GDPR Articles	Digital Omnibus Proposal	Current text of the GDPR	Proposed change	EDRi position
Art. 4 (1) Definition of "personal data"	**Art. 3, Point 1 (a)**	'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;	'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; ***"Information relating to a natural person is not necessarily personal data for every other person or entity, merely because another entity can identify that natural person. Information shall not be personal for a given entity where that entity cannot identify the natural person to whom the information relates, taking into account the means reasonably likely to be used by that entity. Such information does not become personal for that entity merely because a potential subsequent recipient has means reasonably likely to be used to identify the natural person to whom the information relates."***	EDRi strongly supports maintaining the current definition without modification and rejects any attempt to reopen Article 4(1). The GDPR definition of personal data in Article 4(1), read together with Recital 26, already provides a robust and technologically neutral framework to determine identifiability. Any attempt to reopen this definition risks undermining the protection of the fundamental right to data protection and creating legal uncertainty across the EU legal framework. Proposals that shift the identifiability test toward a controller-centric assessment would weaken the existing standard, which considers whether a person is identifiable by means reasonably likely to be used. This broader approach is essential to capture modern forms of identification, including inference, correlation, and linkage across datasets.

GDPR Articles	Digital Omnibus Proposal	Current text of the GDPR	Proposed change	EDRi position
New Art. 41a	**Art. 3, Point 10**	-	***"Article 41a*** ***The Commission may adopt implementing acts to specify means and criteria to determine whether data resulting from pseudonymisation no longer constitutes personal data for certain entities.*** ***For the purpose of paragraph 1 the Commission shall:*** ***(a) assess the state of the art of available techniques; (b) develop criteria and or categories for controllers and recipients to assess the risk of re-identification in relation to typical recipients of data.*** ***The implementation of the 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.*** ***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.*** ***The Implementing Acts shall be adopted in accordance with the examination procedure referred to in Article 93(3)."***	EDRi opposes granting the European Commission implementing powers to define or operationalise pseudonymisation criteria. Pseudonymised data remain personal data under the GDPR. Granting the Commission authority to define technical criteria risks creating new legal categories that could enable some actors to treat pseudonymised data as non-personal data in practice. Interpretation of identifiability and pseudonymisation should remain anchored in Article 4(1) and Recital 26, and should be guided by supervisory authorities through the existing consistency mechanisms. Any clarification in this area should be developed through guidance from the European Data Protection Board rather than through Commission implementing acts.
Art. 4 Definitions	**Art. 3, Point 1 (b)**	-	***(32) 'terminal equipment' means terminal equipment as set out in Article 1(1) of Directive 2008/63/EC;*** ***(33) for 'electronic communications***	Not necessary, as provisions currently governed by the ePrivacy Directive should remain within the sector-specific framework for electronic communications

GDPR Articles	Digital Omnibus Proposal	Current text of the GDPR	Proposed change	EDRi position
			networks' the definition of Article 2(1) of Directive (EU) 2018/1972 shall apply; ***(34) 'web browser' means web browser as defined in Article 2(11) of Regulation (EU) 2022/1925;*** ***(35) 'media service' means a media service as defined in Article 2(1) of Regulation (EU) 2024/1083;*** ***(36) 'media service provider' means a media service provider as defined in Article 2(2) of Regulation (EU) 2024/1083;'*** ***(37) 'online interface' means an online interface as defined in Article 3(m) of Regulation (EU) 2022/2065.***	and should not be transferred to the GDPR.
Art. 4 Definitions	**Art. 3, Point 1 (b)**	-	***(38) "scientific research" means any research which can also support innovation, such as technological development and demonstration. These actions shall contribute to existing scientific knowledge or apply existing knowledge in novel ways, be carried out with the aim of contributing to the growth of society's general knowledge and wellbeing and adhere to ethical standards in the relevant research area. This does not exclude that the research may also aim to further a commercial interest.***	EDRi supports maintaining the current wording of the GDPR and opposes any expansion of the definition through the Omnibus proposal. The existing GDPR framework already provides flexibility for scientific research through Article 89 and the related recitals, while maintaining safeguards for fundamental rights. Expanding the definition of scientific research risks blurring the distinction between research conducted in the public interest and commercial product development. In particular, the development and optimisation of commercial AI systems should not be treated as scientific research unless the

GDPR Articles	Digital Omnibus Proposal	Current text of the GDPR	Proposed change	EDRi position
				activity is genuinely conducted in the public interest and subject to the safeguards foreseen in the GDPR.
Art. 5(1)(b) Purpose limitation	**Art. 3, Point 2**	Personal data shall be: [...] collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation')	Personal data shall be: [...] 'collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), ~~not~~ be considered to be ~~incompatible~~ ***compatible with the initial purposes, independent of the conditions of Article 6(4) of this Regulation***, ('purpose limitation');	EDRi opposes reopening the principle of purpose limitation. Purpose limitation is one of the core principles of the GDPR and plays a central role in preventing the uncontrolled reuse of personal data. The existing framework already provides a clear mechanism for further processing through the compatibility assessment under Article 6(4). Introducing additional concepts such as 'appropriate safeguards' without clearly anchoring them to the compatibility framework risks creating ambiguity and weakening the structured assessment required under Article 6(4). Such ambiguity could enable broader interpretations that allow personal data to be reused for purposes that are not compatible with the original collection purpose. Any clarification in this area must explicitly confirm that further processing remains subject to the compatibility test under Article 6(4). References to safeguards must reinforce the existing GDPR principles, including data minimisation, transparency,

GDPR Articles	Digital Omnibus Proposal	Current text of the GDPR	Proposed change	EDRi position
				and effective rights for data subjects.
Art. 9 (2) Special categories of personal data; biometric verification and AI residuals	**Art. 3, Point 3**	Paragraph 1 shall not apply if one of the following applies: [...]	Paragraph 1 shall not apply if one of the following applies: [...] ***'(k) processing in the context of the development and operation of an AI system as defined in Article 3, point (1), of Regulation (EU) 2024/1689 or an AI model, subject to the conditions referred to in paragraph 5.*** ***(l) processing of biometric data is necessary for the purpose of confirming the identity of a data subject (verification), where the biometric data or the means needed for the verification is under the sole control of the data subject.'*** ***5. For processing referred to in point (k) of paragraph 2, appropriate organisational and technical measures shall be implemented to avoid v the collection and otherwise processing of special categories of personal data.*** ***Where, despite the implementation of such measures, the controller identifies special categories of personal data in the datasets used for training, testing or validation n the AI system or AI model, the controller shall remove such data. If removal of those data requires disproportionate effort, the controller shall in any event effectively protect without undue delay such data from being used to produce outputs, from being disclosed or***	EDRi opposes reopening Article 9. Special categories of personal data receive heightened protection under the GDPR because their processing poses significant risks to fundamental rights. Expanding the list of exceptions risks normalising the processing of highly sensitive data and weakening the safeguards established by the Regulation. With regard to AI training datasets, the proposed derogation risks legitimising the presence of sensitive data within AI systems. The presence of such data should remain exceptional. Processing should only be permitted where sensitive data appear incidentally or unintentionally in datasets and where the functioning of the system does not rely on them. Controllers should be required to demonstrate that effective measures were taken to prevent the collection of such data and that removal is technically impossible rather than merely burdensome. Where sensitive data are detected, controllers should remove them without undue delay and ensure that they cannot influence outputs or be disclosed. With regard to biometric authentication, biometric verification should only be

GDPR Articles	Digital Omnibus Proposal	Current text of the GDPR	Proposed change	EDRi position
			otherwise made available to third parties.'	permitted in narrowly defined authentication contexts where it is strictly necessary. Alternative authentication methods must remain available, and biometric templates should remain under the effective control of the data subject.
new Article 88c AI development/ operation	**Art. 3, Point 15**	-	*Processing in the context of the development and operation of AI* *Where the processing of personal data is necessary for the interests of the controller in the context of the development and operation of an AI system as defined in Article 3, point (1), of Regulation (EU) 2024/1689 or an AI model, such processing may be pursued for legitimate interests within the meaning of Article 6(1)(f) of Regulation (EU) 2016/679, where appropriate, except where other Union or national laws explicitly require consent, and where such interests are overridden by the interests, or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.* *Any such processing shall be subject to appropriate organisational, technical measures and safeguards for the rights and freedoms of the data subject, such as to ensure respect of data minimisation during the stage of selection of sources and the training and testing of AI an*	EDRi opposes the introduction of a specific lawful basis for processing personal data in the context of the development and operation of AI systems. The GDPR is designed to remain technologically neutral. Introducing a dedicated provision for AI development risks creating the perception that large-scale data reuse for AI training is inherently legitimate. Controllers developing AI systems must rely on the existing legal bases under Article 6 and comply fully with the requirements of purpose limitation, data minimisation, transparency, and fairness. If the provision were to remain, it must be clarified that it does not create a presumption of legitimacy and does not modify the requirements of Article 6(1)(f). The legitimate interest test must continue to apply in full, including the balancing test and the right of individuals to object to the processing of their personal data. Large-scale scraping of personal data

GDPR Articles	Digital Omnibus Proposal	Current text of the GDPR	Proposed change	EDRi position
			system or AI model, to protect against non-disclosure of residually retained data in the AI system or AI model to ensure enhanced transparency to data subjects and providing data subjects with an unconditional right to object to the processing of their personal data.'	from publicly accessible sources should not automatically be considered compatible with legitimate interests.
Art. 12 Access requests	**Art. 3, Point 4**	5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either: (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or (b) refuse to act on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.	*5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character* ***or also, for requests under Article 15 because the data subject abuses the rights conferred by this regulation for purposes other than the protection of their data,*** *the controller may either:* *(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or* *(b) refuse to act on the request.* The controller shall bear the burden of demonstrating ~~the manifestly unfounded or excessive character of the request~~ ***that the request is manifestly unfounded or that there are reasonable grounds to believe that it is excessive.'***	EDRi opposes introducing the concept of 'abusive intention' as a ground to refuse the exercise of data subject rights. The right of access is a central accountability mechanism under the GDPR. Individuals rely on this right to understand how their personal data are processed and to exercise other rights effectively. The GDPR does not require individuals to justify the exercise of their rights. Introducing subjective assessments of the motivation of the requester risks enabling controllers to reject legitimate requests and undermines the effectiveness of the rights framework. Access requests should therefore not be considered abusive solely because they are broad, exploratory, or submitted with the aim of verifying the lawfulness of processing. Any refusal on the basis of abusive intention should require clear evidence and be documented and subject to supervisory oversight.

GDPR Articles	Digital Omnibus Proposal	Current text of the GDPR	Proposed change	EDRi position
Art. 13 Information requirements	**Art. 3, Points 5-6**	Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.	'4. Paragraphs 1, 2 and 3 shall not apply where ~~and insofar as~~ ***the personal data have been collected in the context of a clear and circumscribed relationship between data subjects and a controller exercising an activity that is not data-intensive and there are reasonable grounds to assume that*** the data subject already has the information ***referred to in points (a) and (c) of paragraph 1, unless the controller transmits the data to other recipients or categories of recipients, transfers the data to a third country, carries out automated decision-making, including profiling, referred to in Article 22(1), or the processing is likely to result in a high risk to the rights and freedoms of data subjects within the meaning of Article 35.'*** ***'5. When the processing takes place for scientific research purposes and the provision of information referred to under paragraphs 1, 2 and 3 proves impossible or would involve a disproportionate effort subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing, the controller does not need to provide the information referred to under paragraphs 1, 2 and 3. In such cases, the controller shall take appropriate measures to protect the data***	EDRi opposes reopening transparency obligations under Article 13. Transparency is a fundamental element of the GDPR framework. Information obligations enable individuals to understand how their personal data are processed and to exercise their rights effectively. Introducing exemptions risks weakening the ability of individuals to remain informed about data processing activities, particularly in situations characterised by structural information asymmetries between controllers and individuals. If any clarification were to be considered, the exemption should remain strictly limited to situations where the data subject demonstrably already possesses the information and where processing occurs within a clearly defined and limited relationship that is unlikely to result in risks to individuals' rights and freedoms. Controllers should bear the burden of demonstrating that these conditions are fulfilled.

GDPR Articles	Digital Omnibus Proposal	Current text of the GDPR	Proposed change	EDRi position
			subject's rights and freedoms and legitimate interests, including making the information publicly available.	
Art. 22 Automated decision-making (ADM)	**Art. 3, Point 7**	1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. 2. Paragraph 1 shall not apply if the decision: (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;	'***1.*** ~~The data subject shall have the right not to be subject to~~ A decision which produces legal effects ***for a data subject*** or similarly significantly affects him or her ***may be*** based solely on automated processing, including profiling, ***only where that decision:*** (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;***	EDRi strongly opposes reopening Article 22. Article 22 establishes a central safeguard in the GDPR by recognising the right not to be subject to decisions based solely on automated processing that produce legal or similarly significant effects. This structure ensures that individuals are protected against decisions that may significantly affect their lives without meaningful human oversight. Weakening or restructuring this safeguard would normalise automated decision-making in sensitive contexts such as employment, access to services, financial decisions, and public administration. Automated systems often operate with limited transparency and may reproduce or amplify bias and discrimination. The current structure of Article 22 should therefore be preserved. Any future reform should aim to strengthen safeguards, including clearer requirements for meaningful human intervention, stronger transparency obligations regarding automated decision systems, and effective avenues for individuals to contest automated decisions.

GDPR Articles	Digital Omnibus Proposal	Current text of the GDPR	Proposed change	EDRi position
Art. 33 Data breach notification	**Art. 3, Point 8**	1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.	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 ~~72~~ ***96*** 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 t***o the supervisory authority competent in accordance with Article 55 ***and Article 56*** ~~unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.~~ Where the notification to the supervisory authority is not made within ~~72~~ ***96*** hours, it shall be accompanied by reasons for the delay.' ***'1a. Until the establishment of the single-entry point pursuant to Article 23a of Directive (EU) 2022/2555, controllers shall continue to notify personal data breaches directly to the competent supervisory authority in accordance with Article 55 and Article 56.'*** ***'6. The Board shall prepare and transmit to the Commission a proposal for a common template for notifying a personal data breach to the competent supervisory authority referred to in paragraph 1, as well as for a list of the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person. The proposals shall be submitted to the Commission within [OP***	Raising the notification threshold from 'risk' to 'high risk' would significantly reduce the number of breaches reported to supervisory authorities and weaken oversight of data protection violations. Extending the notification deadline from 72 to 96 hours further delays supervisory awareness of breaches. While a common template for breach notifications could improve consistency, granting the Commission implementing powers over risk criteria risks centralising decisions that should remain within the competence of supervisory authorities and the EDPB.

GDPR Articles	Digital Omnibus Proposal	Current text of the GDPR	Proposed change	EDRi position
			date = nine months of the entry into application of this Regulation]. The Commission after due consideration reviews it, as necessary, and is empowered to adopt it by way of an implementing act in accordance with the examination procedure set out in Article 93(2). ***7. The template and the list referred to in paragraph 6 shall be reviewed at least every three years and updated where necessary. The Board shall submit its assessment and possible proposals for updates to the Commission in due time. The Commission after due consideration of the proposals reviews them and is empowered to adopt any updates following the procedure in paragraph 6.'***	
Art. 35 DPIAs (Board tasks)	**Art. 3, Point 9**	4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68. 5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact	'4. ~~The supervisory authority shall establish and make public~~ ***The Board shall prepare and transmit to the Commission a proposal for*** a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. ~~The supervisory authority shall communicate those lists to the Board referred to in Article 68.~~ ***5.*** ~~The supervisory authority may also establish and make public~~ ***The Board shall prepare and transmit to the Commission a proposal for*** a list of the kind of processing operations for which no data protection	EDRi supports greater harmonisation of Data Protection Impact Assessment practices across the Union. Coordinated identification of high-risk processing operations and consistent criteria for DPIA obligations can improve legal certainty for controllers while strengthening the protection of individuals' rights. At the same time, the responsibility for establishing lists of processing operations that require or do not

GDPR Articles	Digital Omnibus Proposal	Current text of the GDPR	Proposed change	EDRi position
		assessment is required. The supervisory authority shall communicate those lists to the Board. 6. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.	impact assessment is required. ~~The supervisory authority shall communicate those lists to the Board.~~ ~~6. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.~~ ***The Board shall prepare and transmit to the Commission a proposal for a common template and a common methodology for conducting data protection impact assessments.'*** ***'6a. The proposals for the lists referred to in paragraphs 4 and 5 and for the template and methodology referred to in paragraph 6 shall be submitted to the Commission within [OP date = 9 months of the entry into application of this Regulation]. The Commission after due consideration reviews them, as necessary, and is empowered to adopt them by way of an implementing act in accordance with the examination procedure set out in Article 93(2).*** ***6b. The lists and the template and methodology referred to in paragraph 6a shall be reviewed at least every three***	require a DPIA should remain with supervisory authorities, coordinated through the European Data Protection Board. This approach preserves the independence of data protection authorities and aligns with the risk-based architecture of the GDPR. The adoption of implementing powers by the European Commission in this area would risk politicising technical risk assessments and undermining the institutional balance of the GDPR enforcement framework. The harmonisation of DPIA practices should therefore be achieved through coordinated guidance and cooperation among supervisory authorities within the existing consistency mechanisms. Recommendation: support harmonisation of DPIA practices while maintaining the central role of supervisory authorities and avoiding Commission implementing powers.

GDPR Articles	Digital Omnibus Proposal	Current text of the GDPR	Proposed change	EDRi position
			years and updated where necessary. The Board shall submit its assessment and possible proposals for updates to the Commission in due time. The Commission after due consideration of the proposals reviews them and is empowered to adopt any updates following the procedure in paragraph 6a. ***6c. Lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment and of the kind of processing operations for which no data protection impact assessment is required established and made public by supervisory authorities remain valid until the Commission adopts the implementing act referred to in paragraph 6a.'***	
Art. 70 (1) Tasks of EDPB	**Art. 3, Point 14**	1. The Board shall ensure the consistent application of this Regulation. To that end, the Board shall, on its own initiative or, where relevant, at the request of the Commission, in particular: [...]	1. The Board shall ensure the consistent application of this Regulation. To that end, the Board shall, on its own initiative or, where relevant, at the request of the Commission, in particular: [...] ***'(ha) prepare and transmit to the Commission a proposal for a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment and for which no data protection impact assessment is required, pursuant to Article 35.*** ***(hb) prepare and transmit to the***	EDRi supports strengthening coordination through the European Data Protection Board with regard to lists of high-risk processing operations and DPIA criteria. Guidance from the Board can improve consistency across Member States while preserving the independence of supervisory authorities. However, guidance on pseudonymisation and identifiability should clearly reaffirm that pseudonymised data remain personal data unless identification is no longer

GDPR Articles	Digital Omnibus Proposal	Current text of the GDPR	Proposed change	EDRi position
			Commission a proposal for a common template and a common methodology for conducting data protection impact assessments, pursuant to Article 35. ***(hc) prepare and transmit to the Commission a proposal for a common template for notifying a personal data breach to the competent supervisory authority as well as for a list of the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person pursuant to Article 33'***	reasonably possible. The interpretation of identifiability must remain anchored in Article 4(1) and Recital 26 of the GDPR. The Board's role should therefore focus on clarifying existing legal standards rather than creating new legal categories for pseudonymised data.
new Art. 88a Storing of personal data or accessing to personal data stored in terminal equipment of natural persons (cookies/ trackers)	**Art. 3, Point 15**	-	***Processing of personal data in the terminal equipment of natural persons*** ***(1) Storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person is only allowed when that person has given his or her consent, in accordance with this Regulation.*** ***(2) Paragraph 1 does not preclude storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person, based on Union or Member State law within the meaning of, and subject to the conditions of Article 6, to safeguard the objectives referred to in Article 23(1).*** ***(3) Storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person without consent, and subsequent***	EDRi strongly opposes moving the regulation of access to terminal equipment into the GDPR framework. Rules governing access to terminal equipment and the confidentiality of communications are central elements of the ePrivacy framework and should remain regulated under the ePrivacy Directive. These rules operate as upstream safeguards that prevent intrusive tracking practices before personal data processing occurs. Transferring device access rules into the GDPR risks fragmenting the legal framework and creating uncertainty about which regime applies. The proposal introduces a distinction based on whether accessed information 'constitutes or leads to' the processing of personal data. This

GDPR Articles	Digital Omnibus Proposal	Current text of the GDPR	Proposed change	EDRi position
			processing, shall be lawful to the extent it is necessary for any of the following: ***(a) carrying out the transmission of an electronic communication over an electronic communications network;*** ***(b) providing a service explicitly requested by the data subject;*** ***(c) creating aggregated information about the usage of an online service to measure the audience of such a service, where it is carried out by the controller of that online service solely for its own use;*** ***(d) 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.*** ***(4) Where storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person is based on consent, the following shall apply:*** ***(a) the data subject shall be able to refuse requests for consent in an easy and intelligible manner with a single-click button or equivalent means;*** ***(b) if the data subject gives consent, the controller shall not make a new request for consent for the same purpose for the period during which the controller can*** ***(c) lawfully rely on the consent of the data subject;*** ***(d) if the data subject declines a request for consent, the controller shall not make a new request for consent for the same***	distinction is technically unstable and risks generating inconsistent enforcement across Member States. A more coherent approach is to maintain a single device-access rule under ePrivacy, applicable regardless of whether the information accessed constitutes personal data. The GDPR should continue to regulate the subsequent processing of personal data once collected. Exceptions to the device-access rule could be modernised within the ePrivacy Directive, provided that strict safeguards are introduced. Any such exceptions should be narrowly defined, technically constrained, and should prohibit persistent identifiers, fingerprinting, cross-service tracking, or reuse of collected data for advertising, profiling, or AI training.

GDPR Articles	Digital Omnibus Proposal	Current text of the GDPR	Proposed change	EDRi position
			purpose for a period of at least six months. This paragraph also applies to the subsequent processing of personal data based on consent. ***(5) This Article shall apply from [OP: please insert the date = 6 months following the date of entry into force of this Regulation]***	
new Art. 88b Automated, machine-readable consent/ objection signals	**Art. 3, Point 15**		***Automated and machine-readable indications of data subject's choices with respect to processing of personal data in the terminal equipment of natural persons*** ***(1) Controllers shall ensure that their online interfaces allow data subjects to:*** ***(a) Give consent through automated and machine-readable means, provided that the conditions for consent laid down in this Regulation are fulfilled;*** ***(b) decline a request for consent and exercise the right to object pursuant to Article 21(2) through automated and machine-readable means.*** ***(2) Controllers shall respect the choices made by data subjects in accordance with paragraph 1.*** ***(3) Paragraphs 1 and 2 shall not apply to controllers that are media service providers when providing a media service.*** ***(4) The Commission shall, in accordance with Article 10(1) of Regulation (EU) 1025/2012, request one or more European standardisation organisations to draft standards for the interpretation of***	EDRi supports the objective of enabling machine-readable signals to express users' preferences regarding tracking and data processing. Such mechanisms can reduce manipulative consent interfaces and provide users with durable tools to express refusal. However, privacy signals must be clearly defined in law and must be binding on controllers from the outset. Key elements such as the semantics of the signal, its scope across web and application environments, and its legal effect should not be left entirely to future technical standards. Without clear legal definitions, implementation risks becoming inconsistent across the digital ecosystem. Privacy signals must also be designed in a way that does not introduce new tracking infrastructures or additional layers of data collection. Their primary function should be to enable effective

GDPR Articles	Digital Omnibus Proposal	Current text of the GDPR	Proposed change	EDRi position
			machine-readable indications of data subjects' choices. *Online interfaces of controllers which are in conformity with harmonised standards or parts thereof the references of which have been published in the Official Journal of the European Union shall be presumed to be in conformity with the requirements covered by those standards or parts thereof, set out in paragraph 1.* (5) *Paragraphs 1 and 2 shall apply from [OP: please insert the date = 24 months following the date of entry into force of this Regulation].* *(6) Providers of web browsers, which are not SMEs, shall provide the technical means to allow data subjects to give their consent and to refuse a request for consent and exercise the right to object pursuant to Article 21(2) through the automated and machine-readable means referred to in paragraph 1 of this Article, as applied pursuant to paragraphs 2 to 5 of this Article.* *(7) Paragraph 6 shall apply from [OP: please insert the date = 48 months following the date of entry into force of this Regulation].*	refusal of non-essential tracking practices.