Council of the European Union
General Secretariat

Interinstitutional files:
2025/0360 (COD)

Brussels, 19 March 2026

WK 3736/2026 INIT

LIMITE

SIMPL
ANTICI
DATAPROTECT
CYBER
TELECOM
CODEC
PROCIV
COMPET
MI

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

WORKING DOCUMENT

From:	General Secretariat of the Council
To:	Antici Group (Simplification)
Subject:	Consultation on Omnibus VII (GDPR/P2B/ePrivacy) digital rules - related to AGS meeting of 27.02.26 (deadline 18.03.26) - first compiled comments: CZ, DE , EE, FI, HU, IE, IT and NL.

Delegations will find attached the compiled comments from the following Member States: CZ, DE , EE, FI, HU, IE, IT and NL on GDPR / P2B and ePrivacy calls for written comments. Additional comments (consolidated table) will follow as ADD1.

Omnibus VII Digital rules
GDPR-P2B-ePrivacy
AGS meeting of 27 Feb. 2026
Table for written comments launched on 27.02 (GDPR-P2B) + updated table on 13.03.26 (ePrivacy) - deadline: 18 March 2026 cob

Table of Contents

CZECHIA

ČESKO

CZ Written input on the first Presidency compromise text of the Digital omnibus

Czechia shares, in writing, the speaking points prepared for the AGS meeting on 27 February as requested during the meeting:

*CZ on the Presidency compromise text on the **GDPR** part of the Digital omnibus*

- We appreciate the efforts made. However, we believe that certain amendments that would remove parts of the Commission's proposal would be worth revisiting, such as the definition of scientific research in the text of the GDPR.
- We believe it may be beneficial to allow for further discussion in order to maintain their intended added value.
- We do not believe that interests of the EU are well served by severely restricting advantages for scientific research. We also have concerns that regulating biometric verification in dozens of laws would be generally helpful. We believe that European industry needs more efficient simplification.
- On the other hand, Czechia welcomes the repeal of the personal data definition revision.
- We would like to ask the Presidency to find a way or venue to address certain of the deleted provisions in detail, on expert level, in order not to lose potential added value.
- We also believe that it is necessary to clarify the relation between DSA and GDPR regulation. For this purpose, we propose to explicitly mention the liability exemption in the article 4.

*CZ on the Presidency compromise text on the **P2B** part of the Digital omnibus*

Regarding the changes made in the P2B regulation part, we would like to stress that if EC plans to allow P2B regulation to work in some form after it is repealed, we are asking for the following parts of the regulation to be preserved:

- Art. 1) – Subject matter and scope - should be kept in the text. We strongly believe that any regulation without subject matter and scope cannot be enforced.
- Art. 2) para 3 - definition of provider – providers need to be defined for similar reasons as the art. 1. Since article 4 requires providers to follow certain rules we need to understand who are providers to follow these rules.
- Art. 2) para 10 – definition of terms and conditions as they are referred in art. 11 para 3, which is supposed to be left in.
- Art. 2) para 13 – definition of the durable medium – this concept is again used in the art. 4 and its definition is needed for effective enforcement.
- Art. 19) - Entry into force and application – since the omnibus plans to keep requirements for enforcement, it is necessary to keep this article as well for functioning of the regulation.

Additionally, we would kindly ask the Council Legal Service to consider our commentary. We are open to explain our points on working level, if needed.

*CZ on the Presidency **Discussion note***

***Question1**: Delegations are invited to express their views on the proposed provisions relating to:*

The processing of personal data in the context of the development and operation of AI systems based on the lawful ground of legitimate interest (Art 88c).

- Czechia is generally supportive of Article 88c. We believe that relatively small changes could clarify that all conditions of Article 6(1)(f) GDPR apply, such as by saying "subject to the conditions of Article 6(1)(f) of Regulation (EU) 2016/679" without repeating its content and by limiting second subparagraph to activities not already required by other provisions of GDPR.
- Additionally, as we already indicated in the drafting suggestions, we believe that this Article should be moved to Article 6a as it is systemically closer to legal grounds for processing.
- Depending on position of the Article and its final wording, any new obligations should be subject to regular GDPR sanctions.

The proposed new derogation from the prohibition on processing special categories of personal data (Article 9 (2)(k) and (5).

- Czechia considers Commission's proposal regarding amendments to Article 9 feasible. We believe that the provisions of Article 9(2)(k) and Article 9(5) are linked together very clearly.
- Relationship to Article 4a of AI Omnibus should be mentioned in a recital, not in a legal text. Contrary to the EDPB and EDPS joint opinion, we do not believe that specific terminology (that would become autonomous notion of EU law) or specific documentation requirements are systemically beneficial.

Question 2: *Delegations are invited to express their views and possible suggestions on the additional exemptions from consent requirement for aggregated information for measuring the audience and for maintaining or restoring the security of a service or the terminal equipment. In particular, the Presidency invites delegations to share their positions on the two following points:*

- In general, Czechia is supportive of Article 88a, but we should make clear that scope of paragraphs 1 and 2 correspond to the scope of ePrivacy, that is to provision of relevant telecommunication services. We can accept insertion of "purposes" in paragraph 3 as proposed by EDPB and EDPS. Sanctions for all infringements of this Article should be ensured as well.

Should the exemption for audience measurement remain limited to its originally intended scope (e.g. the controller of a service requested by a data subject) or more open, in particular concerning to the actors it should cover (other parties in the measurement value chain that are not processors of the controller)?

- The exemption for audience measurement should be primarily limited to the controller (and processor) of a service requested by a data subject, but we are open to discuss this topic more in detail.

Should the exemption for safeguarding the security of a service or a device be further specified and delineated?

- The exemption for safeguarding the security of a service or a device should definitely be further specified. We are flexible as to the method – we could include specific examples or refer to information technology security or to elaborate this issue in a recital.
- Additionally, Czechia would like to express its openness to exploring whether the Act could include an incentive to use less-intrusive forms of advertising online, in particular by supporting contextual advertising, as this is also suggested by EDPB and EDPS. In case of consensus, Czechia is ready to with other MS to work on specific proposals.

Question 3: *Delegations are invited to share their views and overall position on the proposed new Article 88b GDPR on automated and machine-readable indications of data subject's choices with respect to processing of personal data in the terminal equipment of natural persons.*

- We are generally supportive of Article 88b. In terms of data protection, the true extent of paragraphs 2 and 4 should be explained in recitals. Most importantly, sanctions for all infringements of this Article are necessary, keeping in mind a diverse range of obliged entities.

***

GERMANY

DEUTSCHLAND

DE preliminary comments:

Omnibus VII (Digital Omnibus), first compromise text

Proposal for a Regulation amending Regulations (EU) 2016/1679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854, (EU) 2024/1689 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus)

With regard to the partial compromise text on GDPR, DE would like to emphasize that amendments to the text should reflect the simplification agenda and that amendments must be crafted carefully, so that the Omnibus provides legal certainty and normative clarity in a short period of time. Some of our important points are still missing, while most of our concerns we submitted on 30/01 were addressed. DE is grateful for that.

In general, it is important that the Omnibus VII achieves noticeable improvements and simplifications, especially for SMEs, SMCs, start-ups, science and research, public bodies, and volunteers – while maintaining the level of protection provided by the AIA and the GDPR. Specifically, we want ensure that small and medium-sized enterprises, low-risk data processing and particular non-commercial activities can be excluded from the scope of the GDPR, insofar as this is possible in accordance with EU primary law and international law.

Some topics we consider crucial are partially covered by the compromise text, e.g. privileges for research, abusive access requests, and the modification of data breach notifications. DE thanks the Presidency for including these topics. Unfortunately, other items are not yet or not any more included in the compromise text, mainly:

- commercial interest in the field of research, Art. 4 (38), Art. 5 (1) b, Art. 13 (5),
- rules on pseudonymisation/anonymisation (Art. 4),
- reduction of information requirements with regard to low-risk-operations, Art. 13 (4),
- termination of proceedings of supervisory authorities for reasons of expediency, Art. 57 (1) f,
- accountability of manufacturers and suppliers, Art. 25,
- regulatory sandboxes, Art. 57 (1) w,
- level of protection, Art. 32.

1. Definition of personal data and pseudonymization

Article 3(1), Article 3(10), Article 3(14), Recital 27, Recital 27a

The incorporation of the SRB-judgement in the text of the GDPR is crucial to implement the concept of relative anonymity. DE does however take concerns seriously that specific elements of the COM-proposal on Art. 4 did not properly reflect the jurisdiction of the CJEU. Moreover, any amendment must be crafted carefully so that it doesn't lead to further legal uncertainties. That should, however, not result in a full deletion of the proposed amendment to Art. 4 (1). Instead, DE suggests to use the wording of the SRB-judgment and of recital 26 of the GDPR. DE submitted an according drafting proposal to the Presidency.

DE supports the deletion of Art. 41a and the corresponding addition of Art. 70 instead of Art. 41a. The wording should also include guidelines on anonymisation, and not be limited to pseudonymisation. Besides that, DE proposes to clarify whether the process of anonymisation as such represents a data processing operation, consequently requiring in itself the existence of a legal basis within the meaning of Articles 6 or 9 GDPR.

2. Scientific research and purpose limitation

Article 3(1), Article 3(2), Recital 28, Recital 29, Recital 32

While DE welcomes the deletion of the legal definition of "scientific research" in Art. 4 (38), we are of the opinion that scientific research in the public interest, which is also aiming to further a commercial interest or that may also be used for commercial interests, should explictly be covered with respect to the privileges under the GDPR.

In Recital 29 it is stated that scientific research activities should concur to public interest and well-being, prevent individuals from being subjected to harm or other adverse effects due to participating in scientific research and include – among other things – the respect for human autonomy and the notion of consent to participate in research. In order to avoid effects on the privileges for scientific research (e.g. Art. 6 GDPR), it should be ensured that "notion of consent" is not equivalent to the data protection consent ("consent to processing").

3. **New derogation from the prohibition to process biometric data**

Article 3(3), Recital 34

DE does not have any objections on the proposal.

4. **Exercise of the individual's right of access and exemption from information obligations**

Article 3(4), Article 3(5), Article 3(6), Recital 35, Recital 36, Recital 37

Concerning Art. 13 (4), DE welcomes the improvements, but it still seems too complicated to have the simplification effect intended. We refer to the DE proposal.

5. **Automated decision making**

Article 3(7), Recital 38

DE agrees with EDPB/EDPS and the Presidency that the following should still be clarified: When assessing whether a decision is necessary for entering into, or performance of, a contract between the data subject and a data controller (Article 22(2)(a) GDPR) it should not be required that the decision could be taken only by solely automated processing. The following clarification should be added to Recital 38 of the proposal: "The fact that the decision could also be taken by a human does not prevent the controller from taking the decision by solely automated processing. When several equally effective processing solutions exist, the controller should use the less intrusive one."

6. **Data breach notification and data protection impact assessment**

Article 3(8), Article 3(11), Recital 39

Article 3(9), Article 3(11), Recital 40

DE considers the risk level "high risk" as too high. DE proposes a level "more than a low risk". To consider the specific situation of SMEs, DE proposes to introduce an exemption for them.

DE regrets that the deadline to notify data breaches is again lowered to 72 instead of 96 hours. DE would prefer a deadline of 96 hours to consider esp. weekends and public holidays. DE appreciates that the EDPB, instead of the Commission, should be responsible to draft templates.

7. P2B

DE generally supports the proposal to repeal the P2B-Regulation. But in order to protect small and medium-sized enterprises, Art. 3 and 5 should also continue to apply until 31 December 2032. The evaluation of the DSA should then assess whether an adaptation of the DSA is necessary to maintain the protection of SME.

On the questions of the discussion note:

Question 1: delegations are invited to express their views on the proposed provisions relating to

- **the processing of personal data in the context of the development and operation of AI systems based on the lawful ground of legitimate interest (Art 88c).**
- **the proposed new derogation from the prohibition on processing special categories of personal data (Article 9 (2)(k) and (5).**

The proposals on the processing of personal data in the context of the development and operation of AI should be subject to further discussions and drafting. The goal should be a comprehensive and coherent regulation in this area. In order to provide more legal clarity, the requirement that the controller does not aim to process special categories of personal data should be covered in the text of the regulation itself and not only in the recital.

Processing of personal data in the terminal equipment of a natural person and other ePrivacy related provisions

Article 3(15) – new Articles 88a and 88b GDPR, Article 5 ePrivacy-Directive

General remarks:

DE welcomes the Presidency's intent to discuss the Commission's proposals referring to privacy protection of information on terminal equipment. DE supports the intention to find a regulation to simplify procedures for end-users to choose their settings, which strengthens their autonomy and should lead to a better protection of personal data and

privacy and help against “consent fatigue”. However, DE is still in the process of preparing a final position on this.

<u>Question 2</u>: delegations are invited to express their views and possible suggestions on the additional exemptions from consent requirement for aggregated information for measuring the audience and for maintaining or restoring the security of a service or the terminal equipment. In particular, the Presidency invites delegations to share their positions on the two following points:

- **Should the exemption for audience measurement remain limited to its originally intended scope (e.g. the controller of a service requested by a data subject) or more open, in particular concerning to the actors it should cover (other parties in the measurement value chain that are not processors of the controller)?**
- **Should the exemption for safeguarding the security of a service or a device be further specified and delineated?**

The DE position on the regulation in detail is still to be finalized. However, in general DE supports the proposed additional exemptions for audience measuring and security, if the processing in scope of such exceptions is clearly delimited to what is strictly necessary (see EDPB-EDPS Joint Opinion 2/2026, point 101). But further details regarding legal certainty, opt-out options and restrictions on further processing still need to be examined. The new exemptions should in any case apply to all information in terminal equipment regardless whether these are personal data or not. So, in this regard the ePrivacy-Directive should be aligned with the Commission’s proposal for Art. 88a. Therefore, the two additional exemptions should also be added in Art. 5 (3) e-Privacy. As a general remark, these exemptions should be limited as described before. Keeping these conditions, the exemptions should furthermore be designed to lead to a significant simplification for users and costumers and to a reduction of consent banners users and costumers need to interact with while preserving the level of privacy protection. This question should be further examined. Does - for example - the exemption for security purposes meet the demand of the automotive industry to store and access information in terminal equipment in cars?

<u>Question 3</u>: Delegations are invited to share their views and overall position on the proposed new Article 88b GDPR on automated and machine-readable indications of data subject's choices with respect to processing of personal data in the terminal equipment of natural persons.

The DE position on Article 88b is still to be finalized. However, we would like to know how far Article 88b could prevent service providers from asking end-users of their services for consent. Furthermore, how can be ensured that providers of commercial web-browsers with technical obligations regarding consent can stay neutral between users and service providers?

***

ESTONIA

EESTI

Comments by Estonian delegation to the Presidency Compromise Text and Discussion Note for AGS meeting on 27/02/2026

Estonia expresses its gratitude for being given the opportunity to submit written observations regarding the Presidency Compromise proposal, as well as to respond to the questions outlined in the Discussion Note.

Comments on Compromise Text

1. Definition of personal data and pseudonymisation

Article 3(1), Article 3(10), Article 3(11), Recital 27, Recital 27a

We can support the Presidency Compromise.

2. Scientific research and purpose limitation

Article 3(1), Article 3(2), Recital 28, Recital 29, Recital 32

We would welcome the introduction of a common definition of 'scientific research' under the GDPR.

3. New derogation from the prohibition to process biometric data

Article 3(3), Recital 34

We would appreciate further clarification on how the requirement that the means of verification remain exclusively under the control and possession of the data subject can be fulfilled. Additionally, referencing safeguards established by national law may not contribute effectively to the goal of minimizing fragmentation in our opinion.

4. Exercise of the individual's right of access and exemption from information obligations

Article 3(4), Article 3(5), Article 3(6), Recital 35, Recital 36, Recital 37

We can support the Presidency Compromise.

5. Automated decision making

Article 3(7), Recital 38

We would be pleased to continue discussions on this matter. While we are open to supporting the removal of the prohibition in principle, as proposed by the Commission, we believe that, for systemic reasons, it would be beneficial for the article to be clearly articulated as a right of the data subject.

6. Data breach notification and data protection impact assessment

Article 3(8), Article 3(11), Recital 39

Article 3(9), Article 3(11), Recital 40

Estonia is of the view that the threshold for notification of breaches should be linked to risks which cannot be considered minor.

7. P2B

Estonia supports the proposal to repeal the P2B Regulation. In the interest of legal clarity, we endorse the approach whereby certain provisions of this Regulation, as set out in the Digital Omnibus, would remain in force until the relevant EU legal acts referring to them are amended, but no later than 31 December 2032.

Comments on Discussion Note

Processing of personal data for the development and operation of AI systems

Article 3 (3) – new point 9(2)(k) GDPR, new paragraph 9(5) GDPR

Article 3(15) – new Article 88c GDPR

- the processing of personal data in the context of the development and operation of AI systems based on the lawful ground of legitimate interest (Art 88c)

Estonia respectfully maintains that the GDPR should continue to be applied in a technologically neutral manner, recognising that the development of artificial intelligence forms part of broader technological progress and research. It is within this framework that the following observations are offered.

We are of the opinion that the development and operation of AI systems encompass distinct data processing activities, each necessitating its own appropriate legal basis. Although there may be similarities between these legal grounds, the specific conditions attached to each can vary.

Furthermore, Estonia notes that the operation of AI systems may be governed by additional legal bases, including those provided by national legislation. In our view, Article 88c should focus exclusively on the development of AI systems, whilst the operation of such systems should rely on the legal grounds stipulated in Articles 6 and 9 of the GDPR.

- the proposed new derogation from the prohibition on processing special categories of personal data (Article 9 (2)(k) and (5).

Estonia considers that, in instances where the operation of AI systems necessitates the processing of special categories of personal data, legitimate interest should not be relied upon as the legal basis for such processing. We recognise that AI operation has become integral to organisational and enterprise activities, and believe it is important that these activities continue to adhere to the established legal framework. Allowing legitimate interest to serve as the sole basis for the operation of AI, without extending the same approach to other processes, raises questions regarding consistency and fairness. Additionally, there is a potential concern that broadly interpreting AI operation could lead to the classification of a wide range of technological activities under this category, thereby permitting the processing of special categories of personal data on the grounds of legitimate interest. Estonia, therefore, encourages a careful and balanced approach in considering these matters.

Processing of personal data in the terminal equipment of a natural person and other ePrivacy related provisions

Article 3(15) – new Articles 88a and 88b GDPR

Article 5

- Should the exemption for audience measurement remain limited to its originally intended scope (e.g. the controller of a service requested by a data subject) or more open, in particular concerning to the actors it should cover (other parties in the measurement value chain that are not processors of the controller)?

We support that the exemption for audience measurement under Article 88a(3)(c) should be retained within its originally intended scope, specifically applying to the controller of a service as requested by the data subject.

- Should the exemption for safeguarding the security of a service or a device be further specified and delineated?

Estonia suggests that the exemption relating to safeguarding the security of a service or device would benefit from further clarification and definition. In our view, the current wording may be somewhat broad, and introducing a proportionality requirement could help ensure greater precision.

- Views and overall position on the proposed new Article 88b GDPR on automated and machine-readable indications of data subject's choices with respect to processing of personal data in the terminal equipment of natural persons.

Overall, Estonia is supportive of the introduction of the new Article 88b GDPR, which sets out requirements for the use of automated and machine-readable indications of data subjects' choices regarding the processing of personal data in the terminal equipment of natural persons. We would respectfully propose that Article 88b(1) be amended to ensure that online interfaces provide data subjects not only with options to grant or refuse consent, but also with a straightforward means to withdraw consent at any time.

In line with observations made by other Member States, we would also like to express some reservations regarding the potential complexity arising from the coexistence of two parallel systems. We believe that further consideration could be given to how best to achieve simplification and coherence in this area.

***

IRELAND
ÉIRE

IE Comments on First Compromise Text – P2B

27th February 2026

IE welcomes the opportunity to provide observations on the First Compromise Text on Omnibus VII – Digital.

IE has significant concerns about the proposed repeal of the P2B Regulation. We believe that this repeal would weaken protections for business users, particularly small and micro-businesses, without ensuring that equivalent safeguards are replicated elsewhere.

P2B Regulation was designed to address specific imbalances between online platforms and business users. It ensures fairness in platform-business relationships, transparency around terms and conditions, and access to effective redress mechanisms. While DSA and DMA introduce important safeguards, they do not fully replace the protections provided by P2B, potentially creating regulatory gaps rather than merely providing simplification.

The repeal of Article 3(2) P2B is particularly concerning as it requires platforms to provide clear advance notice of changes to terms and conditions with a minimum 15-day notice period. The absence of this obligation in DSA or DMA would undermine business users' ability to plan and adapt, disproportionately affecting small businesses reliant on platform access.

The removal of Articles 11 and 12 P2B, which provide low-cost dispute resolution mechanisms, is another area of concern. The DSA's out-of-court dispute settlement mechanism (Article 21) is narrower and does not cover a wide range of platform-business disputes, potentially leaving many business users without an affordable route to resolve issues.

The experience in Ireland indicates a steady increase in P2B complaints since 2023 and growing awareness and use of P2B rights by business users. Current findings would likely reflect more mature enforcement structures and higher engagement.

***

ITALY

ITALIA

Reference is made to the document "WK02800.en26 explanatory note – testo di compromesso"

P2B

Taking into account the Member States' interventions at our previous AGS meeting on 16 January, and written comments, the Presidency takes that most delegations support the Commission proposal on the repeal of the P2B Regulation. Therefore, no changes were made to Article 10(1) and (2). In order to further clarify the text, recital 59 was amended to provide reasons for the need repeal Articles 4 and 11 and certain provisions of Article 2 at a later stage.

Detailed explanatory table

Recital 59: Redrafting to add a reference on keeping the necessary level of protection for business users and fixing a fixed date for the enforcement application of Article 15.

The P2B Regulation plays a distinct and complementary role within the EU digital regulatory framework: its objective is to ensure transparency, fairness and effective redress for business users of online intermediation services and for corporate website users in relation to online search engines.

The DMA and DSA have different targets and scopes. They do not provide the same substantive obligations, nor do they offer the subsidiarity and proximity afforded by the P2B Regulation. Therefore, they cannot offer the same level of protection in such situations.

The P2B Regulation specifically addresses the commercial relationship between platforms and business users, recognising the structural imbalance in bargaining power that characterises these relationships and the dependence of businesses (in particular SMEs) on online platforms as essential gateways to consumers.

These safeguards include legal certainty and predictability of contractual terms, protection against arbitrary suspension or termination, transparency of ranking and visibility, clarity on differentiated treatment and distribution channels, transparency regarding access to and use of data, and effective dispute resolution mechanisms.

The limited amendments reflected in the proposed compromise texts do not address our fundamental concerns that business users would lose essential protections under Articles 3, 4, 5, 6, 7, 8, 9 and 11 of P2B Regulation.

Simplification should not undermine essential protections for European SMEs, including transparency of terms and conditions, predictability of changes, clarity of ranking parameters and on differentiated treatment, and effective dispute resolution mechanisms tailored to commercial disputes.

We consider it necessary to ensure the continued and permanent application of a number of relevant provisions in order to safeguard these protections. We therefore call on the European Commission to adopt a targeted and proportionate approach in reviewing the P2B Regulation, balancing the need to reduce unnecessary complexity with the imperative to preserve essential safeguards that ensure fair and transparent business relationships. Ensuring durable and predictable protection for business users, and especially for SMEs, is not only a matter of legal compliance but also a strategic necessity to support the competitiveness, resilience, and integrity of the European internal market.

The substantive provisions identified below are crucial to guaranteeing meaningful protection for business users, while strong national enforcement mechanisms are indispensable to prevent regulatory gaps that could undermine the Regulation's objectives:

- ***Clarity of Terms and conditions (Article 3.1):*** the transparency obligations set out in Article 3 offer considerable protection to business users, particularly since non-compliant terms and conditions are automatically null and void. The repeal of Article 3 would remove an important safeguard for business users against arbitrary enforcement, thereby depriving them of the right to be informed in advance, in a clear and comprehensible manner, of the potential conditions under which the service may be restricted, irrespective of the size of the platform.
- ***Right to termination and notice period in case of changed T&C's (Article 3.2)***: without Article 3.2, business users will no longer be informed before terms and conditions are changed and they will lose the right to terminate the agreement on these grounds. This harms the business user's position in their relation to the platform by weakening contractual transparency and predictability.
- ***Notice period in case of termination (Article 4.2)***: the repeal of this provision would lead to business users no longer being granted a notice period before their access to the platform services is terminated. This prevents them from taking appropriate measures or challenging the termination decision before it takes effect, rendering them vulnerable to arbitrary decisions by the platform.
- ***Ranking (Article 5)***: the repeal of this provision would shift the enforcement of these issues away from national regulators and risk reducing the accessibility and effectiveness of redress for SMEs operating on platforms.
- ***Differentiated treatment (Article 7)***: without this provision, platforms are free to put business users at a disadvantage where they compete with the platform's own products and services, or with other business users controlled by the platform, without disclosure. Because there is no obligation of any kind to be transparent, business users will not be able to know whether, how and why this is happening.
- ***Complaint handling system (Article 11)***: the repeal of Article 11 severely limits the business user's ability to challenge unfair or illegal conduct through an internal complaint-handling system. While they will still have access to an internal complaint handling system under the DSA, its scope is limited to illegal content or alleged violations of the platform's terms and conditions. This in turn leaves the business user without quick and effective remedies against P2B non-compliance by the platform, technological issues or any other measures taken by the platform in the context of providing intermediation services that affect the business user.

These protections are not replicated under DSA/DMA. In particular, the DSA does not provide advance notice of contractual changes, nor does it establish complaint-handling mechanisms for disputes arising from the overall commercial relationship, such as technical or operational issues, beyond matters related to illegal content removal or account suspension. Moreover, the DSA does not ensure meaningful transparency on ranking parameters for the purpose of commercial optimisation by business users. Similarly, while the DMA introduces far-reaching obligations in areas such as self-preferencing, parity clauses and data use, its application is limited to platforms designated as gatekeepers.

The repeal of the P2B Regulation would also mark a shift concerning the enforcement of the rules on online platforms. Article 15 explicitly empowers Member States to enforce its provisions, ensuring proximity between the enforcement body on the one hand and the user that is protected on the other hand, in line with the principle of subsidiarity.

In this regard, the P2B Regulation operates as a complementary governance instrument. Whereas the DMA establishes a centralized enforcement model for gatekeepers at Commission level, and the DSA relies predominantly on the country-of-origin principle for oversight of intermediary services, the P2B Regulation provides a more granular and business-user-focused framework enforced directly by Member States. **In conclusion, repealing the P2B Regulation on the basis of an alleged absorption of its obligations by the DSA/DMA would reduce the current powers of national authorities limiting their ability to intervene and ultimately operating to the detriment of business users, who would face a wider protection gap.**

Document WK 2802/2026 INIT – QUESTION 2

Question 2: Given the above and in order to better understand delegations' views and identify avenues for possible compromises, the Presidency considers necessary to hold a further discussion on the proposed extension of the exemptions from consent requirements.

□ Question 2: delegations are invited to express their views and possible suggestions on the additional exemptions from consent requirement for aggregated information for measuring the audience and for maintaining or restoring the security of a service or the terminal equipment. In particular, the Presidency invites delegations to share their positions on the two following points:

□ Should the exemption for audience measurement remain limited to its originally intended scope (e.g. the controller of a service requested by a data subject) or more open, in particular concerning to the actors it should cover (other parties in the measurement value chain that are not processors of the controller)?

□ Should the exemption for safeguarding the security of a service or a device be further specified and delineated?

If the exemption for audience measurement remains limited to its originally intended scope (e.g. the controller of a service requested by a data subject) then measurement systems developed in compliance with industry standards within self-regulatory bodies such as, for example Joint Industry Committees (JICs) and/or so-called "research companies" would be excluded from this exemption.

This provision appears to conflict with Article 24 (1) of the EMFA Regulation, which sets out a series of provisions regarding audience measurement for all providers of audience measurement systems (proprietary audience measurement and non-proprietary audience measurement).

In particular, the exemption rule under Article 88a of the Digital Omnibus appears to conflict with the principles of comparability and verifiability of audience data under Article 24 of the EMFA between different audience measurement systems, since data from measurement systems developed in compliance with industry standards within self-regulatory bodies, such as JICs or research companies, would be less significant and reliable than data from proprietary audience measurement system providers. In fact, since the results of audience measurement activities are aggregated statistical processes, making such statistical processes dependent on user consent data could compromise the objectivity of the process and potentially distort the final outcome of the survey. This distortion would therefore make it difficult to apply the principles of comparability and verifiability of audience data between providers of proprietary audience measurement systems (typically the controller of a service requested by a data subject) and audience measurement systems developed in compliance with industry standards within self-regulatory bodies, such as JICs.

Finally, it is also useful to point out that the current proposal seems to depart also from the draft proposal of the Regulation of 10 February 2021 “ePrivacy”, which suggested a modernization of Article 8 of Directive 2002/58/EC (so-called “ Directive ePrivacy”), including further exceptions to the obligation of consent – one of which, specifically relating to measurement systems of the audience: “*The use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware, other than by the end-user concerned shall be prohibited, except on the following grounds: […] it is necessary for the sole purpose of audience measuring, provided that such measurement is carried out by the provider of the service requested by the end user, or by a third party, or by third parties jointly on behalf of or jointly with provider of the service requested provided that, where applicable, the conditions laid down in Articles 26 or 28 of Regulation (EU) 2016/679 are met*”.

***

HUNGARY
MAGYARORSZÁG

HU comments on guiding questions in Presidency Discussion Note (WK 2802/26)

Question 1: *delegations are invited to express their views on the proposed provisions relating to*
- the processing of personal data in the context of the development and operation of AI systems based on the lawful ground of legitimate interest (Art 88c).
- the proposed new derogation from the prohibition on processing special categories of personal data (Article 9 (2)(k) and (5).

As the EDPB/EDPS Joint Opinion highlights, the current text of the GDPR also allows for the use of legitimate interest as a legal basis, so simply stating this within the framework of the GDPR is not justified. The EDPB/EDPS Joint Opinion therefore recommends that the proposal should clearly define the added value of the amendment. In this regard, Hungary agrees with the position, as follows:
– when drafting the provision, efforts should be made to make it clear that the conditions under Article 6(1)(f) of the GDPR must continue to apply in full (by deleting the "where appropriate" part),
– it is also recommended to indicate that the right to object applies as a new and independent (sui generis) right to object, and it could be considered to place it under Article 21 of the GDPR (as a special objection option for AI systems),
– the possibility should be provided for data subjects to be informed in advance about such data processing (since it may be difficult to remove data afterwards if it is not linked to the data subject).

Question 2*: delegations are invited to express their views and possible suggestions on the additional exemptions from consent requirement for aggregated information for measuring the audience and for maintaining or restoring the security of a service or the terminal equipment. In particular, the Presidency invites delegations to share their positions on the two following points:*
-Should the ***exemption for audience measurement remain limited*** *to its originally intended scope (e.g. the controller of a service requested by a data subject) or more open, in particular concerning to the actors it should cover (other parties in the measurement value chain that are not processors of the controller)?*
-Should the ***exemption for safeguarding the security of a service or a device be further specified*** *and delineated?*

On the one hand, Hungary supports the objective of simplifying the rules on the protection of terminal equipment and addressing consent fatigue, as also acknowledged by the EDPB and the EDPS in their Joint Opinion. On the other hand, creating a double regime (keeping relevant provisions in the ePrivacy directive and inserting it in the GDPR as well risks creating a difficulty of application to the stakeholders and create more burden than simplification). If we maintain the double regime we would welcome the Commission's proposal on how the browsers would distinguish between a legal and natural person, as we do not yet see a solution for this today.
We consider that any additional exemptions from the consent requirement must remain strictly limited and clearly delineated.
As regards audience measurement, the exemption should remain confined to what is objectively necessary and proportionate, and preferably limited to the controller of the service requested by the data subject. Extending it to other actors in the broader measurement value chain could risk weakening the consent principle and create potential circumvention paths.
With respect to the security exemption, Hungary supports its inclusion, but it should be narrowly framed and strictly limited to what is necessary to maintain or restore the security of a service or device. The notion of "security" should not be interpreted too broadly. Clear drafting will be essential to preserve legal certainty and maintain a high level of protection.

***Question 3**: Delegations are invited to share their views and overall position on the proposed new Article 88b GDPR on automated and machine-readable indications of data subject's choices with respect to processing of personal data in the terminal equipment of natural persons.*

Hungary welcomes the objective of reducing the proliferation of cookie banners and strengthening user control through automated and machine-readable preference signals, which is also generally supported by the EDPB and EDPS
However, the effectiveness of this mechanism will depend on enforceability and clarity. Supervisory authorities must be equipped with effective corrective powers.
Without practical enforceability and robust technical standards, such a system risks remaining largely formal. We therefore consider that standardisation must be clear and timely, transparency obligations must remain strong, and the proposed exemption for media service providers should be carefully reconsidered, we do not think it is appropriate to put it here, and it is also criticized by a number of stakeholders.

***

NETHERLANDS

NEDERLAND

NL written answers to discussion note on GDPR

Processing of personal data for the development and operation of AI systems

Article 3 (3) – new point 9(2)(k) GDPR, new paragraph 9(5) GDPR

Article 3(15) – new Article 88c GDPR

***Question 1:** delegations are invited to express their views on the proposed provisions relating to*

*- the processing of personal data in the context of the development and operation of AI systems based on the lawful ground of legitimate interest **(Art 88c).***

- As the EDPB has noted in its opinion, Article 88c is not necessary and can lead to legal uncertainty.
- There are concerns among a majority of the Dutch House of Representatives about this article.[1]
- A separate discussion about Article 88c seems more suitable.

NL notes that the proposed article 88c deviates from the EDPB's Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models, partly because it fails to provide that the reasonable expectations of data subjects must be taken into account, such as whether the personal data were already public and whether there is a relationship between the data subject and the controller. In addition, while the aim of this article is to clarify the current GDPR rules, it raises new questions. For example regarding the "unconditional right to object" and how the article relates to the EDPB Opinion 28/2024.

*- the proposed new derogation from the prohibition on processing special categories of personal data **(Article 9 (2)(k) and (5).***

- NL is concerned that this proposed novel exception to the prohibition on the processing of special categories of data in the proposed Article 9(2)(k) and (5) may significantly reduce the protection of the processing of special categories of personal data in the development and operation of an AI system.
- Operators of AI systems would be allowed to process special categories of personal data if its removal would cause disproportionate effort. This reverses the protective logic of data protection law and risks creating a perverse incentive: the more data is processed, the easier it becomes to justify the processing of special categories of personal data.
- Personal data which are processed via an AI system would be treated more favourable than any "normal" (lower risk) processing operation, which would deviate from the technology-neutral nature of the GDPR. This risks creating situations wherein controllers might unnecessarily use AI simply to make use of this exception.

Processing of personal data in the terminal equipment of a natural person and other ePrivacy related provisions *Article 3(15) – new Articles 88a and 88b GDPR; Article 5*

[1] In December 2025 the House of Representatives adopted a motion related to this article. https://www.tweedekamer.nl/kamerstukken/moties/detail?id=2025D49636&did=2025D49636

Question 2: *delegations are invited to express their views and possible suggestions on the additional exemptions from consent requirement for aggregated information for measuring the audience and for maintaining or restoring the security of a service or the terminal equipment. In particular, the Presidency invites delegations to share their positions on the two following points:*

– Should the exemption for audience measurement remain limited to its originally intended scope (e.g. the controller of a service requested by a data subject) or more open, in particular concerning to the actors it should cover (other parties in the measurement value chain that are not processors of the controller)?

- According to NL the exemption for audience measurement should remain limited to its originally intended scope (e.g. the controller of a service requested by a data subject). The NL even proposed to limit the scope of the exemption to create aggregated information only during the use of the online service by the data subject.
- A more open exemption which would include other actors in the measurement value chain that are not processors of the controller, would make it lawful for these actors to process personal data without a legal basis under Article 6(1) GDPR and therefore without asking for consent or without balancing the interests of the data subjects.
- With the current wording of the proposal, this would undermine the rights of data subjects in several ways. It would for example not be possible for data subjects to object to the processing.
- Therefore, NL proposed to add to Article 88a(3) that the processing for the purposes listed under sub (a), (b) and (c) is only permissible where based upon a legal basis in accordance with Article 6(1) other than consent.

– Should the exemption for safeguarding the security of a service or a device be further specified and delineated?

- NL agrees that the exemption for safeguarding the security of a service or a device should be further delineated. In its current wording, the exemption overrides all consent and proportionality requirements that would otherwise be applicable under the GDPR. As mentioned in the response to the previous question, NL proposes to link the exceptions, meant in Article 88a(3), to the legal bases in Article 6(1) GDPR. These exceptions, especially the new ones (Art. 88a(3) point (c) and (d)), are formulated in broad terms and could otherwise imply blanket lawfulness for storage of or access to information on terminal equipment for these purposes.
- Linking these exceptions to Article 6(1) instead, preserves the required balancing test for legitimate interests and, importantly, ensures that controllers must properly consider data subjects' rights and interests prior to their processing. While maintaining a broad scope regarding the definition of ‘security purposes’ is preferable, this exemption should therefore be explicitly linked to article 6(1)(f) GDPR.
- In addition, a substantial body of case law has already been developed around the concept of legitimate interest. Therefore, linking these exceptions contributes to legal certainty for controllers, as they are able to rely on existing case law for these purposes.

Question 3: *Delegations are invited to share their views and overall position on the proposed new Article 88b GDPR on automated and machine-readable indications of data subject's choices with respect to processing of personal data in the terminal equipment of natural persons.*

- NL welcomes the objective of solving the cookie fatigue. The NL has previously made a study reservation about the exemption for media service providers regarding the impact on solving the cookie-fatigue and welcomes the view of other member states regarding this.
- Furthermore, NL questions how and if giving (general) consent under the proposed Article 88b(1)(a) GDPR can be considered "specific" and lawful according to Recital 32 GDPR and Article 7 GDPR. Therefore, the NL proposes to further specify how this consent has to be given, for example for each purpose and for each controller or for specific categories of data processing.
- Moreover, NL proposes to include in paragraph 1 and 6 that the data subject shall also be able to withdraw consent in accordance with Article 7 GDPR.
- NL also proposes to clarify that the exemption from the obligation to respect a signal transmitted through automated means indicating consent preferences of a user in paragraph 3, does not mean an exemption from asking consent, as the Commission has stated. This could be clarified by adding to paragraph 3 that Article 88a remains fully applicable to these providers.

***

FINLAND

SUOMI

Finland's written comments following the Antici group discussions on 27 February 2026

Finland would like to thank the Commission for its detailed answers and the Presidency for the swift management of the process. Below is our contribution in response to the presented questions and we reserve the possibility to further specify our position in due course.

Contents

Compromise text on GDPR, ePrivacy and P2B Regulation

Finland thanks the Presidency for having considered our written comments and proposals. Finland considers that the compromise proposal goes in the right direction. It alleviates most of the concerns related to upholding the current level of data protection.

Considering the discussion in the Antici group, Finland is flexible to discuss further some of the deleted proposals. At the same, Finland cannot support some of these proposals as they stand.

Finland will provide further comments and amendment suggestions as requested by 18 March 2026.

1. Definition of personal data and pseudonymisation

Article 3(1), Article 3(10), Article 3(11), Recital 27, Recital 27a

Article 4(1), Article 41a GDPR

Definition for personal data: Finland supports the deletion of the Commission proposal to amend the current definition for personal data as well as the corresponding recital. Finland considers this is the best solution, echoing the majority of Member States, the EDPB-EDPS Joint Opinion [paras 11-21] and the overall objective to ensure the current level of data protection.

Finland emphasizes that changing the definition of personal data as proposed would weaken the level of data protection and would not provide further legal clarity, as the need for case-by-case assessment of whether data is personal data or not is not removed. Such would not clarify ambiguities related to anonymization and pseudonymization. On the contrary, it could increase general ambiguity and lead to deliberate misinterpretations.

Regarding the proposal for recital 27a, Finland considers that this recital is neither necessary nor appropriate if the amendment to the definition of personal data is deleted.

Implementing acts: Finland is open to continue to discussions the possibility of implementing acts on anonymization and pseudonymization and providing technical assistance to controllers to clarify the ambiguities related thereto. Such implementing acts must be technical, i.e., they must provide technical expertise to controllers, and they may not affect the interpretation of the definition of personal data and the material scope of the GDPR. Finland stresses that all the essential elements must be regulated in the act itself.

Finland has provided a possible way forward in January, which could alleviate some of the problems with the Commission proposal and serve as the starting point for further discussions.

Finland respectfully proposes the following compromise:

Article 41a

Technical means and criteria for pseudonymisation

(1) The Commission may adopt implementing acts to specify technical means and criteria for pseudonymisation determine whether data resulting from pseudonymisation no longer constitutes personal data for certain entities.

(2) For the purpose of paragraph 1 the Commission shall:
(a) assess the state of the art of available pseudonymisation techniques; and
(b) develop technical means and criteria and or categories for controllers and recipients to assess available pseudonymisation techniques the risk of re-identification in relation to typical recipients of data.
(3) The implementation of the technical means and criteria outlined in an implementing act may be used as an element to demonstrate that data cannot lead to reidentification of the data subjects.
(4) The Commission shall closely involve the EDPB in the preparations of the implementing acts. The EPDB shall issue an opinion on the draft implementing acts within a deadline of 8 weeks as of the receipt of the draft from the Commission.
(5) The Implementing Acts shall be adopted in accordance with the examination procedure referred to in Article 93(3).

2. Scientific research and purpose limitation

Article 3(1), Article 3(2), Recital 28, Recital 29, Recital 32
Article 4(35), Article 5(1)(b) of the GDPR

Definition for scientific research: Although Finland welcomes the objective to clarify uncertainties related to scientific research and ensure uniform interpretation, the proposed definition should be amended and clarified to avoid the abuse of the special provisions on scientific research. Finland considers important to also consider academic freedom and the freedom on science. With this respect, any definition should correspond with what the scientific community considers scientific research. In broader terms, Finland is concerned whether the GDPR is the correct place to determine what is scientific research and what is not.
Finland understands the reasons why the Presidency proposed to delete the definition. However, if the majority is willing to discuss this matter further, Finland can show flexibility to discuss further the definition for scientific research and provides the following comments. Finland underlines that Finland cannot support the Commission proposal as such.
Purpose limitation: Finland can support the Presidency compromise proposal to add “subject to the application of appropriate safeguards” in Article 5(1)(b) of the GDPR. However, Finland urges the Presidency to return the reference to Article 6(4) and the deleted wording “purposes, independent of the conditions of Article 6(4) of this Regulation”.

3. New derogation from the prohibition to process biometric data

Article 3(3), Recital 34

Finland considers that the wording in Article 9(2)(k) GDPR concerning biometric verification needs to be discussed further. Finland is not convinced that the proposal is optimal yet welcomes that the

Presidency has shown interest at amending the Commission proposal. Finland is flexible to find the best way forward and will provide further comments in writing. Clear wording and adequate safeguards remain essential.

4. Exercise of the individual's right of access and exemption from information obligations
Article 3(4), Article 3(5), Recital 35, Recital 36
Article 12(5), Article 13(4) of the GDPR
Finland welcomes the clarifying amendments made to Articles 12 and 13 of the GDPR. Regarding Article 12(5) of the GDPR, Finland considers that it is vital to amend the Commission proposal and to clarify that the aim is to prevent abusive behavior. Therefore, Finland strongly supports the Presidency compromise proposal and deleting especially "for purposes other than the protection of their data".
Regarding Article 13(4) of the GDPR, Finland welcomes and supports the amendments in the Presidency compromise proposal. Finland especially thanks the Presidency for taking account our written proposal to replace "data-intensive" with high-risk processing. Finland also sees the added benefits to mention large-scale processing, special categories of data and complex processing operations.
5. Automated decision making
Article 3(7), Recital 38
Article 22 of the GDPR
Finland understands why the Presidency has proposed to delete the Commission proposal to amend Article 22 of the GDPR. Finland can show flexibility and continue discussions on this proposal. Finland points out that, whilst the EDPB-EDPS Joint Opinion is negative towards structural changes to Article 22, the EDPB and the EDPS are not against the clarification to the current Article 22(2)(a) of the GDPR. Finland requests that the Presidency re-evaluates returning the following part of the Commission proposal:
(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller regardless of whether the decision could be taken otherwise than by solely automated means;
6. Data breach notification and data protection impact assessment
Article 3(8), Article 3(9), Article 3(11), Recital 39, Recital 40
Article 33, Article 35 of the GDPR
Data breach notification: Finland welcomes the amendments to maintain the current 72 h deadline for data breach notifications. Finland has also supported the Commission proposal to raise the threshold to high risk. However, Finland highlights that it is important that the controllers and

processors know what high risk to the rights and freedoms of a natural person means. In this regard, it is important that at least the EDPB provides such a list, but Finland is flexible towards a legally binding implementing act as well.

A legally binding list might be appropriate, considering that the controllers and processors might be subject to administrative fines for the infringements of Article 33. At the same time Finland emphasizes that a possible implementing act for the "high risk" list should respect the role and powers of the EDPB. Finland does not see the added benefit of an implementing act concerning the data breach notification template.

Finland will provide further comments on the proposed single-entry point separately whilst discussing the proposed amendments to Directive (EU) 2022/2555. At this moment, Finland provides only a following technical comment (the deadline should be amended in the last sentence as well) and leaves it to the Presidency discretion to re-evaluate the need for implementing acts for the list:

Article 33

1. In the case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall without undue delay and, where feasible, not later than 9672 hours after having become aware of it, notify the personal data breach [via the single-entry point established pursuant to Article 23a of Directive (EU) 2022/2555] to the supervisory authority competent in accordance with Article 55 and Article 56 of this Regulation. Where the notification to the supervisory authority is not made within 9672 hours, it shall be accompanied by reasons for the delay.'

7. The repeal of the P2B Regulation (EU) 2019/1150

Article 10

Finland shares the concerns of Austria, Belgium, Italy and the Netherlands in their joint non-paper on the repeal of the P2B Regulation. Finland considers it essential to ensure transparent and fair contractual relationships between business users and online platform companies also in the future. Transparent contracts and predictable markets enable especially SMEs to create economic growth and stay competitive.

Finland considers that the key impact from repealing the P2B Regulation would be that the service provider is not obliged to notify in advance of any change, restriction, suspension or termination of the service to the business user. To ensure legal certainty for business users when operating on online platforms of all sizes, Finland proposes that also Articles 3(2) and 4(2) of the P2B Regulation will be retained until 2032. In addition, the Commission should commit to examining

how these articles may be included in the Digital services Act (DSA) before 2032, when the transition period ends.

Discussion paper

Processing of personal data for the development and operation of AI systems (Article 3 (3) – new point 9(2)(k) GDPR, new paragraph 9(5) GDPR; and Article 3(15) – new Article 88c GDPR)

The Commission proposes to introduce specific provisions under the GDPR to clarify and support conditions for the processing of personal data in the context of the development and operation of AI systems and AI models. The proposal for a new Article 88c notably aims at clarifying when a controller may rely on Article 6(1)(f) GDPR to pursue a legitimate interest in the context of development and use of AI systems and models (Article 3(15)). It provides for a non-exhaustive list of technical and organisational measures and safeguards including an unconditional right to object to the processing and enhanced transparency.

In addition, the Commission proposes to introduce a derogation from the prohibition on processing special categories of personal data in the context of the development and operation of AI. The derogation should only apply where the controller does not aim to process special categories of personal data, but such data are nevertheless residually processed, subject to appropriate measures and safeguards.

Delegations already had the opportunity to be provided with further explanations from the Commission during the Q&A session, and the EDPB and EDPS also addressed these specific provisions in their joint opinion 2/2026 on the Digital Omnibus.

The Presidency highlights that the proposed provisions amending the GDPR are to be considered and discussed separately from the ongoing discussion on the AI Omnibus proposal.

Question 1: delegations are invited to express their views on the proposed provisions relating to

- the processing of personal data in the context of the development and operation of AI systems based on the lawful ground of legitimate interest (Art 88c).
- the proposed new derogation from the prohibition on processing special categories of personal data (Article 9 (2)(k) and (5).

Finland supports the Commission’s objectives to clarify the processing of personal data related to AI. Nevertheless, Finland highlights that this type of special provisions could change the nature of the GDPR as general regulation and could also endanger technological neutrality.

Finland remains flexible to keep Article 88c with the following amendments to the Commission proposal:

Concerning the amendments in Article 88c, we should look at the EDPB-EDPS Joint Opinion [paras 39-45], inter alia the need to ensure a proper three-step balancing test and at least delete the wording “where appropriate”.
The proposed Article 88c should consider that authorities cannot use legitimate interest, nor consent, as a legal basis and clarify the legal basis for this type of processing.
Concerning Article 9(2)(k) and (5), Finland remains flexible, but considers that the Commission proposal should be clarified, taking into account the EDPB-EDPS Joint Opinion [paras 46-52].
Finland will provide a written proposal to clarify Article 88c by 18 March 2026.

Processing of personal data in the terminal equipment of a natural person and other ePrivacy related provisions (Article 3(15) – new Articles 88a and 88b GDPR; Article 5)

During the AGS meeting of 16 January 2026, delegations already had the opportunity to express their views on the proposed new Article 88a GDPR updating the rules on storing of or on gaining access to information stored on devices and on the principle of moving the protection already laid down in the ePrivacy Directive under the General Data Protection Regulation.
The Presidency is aware that some Member States have not yet adopted a position or have maintained a scrutiny reservation for the proposed amendments and notes that some Member States have raised serious concerns about the moving of the rules to the GDPR.
However, the Presidency has also noted that other aspects of the proposal – in particular the proposed extension of the exemptions from the consent requirement (aggregated information for audience measurement and security of a service or device) – have found broader support among delegations.
In their joint opinion, the EDPB and the EDPS seems to be generally supportive of this extension, while recommending to clearly delimit the processing in scope of the security exception to what is strictly necessary.
Question 2: Delegations are invited to express their views and possible suggestions on the additional exemptions from consent requirement for aggregated information for measuring the audience and for maintaining or restoring the security of a service or the terminal equipment. In particular, the Presidency invites delegations to share their positions on the two following points:
- Should the exemption for audience measurement remain limited to its originally intended scope (e.g. the controller of a service requested by a data subject) or more open, in particular concerning to the actors it should cover (other parties in the measurement value chain that are not processors of the controller)?

- Should the exemption for safeguarding the security of a service or a device be further specified and delineated?

Finland thanks the presidency for taking the extra time to prepare and discuss further this difficult topic. Finland supports Commission proposal to move the so-called cookie rules to the GDPR. However, stakeholders have raised that this would not simplify the legislation as planned.

Finland supports the new white-listed processing grounds, but these might fall short of reducing the number of cookie banners. In addition, the proposal seems to leave undesirable uncertainties in the interplay between the GDPR and ePrivacy-directive. Thus, further work is needed on the proposal.

On audience measurement, Finland would like to point out that for media companies' advertising sales, it is essential that third-party research organisations conducting audience measurement independently and in line with industry standards can continue to carry out such measurement in the future. Independent audience measurement providers typically operate as joint controllers under the GDPR. Therefore, Finland supports specifically allowing the use of joint controllers to carry out the audience measurement of a service.

Question 3: The Commission proposal also introduces a new Article 88b GDPR on automated and machine-readable indications of data subject's choices with respect to processing of personal data in the terminal equipment of natural persons, with a view to oblige controllers of online interfaces (i.e. web browsers or a mobile application) to respect a signal expressing data subjects' preferences, that were set centrally – for example via a browser or a third party browser plug-in.

To facilitate compliance with this new obligation, the Commission proposes to develop dedicated standards. The obligation for controllers of online interfaces to accept centrally set machine-readable preferences would not apply to the providers of media services.

Delegations are invited to share their views and overall position on the proposed new Article 88b GDPR on automated and machine-readable indications of data subject's choices with respect to processing of personal data in the terminal equipment of natural persons.

Finland supports measures that improve the usability of the service, and which allow the data subjects to exercise control over the personal data collected and processed about them. Therefore, Finland expresses its overall support for the proposed Article 88b. However, data subjects should be provided with adequate information concerning such processing.