Council of the European Union
General Secretariat

PUBLIC

Brussels, 16 January 2026

WK 448/2026 INIT

LIMITE

SIMPL	**TELECOM**
ANTICI	**CODEC**
DATAPROTECT	**PROCIV**
CYBER	**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:	Omnibus VII: Digital Omnibus – Presentation by the Commission (AGS on 16 January 2026)

Delegations will find enclosed a presentation as prepared by the Commission for the meeting of the Antici Group (Simplification) on 16 January 2026 regarding the Digital Omnibus (Omnibus VII) - Slides covering P2B, ePrivacy and GDPR, for presentation in the Q&A session.

European Commission

PUBLIC

DIGITAL OMNIBUS

Q&A session

Antici Group on Simplification

16/01/2025

PUBLIC

Platform-to-Business Regulation

P2B

PUBLIC

How will enforcement of the remaining P2B provisions work?

- For those P2B articles that are not repealed, provisions on enforcement of P2B (Article 15) **remain in place** during the transition period: no change for national authorities in charge of P2B
- Enforcement is based on the country-of-origin principle defined by the **place of establishment of the online platform** used by business users (confirmed by CJEU caselaw in joined cases C-662/22 and C-667/22; case C-665/22)
- For provisions covered by the DSA and the DMA, enforcement and procedures for cross-border cooperation, where applicable, are **more clearly defined** (in DSA and DMA)
- Application of the partial repeal (and the enforcement of the remaining provisions) **will apply** as of the **date of entry into application of the Digital Omnibus Regulation**

P2B

PUBLIC

Will the repealed provisions be integrated in other pieces of legislation?

- If necessary, **case by case** assessment – for example for including definitions in existing laws - without prejudice to the **Commission's right to initiative**

PUBLIC

Data

GDPR

PUBLIC

Questions on ePrivacy in general

Questions on ePrivacy in general

PUBLIC

Could further amendments to the ePrivacy Directive be proposed, e.g. to facilitate use of traffic data in the sense of Article 6 ePrivacy Directive by statistical offices in line with the new provisions 17b to 17e of the amended Regulation on European statistics (Regulation (EC) 223/2009)

Such amendments would be beyond the scope of the proposal. The suggestion will be considered when proposing a reform of the respective remaining provisions of the ePrivacy Directive.

PUBLIC

Questions on Article 88a

Article 88a

PUBLIC

In relation to slide 100 of the slide deck of the AGS of 16/12/25:
Could the Commission clarify how all GDPR principles are applicable if there is no additional legal basis under Article 6 and no balancing or necessity test needed for the whitelisted grounds for processing without consent? How does this comply with Article 5 GDPR?

The proposal adds specific legal bases for certain very concrete low-risk purposes, designed in a manner that does not need a balancing test. Because this new article is part of the GDPR, this means that all GDPR requirements, including the principles under Article 5 apply.

Article 88a

PUBLIC

In relation to slide 102:

- **The Commission states it "would in principle not see greater risks for the rights on individuals". Since there is no impact assessment conducted, where is this statement based upon?**
- **The Commissions states: "General principles apply and protect against abuse", but how does this relate to the fact that no necessity or proportionality test is needed to conduct these processing activities? (cf. slide 100)**

- The legal assessment of the Commission is based on extensive desk research and stakeholder consultation, including a dedicated "reality check" and numerous bilateral stakeholder meetings with e.g. civil society organisations and publishers. An Impact Assessment report is only one specific element for the Commission to report on its findings. For the Omnibus, the Staff Working Document reports on all the findings of the Commission's evidence collection.
- The whitelisted grounds are proposed on the basis of a necessity and proportionality assessment conducted by the Commission (and the legislator once adopted). Because this new article is part of the GDPR, this means that all GDPR requirements, including the principles under Article 5 apply.

Article 88a

PUBLIC

In relation to previous slide 103:
Could the Commission include the right to withdraw explicitly in the wording of Article 88a(4) and could the fact that Article 7 fully applies be included explicitly in the wording of the corresponding Recitals?

We see no need to reference Article 7 and the right to withdraw consent here as this Article applies without such reference, because this Article relies on the notion of consent under Article 4 GDPR and all requirements for valid consent under Article 7 GDPR.
Also, Article 88a(4) seeks to regulate how a consent request can be easily refused (letter a) or during what time period a controller is prevented from making a new consent request (letters b and c).

Article 88a

PUBLIC

In relation to previous slide 104:
How does the sentence: "It is important to note that the GDPR's principles and all other requirements continue to apply fully, this includes the compatibility test of Article 6(4) GDPR" relate to the sentence: "Subsequent processing addresses the processing after the storage or gaining access as mentioned in the first sentence of Article 88a(1) ≠ "further compatible processing" in the sense of Article 6(4)."? These sentences seem to be contradict each other?

This is no contradiction. It is meant to emphasise that "subsequent processing" and "further compatible processing" are not the same thing. Subsequent processing refers to the processing of personal data after the initial storage or gaining access to the device. If such subsequent processing is based on consent, Article 88 (4) applies. However, if after collecting consent for either the initial storage or gaining access to information in the device and the subsequent processing of the data, the controller wants to process the data for other purposes, for which no consent has been collected, then Article 6(4) applies.

Article 88a

PUBLIC

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

The Commission does not intend to say that the GDPR offers a stronger protection framework than the ePrivacy Directive. Moving the provisions under the GDPR has however, significant benefits: By moving the provision under a Regulation, its interpretation and application will be harmonized. Furthermore, the rules will be subject to enforcement by the national DPAs and also subject to the fines in the GDPR.

Article 88a

PUBLIC

Could the Commission clarify if the sentence "Article 5(3) of the ePrivacy Directive is maintained for connected devices of legal persons and non-personal data" (sheet 39) implies that the exceptions of Article 88a(3)(c)(d) do not apply (accordingly) for such data? Does this mean that the protection for personal data is in fact lower than for connected devices of legal persons and non-personal data?

The Commission does not think that the protection of non-personal data is higher than for personal data merely because there are now carefully crafted grounds of processing in Article 88a(3) which do not exist under the current ePrivacy Directive. Making data processing subject to consent is not necessarily creating stronger protection. The GDPR should regulate the processing of personal data in accordance with its risk based approach.

Article 88a

- **If a website no longer works after rejecting cookies, is Article 88a fulfilled?**
- **How should one-click principle be interpreted in cases where media service providers rely on their exemption in art. 88b, in particular where 'pay or consent' models are used? Commission has indicated that the proposal does not change the approach to 'pay or consent' models. Does the requirement of one-click lead to limiting the use of pay or consent -models in practice?**

- Where consent-based cookies have an impact to access a website, this needs to meet the conditions of the GDPR as interpreted by the CJEU, including where the website uses a 'pay or ok'/'consent or pay' model.
- The new rule on single-click refusal should not impact on the possibility to offer a paying option as an alternative.
- In practice this could lead to several models, for example:
  - The paying option could be presented as an alternative to the consent solution, provided it complies with the case law of the CJEU
  - A separate option for refusal of the placing of (certain) cookies could also be presented as an alternative, where the media service provider would present a more restricted choice of articles, for example.

PUBLIC

Article 88a

PUBLIC

The exception in paragraph 2 with regard to "member state law" can lead to fragmentation and divergent rules. Paragraph 2 appears to go further than the existing Article 5(3) of the e-Privacy Directive and seems to go beyond just cookies. What specifically does paragraph 2 cover, and why is it necessary?

The current proposal aims at safeguarding the scope and level of protection of Article 5(3) ePD to the widest extent possible. Referring to national laws is necessary to ensure alignment with Article 15 ePD and Article 6 GDPR. This way, Member States can establish by law which pursues the objectives of Article 23 GDPR that consent is not required. This must be done however under the conditions and safeguards set out in the GDPR. Article 6 GDPR also allows Member States to set out legal obligation in their national law (para 3). The approach is thus consistent with the GDPR's approach.

Article 88a

PUBLIC

Is a legal basis within the meaning of Article 6 GDPR still required in addition to Article 88a(3)?

No. Article 88a(3) are the legal bases.

Article 88a

PUBLIC

Art. 88a GDPR, especially para. 3, only uses the term "service", whereas Art. 5 (3) ePrivacy Directive uses the term "information society service". Is the term „service" in Art. 88a GDPR meant to be broader than in Art. 5 (3) ePrivacy Directive?
Please explain in further detail the operational simplifications brought about by the proposed Art. 88a GDPR.

The term "service" can have a broader meaning than information society service. An examples is a "pay-as-you-drive" insurance that needs access to vehicle information to verify driving patterns.
Operational simplifications are:

- the provisions in Article 88(3) lit. (c) and (d) which allow a controller to justify certain data processing directly on the basis of these legal grounds;
- the provisions in Article 88(4) reduce the burden on users when consent is being used as a legal basis.
- broader scope of the exemption from consent for a service explicitly requested (not just an information society service).

Article 88a

PUBLIC

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

If “anonymous first party cookies” are understood as cookies that collect only usage information without making it possible to identify the user, then the answer is no. Because in this case, there would be no personal data in the first place. Article 88a(3)(c) makes it possible to collect personal data if the sole purpose of processing such data is to extract aggregated usage statistics information.

Article 88a

PUBLIC

What practical example is there for the regulatory alternative in Art. 88a (3) (d) GDPR regarding the request only by the terminal equipment? (Art. 88a (3) *(d) reads: „maintaining or restoring the security of a service provided by the controller and requested by the data subject or the terminal equipment used for the provision of such service.“)?*

This is about “maintaining or restoring the security of the terminal equipment”.
Examples are:

- cookies used to prevent unauthorized access to user accounts or account hijacking while a session is open;
- reduction of malicious traffic generated by bots that would exploit the computational capacities of the device;

Article 88a

PUBLIC

Was a further alignment of the remaining ePrivacy-directive art. 5(3) with the newly introduced grounds considered? Why does the proposed white-listing allow for more grounds of processing of personal data than non-personal data?

With the proposal, the Commission tries to bring the processing of personal data within the GDPR, with the advantages of aligning the system for processing of personal data, regardless on whether it happens on a terminal equipment or not – at least to an extent.
It would have stretched the GDPR to also include rules on processing of non-personal data.
The newly added grounds for processing personal data are aligned with the risk-based approach of the GDPR and can be justified as a means to reduce the use of consent as a legal basis which can lead to "consent fatigue".

Article 88a

PUBLIC

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

As far as the new cookie rules are brought under the remit of the GDPR (Article 88a situations), the GDPR enforcement applies. For processing of non-personal data, the enforcement regime for Article 5(3) ePD remains untouched.

PUBLIC

Questions on Article 88b – central cookie management

Article 88b

PUBLIC

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

The Commission will need to examine this on the basis of concrete textual proposals.

Article 88b

PUBLIC

As in Article 88a, this article also doesn't mention the option to withdraw consent in paragraphs 1 and 6. How does this relate to Article 7?

- Article 88b is about elements that can be automated in consent/rejection of consent requests situations or to object to data processing in the sense of Article 21 GDPR. It is difficult to see how a withdrawal would be automatable as it would always need to be triggered by a data subject in an individual situation.
- Article 7 GDPR fully applies since Article 88a(1) clearly states that consent is provided pursuant to the GDPR. This means that the right to withdraw consent applies fully.
- Paragraph 4 sets out conditions to simplify cookie banner designs, for example with the single click requirement.
- It applies where the "initial" access to personal data relies on consent and where the subsequent processing is also based on consent. This is done to prevent loopholes to these measures designed to help users.

Article 88b

Could paragraph 1, paragraph (b), be split into paragraphs (b) and (c)? The current formulation of paragraph (b) could unintentionally suggest that a refusal of consent must be related to an objection based on Article 21, paragraph 2, of the GDPR (objection to data processing for direct marketing purposes). Incidentally, it is unclear why this paragraph mentions the 'right to object', unlike Article 88a.

- The use of the word "and" ensures in principle, that there are two different components to (b) - it stems from the logic of the GDPR that refusing consent and exercising the right to object are not tied together. The Commission is, however, open to textual proposals that increase the clarity of the text.
- The second leg of Article 88b(1)(b) reflects the situation mentioned in Article 21(5) and the rights in Article 21. Therefore, it is not necessary to reflect this in Article 88a which does not include the legal bases for which a right to object exists (legitimate interest, performance of a task in the public interest).

PUBLIC

Article 88b

PUBLIC

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

- Given the great importance of a diverse media landscape for European democracies, an exemption is necessary in order to maintain the possibility – especially for smaller, local media service providers – to generate revenue from add marketing services, which rely on the possibility to ask the website user for consent.

PUBLIC

GDPR: Article 41a pseudonymisation

Article 41a

Article 41a does not seem suitable for an implementing act. Because the implementing acts would relate to the definition of personal data, this is a core element that does not lend itself to elaboration in implementing acts.
If the Commission does not want to re-define what personal data are, has the Commission considered to limit the proposed implementing acts to techniques that controllers should use for pseudonymisation as a protective measure and to disconnect this from the definition of personal data?
Could the Council Legal Service and the Legal Service of the Commission reflect on this?

- The Commission considers a legislative intervention necessary in light of multiple feedback that technical guidance on the foundational concepts of the GDPR is missing.
- Such guidance is now ever more important with the clarifications brought by the CJEU in the SRB case and the proposed clarifications in the definitions of the GDPR. Pseudonymisation can thus have a more fundamental function which is to exempt a recipient of this data from GDPR obligations.
- The implementing act can indeed not – not even implicitly – define the borders of the notion of what constitutes personal data.
- As Article 41a(3) specifies, the legal effect of complying with the elements set out in the implementing act may be used by controllers to demonstrate that data cannot lead to reidentification of the data subjects. (cf. similar wording for codes of conduct/ certification schemes in Article 24(3), 25(3), 32(3)).

Article 41a

PUBLIC

The Commission states (sheet 111) that the implementing acts will contain an "Assessment of techniques against the requirements of the GDPR and its interpretation by the courts and the data protection authorities". On the same sheet, the Commission states: "Fully respects powers of DPAs and the courts".

- **If the interpretation by the Courts and the data protection authorities is leading and if the intention is to fully respect the existing powers, what is the reason to not leave this to the DPAs (EDPB) and the Court?**
- **Could adoption of guidelines by the EDPB not also provide sufficient legal certainty?**

- With the possibility to propose Implementing Acts on important compliance questions, the Commission seeks to use its power to bring together technical expertise to contribute to the debate and give more legal certainty to controllers.
- Guidance by the EDPB will lead to additional legal certainty. The Commission understands that such guidance is in preparation. However, we see an Implementing Act as additionally necessary in order to bring specific technical guidance and more legal certainty on which controllers can rely in their compliance efforts.

Article 41a

According to Article 41a(4), the Commission shall "closely involve the EDPB in the preparations of the implementing acts", and the EDPB will be asked for an opinion. The provision does not specify what happens if the EDPB has serious objections (during the drafting process and in its subsequent opinion).

Can the implementing act still be adopted in the event of a negative opinion from the EDPB? And what is its legal status in that case?

- Under the wording of the proposal, the Commission has the responsibility and decision power to propose an Implementing Act.
- Technically speaking, it can adopt an implementing act despite a negative opinion without there being a different legal effect. The Commission will, however, take the EDPB concerns very seriously and assess the proposal against the EDPB's comments.

PUBLIC

Article 41a

PUBLIC

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

- We believe that this is not an unremarkable benefit. It is akin to compliance with codes of conducts or certification schemes (cf. Articles 24(3), 25(3), 32(3)). The difficulty will remain to give sufficiently precise elements that can support individual compliance efforts while being able to capture a potentially wide range of cases.

Article 41a

PUBLIC

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

- The legal effects could be similar to codes of conduct and certification schemes (cf. Article 24(3), 25(3), 32(3)) in terms of their use as an element to demonstrate a lack of breach of the GDPR.
- However, an important difference is that such codes and schemes are used to demonstrate compliance with the GDPR, whereas pseudonymisation would be used to demonstrate that the GDPR does not apply (if it is shown that the data subjects cannot be identified by the entity in question).
- A header could be added.

GDPR: Definition of personal data

PUBLIC

The new definition of personal data in Art. 4 (1) GDPR leads to narrowing down the scope of personal data and goes beyond the CJEU judgment in EDPS ./. SRB?

The Commission does not consider that it is a “new definition”.

The changes build on EDPS/SRB judgement and provide a clarification that a potential subsequent transmission of the information to third parties who have means reasonably likely to identify the data renders that information personal only for those third parties who have such means at their disposal.

There is no “narrowing” because the CJEU builds on its previous case law, in particular the Breyer Case. The CJEU always sustained that the data is personal only to the entity which has means reasonably likely to render the data personal to it. Such means do need however to be in its hands but it needs to have legal access to them.

GDPR: Definition of personal data

Would controllers who, due to the manner of processing, no longer regard certain data as personal data be permitted to transfer such data to a recipient in a third country, regardless whether this recipient has means reasonably likely to be used to identify the individual?

On the impact of the change on international transfers: Chapter V GDPR is based on the premiss that **the sender (controller in the EU) is responsible for GDPR compliance.**

If the sender has the "means reasonably likely", the data is personal for that sender, who thus must comply with Chapter V.

If the data is personal for the controller – **the Chapter V will always apply independent of the means reasonably likely available or not to a recipient in a third country.**

PUBLIC

GDPR: Definition of personal data

PUBLIC

Why are the clarifications necessary if the case law says it?

There is a fragmentation in the application of the GDPR in the EU. Including the clarification in the operative part of the GDPR will provide for legal certainty and harmonisation.

GDPR: Definition of personal data

PUBLIC

The test of not having the “means” is very high: the risk of identification must be non-existent or insignificant”?
Several requests on including some of the clarifications provided in the slides presented by the Commission at the previous AGS meeting in either Article 4(1) or in the Recitals

The test should be high but it is not that the risk of identification should be “non-existent”: the CJEU in SRB para 82 stated that “*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*** *(see, to that effect, judgment of 7 March 2024, OC v Commission, C-479/22 P, EU:C:2024:215, paragraph 51 and the case-law cited).*”

The Commission is ready to work with the Council on how to include some of the clarifications in either Article 4(1) or in the Recitals.

GDPR: Personal data processing for scientific research

PUBLIC

Regarding the definition “scientific research”, could the COM further clarify why the proposal includes commercial interest? Why isn’t there any references to the competence of the researcher?

Research and commercial interests are commonly intertwined and should not be seen as two separate aims by themselves. A very clear example is health research that is clearly aimed at releasing new medications/treatments/ services on the market and aims to save lives, improve wellbeing etc. Moreover, testing and validation of research in its way to market is an important step towards research results reaching their final users: patients and healthy individuals.

GDPR: Personal data processing for scientific research

PUBLIC

Has the Commission considered to include in the definition the adherence to “the relevant sectoral standards of methodology”, like in the definitions of the EDPS and EDBP?

The proposed definition of scientific research refers to adherence to “ethical standards in the relevant research area”. Such standards are defined in the *European Code of Conduct for Research Integrity* (ALLEA) and include, for instance, transparency and verifiability, meaning that research activities aim to achieve verifiable results, and the conduct of research allows the hypotheses, methods, data and conclusions to be open to criticism, normally following peer review. The results of the research are shared with other parties, for example by publication, or will be shared in the future, with due regard to legitimate limitations to access such as protection of intellectual property.

GDPR: AI and legitimate interest - Article 88c

Does this create new legal grounds for processing? Can other legal basis be relied upon?

- The provision does not create a new ground for lawful processing.
- The proposed amendment clarifies the current GDPR rules: a controller may rely on Article 6.1.f for pursuing a legitimate interest in the context of AI development and operation, where all conditions of that provision and the other GDPR requirements are met.
- It is up to the controller to choose the appropriate lawful ground of processing pursuant to Article 6 GDPR. This could be, for example, consent or legal obligation.
- It does not overrule other sectoral laws requiring, for example, a legal obligation or providing for the processing for an objective of public interest, incompliance with Article 6(1)(c) or Article 6(1)(e) and Article 6(3) GDPR.

The right to object – what is the relationship with Article 21(3) GDPR and how will it work in practice?

- Article 21(3) GDPR is applicable to automated processing when personal data is processed for direct marketing purposes. This provision is broader than direct marketing
- It will be up to controllers to ensure that the unconditional right to object is implemented in a meaningful and effective manner.

Can the Commission add that this provision reflects EDPB Opinion 28/2024 to a recital?

- It has not included that the provision reflects EDPB Opinion 28/2024 as it is unnecessary.

GDPR: Processing of special categories of personal data for AI

PUBLIC

What is the relationship between Article 10(2) *[COM note: we assume it refers in fact to Art 10(5)]* **AI Act and proposed Article 9(2)(k) GDPR? Can the requirement of a proportionality test be added to this provision or its recital?**

- The specific legal ground for processing in Article 10(5) AI Act is separate from the amendments to Article 9 GDPR. They are mutually independent.
- The GDPR data protection principles of necessity and proportionality apply to any processing of personal data under this provision.

GDPR: Biometric data processing

PUBLIC

Inclusion of relevant safeguards if the controller gains knowledge of the biometric data

- Article 9(2)(l) is applicable where the biometric data or the means needed for the verification is under the sole control of the data subject.
- This means that the controller does not gain knowledge of the biometric data or only for a very limited time.
- If the data subject does not genuinely have sole control of the verification process, then the provision is not applicable and the exception cannot be relied upon.

GDPR: Automated individual decision-making

Why to remove the explicit reference to the data subject's right in Article 22(1)? Why not simply amend point (a) of Article 22(2) as proposed? What is meant by 'regardless of whether the decision could be taken otherwise...'? Should not the reference to 'equally effective' in recital 38 be moved to the operative part?

- The current wording has led to a restrictive interpretation (by some authorities) that hinders the use of automated tools, including in areas of cybersecurity and fraud prevention or in pre-contractual phase to protect their and their clients' interest.
- The proposed change of paragraph 1 from a right with exceptions into permission with strict conditions is clearer to operators and therefore provides more legal certainty.
- The proposed amendments in letter (a) ('regardless of whether the decision could be taken otherwise than by solely automated means') further clarifies the threshold for necessity assessment in case of a contract. As explained in Recital 38, to fulfil the requirement of 'necessity, it should not be required that the decision could be taken only by solely automated processing.
- The clarification in Recital 38 ('When several equally effective automated processing solutions exist, the controller should use the less intrusive one') should not be added in the operative part of the Regulation as this requirement stems directly from the general requirement of necessity, as interpreted by CJEU, and mentioning this one aspect of 'necessity' in the operative part could lead to restrictive interpretation of this requirement.

GDPR: Controllers' information requirements

PUBLIC

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

- The changes to Article 13 will benefit small operators including sports clubs.
- It exempts controllers from providing certain information to a data subject where:
  - there is a relationship between the controller and the individual (so Article 14 is out of scope),
  - the processing is non data-intensive,
  - the processing not likely to result in a high risk to the data subject, and
  - where there are reasonable grounds to expect that the data subject already has the information (when for instance the processing is based on consent or contract).
- It is difficult to identify situations where public authorities would meet the above conditions.

GDPR: Exercise of the right of access

PUBLIC

What is the objective of the provision and what do data subjects need to specify in their access request?

- The objective is to prevent abusive practices. Recital 35 sets down examples as to what this would include.
- The right of access is a core right of data protection – however, as the EU general legal principle of prohibition of abuse makes clear, individuals cannot invoke Union law by means of such abuse. The abuse of rights doctrine which is well established by the CJEU requires intent. This is also referenced in the recitals.
- The data subject is not obliged to specify the purpose of the request but, as per recital 35 data subjects should be as specific as possible when submitting their request.

GDPR: Data breach notifications to supervisory authority

PUBLIC

Does not the extended time limit for notifications combined with the higher threshold lower the level of protection? Does the list of circumstances under Article 33 apply also to Article 34 (communication of data breaches to data subjects)? Does not the deletion of current Article 70(1)(h) (referring to Article 34) potentially leave a gap?

- The time limit of 96 hours is a maximum time ('not later than'). It is likely to reduce the unvoluntary non-compliance with the required timeline causing additional administrative burden (para. 1 of Art 33 GDPR) and the need to rely on the possibility to 'provide information in phases without undue further delay' (para. 4).
- The incentive for a swift notification of data breaches should be high due to the data subject's right to compensation for the possible damage suffered as a direct result of the infringement of the GDPR (including measures to mitigate possible adverse effects).
- It is proposed that the notion of 'high risk' under Article 33 and 34 GDPR be the same. The list of circumstances in which a personal data breach is likely to result in a 'high risk to the rights and freedoms of data subjects' (amended Article 33) applies also to 'high risk' data breaches to be communicated to data subjects concerned (Article 34).

GDPR: Processing activities requiring and not requiring Data Protection Impact Assessment

PUBLIC

Should not COM be obliged to ask at least an opinion from the EDPB before changing the proposed DPIA lists?

- The aim is to ensure that the procedure for adopting the whitelists and blacklists and the necessary updates to them is as simple and swift as possible.
- The adoption by means of a COM implementing act allows to take into account also MS views and input before the adoption of the lists. MS may consult their DPAs about possible adjustments to the EDPB draft lists, etc. when they are discussed in the examination procedure.



© European Union 2025

Unless otherwise noted the reuse of this presentation is authorised under the CC BY 4.0 license. For any use or reproduction of elements that are not owned by the EU, permission may need to be sought directly from the respective right holders.