORA and CER + said report "shall in particular consider concrete steps and a timeline for introducing the unified approach to incident reporting under the Union legal acts".

We find that there is the need to harmonize said work, especially the notification timelines across all relevant Union legal acts. Otherwise, there might be a situation where the entity is expected to use the NEP several times for notifying one incident. Although we would like it so that this harmonization is concluded with this omnibus, but this paragraph is better than no harmonization.

- Paragraph (3) (see the introduction's first sentence) should also have the same amendment that was made to Article 23a (3) and Article 23b (4). Meaning: the mentioned guideline should be also drafted in cooperation with "other relevant bodies or groups established at Union level under relevant Union legal acts". This is especially relevant due to said paragraph point (c) that is related to stages of incident notifications under different Union legal acts.
- Paragraph (3) point (b) mentions an analysis – does this also entail an incident classification taxonomy?

Article 23d

- We welcome the amendment at the first sentence ("as well as with other relevant bodies or groups established at Union level under relevant Union legal acts").

Article 8

- We still find that there is a need to add a new paragraph to Article 30 regarding those entities that are subject to NIS2 *(as they are MSP or MSSP)* and DORA (they are the ICT third-party service provider). This is due to the fact that there are instances where one entity has obligations regarding cybersecurity risk management that are set in NIS2 and DORA. Then again – there is no provision that foresees that if the same entity has fulfilled NIS2 Article 21 requirements, then said entity is in compliance with requirements deriving from Article 30 of DORA. Therefore, there should be a provision that foresees said outcome.

We already provided said wording and reasoning in writing – said our input on 02.06.2026.

Written comments on the Data Act

Thank you for the opportunity to submit written comments. Our main concern remains the handling of data and documents in the text. While some of our comments have been reflected and we appreciate it, further clarification is still needed to ensure that the provisions are applicable in

practice. The definition of a document, excluding digital forms, is confusing for the following reasons:

1. it contradicts the commonly accepted definition of a document in archiving, information management, the Tromsø Convention, etc.;
2. it creates significant confusion. Although data is defined as 'digital' and a document as 'non-digital', Article 2(53) provides that 'data' means 'data and documents', and Chapter VIIc still requires digital handling of documents, including access through a virtual secure environment. This shows that separating data and documents is not useful. Please see our further suggestion in our written comment of 15th May. The Digital Omnibus should instead focus on making public sector information of evidentiary or informational value, i.e. records, findable and accessible regardless of format or medium.

We support amending the EU Data Act to allow public authorities to request data from the private sector in situations of public emergency. However, such powers must respect fundamental rights, rely on clear and harmonised criteria, and remain limited to exceptional cases. The wording should therefore retain the term "exceptional need" to avoid unnecessary burdens for businesses.

Regarding the data intermediation service (Article 2b), the reference to services whose main purpose is not the intermediation of copyright-protected content is difficult to apply. It is unclear how the "main purpose" should be determined and whether secondary or incidental copyright intermediation is covered. We therefore suggest avoiding this ambiguous threshold and using terminology aligned with EU copyright law.

Regarding Article 32n, the following two points are particularly important to us:

1. Estonia considers that Article 32n should clearly define when personal data may be made available as open data. Such disclosure should be allowed only with valid consent or where expressly provided for under Union or national law, in full compliance with data protection rules.

Thus, we suggest adding an additional paragraph 3 as follows:
(3) Personal data may only be disclosed as open data where the data subject has given valid consent or where such disclosure is expressly provided for under Union or national law, in full compliance with the applicable data protection framework.

2. Datasets whose disclosure would jeopardise the internal or external security of the Union or Member States should not be made publicly available, especially in the current geopolitical situation. This may include, for example, energy-related data. We therefore suggest adding the following principle:

(4) Datasets whose disclosure would jeopardise the internal or external security of the Union or Member States must not be made publicly available.

Finally, regarding trade secrets (Articles 4(8) and 5(11)), we welcome the guidance. However, the current wording may create additional burdens, uncertainty and practical difficulties:

- The ground for refusing disclosure and the burden of proof are difficult to substantiate in practice, in particular how a trade secret holder should demonstrate serious economic damage.
- The limitations on use and oversight mechanisms should be set out more precisely.

We also wish to express our appreciation for the constructive and professional cooperation and hope that this good cooperation will continue.
***

GREECE

ELLÁDA

EL comments on Data

1. Article 4 para. 8

We welcome the new mandate for the Commission to issue guidelines, in consultation with the European Data Innovation Board (EDIB), on the application of this paragraph, including the assessment of serious economic damage and the enforceability of trade-secret protection in third countries.

We are concerned, however, that the current drafting weakens the safeguards confining refusal to genuinely exceptional cases. It allows refusal without any showing of exceptionality, on the basis of a mere likelihood for serious economic damage. Moreover, it opens the door to blanket refusals and converts a binding obligation to justify the refusal into a discretionary one. These changes shift the balance away from data availability for artificial intelligence, research and innovation, to the disproportionate detriment of SMEs that depend on the access this Regulation provides.

We would therefore welcome retaining the safeguards that have been removed, so that refusal remains a justified and well-substantiated exception. We also note a possible inconsistency between the recitals (Recital 14) and the enacting terms as regards the standard of substantiation, which it would be useful to align. Finally, we propose that Member States' role in reviewing refusal notifications for proportionality be confirmed, and that aggregate statistics on refusals be included in the relevant annual reporting under this Regulation, to ensure transparent monitoring.

2. Article 5 para. 11

We welcome the new mandate for Commission guidelines developed with the EDIB. We are concerned, however, by the weakened safeguards, in identical terms with Article 4 para. 8. These changes reduce third parties' ability to obtain data at the user's request and disadvantage smaller actors in particular. **We propose the restoration of the safeguards**.

3. Article 11 para. 1

We welcome the new Article 11(1), which allows a data holder to apply appropriate technical protection measures, including encryption, to prevent unauthorised access to data and ensure compliance, while providing that such measures must not discriminate between data recipients or hinder a user's right to obtain, retrieve, use or access data or to provide data to third parties, and that users, third parties and data recipients must not alter or remove those measures unless agreed by the data holder. We note, however, that the provision addresses the use and limits of such measures but not the consequences of their unauthorised alteration or removal. It would be useful to clarify how such circumvention is to be addressed, so that the rule is effective in practice.

On behalf of the EL side (Special Secretariat for Artificial Intelligence and Data Governance - Hellenic Ministry of Digital Governance), following the Meeting this morning and the written comments sent on the Data Act, we confirm that we propose the restoration of the safeguards both in Article 4 para. 8 and Article 5 para. 11.

***

PUBLIC

SPAIN

ESPAÑA

WRITTEN COMMENTS FROM SPAIN ON THE DIGITAL OMNIBUS PACKAGE – AGS MEETING.

Exchange of views on the provisions relating to the Data Act

In general terms, we have no objections that would prevent us from accepting the text. However, there are aspects regarding which we wish to put on record some concerns that remain:

With regard to the **Data Act**, we wish to highlight two issues relating to Chapter V.

The first is the absence of the term 'mitigation'. Its removal unnecessarily restricts the scope of action to the response and recovery phases, and limits the possibility of accessing data held by private entities when early intervention could reduce damage. **This issue is particularly relevant because the text has already scaled back its ambition by removing references to situations of 'exceptional necessity' and restricting the scope to public emergencies**. In this context, **retaining an explicit reference to mitigation is essential to preserve a preventive and anticipatory dimension** within the mechanism.

The second concerns the opinion provided for in Article 32(3). **We consider that this should be issued by the European Commission, which would simplify the procedure and ensure more harmonised application** across the Union, particularly given the complexity involved in assessing the legal regimes of third countries.

Provisions relating to the P2B Regulation (ST 10426/26)

P2B (Platform to Business)

ES can support the Presidency's compromise text, as it strikes a balance and initiates and advances the simplification of the rules applicable to platforms, whilst maintaining safeguards for the protection of professional users. We welcome the retention of Article 18(1)

Provisions relating to cyber and national points of entry (ST 10426/26)

Spain **welcomes the significant improvements introduced** in the revised compromise text ST 10426/26, **in particular the redefinition of ENISA's role as an information point for incident reporting**, without the capacity to receive or process notifications, **and the flexibility granted to Member States in recital 50a to configure their national entry point as a technical interoperability centre**. These elements reflect Spain's consistent position throughout the negotiations.

However, **Spain maintains a fundamental objection to Article 23b(1) as currently drafted**. The list of tasks assigned to the national entry point includes the receipt and processing of notifications as a recognised function. Furthermore, **the Presidency note (WK 8070/2026) describes the tasks listed in paragraph 1 as 'core tasks'.** When the Presidency consulted delegations last week on whether this list could be introduced with optional wording, Spain indicated that this would not be acceptable. **The current wording does not address this concern. It exacerbates it** by incorporating the receipt and processing of notifications into the operative text and provides sufficient textual basis for the European Parliament to consider it a minimum operational requirement during the trilogue.

Spain's position has been, and remains, that the receipt of notifications should NOT be listed as a recognised task of the national entry point, regardless of the permissive wording surrounding it.

PUBLIC

Provisions relating to the GDPR

BIOMETRICS

We thank the Presidency for its efforts on this new compromise proposal.

We are still analysing the proposal, and these are therefore preliminary comments. In principle, we agree with the current approach, but my experts insist on certain changes or improvements to the wording, which are attached:

The reasoning is that, in the current context where low-risk biometric technologies exist for verification (one-to-one), it is not appropriate to delegate safeguards to national regulations, as this only leads to fragmentation. In such cases, the EDPB's guidelines, which can be adapted to the evolution of these new low-risk technologies, are more effective and harmonised.

Therefore, on this point, they request that the new Article 29(a) include an obligation for the EDPB to draw up guidelines setting out safeguards for low-risk biometrics in verification (one-to-one).

Consequently, we propose adding text to Recital 34, removing the reference to possible national legislation in Article 9(2)(l) regarding safeguards, and referring these to EDPB guidelines
Amend 9.4 so that the reference to national legislation on biometrics applies only to identification (1-to-N), which remains high-risk, but NOT to verification (1-to-1) using new low-risk technologies

NOTIFICATION OF DPOs TO SUPERVISORY AUTHORITIES

Nor do we agree with removing the obligation for the DPO to notify the authorities, as this does not reduce the bureaucratic burden on organisations that have a DPO and where the DPO themselves wishes to be known and recognised by the supervisory authorities so that they may be included in training activities and campaigns carried out by the authorities for DPOs. If the authorities do not know who they are, it is difficult for us to include them in our training initiatives.

E-privacy and cookies

In general terms, we reserve judgement on this part of the proposal regarding the ePrivacy Directive and cookies. At this preliminary stage, we have no specific objections. However, there are aspects on which we wish to record some concerns that remain:

Firstly, regarding **Articles 8a and 88b of the GDPR** and the decision adopted by COREPER, we understand and support the reasons behind that decision; however, my comments are in line with those made by BE, but this should not be the end of the matter. We too wish to emphasise, as other delegations have already mentioned, that these amendments respond to a real need: to give citizens back effective control over their personal data and to reduce cookie fatigue. **We consider it a priority for the Commission to take the initiative again, with an appropriate impact assessment, within the most suitable legislative framework and avoiding excessive delays**.

Secondly, regarding **Article 5(2) of the ePrivacy Directive**, **the expansion of the list of exemptions from consent is very significant and is not accompanied by an** impact **assessment** demonstrating its low risk, as was provided for in the original proposal. **We request two specific adjustments**.

1. Regarding the exemption for **fraud prevention**: the concept of fraud in digital environments is not limited to identity theft, but may also encompass click fraud in advertising. Without an explicit definition, **this exemption could cover continuous monitoring of users without their consent**. We ask that a clarifying recital be included to define the scope of this provision with specific examples.

2. Regarding **audience measurement**: the exemption applies to all websites and analytics tools, not just the media. The only condition required is that the final statistics be anonymised , but no restrictions are imposed on the raw data, which would allow users to be tracked and profiled without their consent. **We call for the reintroduction of the requirement for immediate anonymisation that featured in the previous text, and for the conditions currently set out only in a recital** — the prohibition on cross-referencing data, sharing it or using it for other purposes — **to be incorporated into the articles**

PUBLIC

Article 49 GDPR

(ES Drafting suggestions): *Article 49 Derogations for specific situations* *1. (...)* *Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.* ***The requirement that the transfer be non-repetitive shall not apply to transfers based on point (d) of the first subparagraph, where such transfers are necessary for important reasons of public interest recognised in Union law or in the law of a Member State, including transfers carried out pursuant to international or administrative agreements on mutual assistance or cooperation.***	(ES Comments): The purpose of this amendment is to clarify and specify the scope of the derogation for important reasons of public interest laid down in Article 49 of Regulation (EU) 2016/679, in particular as regards international data transfers carried out in the context of periodic exchanges of information between public authorities. The proposed amendment clarifies that transfers necessary for important reasons of public interest under Article 49(1)(d), including those carried out pursuant to international or administrative cooperation agreements, may in practice take place on a recurring basis. It therefore specifies that the requirement of non-repetitiveness, which applies to the residual ground of compelling legitimate interests, should not be understood as limiting such public interest transfers. This clarification does not affect the exceptional nature of Article 49 derogations, which remain subject to strict necessity, proportionality and appropriate safeguards ensuring a high level of protection of personal data.

PUBLIC

Spain. comments on 4th compromise text from CY presideny

Recital 34. In line with the proposal in the new recital 27(a) on anonymization, we suggest the following text and the amendment of Article 9(4) so that it is used exclusively for biometric identificacion. In this way, we promote the innovative use of biometric verification based on current new low-risk technologies, avoiding the current fragmentation in this area within the EU: "The European Data Protection Board should ensure consistency and support controllers and processors by adopting an opinion on the processing of biometric data for verification purposes, assessing and specifying the state of the art of available decentralized architectures, as well as the technical and organisational measures and criteria to apply one-to-one verification effectively. The opinion should clarify the circumstances whether and when the retention of biometric templates or data under the sole control of the data subject effectively prevents the controller or any third party from accessing, storing, or centralizing such data. It is important that the Board carries out a public consultation with relevant stakeholders prior to issuing its opinion. While controllers remain fully responsible to determine and demonstrate that the chosen biometric system ensures strict necessity and maintains data under the user's exclusive control without leading to unauthorized tracking or secondary use, the opinion should support and provide guidance to controllers regarding the effective application of appropriate safeguards to protect the fundamental rights and interests of data subjects."

9.2.l) As explained in recital (34), we suggest this wording for the following reasons:

1. New biometric verification technologies (1 to 1) with low risk to the rights and freedoms of data subjects are now available (e.g..: **Non-reversible biometric templates, ISO/IEC 24745:2022**). We are not in the same situation as in 2016, when the GDPR was enacted, regarding biometric technologies, all of which presented a high risk.

2. For the above reason, the Commission introduced its proposal in the new paragraph 9.2(l), which we support, but with the addition of appropriate safeguards for the use of new, low-risk technologies instead of the old, high-risk ones.

3. By referencing the safeguards to EDPB guidelines (similar to the anonymization proposal), we promote harmonization instead of the current fragmentation, identified in the Commission's 2024 report on GDPR implementation and widely criticized by stakeholders, which is a consequence of different national regulations. In the current context of the existence of low-risk biometric technologies for verification (1 to 1), it is not appropriate to delegate safeguards to national regulations. In these cases, the EDPB guidelines, which can be adapted to the evolution of these new low-risk technologies, are more efficient.

4. This proposal supports innovation by promoting the use of new low-risk technologies for biometric identification (1 to 1).

5. The use of biometric technologies for identification purposes (1 to N) continues to present high risks. Therefore, this purpose is not included in the Commission's proposal for paragraph 9.2(l). We agree with this position and propose amending Article 9.4 to allow Member States to establish conditions and limitations for biometric technologies for identification purposes (1 to N), but not for verification purposes (1 to 1).

9.4 According to the proposed recital (34), new low-risk technologies for biometric verification (1 to 1) can be harmonised, avoiding fragmentation within the EU and promoting innovation with

appropriate guidelines provided by the European Data Protection Board. In this context, only the use of biometrics for identification purposes (1 to N), which remains a high-risk processing activity, may be subject to further national regulations.

12.5We suggest including this paragraph *The exercise of the rights recognized in Articles 15 to 22 shall not be conditional upon the obligation of the interested party to justify his request. However, the total absence of indication on the purpose of the access may be taken into account together with the other concurrent circumstances to assess the manifestly unfounded or excessive nature of the request.*

13.5 5?, I think it should be 4

33.1 We prefer 72 hours. In others regulations, this period is even shorter. If we want to harmonize this period, has no sense to increase it here.

33.8 We suggest to include this point8. The data breach management should be ready and documented in advance, integrated in the incident management system of the controller, and, when applicable, the DPO should be involved in the process of a data breach[A7]

37.7 We prefer the current wording of the GDPR. Not notifying the supervisory authority of the DPO's identity does not reduce the bureaucratic burden on an organization that has a DPO. Our experience as a supervisory authority is that DPOs want to be known by supervisory authorities and be included in training and awareness campaigns. If the authorities do not know who the DPOs are, we cannot carry out these actions to benefit the DPOs. We propose to add: *and communicate them to the supervisory authority*

70.1 hcc In accordance with our suggestion on recital (34) and 9.2(l), we suggest this new point. hcc) *Issue guidelines recommendations and best practices in accordance with point 9.2(l) that establish safeguards on the use of biometric technologies for verification (1 to 1)[A9]*

***

PUBLIC

FRANCE

FRANCE

PUBLIC

Commentaires des autorités françaises sur l'Omnibus

1) Data Act

France thanks the Presidency for its text, and would like to make the following drafting suggestions to the Data Act:

Article 32.1: FR considers that the text needs to include this precision

« *Providers of data processing services, the public sector body making available data or documents in accordance with Chapter VIIc Section 3, the natural or legal person to which the right to re-use data or documents in accordance with Chapter VIIc Section 3 was granted, a data intermediation services provider or a recognised data altruism organisation shall take all adequate technical, organisational and legal measures, including contracts, in order to prevent international and third-country governmental access and transfer of non-personal data held in the Union where such transfer or access would create a conflict with Union law or with the national law of the relevant Member State State,* ***including mandatory criminal law provisions of Member States, in particular those protecting their essential security interests within the meaning of Article 4(2) of the Treaty on European Union****, without prejudice to paragraph 2 or 3* ».

Article 37: as mentioned as well by Germany in its non-paper, FR asks for maintaining current 37(3) of the Data Act, that is an important point on governance currently in the transposition process and a crucial balance for authorities, particularly awaited for the ecosystem.

Article 32la: it seems to create an obligation for national authorities to communicate the data which might go against national regulations. **FR propose to add the following precision**:
(1) Public sector bodies shall, through electronic means where possible and appropriate, process requests for re-use and shall make the data or document available for re-use to the applicant or, if a licence is needed, finalise the licence offer to the applicant within a reasonable time that is consistent with the time frames laid down for the processing of requests for access to data or documents.
(2) Unless shorter time limits have been established in accordance with national law, public sector bodies and in the case of protected data public sector bodies or the competent bodies referred to in paragraph 1 of Article 32z shall process the request and shall deliver **a response concerning the delivery of** the data or documents for re-use to the applicant or, if a licence is needed, finalise the licence offer to the applicant as soon as possible and in principle within 20 working days of receipt. In case of particularly complex requests, that period shall not exceed two months of receipt and in case of requests relating to protected data, that period shall not exceed three months of receipt.
(3) In the event of a negative decision, the public sector bodies shall communicate the grounds for refusal to the applicant on the basis of the relevant provisions of the access regime in that Member State or the provisions of this Regulation.

2) Cyber issues:

FR calls for the merging of the tasks set forth in paragraphs (1) and (2) of Section 23b, which would bring about the flexibility sought by the Member States and expressed at the COREPER meeting on June 8.

3) GDPR issues:

FR indicates that the reference to the interests of artists and professionals in the creative industries in Recital 33a has no place in a regulation dealing with the protection of personal data, and asks for the deletion to its reference
Regarding questions from the Presidency on the bracket propositions in article 12(5), with regard to the exercise of right, **FR is not in favour of the propose addition and asks for the deletion of both addition proposed in the steering note**.

FR has otherwise no opposition to the rest of the Presidency text on GDPR.

***

PUBLIC

ITALY

ITALIA

Italy's proposed drafting for art. 23 b and its rationale.

Modification of article 23b

National entry point for incident reporting
(1)*Member States shall establish and maintain a national entry point for the reporting of incidents and related events under the Union legal acts where those Union legal acts provide so. The national entry point may carry out different tasks depending on national organisational arrangements, such as, but not limited to:*

(a) enabling the submission of a single notification at national level;
(b) receiving and process notifications submitted by entities;
(c) ensuring or facilitate access to such notifications for the relevant competent authorities;
(d) transmitting or make available relevant information to other national authorities, where necessary;
(e) supporting coordination among competent authorities in relation to reported incidents or information;
(f) providing guidance or assistance to entities regarding notification procedures;
(g) performing any other function necessary to facilitate the effective management and sharing of notifications at national level.

Member States should retain flexibility to configure such infrastructure or arrangement a national entry point in accordance with their national infrastructures and the allocation of competences

Please also find Italy's rationale

- ***It is essential that the list of tasks set out in Article 23b(1) be expanded to explicitly allow the national entry point for incident reporting to provide guidance and assistance to entities on notification procedures.***
- *We insist on a clear and targeted rephrasing that reinstates the previous wording of paragraph 1 as proposed by Italy as a matter of* ***high priority,***
- *On Article 23b(1), the fundamental principles must be fully safeguarded. The national entry point must not replace or dilute the obligation for entities – including those covered by Directive (EU) 2022/2555 (NIS2) – to notify their competent national authorities.*
- *In any event, the possible establishment of a single national platform for managing compliance obligations and incident notifications, even if conceived as a tool for intergovernmental use only, would raise significant issues in relation to the national legal framework on document management, record-keeping, and administrative accountability. Addressing these issues would require wide-ranging legislative and organizational adjustments in order to ensure consistency with Italian law.*
- *Furthermore, the economic and financial sustainability of such a single national entry point would need to be carefully assessed, as Member States would bear the structural and recurring costs related to its management and further development. In addition, the requirement to ensure interoperability between national entry points across Member States would entail further development costs.*

PUBLIC

Italy's proposal on the E-Privacy part.

Proposals to amend the new compromise text (new text in bold):

- ***Recital 44***

Measuring the audience of an online service in order to create anonymous aggregated information about the usage of an online service, where it is carried out by the provider of that online service, or by a third party **acting together with or on behalf of this provider or by an independent controller** such as a market research company or a Joint Industry Committee, ~~acting together with or on behalf of this provider~~, also referred to as 'audience measurement'- **as defined in Regulation (EU) 2024/1083, arts. 2 (16) and 24 -** means processing such data and information to obtain insight into the performance and use of the online service in an anonymised, aggregated and general manner. ~~This includes the performance of audience by an entitled and independent third party performing audience measurement as defined in Regulation (EU) 2024/1083.~~

- ***Art.5 par.2***

It is proposed that Article 5(3)(c) of Directive 2002/58/EC be supplemented as follows:

c) Measuring the audience of an online service in order to create anonymous aggregated information about the usage of that online service, where it is carried out by the provider of that online service, or by a third party acting together with or on behalf of this provider, **or by an independent controller such as a market research company or a Joint Industry Committee,** including where the third party is an entitled and independent third party performing audience measurement in accordance with Article 24 of Regulation (EU) 2024/1083;

Rationale

Recital 44: We welcome the introduction of an explicit reference to the 'Joint Industry Committee' and the 'market research companies', as well as the removal of the reference to 'instantly' processing, which is not consistent with the operating practices of the audience measurement sector. However, concerns remain regarding the prohibition of data combinations, which may limit cross-media measurements, prevent audience deduplication and the integration of census and panel data, which is essential to ensure accuracy and representativeness while respecting user privacy. It is therefore proposed to introduce an explicit exemption for audience measurement, in line with Article 24 EMFA and the definition in Article 2 (16), in order to safeguard the established methodologies of the sector. It is also appropriate to include a more explicit reference to the responsibility of JICs as data controllers.
Article 5(2). We welcome the new wording amending Article 5(3)(c) of Directive 2002/58/EC (e-Privacy) by introducing an explicit reference to 'entitled and independent third parties' and Article 24 EMFA and by providing for the removal of the wording 'solely for its own use', which limited the action of the Joint Industry Committees (JICs) and market research companies.

It is suggested to introduce the same explicit reference to the activities of the JIC as data controller, harmonising the new wording of the aforementioned Article 5(3)(c) of the e-Privacy Directive with what is suggested for Recital 44.
In parallel, it is also appropriate to harmonise Article 4(8) of the Digital Omnibus, which insists on Article 37(4)(c) of the EUDPR.

***

LUXEMBOURG

LUXEMBOURG

Written amendment proposal by Luxembourg regarding Article 23.b (1).

Luxembourg expresses its concerns regarding the optional nature of option (a) in Article 23.b (1), which nevertheless constitutes the very core of the concept of a national single-entry point. We have doubts that the central objective of the regulation – namely to streamline and simplify the reporting of cybersecurity incidents – can be achieved under such conditions.

15 June 2026

The delegation of Luxembourg wishes to thank you for presenting the new compromise proposal. During last week's Coreper II meeting, Luxembourg expressed its **openness to greater flexibility** in order to facilitate the emergence of a compromise acceptable to all delegations.

However, we wish to express **our concerns** regarding **the optional nature of option (a) in Article 23.b (1),** which nevertheless constitutes the very core of the concept of a national single-entry point. **We have doubts** that the **central objective of the regulation** – namely to streamline and simplify the reporting of cybersecurity incidents – **can be achieved under such conditions.**

In this context, we suggest the following amendment:

« (1) Member States shall establish and maintain a national entry point for the reporting of incidents and related events under the Union legal acts where those Union legal acts provide so. The national entry point shall allow for enabling the submission of notifications at national level and for at least one of the following tasks, depending on national organisational arrangements:
~~**(a) enabling the submission of notifications at national level;**~~
(b) receiving and processing notifications submitted by entities;
(c) ensuring or facilitating access to such notifications for the competent authorities under the relevant Union act;
(d) transmitting or making available relevant information to other national authorities, where foreseen under Union or national law; »

AGS 15 juin 2026 - SSP Cookies and GDPR– Written comments by Luxembourg

On the provisions on pseudonymized data (recital 27a and updated version of article 29a) :
We see the merits of the proposed provisions towards creating more legal certainty for business. The exact wording of these provisions is under examination as to whether they can bring the desired simplification effects.
On **the personal data procession for purposes of AI training**, Luxembourg is satisfied with recital 33a.
On **data breach notifications in article 8**, Luxembourg would like to thank the presidency for having come back to a threshold of 96 hours.
On the part on **cookies**, Luxembourg has 2 comments:

- We would like to thank the PRES for the deletion of the proposed article 8a (88b) on a centralized mechanism for consent. While **we support the objective of significantly reducing cookie fatigue and improving citizens' digital experience**, we recognise both the significant implications of any modification to the "cookies" regime and the complex

nature of assessing its practical and economic impact. Digital Omnibus is not the right place to address this, because it presents inherent constraints for addressing such a technically complex topic. We therefore align with other Member States which consider that it would benefit from a thorough impact assessment. We support **continuing evidence-based discussions on this provision outside the scope of the current Digital Omnibus process.**

- Luxembourg furthermore supports the initial proposal by the European Commission to **keep all cookie-related provisions in GDPR.** Amending the e-privacy directive is counter to the principle of simplification through consolidating legal regimes.

Eventually, we have 3 other GDPR-related comments:

On article 12 paragraph 5 (abusive intention), we prefer the text that is **not in brackets** and particularly support the reference of taking into consideration "*all the relevant circumstances in the case*" .

On article 22 we would still prefer the original proposal by the Commission. This article of the GDPR has long been regarded as offering limited legal clarity and is frequently perceived as difficult to understand in practice. Moreover, the concrete legal result of an explicit reference to a 'right' not to be subject to an automated decision remain uncertain, a point clearly reflected in the ongoing debate surrounding this provision.

Unlike the PRES suggests in its preparatory note**, we still see the potential to further improve the text by amending article 49, as suggested by Spain.** Luxembourg agrees with Spain (and others) that the interaction between Article 49 GDPR and the international and administrative cooperation instruments on which Member States rely in the area of taxation deserves further reflection.

Luxembourg written comments on the PRES compromise text (ST 10426/26)

Compromise text (ST 10426/26)	**Drafting suggestion**	**Comments**
HAVE ADOPTED THIS REGULATION:		
Article 1 **Amendments to Regulation (EU) 2023/2854**		
Regulation (EU) 2023/2854 is amended as follows:		
1. Article 1 is amended as follows:	(c) the making available of data by data holders to public sector bodies, the Commission, the European Central Bank and Union bodies, where there ~~is an exceptional~~ **the** need for those data for the performance of a specific task carried out in the public interest;	Point (c) of this paragraph in the current version of the DA is no longer in line with the current version of Article 15a ('exceptional need'). Luxembourg suggests to adapt the wording of the point to align it with the work done in Article 15a.
[…]		
2. Article 2 is amended as follows:		
[…]		
'(28a) 'bodies governed by public law' means bodies ~~that have all of the following characteristics:~~***as defined in***		We reiterate our comments on the possible legal uncertainty by referring to Directives not using the same notions as well

Article 2(1)(4) of Directive 2014/24/EU		as the use of "national authorities" opposed to "State" of the DA as in other legal instruments in point (28). This would not only have an impact on the scope of the DGA but also of the EHDS Regulation will directly refers to this definition. As long as these preoccupations are not clarified, Luxembourg considers this point as a **red line**. **Previous comment:** The current definition of "public sector bodies" (Art. 2 (28) of the DA) retained by the digital omnibus, would not correspond with the ones of the ODD and DGA. This could potentially impact the regimes of the ODD and the DGA. To be more specific, the definition of the DA refers to national authorities of Member States, whereas the definitions of the ODD and DGA refer to the State. Why did the Commission not include the definition of the DGA or the ODD and what is the impact of this change? Especially, since the wording chosen for the DA seems to be the exception (See for example Directive 2014/24/EU or Directive 2014/25/EU which also refer to the State). We would prefer aligning the DA with the terminology used in other instruments. Furthermore, (28a) simply refers to Directive 2014/24/EU. Whilst we are not explicitly against referring to other instruments for definitions since it helps to streamline them across legal frameworks, we are however not certain whether this works in the current

		context. The terminology used in the DA, ODD and DGA does not correspond to the one used by Directive 2014/24/EU. To be more specific, where the ODD, DGA and DA refer to 'public sector bodies', Directive 2014/24/EU refers to 'contracting parties'. Even if both notions ('public sector bodies' and 'contracting parties') mean the same in essence, we are not certain whether this would not create legal uncertainty and confusion. We would suggest seeking advice from the Council Legal Service on this point.
[…]		
(48) 'document' means:		As already mentionned in our previous comments, L**uxembourg has strong reservations** regarding the extension of the scope of the DGA regarding 'documents' since this creates legal uncertainty. which in our view does not make sense for a regime that was designed for the digital sphere only. We do not see how this could work in practice. **<u>Previous comment :</u>** In line with our general comment, we have strong reservations regarding the applicability of this definition in the DGA regime. While the notion of 'document' in the ODD regime encompasses any content regardless its medium, the DGA is limited to the digital form. The same is true for the DA. The merger of this ODD notion into the DA and DGA regimes has however a considerable impact on the scope of these two instruments. This enlargement raises not only organisational but also

		practical questions, and we have serious doubts that this merger ultimately serves the simplification goal of the digital omnibus. For example, Article 32w(3)(b) which states that public sector bodies may establish the requirement that protected data can only be accessed remotely within a secure processing environment. While this is possible for 'data' it remains questionable how this could work for 'document'. The same is true for Article 32w(3)(c) where documents could be consulted in the premises of the secure processing environment. We do not see how the regime of the DGA, which was conceived for the digital world, could be applied to any physical medium. Consequently, we are strongly opposed to enlarge the scope of the DGA and the DA by including 'documents' in the respective regimes. We consider the simple merger of the regimes as creating legal uncertainty especially regarding the DGA regime. Luxembourg can support the idea to consolidate the regime of the ODD and the DGA into a single document. However, the regimes should remain unchanged and strictly separated. Therefore, we consider that the initial definition of 'documents' of the ODD could be maintained as long as its application is limited to the provisions relating to the ODD
(a) any content that is non-digital whatever its medium (paper or as a sound, visual or audiovisual recording); or		
(b) any part of such content;		

[…]		
(55) ‘re-user’ means a natural or legal person who was granted the right to re-use data or documents held by a public sector body or a public undertaking under Chapter VIIc or to research data or certain categories of protected data;		This definition does not read well and does not clearly enough reflect what it covered, since it mixes up the DGA and ODD regimes. Is the intended meaning the following, expressed in other words: ‘re-user’ means natural or legal person granted the right to re-use of data or documents in accordance with Chapter VIIc?
[…]		
‘Article 15a		
Obligation for data holders to make data available on the basis of a public emergency		
1. Where a public sector body, the Commission, the European Central Bank or a Union body demonstrates ~~an exceptional~~ **the** need to use certain data to carry out its statutory duties in the public interest when responding to, ~~mitigating~~, or supporting the recovery from a public emergency, it may request from data holders that are legal persons, other than public sectors bodies, to make available those data, including the metadata necessary to interpret and use those data. Upon such duly reasoned request, data holders shall make the data and metadata available to the requesting public sector body, the Commission, the European Central Bank or Union body. Such requests may also be made where the production of official statistics is required in relation to a public emergency.		First, we would like to thank the PRES for taking up our comment from 15 May 2026. There is however further need to clarify this provision since the last sentence of paragraph 1 is too ambiguous. It will, in practice, not be possible for competent authorities to assess the request since the scope of the request is not clear. Does “in relation to” mean “responding to” AND “supporting the recovery from”? Or can it even be outside of these two scopes? Can these requests contain personal data? Can these requests be made to microentreprises and small enterprises? We consider that this provision entails too much legal uncertainty. Additionally, if requests for official statistics are considered as its own category of requests, Article 18(2) of the DA needs to be adapted in the sense that an additional deadline to respond to requests needs to be foreseen. We have a **strong reservation** as long as this is not clarified.

[…]		
Chapter VIIc		
Re-use of data and documents held by public sector bodies		
Section 1		
General Provisions		
article 32c (d) iii		On article 32c (d) iii "the definition of a 'data intermediation service' is altered and the requirement for a separate legal person is removed. Instead, an obligation to keep value added services "**functionally separate"** is introduced, except for micro or small entities. We recommend including **criteria for functional separation** or, at the very least provide more context in the relevant recital (8). The fulfilment of such criteria should be verifiable for the supervisory/competent authority."
Article 32i		
Subject matter and scope		
[…]		
(4) Section 3 of this Chapter does not apply to:		
[…]		
(c) data or documents held by cultural establishments and educational establishments;		We **strongly reiterate** our comment that the relevant recitals of the DGA should be included in the DA. In this case, especially recital (12) of the DGA should be included.
[…]		
Article 32k		
Exclusive arrangements		
(1) The re-use of data or documents shall be open to all potential actors in the market, even if one or more market actors already exploit added-value products based on those data or documents. Agreements or other arrangements or practices	The re-use of **public sector open** data or documents shall be open to all potential actors in the market, even if one or more market actors already exploit added-value products based on those data or documents. Agreements or other arrangements or	The wording of the ODD used here does not work with the regime of the DGA. Luxembourg therefor suggests re-wording the part of the sentence "the re-use of data or documents shall be open" in order to avoid conflicting understanding with Article

PUBLIC

pertaining to the re-use of data or documents, which have as their objective or effect to grant exclusive rights or to restrict the availability of data or documents for re-use by entities other than the parties to such agreements, arrangements or practices, shall be prohibited.	practices pertaining to the re-use of data or documents, which have as their objective or effect to grant exclusive rights or to restrict the availability of data or documents for re-use by entities other than the parties to such agreements, arrangements or practices, shall be prohibited.	32(i)(4) sub-paragraph 2 stating that the Regulation does not create an obligation to allow re-use. We consider this as an **important clarification** to provide the necessary protection for the DGA regime.
(2) By way of derogation of paragraph 1, where an exclusive right is necessary for the provision of a service of general interest, such a right may be granted to the extent necessary for the provision of the service or the supply of the product under the following conditions:	By way of derogation of paragraph 1, where an exclusive right **would not be otherwise possible** ~~is necessary~~ for the provision of a service of general interest, such a right may be granted to the extent necessary for the provision of the service or the supply of the product under the following conditions:	The wording of the DGA is stronger "would not be otherwise possible". We suggest replacing "necessary" by this wording of the DGA.
[…]		
(5) For certain categories of protected data, the duration of an exclusive right to re-use data shall not exceed 12 months. Where a contract is concluded ***or administrative act is adopted***, the duration of the ~~contract~~***arrangement*** shall be the same as the duration of the exclusive right.		Since this is a condition, it should also be listed in Article 32k point 2 among the other conditions. Or, since it is our understanding that this is only applicable to the DGA as it refers to «certain categories of data» we consider that this condition should be included in Section 3.
[…]		
(7) For existing exclusive arrangements, the following shall apply:		
[…]		
(b) exclusive arrangements concerning data and documents within the scope of Section 2 existing on 16 July 2019 that do not qualify for the exceptions set out in paragraphs 2 and 3, and that were entered into by public undertakings, shall be terminated at the end of the contract and in any event not later than 17 July 2049;	(b) exclusive arrangements concerning data and documents within the scope of Section ~~2~~**3** existing on 16 July 2019 that do not qualify for the exceptions set out in paragraphs 2 and 3, and that were entered into by public undertakings, shall be terminated at the end of the contract and in any event not later than 17 July 2049;	We believe that this provision contains a wrong reference. Shouldn't it refer to Section 3 instead of Section 2?

[…]		
Article 32la		
Procedure for re-quests for re-use		Luxembourg has **strong reservations** regarding the 20-day deadline to answer requests. We consider that this procedure needs to work in practice and that it needs to be aligned with the EHDS Regulation.
[…]		
(4) Any natural or legal person directly affected by a decision as referred to in paragraph 1 shall have an effective right of redress in the Member State where the relevant body is located. Such a right of redress shall be laid down in national law and shall include the possibility of review by an impartial body with the appropriate expertise, such as the national competition authority, the relevant access-to-documents authority, the supervisory authority established in accordance with Regulation (EU) 2016/679 or a national judicial authority, whose decisions are binding upon the public sector body or the competent body concerned.		We consider this reference as wrong. It should refer to paragraph 2.
(5) This Article shall not apply to the following entities:		These exclusions from the procedure foreseen in the present Article create legal uncertainty as to which procedure would apply to them and does not facilitate re-use of existing data of great value.
(a) public undertakings;		
(b) educational establishments, research performing organisations and research funding organisations.		
[…]		
Article 32w		

Conditions for re-use ***of protected data***	Conditions for re-use ***of <u>certain categories of</u> protected data***	This should read ”certain categories of” protected data.
[…]		
(3) To ensure the preservation of the protected nature as referred to in paragraph 2, public sector bodies may establish the following requirements:		We consider it important to include the relevant recitals of the DGA into the DA.
[…]		
(c) to access and re-use the data or documents within the physical premises in which the secure processing environment is located in accordance with high security standards, provided that remote access cannot be allowed without jeopardising the rights and interests of third parties.		
In the case of re-use allowed in accordance with the first subparagraph, point (a)(i), the re-use of data or documents shall be subject to the rules on ***public sector open*** ~~open government~~ data set out in Section 2. This is without prejudice to Article 32y, which prevails in case of conflict.		We reiterate our previous comment regarding this provision, and the legal uncertainty that it creates. It remains uncertain which regime is applicable, also because Article 32i(3)(b)(ii) excludes the application of section 2 to certain categories of protected data (section 3) for reasons of data protection. Luxembourg considers this provision as **<u>unacceptable</u>** if this point is not clarified.
[…]		
(4) The public sector body shall reserve the right to verify the process, the means and any results of processing of data or documents undertaken by the re-user to preserve the integrity of the protection of the data or documents. It shall also reserve the right to prohibit the use of results that contain information jeopardising the rights and interests of third parties. The decision to prohibit the use of the results shall be comprehensible and transparent to the re-user.		The following sentence of Article 5(5) of the DGA is missing : “Re-users shall be prohibited from re-identifying any data subject to whom the data relates and shall take technical and operational measures to prevent re-identification and to notify any data breach resulting in the re-identification of the data subjects concerned to the public sector body”. We have a strong reservation as long as this paragraph is not included.

PUBLIC

[…]		
Article 32x		
Requirements for transfers of non-personal **protected** data to third countries by re-users		
[…]		
(7) Specific Union legislative acts may deem certain non-personal data categories held by public sector bodies to be highly sensitive for the purposes of this Article where their transfer to third countries may put at risk Union public policy objectives, such as safety and public health or may lead to the risk of re-identification of non-personal, anonymised data. Where such an act is adopted, the Commission shall adopt delegated acts in accordance with Article 45 supplementing this Regulation by laying down special conditions applicable to the transfers of such data to third countries.		
If required by a specific Union legislative act referred to in the first subparagraph, such special conditions may include terms applicable for the transfer or technical arrangements in this regard, limitations with regard to the re-use of data in third countries or categories of persons entitled to transfer such data to third countries or, in exceptional cases, restrictions with regard to transfers to third countries.		The paragraph previous to this paragraph of Article 5(13) of the DGA is missing : "Those special conditions shall be based on the nature of the non-personal data categories identified in the specific Union legislative act and on the grounds for deeming those categories to be highly sensitive, taking into account the risks of re-identification of non-personal, anonymised data. They shall be non-discriminatory and limited to what is necessary to achieve the Union public policy objectives identified in that act, in accordance with the Union's international obligations."
[…]		
Article 32y		
Fees ***for the re-use of protected data***	Fees ***for the re-use of <u>certain categories of</u> protected data***	This should read "certain categories of" protected data.

PUBLIC

[…]		
Article 32z		
Competent bodies		
[…]		
(2) The competent bodies may be empowered to grant access for the re-use of certain categories of protected data pursuant to Union or national law which provides for such access to be granted. ~~Where they grant or refuse access for re-use, those competent bodies shall be subject to Articles 32k, 32w, 32x, 32y and 32ab.~~		Luxembourg **strongly opposes** the deletion of the second sentence. We ask to reintroduce this sentence but to rely on the wording of the DGA, which reads as follows: « Where they grant or refuse access for the re-use, Articles 4, 5, 6 and 9 shall apply to those competent bodies. » Luxembourg considers that the deletion does not contribute to a simplification but rather the opposite. It also creates legal uncertainty regarding these matters since Members States need to decide if and how to address the void caused by the deletion (ex. foresee their own rules). This will inevitably lead to different regimes and thus complexify the system and at the same time increase administrative burdens for applicants.
[…]		
~~(4)~~***(3)*** The assistance referred to in paragraph 1 shall include, where necessary:		
[…]		
(b) providing guidance and technical support on how to best structure and store data to make that those data or documents easily accessible;	providing guidance and technical support on how to best structure and store data to make that ~~those~~ data or **those** documents easily accessible;	The sentence needs to be redrafted a bit.
[…]		
Article 32aa		
Single information point		
[…]		
(3) The single information point may include a separate, simplified and well-documented information channel for SMEs, SMCs, start-ups and research establishments addressing their needs and capabilities in		We believe that this is the wrong reference. It should read Article 2(53).

requesting the re-use of ~~the~~ ***certain*** categories of data referred to in Article 2(54).		
[…]		
'Article 41a		
European Data Innovation Board		
[…]		
(2) It shall be composed at least of representatives of Member States competent for matters related to data, the competent authorities for enforcement of Chapters II, III, V, VIIa and VIIc of this Regulation, the European Data Protection Board, the European Data Protection Supervisor, ENISA, the EU SME Envoy or a representative appointed by the network of SME envoys. ***If a Member State has designated more than one competent authority or competent body, they are represented in the plenary meetings of the Board by the designated data coordinator. Other competent authorities or competent bodies entrusted with specific operational responsibilities for the application and enforcement of this Regulation may participate in the thematic subgroups of the Board relevant for their responsibilities.*** The Commission may decide to add additional categories of members. In its appointments of individual experts, the Commission shall aim to achieve gender and geographical balance among the members of the group.	(2) It shall be composed at least of representatives of Member States competent for matters related to data, the competent authorities **or competent bodies** for enforcement of Chapters II, III, V, VIIa and VIIc of this Regulation, the European Data Protection Board, the European Data Protection Supervisor, ENISA, the EU SME Envoy or a representative appointed by the network of SME envoys. ***If a Member State has designated more than one competent authority or competent body, they are represented in the plenary meetings of the Board by the designated data coordinator. Other competent authorities or competent bodies entrusted with specific operational responsibilities for the application and enforcement of this Regulation may participate in the thematic subgroups of the Board relevant for their responsibilities.*** The Commission may decide to add additional categories of members. In its appointments of individual experts, the Commission shall aim to achieve gender and geographical balance among the members of the group.	The PRES modified this paragraph by adding the competent bodies. However, this addition was not made in the first sentence of this paragraph. Hence Luxembourg suggests to make the necessary modification of the provision and include 'competent bodies' also in the first sentence.
Article 49	*Article 49* *Evaluation and review*	The Digital Omnibus does not currently provide for the amendment of Article 49 of the Data Act. However, this article

PUBLIC

	1. By 12 September 2028, the Commission shall carry out an evaluation of this Regulation and submit a report on its main findings to the European Parliament and to the Council, and to the European Economic and Social Committee. That evaluation shall assess, in ~~particular~~: *~~(a) situations to be considered to be situations of exceptional need for the purpose of Article 15 of this Regulation and the application of Chapter V of this Regulation in practice, in particular the experience in the application of Chapter V of this Regulation by public sector bodies, the Commission, the European Central Bank and Union bodies; the number and outcome of the proceedings brought to the competent authority under Article 18(5) on the application of Chapter V of this Regulation, as reported by the competent authorities; the impact of other obligations laid down in Union or national law for the purposes of complying with requests for access to information; the impact of voluntary data-sharing mechanisms, such as those put in place by data altruism organisations recognised under Regulation (EU) 2022/868, on meeting the objectives of Chapter V of this Regulation, and the role of personal data in the context of Article 15 of this Regulation, including the evolution of privacy-enhancing technologies;~~*	refers to Articles 15 and 18(5) Article 15 and paragraph 5 of Article 18 are removed by the omnibus. Consequently, Article 49 should be adjusted, which is not currently planned.

***

PUBLIC

NETHERLANDS

NEDERLAND

NL Written Comments Digital Omnibus 15 June 2026

1. Data legislation

Regarding the data acquis, the Netherlands can support large parts of the compromise text. However, the Netherlands has remaining concerns regarding the current compromise text as it creates exemptions that may allow for loop holes that are contrary to the purpose of the Data Act and may weaken the effectiveness of the Data Act. We would like to reiterate our concerns regarding article 15 of the omnibus and especially proposed article 31(1a) and 31(1b) of the Data Act. This article may restrict or delay the operationalization of the cloud provisions of the Data Act, which the Netherlands opposes given their importance in improving the functioning of the European cloud market.

Regarding articles 3 and 4 of the omnibus, on trade secret exemptions to the Data Act, we have concerns regarding the changes made in the last compromise text. For the Netherlands only the deletion of 'In exceptional circumstances' is acceptable. The fact that refusals to share data no longer have to be made 'on a case-by-case basis' and the change that refusals to share data no longer 'shall be duly substantiated', but only 'may be substantiated' raise serious concerns. These deletions could allow data holders to easily refuse a large amount of data sharing requests, also for broader purposes than this exemption is intended for. This is contrary to the purpose of the Data Act. Additionally, the lack of substantiation for refusing requests makes it very difficult for competent authorities to properly oversee and enforce this article. We therefore propose to reinstate that refusals should be done on a case-by-case basis and should be duly substantiated:

3. In article 4, paragraph 8 is replaced by the following:

~~*In exceptional circumstances,*~~ *Where the data holder who is a trade secret holder is able to demonstrate that, despite the technical and organisational measures taken by the user pursuant to paragraph 6 of this Article, it is highly likely to suffer serious economic damage from the disclosure of trade secrets or that the disclosure of trade secrets to the user poses a high risk of unlawful acquisition, use, or disclosure to third country entities, or entities established in the Union under the direct or indirect control of such entities, which are subject to jurisdictions offering weaker or non-equivalent protection compared to that under Union law, that data holder may refuse* ***on a case-by-case*** *basis a request for access to the specific data in question. That demonstration* ***shall be duly*** ~~***may be***~~ *substantiated on the basis of objective elements, such as the enforceability of trade secrets protection in third countries, the nature and level of confidentiality of the data requested, and the uniqueness and novelty of the connected product. It shall be provided in writing to the user without undue delay. Where the data holder refuses to share data pursuant to this paragraph, it shall notify the competent authority designated pursuant to Article 37.;* ***The Commission shall issue guidelines, in consultation with the European Data Innovation Board (EDIB), on the application of this paragraph, such as the assessment of serious economic damage, and the enforceability of trade secrets protection in third countries.'***

4. in Article 5, paragraph 11 is replaced by the following:

~~*In exceptional circumstances,*~~ *Where the data holder who is a trade secret holder is able to demonstrate that, despite the technical and organisational measures taken by the user pursuant to paragraph 6 of this Article, it is highly likely to suffer serious economic damage from the disclosure of trade secrets or that the disclosure of trade secrets to the user poses a high risk of unlawful acquisition, use, or disclosure to third country entities, or entities established in the Union under the direct or indirect control of such entities, which are subject to jurisdictions offering weaker or non-equivalent protection compared to that under Union law, that data holder may refuse* ***on a case-by-case*** *basis a request for access to the specific data in question. That demonstration* ***shall be duly*** ~~***may be***~~ *substantiated on the basis of objective elements, such as the enforceability of trade secrets protection in third countries, the nature and level of confidentiality of the data requested, and the uniqueness and novelty of the connected product. It shall be provided in writing to the user without undue delay. Where the data holder refuses to share data pursuant to this paragraph, it*

shall notify the competent authority designated pursuant to Article 37.; ***The Commission shall issue guidelines, in consultation with the European Data Innovation Board (EDIB), on the application of this paragraph, such as the assessment of serious economic damage, and the enforceability of trade secrets protection in third countries.***

2. GDPR provisions

Introductory remarks NL about GDPR provisions:

- NL would like to thank the presidency for the important work it has done in guiding the discussions about the Digital Omnibus.
- NL wholeheartedly agrees with presidency's assessment that these discussions have demonstrated **need for caution** when considering changes that could have broader consequences, when these extend beyond the targeted simplification objectives of this initiative. For NL, the **core commitment** is to ensure that these omnibuses focus on simplification, clarification, and streamlining of legislation, and that the objectives of the legislation remain intact. In this context, NL can all but agree with the presidency about the **importance of striking the right balance** between the substantial depth of amendments and the framework in which the present discussions are taking place.
- NL would like to draw attention the importance of **safeguarding** this **carefully sought balance by the presidency** during the remainder of the negotiations.
- For NL, the Presidency compromise proposal is **in the right direction**.
- **A number of important points remain in the GDPR part, notably:**
    - **Article 29a on pseudonymisation**;
    - **Article 9(2)(k) and 9(5) – residual processing of special categories of data for AI**
- In addition, **some recitals require attention**, especially in light of the importance of legal certainty, notably.
    - **Recital 33a: 'legitimate interest' as a legal basis for AI data processing**;
    - **Recital 28 on the definition of scientific research.**

Article 29a: Application of pseudonymisation and identification of a natural person

Text proposal: Delete Article 29a(2) or amend the final part of Article 29a(2):
…effectively prevent persons other than the controller from attributing the personal data to an identified or identifiable natural person ~~identifying a data subject, in such a way that, for them, the data subject is not or is no longer identifiable~~

- NL is concerned about Article 29a, paragraph 2. The Presidency Note explains that this paragraph "fully anchors in the operative part of the GDPR the main elements of the CJEU ruling in the SRB case". NL recalls that the EDPB and EDPS has noted that "a *selective* codification of that case-law (…), introducing only a *single* element from a *single* case, lacks the necessary context". This "ignores the specific characteristics of the case and will undermine – rather than improve – legal certainty".
- Therefore NL proposes to delete paragraph 2, or to amend it as proposed by NL in the last written comments (2 June, see above). With this text proposal, paragraph 2 is brought into line with the definition of pseudonymisation from the current Article 4(5) GDPR.
- An alternative is to delete Article 29a entirely.

PUBLIC

Article 9(2)(k) and 9(5) GDPR– residual processing of special categories of data for AI

Text proposal: Amend Article 9, fifth paragraph, third sentence:
"If erasure of those data proves to be technically impossible ~~or requires manifestly disproportionate effort~~, the controller shall, without undue delay and in any event, effectively protect such data from being further processed or processed for other purposes, used to produce outputs, disclosed or otherwise made available to third parties."

- NL remains seriously concerned about the proposed derogation to the prohibition on processing special categories of personal data for "residual" data when training and using AI (Article 9(2)(k) and 9(5) GDPR). NL has repeatedly proposed to delete this exception as it risks broad misuse. It decreases the incentive for privacy by design. AI model providers should scrape data from privacy friendly sources rather than indiscriminately gathering information from all kind of sources.
- However, if a majority of the Member States supports this exception, NL considers it crucial that these provisions should be limited more strictly. At least, the reference to "disproportionate effort" should be deleted. That means that the exception should not be applicable in case of a 'disproportionate effort' to remove the personal data, but only in case the removal is "technically impossible". The reference to disproportionate effort reverses the protective logic of data protection law: the more data are processed for AI, the easier it becomes to justify that it requires a disproportionate effort to erase the special categories of personal data.
- If the phrase "disproportionate effort" remains in place, this effectively means that poorly built AI systems can remain permanently as they are, even though they were never actually built correctly. Systems that are not built with privacy by design would effectively gain an extra advantage over systems that are configured with privacy by design. The reference to "disproportionate effort" makes it very easy to avoid having to erase special categories of personal data. This becomes even more problematic because Recital 33 states that a "disproportionate effort" exists "where the erasure of special categories of data memorised in the AI system or AI model would require re-engineering the AI system or AI model". Re-engineering is not defined anywhere. As a result, even small, simpler "re-engineering" can be designated as a "disproportionate effort". Some "re-engineering" can probably be done relatively easily in a relatively short time (e.g., adjusting prompts, changing parameters, changing rules, etc.).
- NL also proposes to add to recital 33: "This is without prejudice to the obligation to erase data that have been processed without a valid legal base."

Recital 33a: Personal data processing for purposes of AI Training

Text proposal: Delete recital 33a or amend it as follows, building on case law / EDPB guidance:
(33a) The processing of personal data to the extent strictly necessary and proportionate for the purposes of the controller in the context of the development and deployment of an AI system or of an AI model, may be regarded as carried out for a legitimate interest of the controller concerned and be carried out in accordance with Article 6(1)(f) of Regulation 2016/679, where appropriate, except where such interests are overridden by the interests, or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child, or where other Union or national laws explicitly require consent. The reasonable expectations of data subjects should be taken into account in this assessment, which should include whether or not the personal data were publicly available, the nature of the relationship between the data subject and the controller and whether a link exists between the two, the nature of the service, the context in which the personal data were collected, the source from which the data were

collected, the potential further uses of the model, and whether data subjects are actually aware that their personal data are online at all. The interests of artists and creative professionals are to be taken into account. This does not affect the obligation of the controller to choose an appropriate lawful ground of processing set out in Article 6 of Regulation (EU) 2016/679, such as Article 6(1)(e) with regard to processing by public authorities. Regardless of the lawful ground of processing, any such processing should be subject to appropriate organisational, technical measures and safeguards for the rights and freedoms of the data subject, such as to protect against non-disclosure of residually retained data in the AI system or AI model. Other provisions of this Regulation remain unaffected by the fact that a controller relies on this legal basis.

- NL strongly supports the deletion of the regulation of a legitimate interest basis specifically for AI (proposed Article 88c GDPR), but is concerned about the substitute recital 33a.
- The Presidency justifies recital 33a as follows: "This approach follows already existing references to examples of legitimate interest within the GDPR" (Presidency note, page 8). The Presidency rightly notes that recital 49 of the current GDPR gives an example of a legitimate interest. However, we are missing a crucial phrase in the proposal that is explicitly present in the example just cited, namely "**to the extent strictly necessary and proportionate for the purposes**" of the controller.
- Building on this example of recital 49, NL considers it crucial to copy this phrase into recital 33a, to avoid a contrario reasoning and to avoid the impression that this legal basis is given by default in case of AI, without a necessity and proportionality test.
- Furthermore, NL considers it essential to refer to the reasonable expectations of data subjects and to include the assessment factors which are given by the EDPB, specific for AI context, into recital 33a (source: EDPB Opinion 28/2024, page 3, penultimate paragraph).
- There are concerns among a majority of the Dutch House of Representatives, which adopted a motion against the use of personal data for AI training without consent.

Article 12(5): GDPR data requests with an abusive intention

Text proposal:

- **Delete the two phrases within brackets in Article 12(5):**
  - **~~[also, for requests under Article 15,]~~**
  - **~~[that there are reasonable grounds to believe that it is excessive or submitted with an abusive intention, based on objective circumstances related to the request or the conduct of the data subject].~~**
- **Amend the final part of the related recital 35: …"or when the exercise of a right is made with the intention to adversely affect a judicial procedure or with deliberate intention to ~~adversely~~ maliciously affect and burden public authorities."**

- The two phrases within brackets in Article 12(5) should not be included in Article 12(5), because NL considers that the possibility to refuse a GDPR request because of an abusive intention should not be limited to data access requests because other data subject rights, such as rectification or erasure, could also be misused with an abusive intention. The phrase "reasonable grounds to believe" should not be included because that would constitute too low a burden of proof. NL supports the Presidency's considerations.
- NL proposes to find an alternative for the word "*adversely"* in the phrase relation to "affect a judicial procedure" in recital 35, for example "*maliciously*". The mere fact that a judicial procedure could adversely affect a party, does not make the data request abusive, because there may be legitimate reasons for a judicial procedure and the data request.

Recital 28: scientific research

Text proposal: Addition to recital 28:
"Scientific research applies the scientific method of observing phenomena, formulating and testing a hypothesis for those phenomena, and concluding as to the validity of the hypothesis. The notion of scientific research may not be stretched beyond its common meaning."

- Although the Presidency added various improvements in the definition of scientific research, NL is still concerned that the proposed definition is prone to abuse and that it extends the scope of exceptions for scientific research also in unintended and undesired ways. A (too) broad definition has an impact on many exceptions for scientific research (in particular Article 5(1)(b), Article 9(2)(j); 14(5)(b); 17(3)(d) and 21(6) GDPR).
- NL fears that this definition could also be invoked with regard to commercial AI development and refers to the NL text proposal for recital 28 (written comments 2 June, see above). This proposal is based on EDPB and EDPS guidance.

ePrivacy Directive and cookies

Centralised consent – Proposed article 8a GDPR (now deleted)

Text proposal: Reinstatement of article 8a GDPR:
"Controllers shall ensure that their online interfaces allow data subjects to:
(a) Give consent through automated and machine-readable means, provided that the conditions for consent laid down in this Regulation are fulfilled;
(b) decline a request for consent and exercise the right to object pursuant to Article 21(2) through automated and machine-readable means.
(ba) withdraw consent through automated and machine-readable means.

[…]"

- We are disappointed that this key provision has been removed from the proposal at this stage of negotiations. The development and regulation of centralised consent management solutions in EU legislation have been a long time coming, and mark an essential modernisation of the current regime, which dates back to 2009.
- As demonstrated in the technical workshop earlier this year, these solutions are recognised internationally as the appropriate response to the problems of consent fatigue and surveillance advertising created by the current, severely outdated, legal regime. Moreover, these solutions have already been thoroughly assessed by the European Commission in 2017 in terms of their added value and impact and were identified at that time as the most suitable solution to these issues.
- In our view, these solutions would lead to significant and tangible improvements both in terms of citizens' control over their data and the compliance burdens faced by European companies. We therefore strongly urge the Presidency to reinstate this article.

Fraud exception – Proposed article 5(3)(e) ePrivacy-directive

- The delineation of this exception remains too broad to protect the fundamental rights of citizens. The mere reference to fundamental rights does not provide for enough legal certainty in this regard. We therefore urge the Presidency to further limit this exception to what is strictly necessary for specific use-cases, as it has done for the other exceptions included in this article, in order to prevent unintended or undesirable applications.

Proposed article 5(3)(c) and (b) ePrivacy-directive

Text proposal: Amend Article 5(3)(c) ePrivacy-directive

- c) Measuring the audience of an online service in order to create anonymous aggregated information **solely for the provider's own use** about the usage of that online service **requested by the user**, where it is carried out by the provider of that online service, or by a third party acting together with or on behalf of this provider, including where the third party is an entitled and independent third party performing audience measurement in accordance with Article 24 of Regulation (EU) 2024/1083;

Text proposal: Amend recital 44b:

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

- The amendments made in relation to paragraph (c) significantly broaden the scope of parties eligible to make use of this exception; furthermore, the phrase stating that this exception applies only to a service requested by the data subject has been deleted.
- With regard to paragraph (b) – particularly in conjunction with recital 44b – we consider that the term 'ensuring functionality' is not sufficiently delineated.

3. Cyber provisions

- The NL welcomes the proposal and would like to thank the presidency for echoing the comments of the MS. We believe that it provides a strong basis for a compromise, but the current proposal still needs a thorough review.

- There are some inconsistencies in the used concepts and definitions: 'Single Information Point' and 'Single Entry Point' are, for example, still used as concepts in the recitals, when article 23.b now clearly refers to a 'Incident Reporting Information Point' (Art. 23a).
- We would also like to underline that we are not - as other MS expressed during Coreper- in favour of a 'single notification' on national level. This seems however to be inconsistent with article 23.b.1.a, where a reference is made to 'notifications'.

***

The Netherlands still have significant concerns relating to last compromise text, particularly regarding trade secrets (Data) and GDPR provisions. In this context, we believe that our text proposal for Article 29a (on GDPR – Pseudonymisation), as supported by POL and BEL in the AGS, could provide much-needed clarity and would not be difficult to accept for other Member States, as it mostly clarifies the Article. Below, you will find our proposed text for this again.

Article 29a: Application of pseudonymisation and identification of a natural person

Text proposal: Delete Article 29a(2) or amend the final part of Article 29a(2):
…effectively prevent persons other than the controller from attributing the personal data to an identified or identifiable natural person ~~identifying a data subject, in such a way that, for them, the data subject is not or is no longer identifiable~~

***

AUSTRIA

ÖSTERREICH

Austrian questions and comments regarding Omnibus VII
– 15 June 2026

PUBLIC

In light of the short deadline for comments, AT refers to its previous oral and written comments on Omnibus VII. Without prejudice to its position, AT reserves the right to submit further comments in due course.

ad Art 3 – amendments to Reg. (EU) 2016/679 (GDPR):

- AT refers, in particular, to its written comments on the third compromise text submitted on 2 June 2026.

ad Article 6 – amendments to Dir. (EU) 2022/2555 (NIS-2):

Art23b – National entry point for incident reporting

- In light of well-established and effective national reporting systems already in place, Member States should be granted sufficient flexibility in the implementation and organisation of the National Entry Point (NEP). This would enable NEP functions to be carried out in a manner consistent with national structures, competences and existing arrangements, while avoiding disproportionate administrative and financial burdens. In addition, the requirements associated with the NEP should be limited to what is strictly necessary to achieve the objectives of the Regulation.
- Against this background, AT considers the distinction between the tasks set out in Article 23b(1) and Article 23b(2) to be unnecessary. All tasks currently listed in Article 23b(2) should therefore be incorporated into Article 23b(1). Furthermore, we believe that the wording should be "**Member States ~~shall~~ may establish and maintain a national entry point for the reporting of incidents and related events under the Union legal acts where those Union legal acts provide so. The national entry point ~~shall~~ may allow for at least one of the following tasks, depending on national organisational arrangements: (…)"**
- Art 23b (5) foresees that ENISA "shall" develop an open-source solution that "may" be used by member states. The cost /value ratio of this para seems unbalanced. It would be of utmost importance, before adding para 5, to check how many member states would need and actually use and implement such an open-source tool before deciding that ENISA "shall" develop and invest resources in such a tool. Needless to say that member states themselves will have to invest significant resources and time in order to implement an open source tool in their national IT systems.

Art 23d – Harmonising incident notification framework

- AT strongly welcomes the efforts to further harmonise reporting obligations. Irrespective of the ongoing discussions regarding reporting channels, further work on the harmonisation of reporting requirements remains important.
- AT therefore calls, as a first step and key priority, for enhanced harmonisation to provide companies with legal certainty and to further reduce administrative burdens.

ad Art 10 – amendments to Reg. (EU) 2019/1150 (P2B):

- AT welcomes amendments made to Art 10 (amendment of the P2B) in the compromise text ST 10426/26.
- We welcome the text in its current form, which retains key provisions such as Art 4 and 11 on a permanent basis and, in our view, strikes a balance between simplification and the protection of business users, particularly SMEs.

- AT expressly supports the aim of simplifying provisions and eliminating duplication. In doing so, it is important to take a long-term perspective and to structure the legal framework in such a way that it withstands future developments and avoids unnecessary overlaps.
- Against this backdrop, we welcome the retention of the provision regarding an evaluation in Art 18(1) in the compromise text.
- In the long term, consideration could also be given to integrating the provisions on the protection of business users into the Digital Services Act (DSA).

***

PUBLIC

POLAND

POLSKA

15.06.2026

PUBLIC

PL comments regarding Digital Omnibus

General comment

- We would welcome having more time for discussions at the technical level, especially on GDPR, to make sure we achieve a text that provides real simplification.

Open Data Directive

- Our main concerns regarding the Open Data Directive remain unresolved. Many provisions are not sufficiently clear or precise for direct application and may create significant interpretative difficulties. We have raised these concerns consistently, both orally and in writing.
- Legal provisions must be clear and precise. Some provisions of the Omnibus concerning the Open Data Directive would therefore be difficult or impossible to apply in practice.
- We would like to reiterate several key drafting comments:
- **Article 32i – "general interest" / "public task"**. We propose aligning the terminology by referring consistently to "public tasks". If this is not possible, the distinction between "public task" and "services in the general interest" should be clarified in the recitals.
- **Article 32la – grounds for refusal**. Grounds for refusal should be clearly specified in the Regulation. The current wording lacks clarity and creates uncertainty as to which rules apply. If no harmonised grounds are introduced, this issue should remain for Member States to regulate nationally.
- **Title of Section 2**. We suggest replacing "re-use of public sector open data" with "re-use of data and documents", as documents are also covered by the section.
- **Article 32q(3) – list of public sector bodies**. This obligation should be deleted or made optional. The list would be highly dynamic and based on unclear criteria, making it impractical for Member States to compile and maintain.
- **Article 32q(4) – criteria for charges**. We propose deleting the obligation for Member States to define charging criteria. The obligation is too vague and would be more appropriate in a directive. If retained, the Commission should specify the criteria through delegated acts, supported by examples in the recitals.
- **Article 32r – standard licences**. Public sector bodies and public undertakings should be able to establish conditions for the re-use of data or documents containing personal data.
- **Article 32v – high-value datasets**. We propose clarifying that general exemptions from the scope of the Directive do not apply to high-value datasets (HVD). Otherwise, some HVD obligations may become unenforceable in practice.
- **Article 32w – conditions for re-use of protected data**. The obligation to publish conditions for re-use in advance is problematic. Such conditions must be assessed case by case, depending on the data, intended use, legal requirements, and risks involved. We therefore propose making this obligation voluntary.
- **Article 32aa – single information point**. For the same reasons, we propose removing the obligation to include conditions for re-use in the single information point, as these conditions cannot realistically be determined in advance.

- **Article 10 – transitional provisions**. We propose clarifying that Commission Implementing Regulation (EU) 2023/138 on high-value datasets remains in force after the repeal of Open Data Directive.

Entry into application

- We maintain our reservation regarding the short vacatio legis. The 18-month transition period applies only to Chapter VIIc. Other provisions, including those concerning the Data Act, data intermediaries, and data altruism organisations, would apply much earlier.
- We believe that the minimum application period for the new framework should be 24 months, at least for areas currently covered by the Open Data Directive and the DGA.

Protection of trade sec/rets in IoT data sharing

- On trade secrets, we maintain the position expressed at COREPER. We do not support additional provisions that would further strengthen trade secret protection while restricting access to and use of IoT-generated data, as this would run counter to the objectives of the Data Act.

Cyber provisions

- We fully support the compromise text and again thank the PRES on the excellent work on this part.
- It is crucial to have one single entry point at the national level.
- We welcome the provision that ENISA can deliver a solution for Member States not wishing to develop by themselves

GDPR provisions

- **On Article 29a** GDPR, we maintain that the relationship between pseudonymisation and the assessment of the identifiability of a natural person for the purposes of the application of the GDPR should remain clear and provide legal certainty for controllers and processors. Current wording does not provide needed clarifications and risks divergent interpretations. We propose an alternative approach to move away from determining whether effectively pseudonymised data lose their character as personal data for certain entities, and instead recognise that they remain personal data, while effective pseudonymisation may justify a proportionate limitation of the application of selected GDPR principles and obligations with regard to an entity which does not have and cannot reasonably obtain means enabling the identification of the natural person.
- **On definition of scientific research (Article 4(38))**, it is crucial to maintain the approach according to which the qualification of a given activity as scientific research is determined by its nature, in particular its autonomy, applied methodology, transparency and contribution to the development of knowledge, rather than by the legal status of the entity conducting the research.

  We propose the following wording

  "scientific research" means research conducted in a methodological and systematic manner, consistent with ethical standards of the relevant scientific field, with the aim of generating new or complementing existing knowledge and contributing to scientific understanding and societal wellbeing.

- **On Article 9**, we acknowledge the clarifications in the recitals and the safeguards on incidental and residual processing of special categories of personal data by AI systems and

models, including biometric data for identity verification. We support having legal clarity when it comes to training of AI models and we see a need for further discussions on this topic. Derogations should be interpreted strictly and in line with their purpose, and should not allow intentional processing of special categories of personal data for AI development.

We propose the following amendment

'(k) incidental and residual processing, which is strictly unintended and unavoidable despite the implementation of appropriate technical and organisational measures, in the context of the development and operation of an AI system (…)'

- **On Article 12(5)**, we propose the following wording, presented together with DE :

  „The controller shall bear the burden of demonstrating that the request is manifestly unfounded or that there are reasonable grounds to believe that it is excessive or submitted with an abusive intention, based on objective circumstances related to the request or the conduct of the data subject."

- **On Article 13(4)**, we propose the following wording, presented together with DE:

  "(4) Paragraphs 1, 2 and 3 shall not apply if and to the extent that the data subject already has the information or if the provision of such information proves impossible or, provided the processing is to result in a low risk to data subjects, would involve a disproportionate effort, especially in every-day business. Article 14(5)(b) shall apply accordingly."

  "Sentence 1st, 2nd and 3rd alternative, shall not apply where the processing concerns personal data referred to in Articles 9 or 10 of this Regulation, or where the personal data are further processed for purposes other than those for which the data were originally collected."

- **On Article 22**, as it still do not address our comments, we maintain our previous position. We preferred the COM proposal.
- **On Article 33**, we thank the PRES for extending the breach notification deadline for from 72 to 96 hours. This is important simplification, providing a more realistic timeframe for controllers and providers.

  We propose the following changes to par. 6

'6. The Board shall ~~prepare and transmit to the Commission a proposal for~~ **establish and make public** a common template for notifying a personal data breach to the competent supervisory authority referred to in paragraph 1 as well as ~~for~~ a list of the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person **and a list of the circumstances in which it is not likely to result in such a high risk. The template and lists**~~. The proposals~~ shall be ~~submitted to the Commission~~ **available** within [OP date = nine months of the entry into application of this Regulation]. The Commission ~~after due consideration reviews it, as necessary, and is empowered to~~ **may** adopt ~~it~~ **the template** ~~as established by the Board~~ by way of an implementing act**,** in accordance with the examination procedure set out in Article 93(2).

- Art. 35.6a we propose the following wording:

The Commission ~~after due consideration reviews them, as necessary, and is empowered to~~ **may** adopt ~~them~~ **the template** ~~as established by the Board~~ by way of an implementing act**,** in accordance with the examination procedure set out in Article 93(2).

- **On Article 37(7)**, we maintain our previous position. Publishing the DPO's[1] contact details and communicating them to the supervisory authority serve different purposes. Removing the obligation to notify the supervisory authority may hinder cooperation and the performance of supervisory tasks.
- **On Article 57(4)**, we should ensure consistency with our proposal on Article 12(5). While the text refers to abusive intention, it does not reflect the supervisory authority's burden to demonstrate it.
- **On Article 70(1)(f)**, our position is linked to our comment on Article 22.
- **On Article 88c –** we would welcome further discussions on keeping this provision. We agree with other delegations, especially DE, that this provision constitutes important element of the simplification package when it comes to ensuring legal clarity for AI systems development. At the same time, we see need to further work on a suitable wording.

Cookies and ePrivacy provisions

- We welcome the deletion of Article 8a and recital 46a on central consent management mechanisms. Cookie fatigue remains an important issue, but it should be addressed in the appropriate and separate legal framework.
- The proposal went beyond a technical simplification exercise. In its proposed form, it could concentrate user consent and data in the hands of a limited number of major technology providers, without sufficient standards or clarity on how the mechanism would function in practice.
- As presented in our non paper, we see a two stage approach. As an interim response to cookie fatigue, **we propose expanding the whitelist under Article 88a to include purely operational, additional low-risk and strictly necessary purposes**, such as functional cookies, fraud prevention and security-related processing.
- In the longer term, we need a broader strategic discussion on privacy-enhancing technologies (PETs). Cookies are increasingly an outdated technological solution. However, replacing them requires careful assessment, technical standardisation and the development of privacy-preserving alternatives that are compatible with European values, competition objectives and data protection requirements.
- A dedicated technical discussion on automated and machine-readable indications of data subject's choices is still needed. This should support the development of standards and an effective regulatory framework. Without a proper impact assessment and clearer operational details we risk creating legal uncertainty for businesses without delivering meaningful improvements in addressing cookie fatigue.
- Regarding the amendments to the ePrivacy Directive, it remains unclear why Article 5(3), second sentence, refers to a "natural person", while the first sentence refers "subscriber or user". It seems that this should be aligned by referencing "subscriber or user".

We propose the following changes to art. 5:

~~'This paragraph~~**3. Member States** shall ~~not apply if the~~ **ensure that the storing of information, or gaining of access to information already stored, in the terminal equipment of a** subscriber or user

[1] DPO – Data Protection Officer

is **only allowed when that person has given his or her consent, in accordance with Regulation (EU) 2016/679.**

Storing of information, or gaining of access to information already stored, in the terminal equipment of ~~a natural person~~ a subscriber or user without consent, and subsequent processing for the same purpose, shall be lawful to the extent it is strictly necessary for any of the following purposes:

d) maintaining, ~~or~~ restoring, or ensuring the security of the interface strictly necessary for the provision of an information society service requested by the subscriber or user or the security of the terminal equipment used for the provision of such service, including in particular cybersecurity, the protection of personal data **and privacy of the user and prevention of fraud and unauthorised access provided that such measures do not override the fundamental rights and interests of the subscriber or user;**

(e) processing where the controller deploys recognised privacy-enhancing technologies (PETs) that effectively mitigate risks to the rights and freedoms of data subjects, in accordance with the technical specifications adopted pursuant to paragraph 4, 5 and 6.

In Article 5, paragraph 4 is added:

For the purpose of Article 5 paragraph (3)(e), the Commission shall:

(a) assess the state of the art of available technologies;

(b)develop criteria to assess the effectiveness of risk mitigation in relation to the specific categories of data and processing operations.

In Article 5, paragraph 5 is added

(5) Article 5(3)(e) enters into force only 6 months after the adoption of relevant implementing acts by the European Commission. The implementing acts shall specify the technical standards and

criteria to determine whether a technology qualifies as a recognised Privacy Enhancing Technology (PET) and effectively mitigates risks as referred to in paragraph 3(e).

***

PUBLIC

PORTUGAL

PORTUGAL

Round 4: Application of pseudonymisation and identification of a natural person The Presidency will invite delegations to express their positions in a constructive manner and provide concrete feedback on the updated proposal for a new Article 29a on pseudonymisation.

We agree with the Presidency's proposal regarding not proceeding with the amendment of the definition of personal data set out in Article 4(1), and instead addressing the issue of pseudonymisation in a separate article (Article 29a).

We consider, however, that the Presidency's proposal for Article 29a falls short of what is possible and necessary with regard to the codification of the Court of Justice of the European Union's case law on pseudonymisation. In particular, we consider it essential that the new article also addresses the obligations of entities that process data which, from their perspective, does not constitute personal data because it has been pseudonymised, notably when they transfer such data to a third party (in such cases, the entity will need to assess whether the data remains pseudonymised for that third party, or whether, on the contrary, the third party has the capacity to re-identify the data, thus making it personal data from the third party's perspective).

For this reason, we consider that the Presidency's proposal should be read in conjunction with the Swedish Presidency's proposal on pseudonymisation, which effectively and satisfactorily addresses the question of the duties of an entity that transfers pseudonymised data.

We also consider it essential to ensure (whether by improving the wording of the operative text and/or the recitals, or, above all, by ensuring that the evolution of the negotiations does not dilute these rules):

-That it is made very clear in the text that an entity holding pseudonymised data (whether because it carried out the pseudonymisation itself, or because it already received the data in pseudonymised form) may only transfer such data to another entity if it has assessed and concluded that the receiving entity does not have the means to re-identify the data. The transferring entity must also inform the receiving entity that the data is pseudonymised (so

as to enable the receiving entity to adopt the specific measures applicable to pseudonymised data, even if such data does not constitute personal data from its perspective). These obligations must apply throughout the entire data transfer chain (that is, to all entities that receive and transfer pseudonymised data);

-That entities which fail to comply with these obligations may be held accountable, both by supervisory authorities and through judicial proceedings; this clarification is important because, in such cases, supervisory authorities will need to supervise and potentially impose fines for the processing of data that may not constitute personal data from the perspective of the entity under supervision; the difference in the nature of the data as perceived by the supervised entity must not be allowed to prevent supervisory authorities from acting.

These clarifications are essential to ensure the accountability of all entities involved in the processing and transfer of such data, so as to prevent situations of abuse or circumvention of the law. In particular, it is essential that it should not be possible for pseudonymised data, through successive transfers, to reach an entity capable of re-identifying it, thereby gaining access to personal data to which it would not otherwise have had access.

Round 5: Other GDPR provisions (The Presidency will invite delegations to express their positions and provide guidance on all other elements of the Presidency compromise text, as outlined in the following sections.)

Article 12(5)

Portugal can accept these amendments (in square brackets at the end of the provision), although it is necessary to understand what consequences they will have on recital (35) (which should be amended to ensure consistency with this new wording).

We consider it important, however, and in light of certain questions that have arisen throughout the discussion, that it be made clear – in particular in recital (35) – that data subjects are never required to justify the exercise of their rights, namely by indicating the reason underlying such exercise (in particular, data subjects are not required to indicate to the controller why they wish to access the information to which they are entitled through the exercise of the right of access).

Articles 33 and 35

We still have the doubts previously expressed regarding the involvement of both the Commission and the European Data Protection Board (EDPB) in the approval of the lists and templates. In particular, we consider that this dual involvement may raise significant questions for controllers when there is no coordination or agreement between the two Institutions. For example, if EDPB approves a template that is not adopted by the Commission, what would be the legal value of that template? Or if EDPB amends a list previously adopted by the Commission and the Commission does not adopt that amendment, are controllers required to comply with that list?

Article 37

We do not agree with this amendment, as we consider that controllers should continue to provide supervisory authorities with the contact details of their data protection officer (DPO).

First, because this obligation does not represent a significant administrative burden for controllers (nor has the proposal been accompanied by any data allowing us to conclude that such administrative burden is, in fact, significant), meaning that the benefits for controllers will be marginal.

Second, because this information is important for the work of supervisory authorities, since it provides a much clearer picture of the number of organisations that have appointed a DPO, as well as of how this role is being performed (for example, by revealing how many DPO's simultaneously perform their functions across multiple organisations).

Additionally, the contact details of the DPO provided to the supervisory authority are not, as a rule, the contact details publicly available on organisations' websites (namely the organisational email addresses through which data subjects may exercise their rights), but rather the direct contact details of the DPO. Making this information available to supervisory authorities enables direct and significantly faster contact, which is essential in urgent situations (such as in cases of personal data breaches), being also important for a range of other interactions between the supervisory authority and the DPO, and without which the work of supervisory authorities will become less efficient.

***

PUBLIC

FINLAND

SUOMI

15.6.2026 Antici group on Simplification: Finland's position

1.Data Act and data acquis

Finland is generally satisfied with the Council's work and can support the compromise proposal. **We can also support the proposed amendments to Articles 4(8) and 5(11) of the Data Act**, which aim to strengthen the protection of trade secrets, even though these changes may go beyond targeted simplification and do not necessarily improve legal certainty.
Given the extent of proposed changes to the trade secret provisions in the Data Act, Finland finds it necessary to retain the current wording of recitals 11-14, as well as the obligation to notify the competent authority.

2.P2B Regulation

Finland supports the Presidency's revised compromise text on the P2B Regulation.

3.Cyber provisions

Finland supports the revised compromise text on incident reporting. We consider that the proposed changes to Article 23b to mandate ENISA to develop an open-source solution for Member States could lead to more effective development and implementation of national entry points.

4.GDPR and cookies

General remarks:

- **Overall, Finland is satisfied with the Council's work and the compromise proposal concerning the GDPR. While remaining constructive, Finland would like to highlight some concerns related to certain changes introduced after Coreper.**
- **Finland states that the definition for personal data and pseudonymisation is a key/red line issue for Finland,** as possible amendments could change the scope and application of the GDPR and endanger the current level of protection.
- **Finland supports targeted amendments to simplify regulation and reduce burdens for SMEs while preserving the current high level of data protection. Any broader simplification efforts could be best pursued in a dedicated process and with an impact assessment.**
    - **Finland welcomes the COM to evaluate further simplification possibilities in the Digital Fitness Check evaluation.** Finland has provided a non-paper on possible areas to evaluate.
- At this stage of the negotiations, and in light of the objective to reach an agreement this month, Finland would find it challenging to assess entirely new proposals.
- **Concerning cookies, Finland has supported previous versions from April and May but Finland could, if there is majority, show flexibility to the recent proposed changes.** Deleting the provisions for automated and machine-readable consent is a missed opportunity but would not be a red line though it comes very close, especially if the COM continues the work on updating ePrivacy rules. The media sector should be taken account in this evaluation.

Definition for personal data and pseudonymisation

- **Concerning the definition for 'personal data', Finland primarily supports remaining the current definition in the GDPR.** The definition for 'personal data' is a key element in determining the scope and application of the Regulation and the level of data protection in the EU.
    - **Alternatively,** Finland can support the codification of the case law of the Court of Justice of the European Union, provided that all relevant case law is duly taken into account (as the COM proposal does not). For instance, especially paras 83-85 (and the case-law cited) in Case C-413/23 P should be taken account.
        - If the majority supports codifying case law in the definition, it is necessary that the Council work would continue during the Irish Presidency. Finland emphasises that these types of changes should be prepared with due caution.
- Finland **can primarily support the proposed Article 29a on the application of pseudonymisation, although Finland prefers the previous version.**
    - Finland can support the proposed amendments, **if para 2 is either removed or at minimum amended** (see also comments/suggestions concerning recitals).
        - **The wording somewhat differs from the language used in the GDPR and in CJEU case law and at least the last part of the para should therefore be amended** "- - *the data in question from being attributed to the data subject the data in question from being attributed to the data subject, effectively prevent persons other than the controller from identifying the data subject in such a way that, for them, the data subject is not or is no longer identifiable*".
        - Para 2 could be amended in a following way:

            "(2) The application of pseudonymisation to personal data may, depending on the circumstances of the case and provided that appropriate technical and organisational measures are put in place, prevent *the identification of a data subject by persons or entities other than the controller,* provided that these persons or entities do not have the means reasonably likely to enable the data subject to be identified."
    - **In para 4, Finland prefers the previous version**, especially as para 2 should be removed (there is a reference to para 2). **However, Finland can accept para 4, if para 2 is amended as proposed**.
    - Taking account that the EDPB is planning to adopt the guidelines in the July Plenary, **Finland can be flexible regarding the 6 months deadline**. However, it is somewhat questionable to propose short deadlines, as it is necessary to ensure that the EDPB can produce high-quality guidelines. This timeline should not constitute a precedent for other guidelines.
- Finland **can support the proposed recitals concerning pseudonymisation.**
    - **However, if the proposed para 2 is kept in Article 29a, the recitals should include referrals to the CJEU SRB case that clarifies that information which may be impersonal could become personal in nature where the controller puts them, or is likely to put them, at the disposal of other persons or entities who have means reasonably likely to enable the data subject to be identified.**
        - **The following could be added in the recitals:**

            'It should also be clarified that information, which is apparently impersonal, may still be considered personal data if the data subject can be identified with additional information obtained from another person or entity through means reasonably likely to be used making it possible to identify the data subject. In such circumstances, the fact that the information enabling the data subject to be identified is in the hands of other people does not prevent

that data subject from being identifiable for the controller. The Court of Justice of the European Union has also held that information which are in themselves impersonal may become personal in nature where the controller puts them, or is likely to put them, at the disposal of other persons or entities who have means reasonably likely to enable the data subject to be identified. It is apparent, in particular, that if that information is put at these other persons or entities' disposal – then this information is personal data for these persons and entities and, indirectly, for the controller. Accordingly, in so far as it cannot be ruled out that those persons or entities have means reasonably allowing them to attribute pseudonymised data to the data subject, such as cross-checking with other data at their disposal, the data subject must be regarded as identifiable as regards both that transfer and any subsequent processing of those data by those persons and entities. In such circumstances, pseudonymised data should be considered to be personal data.'

Personal data processing of AI training

- **Finland can support the proposed recital 33a concerning AI-processing. Finland welcomes that the Presidency has clarified the legal basis for public authorities as well, this is important for us. The proposed recital is balanced and brings clarity.**
    - Finland could have accepted clarifying legal basis in Article 88c as well, with certain clarifications and amendments suggested by the EDPB-EDPS Joint Opinion.

Data Breach Notifications

- **Finland <u>primarily supports 72 hours</u>, as a longer timeline could jeopardise the current level of protection.**
    - **However, <u>if the majority supports a longer period and if the definition for personal data remains intact</u>, Finland can show flexibility and accept 96 hours.**

Information obligations

- Concerning Article 3(4) (Article 12(5) GDPR), **Finland considers that the controller should bear the burden of proof when refusing malicious requests and primarily we support to keep this**. **<u>Therefore, Finland supports the compromise proposal (not the alternative).</u>** Finland considers that the alternative proposal that would lower this burden of proof, goes against the recent CJEU case law.
    - **However, <u>if majority supports a lower burder of proof and</u> <u>if the definition for personal data remains intact</u>, Finland can show flexibility and support this.**

Cookies

- **Finland supports the proposed "whitelist" for cookies and the placement in Article 5(3) ePrivacy directive.** FI welcomes the changes made concerning the provision on audience measurement. Finland can support that the DPAs would supervise cookie rules.
    - **However, Finland proposes to delete the new subpara e.** We are not sure of the meaning and the possible impacts of this para. The proposed recital text was not clear to our authorities.
    - **In addition, there are some technical and minor tweaks that are needed in the wording to ensure a consistent level of protection and that the text is clear and coherent.**
        - The wording "terminal equipment of *a natural person*" should be amended to "terminal equipment of a ***<u>subscriber or user</u>***".

- 3. Member States shall ~~not apply if the~~ ensure that the storing of information, or gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed when that person has given his or her consent, in accordance with Regulation (EU) 2016/679. Storing of information, or gaining of access to information already stored, in the terminal equipment of a **~~natural person~~ subscriber or user** without consent, and subsequent~~, and the information stored or accessed constitutes or leads to the~~ processing of personal data for the same purpose, shall be lawful to the extent it is strictly necessary for any of the following purposes:- -

  - It should be assessed, if the last para of article 5(3) could be moved to article 15a, which contains the rules on competent authorities.
    - Drafting suggestion: **In Article 15a, the following paragraph is added:**

      5. Member States shall designate the competent supervisory authority under Regulation (EU) 2016/679 for the supervision and enforcement of the rules under Article 5(3).

- Further, though we welcome the changes made to text regarding audience measurement, **recital 44b should be fully aligned with the European Media Freedom Act**, as Finland has previously commented. Finland calls for the deletion of requirements that would undermine the conditions necessary to ensure comparability and verifiability of audience measurement, thereby conflicting with article 24(1) of the EMFA.
  - Measuring the audience of an online service in order to create anonymous aggregated information about the usage of an online service, where it is carried out by the provider of that online service, or by a third party such as a market research company or a Joint Industry Committee, acting together with or on behalf of this provider, also referred to as 'audience measurement', means ~~the~~ processing such data and information to obtain insight into the performance and use of the online service in an anonymised, aggregated and general manner. This includes the performance of audience by an entitled and independent third party performing audience measurement as defined in Regulation (EU) 2024/1083. The aggregated information should not relate to a specific data subject and should therefore be anonymous aggregated information. The anonymous aggregated information can be shared with third parties, including companies and non-commercial organizations. Processing of personal data with the aim of creating anonymous aggregated information contributes to the sustainability of the media ecosystem as highlighted in Regulation 2024/1083 and should be subject to strict limitations designed to ensure that the personal data is not reused for providing personalised advertising, profiling or other unrelated purposes. The personal data initially collected should not be further processed for another purpose, **~~combined with data from other services from the provider of the online service or from a third party, such as analytics information from other websites or apps,~~** or shared with third parties.

- **Finland has supported the Presidency's compromise texts on automated and machine-readable consent.**
  - **Primarily**, Finland supports keeping the provisions as they ensure that data subjects have opportunity to influence the collection and processing of their personal data an enhance transparency. Finland still considers that a consensus could be found combining the previous versions from April and May.

- **Alternatively**, Finland can show flexibility to delete the provisions, although it is a missed opportunity to remove cookie fatigue. However, Finland emphasizes that the COM should continue evaluating and updating ePrivacy regulation in Digital Fitness Check, accompanied with a broad impact assessment, including the impacts to the media sector.

Automatic exchange of tax information

- **We support the Presidency on this and FI cannot support the Spanish proposal on Automatic exchange of tax information**.
- **The COM could possibly evaluate this further, but overall Finland is cautious whether these types of changes are needed and/or whether these could change the nature of Article 49 of the GDPR.** Article 49 is meant for derogations for specific situations and this proposal could mean continuous, rather than exceptional, exchange of information. The COM should also take a look at EN108+.

***

PUBLIC