GDPR Articles (ePD in some cases)	Digital Omnibus Proposal	Current text of the GDPR (ePD in some cases)	Commission's proposal	Council's General Approach	EDRi position
Art. 4 (1) Definition of 'personal data'	**Art. 3, Point 1 (a)** **Recital 27**	'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***	**Deletion**	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

GDPR Articles (ePD in some cases)	Digital Omnibus Proposal	Current text of the GDPR (ePD in some cases)	Commission's proposal	Council's General Approach	EDRi position
			reasonably likely to be used to identify the natural person to whom the information relates.		linkage across datasets.
New Art. 25a Application of pseudonymisation and identification of a natural person	**Art. 3(10) New Recitals 27a-27c**	**No Article 25a**	**No Article 25a**	***Article 25a - Application of pseudonymisation and identification of a natural person*** ***(1) Controllers and processors may apply pseudonymisation in order to reduce the risks to the data subjects concerned and to comply with their obligations under this Regulation, in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information. The application of pseudonymisation shall be subject to appropriate technical and organisational measures, including security measures, to prevent other persons from identifying the data subject.*** ***(2) Pseudonymised data shall not be considered personal data for***	Reject: the text says pseudonymised information is not personal for a third party unable to identify the person. Recital 27b insists on objective, contextual factors, including singling out, available technical measures, legal barriers and onward transfers. Article 25a(3) also treats disclosure to a recipient able to identify as personal-data processing for both actors. These qualifications are relevant, and prevent an entirely subjective interpretation, but do not solve the difficulty: the Regulation would now require actors, individuals and authorities to reconstruct the identifiability

GDPR Articles (ePD in some cases)	Digital Omnibus Proposal	Current text of the GDPR (ePD in some cases)	Commission's proposal	Council's General Approach	EDRi position
				third party if that third party is unable to identify the natural person to whom the data relates. ***(3)Where a third party discloses, transmits or otherwise makes data referred to in paragraph 2 available to another third party and, in light of all relevant circumstances, that other third party possesses or can obtain means reasonably likely to enable the data subject to be identified, both the transmission of the data to that other third party and the subsequent processing of the data by that other third party is processing of personal data.*** ***(4)Where a processor processes personal data on behalf of a controller, that data shall be considered personal data for the processor, and the processor continues to be subject to the obligations applicable under this Regulation.*** ***(5) To determine whether a natural person is identifiable, including through personal data having undergone pseudonymisation, account shall be taken of all the means reasonably likely to be used to identify the natural person***	of each recipient at each point in a chain before establishing whether basic rights and duties apply. Parties with asymmetric information could assert non-applicability, impeding access, transparency, transfer safeguards and enforcement. Recital 27c's emphasis on guidance does not make these determinations verifiable. If any clarification survives, limit it to existing EDPB guidance on the existing Article 4(1) and Recital 26 test. Article 25a(7) also contains a plain cross-reference error: it asks for the opinion in paragraph (4), while the opinion is prescribed in paragraph (6).

GDPR Articles (ePD in some cases)	Digital Omnibus Proposal	Current text of the GDPR (ePD in some cases)	Commission's proposal	Council's General Approach	EDRi position
				directly or indirectly. ***(6) The Board shall issue an opinion, in accordance with Article 64(2) of this Regulation, addressing the application of pseudonymisation and anonymisation, including related technical and organisational measures.*** ***(7) The Chair of the Board shall request the opinion referred to in paragraph 4 no later than 6 months after the entry into force of this Regulation. The opinion shall be reviewed and updated where necessary.***	
New Art. 41a	**Art. 3, Point 10** **Recital 27**	-	***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***	**Deletion**	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-

GDPR Articles (ePD in some cases)	Digital Omnibus Proposal	Current text of the GDPR (ePD in some cases)	Commission's proposal	Council's General Approach	EDRi position
			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).*		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)** **Recitals 44, 46 and 47**		*(32) 'terminal equipment' means terminal equipment as set out in Article 1(1) of Directive 2008/63/EC;* *(33) for 'electronic communications networks' the*	*Deleted*	Not necessary, as provisions currently governed by the ePrivacy Directive should remain within the sector-specific framework for electronic

GDPR Articles (ePD in some cases)	Digital Omnibus Proposal	Current text of the GDPR (ePD in some cases)	Commission's proposal	Council's General Approach	EDRi position
			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.*		communications and should not be transferred to the GDPR.
Art. 4 Definitions	**Art. 3, Point 1 (b)** **Recital 28**	-	*(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*	*(38) 'scientific research' means any research conducted with the aim of contributing to the growth of society's general knowledge and wellbeing, generating new or complementing existing scientific knowledge, following a methodological and systematic approach consistent with standards of the relevant scientific field, including ethical standards, and*	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

GDPR Articles (ePD in some cases)	Digital Omnibus Proposal	Current text of the GDPR (ePD in some cases)	Commission's proposal	Council's General Approach	EDRi position
			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.	***producing verifiable and transparent results in an autonomous and independent manner. This does not exclude that the research may also aim to further a commercial interest.'***	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 activity is genuinely conducted in the public interest and subject to the safeguards foreseen in the GDPR. The **Council's General Approach** materially improves the Commission draft by requiring a methodological and systematic approach consistent with scientific standards, verifiable and transparent results, and independent conduct. These criteria offer useful limits, but the continued acknowledgement of commercial interests needs to be read with Recitals 29 and 32, the rewrite of purpose limitation

GDPR Articles (ePD in some cases)	Digital Omnibus Proposal	Current text of the GDPR (ePD in some cases)	Commission's proposal	Council's General Approach	EDRi position
					and the new research information derogation. Together, these may let ordinary commercial product testing or AI optimisation invoke research privileges without a genuine scientific objective. If a definition is retained, decision-makers should make clear that routine product development or commercial optimisation do not qualify simply because they use research methods, and that Article 89 safeguards, purpose limitation, transparency and legal bases remain applicable.
Art. 5(1)(b) Purpose limitation	**Art. 3, Point 2** **Recital 29**	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,	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	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, ***subject to the application of***	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

GDPR Articles (ePD in some cases)	Digital Omnibus Proposal	Current text of the GDPR (ePD in some cases)	Commission's proposal	Council's General Approach	EDRi position
		in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation')	considered to be ~~incompatible~~ ***compatible with the initial purposes, independent of the conditions of Article 6(4) of this Regulation***, ('purpose limitation');	***appropriate safeguards*** in accordance with Article 89(1), be considered to be compatible with the initial purposes, independent of the conditions of Article 6(4) of this Regulation ('purpose limitation');	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, and effective rights for data subjects. The **Council's General Approach** wording explicitly requires appropriate safeguards under Article 89(1), which is better than treating research reuse as

GDPR Articles (ePD in some cases)	Digital Omnibus Proposal	Current text of the GDPR (ePD in some cases)	Commission's proposal	Council's General Approach	EDRi position
					unconditional. However, it also makes qualifying further processing compatible with the initial purpose independently of Article 6(4). Recital 29 expressly confirms that no Article 6(4) compatibility assessment is needed: this is a substantive change to purpose limitation, and its effect grows when Article 4(38) expands research and Article 13(6) relaxes individual notice. Safeguards should not amount to an unrestricted authorisation for secondary use.
Art. 9 (2) Special categories of personal data; biometric verification and AI residuals	**Art. 3, Point 3** **Recitals 33 and 34**	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***	Paragraph 1 shall not apply if one of the following applies: [...] ***'(k) incidental processing of residual data, where not intended by the controller, in the context of the development and technical operation of an AI system as defined in Article 3, point (1), of Regulation (EU) 2024/1689 or an AI model as referred to in Regulation (EU) 2024/1689, subject to the conditions referred to in paragraph 5.***	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.

GDPR Articles (ePD in some cases)	Digital Omnibus Proposal	Current text of the GDPR (ePD in some cases)	Commission's proposal	Council's General Approach	EDRi position
			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 otherwise made available to third parties.'*	*(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 one-to-one verification is under the sole control of the data subject and, where applicable, subject to appropriate safeguards to protect the fundamental rights and the interests of the data subject as laid down in Union law or Member State law, in accordance with paragraph 4 of this Article.* *5. For processing referred to in point (k) of paragraph 2, appropriate organisational and technical measures shall be implemented to avoid 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 that are incidentally and residually involved in the datasets used for the development of and technical operation of the AI system or AI model, including training, validation*	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 permitted in narrowly defined

GDPR Articles (ePD in some cases)	Digital Omnibus Proposal	Current text of the GDPR (ePD in some cases)	Commission's proposal	Council's General Approach	EDRi position
				and testing, the controller shall erase such data without undue delay. If erasure of those data proves to be technically impossible or requires manifestly disproportionate effort, the controller shall, without undue delay and in any event, effectively protect such data from being further processed or processed for other purposes, used to produce outputs, disclosed or otherwise made available to third parties.'	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. In the **Council's General Approach** , Art. 9(2)(k) is narrower than the Commission's proposal, as it covers unintended incidental and residual special-category data in development or technical operation, rather than any sensitive processing for AI. Art. 9(5) further requires preventive measures, erasure without undue delay and, only where erasure is technically impossible or manifestly disproportionate, effective protection from further processing, outputs and disclosure. Recital 33 excludes intentional use, including use of sensitive features necessary to a model. These changes reduce the risk but do not establish why a new GDPR exception is

GDPR Articles (ePD in some cases)	Digital Omnibus Proposal	Current text of the GDPR (ePD in some cases)	Commission's proposal	Council's General Approach	EDRi position
					necessary, who can verify that sensitive attributes are truly isolated inside model parameters, or how a data subject can secure erasure or challenge retained data. In point (l), the Council introduces one-to-one verification, necessity, sole control and a reference to safeguards under Union or Member State law. Recital 34 gives a more detailed meaning to sole control and recommends less intrusive means. Nevertheless, the operative clause creates a technology-specific Art. 9 derogation even where an employer or essential service makes biometrics a practical condition of access. Sole technical control does not address coercion, function creep or the absence of an alternative.
new Article 88c/88bis	**Art. 3, Point 15** **Recitals 30**	**No Article 88c/88bis**	***Processing in the context of the development and operation of AI*** ***Where the processing of personal data is necessary for the***	***Processing in the context of the development and operation of AI*** ***(1) The processing of personal data in the context of the development and***	EDRi opposes the introduction of a specific lawful basis for processing personal data in the context of the development and

GDPR Articles (ePD in some cases)	Digital Omnibus Proposal	Current text of the GDPR (ePD in some cases)	Commission's proposal	Council's General Approach	EDRi position
AI development/ operation	**and 31**		***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 system or AI model, to protect against non-disclosure of residually retained data in the AI system or AI model***	***operation of an AI system or of an AI model, may be carried out for a legitimate interest of the controller or a third party in accordance with Article 6(1)(f) of this Regulation.*** ***(2) Paragraph 1 does not affect the obligation of the controller to choose an appropriate lawful ground of processing set out in Article 6 of this Regulation.*** ***(3) Regardless of the lawful ground of processing pursuant to Article 6, processing in the context of the development and operation of AI shall be subject to appropriate technical and organisational measures and safeguards to protect the rights and freedoms of the data subject in accordance with this Regulation, including the right to object under Article 21.***	operation of AI systems. The GDPR is designed to remain technologically neutral. Introducing a dedicated provision for AI 'development and operation' (extremely broad terms) 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.

GDPR Articles (ePD in some cases)	Digital Omnibus Proposal	Current text of the GDPR (ePD in some cases)	Commission's proposal	Council's General Approach	EDRi position
			to ensure enhanced transparency to data subjects and providing data subjects with an unconditional right to object to the processing of their personal data.'		Large-scale scraping of personal data from publicly accessible sources should not automatically be considered compatible with legitimate interests. The **Council's General Approach** Article 88bis is shorter than Commission Article 88c and expressly points back to Article 6(1)(f), the controller's responsibility to choose a lawful basis and all existing safeguards, including the Art. 21 right to object. Recital 33a adds that AI development does not itself constitute a legitimate interest and that assessment must depend on the specific underlying purpose. These look like meaningful improvements in drafting, but most are explanations in a recital and the operative provision still singles out AI for explicit legislative recognition of legitimate interests. The reference to interests of a controller or third party could be invoked to

GDPR Articles (ePD in some cases)	Digital Omnibus Proposal	Current text of the GDPR (ePD in some cases)	Commission's proposal	Council's General Approach	EDRi position
					legitimise extensive collection, scraping and reuse without adequate necessity, fairness, reasonable expectations or compatibility assessments. Even if the three-step test formally survives, Art. 88bis may tilt its interpretation, especially alongside Art. 9(2)(k) and reduced information duties.
Art. 12 Access requests	**Art. 3, Point 4** **Recital 35**	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	*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*	*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,* ***for a request under Article 15, where an abusive intention on the part of the data subject submitting those requests can be demonstrated****, the controller may either:* *(a) charge a reasonable fee* ***proportionate to*** *the administrative costs of providing the information or communication or taking the action requested; or* *(b) refuse to act on the request* ***and inform the data subject of the***	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

GDPR Articles (ePD in some cases)	Digital Omnibus Proposal	Current text of the GDPR (ePD in some cases)	Commission's proposal	Council's General Approach	EDRi position
		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.	*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.'***	***reasons thereof****.* *The controller shall bear the burden of demonstrating that the request is manifestly unfounded or that there are reasonable grounds to believe that,* ***in the light of all the relevant circumstances of the case, that the request is excessive or that there is an abusive intention on the part of the data subject****.*	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. The **Council's General Approach** replaces the Commission's open-ended reference to exercising rights for purposes other than data protection with 'abusive intention' that must be demonstrated. It also requires controllers to give reasons for refusal and places the evidential burden on them. These modifications are narrower, but subjective motives still introduce an unnecessary source of litigation and discretion into a right that individuals need to

GDPR Articles (ePD in some cases)	Digital Omnibus Proposal	Current text of the GDPR (ePD in some cases)	Commission's proposal	Council's General Approach	EDRi position
					uncover unlawful profiling, discrimination and surveillance. Legal challenges, representative actions, journalistic inquiries and parallel consumer or employment claims can involve several legitimate motivations. Abuse of the law is a legally recognised figure, as reiterated by the CJEU, and neither broad scope nor adversarial purpose should establish it exists. Recitals 35 and 35a should not be read to permit conjecture about someone's motives.
new Article 57(4) Requests to supervisory authorities	**Art. 3(11) (ab) Recital 35a**	4. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the supervisory authority may charge a reasonable fee based on administrative costs, or refuse to act on the request. The supervisory authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.	No equivalent amendment to Article 57(4)	4. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character ***or where an abusive intention on the part of the data subject submitting those request can be demonstrated,*** the supervisory authority may charge a reasonable fee based on administrative costs, or refuse to act on the request. The supervisory authority shall, ***in the light of all the relevant circumstances of the case,*** bear the burden of	The **Council's General Approach** extends the abusive-intention concept to requests addressed to supervisory authorities. Article 57(4) already permits refusal or a fee for objectively manifestly unfounded or excessive requests and places the burden of proof on the authority. A motive-based addition risks curtailing the right to lodge complaints and obtain effective

GDPR Articles (ePD in some cases)	Digital Omnibus Proposal	Current text of the GDPR (ePD in some cases)	Commission's proposal	Council's General Approach	EDRi position
				demonstrating the manifestly unfounded or excessive character of the request.	supervision where individuals submit repeated evidence, coordinate complaints or pursue strategic litigation, and will also create a chilling effect. Recital 35a gives illustrations of conduct alleged to be abusive, but cannot turn disagreement with a complainant's purpose into grounds to refuse examination.
Art. 13 Information requirements	**Art. 3, Points 5-6 Recitals 36 and 37**	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***	***5*** Paragraphs 1, 2 and 3 shall not apply ***if and to the extent that:*** ***a) there are reasonable grounds to believe that the data subject already has the information referred to in points (a) and (c) of paragraph 1, and*** ***b) the processing is not likely to result in a high risk to the rights and freedoms of data subjects within the meaning of Article 35. This paragraph shall not apply where the processing requires complex processing operations, the processing of large amounts of personal data, or personal data referred to in Articles 9 and 10.***	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

GDPR Articles (ePD in some cases)	Digital Omnibus Proposal	Current text of the GDPR (ePD in some cases)	Commission's proposal	Council's General Approach	EDRi position
			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 subject's rights and freedoms and legitimate interests, including making the information publicly available.*	*6. When the further processing takes place for scientific research purposes by the same controller and where and insofar as the provision of information referred to under paragraphs 1, 2 and 3 proves impossible or would involve a disproportionate effort 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 further processing, subject to the conditions and safeguards referred to in Article 89(1), 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 subject's rights and freedoms and legitimate interests, including making the information publicly available.*	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. The **Council's General Approach** narrows the Commission's proposed exception. Art. 13(5) requires reasonable grounds to believe the person already knows the identity of the controller and the purpose of processing, limits the provision to non-high-risk processing, and excludes complex processing,

GDPR Articles (ePD in some cases)	Digital Omnibus Proposal	Current text of the GDPR (ePD in some cases)	Commission's proposal	Council's General Approach	EDRi position
					large-scale personal data and Arts. 9–10 data. Recital 36 illustrates simpler relationships. Those constraints are welcome, but the result remains wider than the existing Article 13(4) rule that exempts information only to the extent the individual already has it. Knowledge of Article 13(1)(a) and (c) cannot replace notice of lawful basis, retention, recipients, rights, international transfers and automated decisions. In particular, the exception appears to relieve the full set of duties in paragraphs 1–3 after establishing presumed knowledge of just two elements. The Council also limits the new scientific-research exemption to further processing by the same controller and links it to impossibility, disproportionate effort or serious impairment of the research objective. It also cross-refers to Art. 89(1) safeguards and requires

GDPR Articles (ePD in some cases)	Digital Omnibus Proposal	Current text of the GDPR (ePD in some cases)	Commission's proposal	Council's General Approach	EDRi position
					alternative protection, including public information. Recital 37 explains those limitations. This is narrower than a general exemption for scientific research but still removes individual information duties precisely when data are reused for a new purpose. As mentioned, the implications grow with the expanded research definition in Art. 4(38) and the special compatibility rule in Art. 5(1)(b). Public notices are rarely equivalent to targeted information, particularly when a researcher can contact participants or where sensitive data are involved.
Art. 22 Automated decision-making (ADM)	**Art. 3, Point 7** **Recital 38**	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	***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,	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, ***unless such processing:*** (a) is necessary for entering into, or	EDRi strongly opposes reopening Article 22 in a context of deregulation. The provision 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

GDPR Articles (ePD in some cases)	Digital Omnibus Proposal	Current text of the GDPR (ePD in some cases)	Commission's proposal	Council's General Approach	EDRi position
		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; (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or (c) is based on the data subject's explicit consent. 3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.	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;***	performance of, a contract between the data subject and a data controller; (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or (c) is based on the data subject's explicit consent. ***2.*** In the cases referred to in points (a) and (c) of paragraph ***1***, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision. ***3.*** Decisions referred to in paragraph ***1*** shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place	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 (ePD in some cases)	Digital Omnibus Proposal	Current text of the GDPR (ePD in some cases)	Commission's proposal	Council's General Approach	EDRi position
		4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.			The **Council's General Approach** refuses the Commission's proposal. However, Recital 38 affirmatively says a human alternative does not prevent a controller from treating an automated decision as necessary to perform a contract. It also instructs controllers to choose the less intrusive option only among equally effective automated solutions, excluding a human alternative from that comparison. This would weaken the substantive necessity and proportionality analysis, despite deletion of the express sentence in the article.
new Article 25(1)–(2) Data protection by design/ default	**Article 6(a) Recital 39a**	1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the	No proposed change	1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, ***with particular regard to the lists referred to in Article 35(4) and (5),*** the controller ***and the processor*** shall, both at the time of	The **Council's General Approach** expressly extends Article 25's design-and-default duties to processors, not just controllers, and links the assessment to EDPB DPIA lists under Article 35. Recital 39a explains that processors should apply these requirements in their own technical means and services

GDPR Articles (ePD in some cases)	Digital Omnibus Proposal	Current text of the GDPR (ePD in some cases)	Commission's proposal	Council's General Approach	EDRi position
		determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects. 2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures		the determination of the means for processing and at the time of the processing itself ***as applicable,*** implement, ***in an effective manner,*** appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects. 2. The controller ***and the processor*** shall implement appropriate technical and organisational measures ***to ensure*** that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible to an indefinite number of natural persons ***without the individual's intervention.***	while controllers remain responsible for purposes, means and accountability. Stronger duties on processors that design tracking SDKs, cloud architectures and AI infrastructure could be valuable. Yet the proposed words 'controller and processor' apply to both paragraphs without clearly limiting processors to aspects they control, while the phrase 'as applicable' could create uncertainty. Equally, a DPIA whitelist cannot become a waiver of Art. 25 duties, which apply regardless of whether an impact assessment is required.

GDPR Articles (ePD in some cases)	Digital Omnibus Proposal	Current text of the GDPR (ePD in some cases)	Commission's proposal	Council's General Approach	EDRi position
		shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.			
Art. 33 Data breach notific ation	**Art. 3, Point 8** **Recital 39**	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***	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 ***96*** hours after having become aware of it, notify the personal data breach ***with the support of the national entry point established pursuant to Article 23b 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 ***96*** hours, it shall be accompanied by reasons for the delay. ***1a. Until the establishment of the national entry point pursuant to Article 23b of Directive (EU) 2022/2555, controllers shall continue to notify personal data breaches directly to the***	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. The Council's General Approach retains both substantive changes

GDPR Articles (ePD in some cases)	Digital Omnibus Proposal	Current text of the GDPR (ePD in some cases)	Commission's proposal	Council's General Approach	EDRi position
			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 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).*	*competent supervisory authority in accordance with Article 55 and Article 56 of this Regulation.* *6. The Board shall establish and make public a list of the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person and a list of the circumstances in which it is not likely to result in such a high risk. The lists shall be available by [OP date = nine months from the date of entry into application of this Regulation].* *7. The lists referred to in paragraph 6 shall be reviewed by the Board at least every three years and updated where necessary.* *8. 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. That proposal shall be submitted to the Commission by [OP date = nine*	opposed by EDRi: the higher notification threshold and the extension to 96 hours. Neither addresses the underlying need for effective oversight, and both should be rejected. However, the Council does introduce improvements compared with the Commission proposal: it assigns responsibility for establishing and publishing the risk-assessment lists directly to the EDPB, rather than requiring their adoption through Commission implementing acts; and introduces lists covering circumstances both likely and unlikely to result in high risk. Nevertheless, the introduction of a list of circumstances considered unlikely to result in high risk raises concerns, because controllers could treat such lists as categorical exemptions from notification, without adequately considering the context, scale, affected populations or cumulative consequences of incidents. This concern becomes

GDPR Articles (ePD in some cases)	Digital Omnibus Proposal	Current text of the GDPR (ePD in some cases)	Commission's proposal	Council's General Approach	EDRi position
			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.'	*months from the date of entry into application of this Regulation]. The Commission after due consideration of the proposal reviews it and is empowered to adopt it by way of an implementing act in accordance with the examination procedure set out in Article 93(2).* *9. The template referred to in paragraph 8 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 proposal reviews it and is empowered to adopt any updates by way of an implementing act in accordance with the examination procedure set out in Article 93(2).*	more significant when reading amended Recital 39. The Council's explicit reminder that controllers must conduct individual assessments and maintain complete documentation under Article 33(5) is welcome. However, documentation held internally cannot replace the independent scrutiny made possible through notifications to supervisory authorities. Nor does the preservation of Article 33(5) address the potential loss of information concerning recurring lower-risk incidents across different controllers or sectors. The Council also retains the development of a harmonised notification template, which EDRi supports.
Art. 35 DPIAs (Board	**Art. 3, Point 9**	4. The supervisory authority shall establish and make public a list of the kind of	'4. ~~The supervisory authority shall establish and make public~~ *The Board shall prepare and transmit*	4. The *Board* shall establish and make public a list of the kind of processing operations which are	EDRi supports greater harmonisation of Data Protection Impact

GDPR Articles (ePD in some cases)	Digital Omnibus Proposal	Current text of the GDPR (ePD in some cases)	Commission's proposal	Council's General Approach	EDRi position
tasks)	**Recital 40**	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 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	***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 impact assessment is required. ~~The supervisory authority shall communicate those lists to the Board.~~ *6.* ~~Prior to the adoption of the lists~~ ~~r~~eferred 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~~	subject to the requirement for a data protection impact assessment pursuant to paragraph 1. 5. The ***Board shall*** establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. ***6. The lists referred to in paragraphs 4 and 5 shall be published by [OP date = 9 months from the date of entry into application of this Regulation]. These lists shall be reviewed by the Board at least every three years and updated where necessary.' (b) the following paragraph is inserted: '6a. 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. The template and methodology shall be submitted to the Commission by [OP date = 9 months from the date of entry into application of this Regulation]. The Commission after due consideration reviews them, as necessary, and is empowered to***	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 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

GDPR Articles (ePD in some cases)	Digital Omnibus Proposal	Current text of the GDPR (ePD in some cases)	Commission's proposal	Council's General Approach	EDRi position
		Member States, or may substantially affect the free movement of personal data within the Union.	~~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 years and updated where necessary. The Board shall submit its assessment and possible***	***adopt them by way of an implementing act in accordance with the examination procedure set out in Article 93(2). 6b. The template and methodology referred to in paragraph 6a 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 by way of an implementing act in accordance with the examination procedure set out in Article 93(2). 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 Board establishes and makes public the lists referred to in paragraph 4 and 5.***	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. The **Council's General Approach** gives the EDPB responsibility for a Union-wide list of processing requiring a DPIA and a list

GDPR Articles (ePD in some cases)	Digital Omnibus Proposal	Current text of the GDPR (ePD in some cases)	Commission's proposal	Council's General Approach	EDRi position
			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.'		for which a DPIA is considered unnecessary, with transitional continuity for national lists. It also requires an EU-wide methodology and template, with Commission implementing acts. Recital 40 presents convergence and predictability as the main goals. Common standards can reduce inconsistent obligations, but a mandatory 'no DPIA' list may encourage formalistic exemptions from an assessment that should be triggered by actual high risk under Art. 35(1), including combinations of processing operations. The Board must be able to revise lists promptly, and national supervisory authorities must retain powers to investigate

GDPR Articles (ePD in some cases)	Digital Omnibus Proposal	Current text of the GDPR (ePD in some cases)	Commission's proposal	Council's General Approach	EDRi position
					unanticipated risks. Prior consultation under Art. 36 should be kept meaningful and guarded against Commission control over substantive risk methodology.
Art. 70 (1) Tasks of EDPB	**Art. 3, Point 14** **Recitals 39, 40 and 27**	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: [...] ***(point (h) is deleted)*** ***'(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 Commission a proposal for a common template and a common methodology for conducting data protection impact assessments,***	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: [...] ***(f) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for further specifying the criteria and conditions for decisions based on profiling pursuant to Article 22(1);*** ***(point (h) is deleted)*** ***(ha) establish 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.*** ***haa establish a list of 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 reasonably possible. The interpretation of identifiability must remain anchored in Article 4(1) and

GDPR Articles (ePD in some cases)	Digital Omnibus Proposal	Current text of the GDPR (ePD in some cases)	Commission's proposal	Council's General Approach	EDRi position
			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'*	*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 and a list of the circumstances in which it is not likely to result in such a high risk.* *(hb) prepare and transmit to the Commission 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 common template for notifying a personal data breach to the competent supervisory authority pursuant to Article 33.* *(hca) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for the purpose of further specifying the appropriate technical and organisational measures to ensure a level of security appropriate to the level of risk pursuant to Article 32.* *(hcb) issue the opinion on the application of pseudonymisation and anonymisation referred to in Article 25a.*	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. The **Council's General Approach** revises and expands the EDPB's responsibilities for Art. 22 profiling guidance, Art. 33 breach-risk lists and templates, Art. 35 DPIA lists and methodologies, Art. 32 security guidance and Art. 25a pseudonymisation advice. These functions could strengthen consistency, but their usefulness depends on the underlying legal standards: a common EDPB list cannot compensate for raising the breach-notification threshold, and a pseudonymisation opinion cannot legitimise an exclusion from the scope of the GDPR. EDPB independence also requires that Commission

GDPR Articles (ePD in some cases)	Digital Omnibus Proposal	Current text of the GDPR (ePD in some cases)	Commission's proposal	Council's General Approach	EDRi position
					implementing powers on templates and methodologies do not override the Board's expertise. The Council also deletes existing EDPB tasks linked to the changed system, so safeguards against gaps in responsibilities are needed
new Art. 88a Storing of personal data or accessing to personal data stored in terminal equipment of natural persons (cookies/ trackers) **Council's GA**	**Art. 3, Point 15** **Council's GA Art. 5(2)** **Recitals 44, 45, 46 and 47, new 43a**	Current text of the Art 5(3) ePD 3. Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications	***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***	**Art 88a is deleted** **Proposal for Art. 5(3) ePD: 3.** Member States shall ensure that the storing of information, or gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed ***when that person*** has given his or her consent, ***in accordance with Regulation (EU) 2016/679.*** ***Storing of information, or gaining of access to information already stored, in the terminal equipment of a subscriber or user without consent, and subsequent processing of personal data for the same purpose, shall be lawful to the extent it is solely related to and strictly necessary for the following purposes:*** ***a) carrying out the transmission of an electronic***	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

GDPR Articles (ePD in some cases)	Digital Omnibus Proposal	Current text of the GDPR (ePD in some cases)	Commission's proposal	Council's General Approach	EDRi position
Art. 5 (3) Terminal equipment and tracking exemptions		network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.	*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 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*	*communication over an electronic communications network;* *b) providing a service, including its functionality, explicitly requested by the subscriber or user;* *c) Creating anonymous aggregated information about the usage of an online service to measure the audience of that service, provided that it is carried out by the provider of the service requested by the subscriber or user, or by a third party on behalf of that provider, and the data collected for the purpose of aggregating the information are not processed for another purpose, shared with third parties or combined with data from third parties;* *d) performing audience measurement in compliance with Article 24 of Regulation (EU) 2024/1083, provided that personal data are pseudonymised after collection and not processed for another purpose, that the processing of personal data does not involve tracking the activity of*	applies. The proposal introduces a distinction based on whether accessed information 'constitutes or leads to' the processing of personal data. This 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-

GDPR Articles (ePD in some cases)	Digital Omnibus Proposal	Current text of the GDPR (ePD in some cases)	Commission's proposal	Council's General Approach	EDRi position
			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 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*	*the subscriber or user outside of the service or the media content to be measured, and that any information shared with third parties other than those acting either on behalf of or jointly together with that provider does not contain personal data;* *e) maintaining or restoring the technical security of the means strictly necessary for the provision of a service requested by the subscriber or user or the technical security of the terminal equipment used for the provision of such service;* *f) measuring the display and performance of advertising that is based solely on the immediate content displayed on a subscriber or user's online interface during an individual visit or on the basis of a single search query and that does not involve the processing of personal data, where such measurement is carried out by the provider of an online service, including jointly with others, or on behalf of that provider. Such measurement shall not involve profiling or processing of data*	service tracking, or reuse of collected data for advertising, profiling, or AI training. The **Council's General Approach** adequately preserves the core ePrivacy rule that access to terminal equipment requires consent, regardless of whether the information is personal data. It also sets a 'solely related to and strictly necessary' threshold for listed exceptions. Point (b) is welcome but must remain tied to functionality explicitly requested by the user. However, points (c), (d) and (f) authorise new consent-free measurements that go beyond the narrow transmission and explicitly requested service exceptions of today's Article 5(3) and what was accepted for the withdrawn ePrivacy Regulation proposal. It is important to note that these are separate policy choices affecting device confidentiality, not mere banner simplification. The opening sentence also purports to make

GDPR Articles (ePD in some cases)	Digital Omnibus Proposal	Current text of the GDPR (ePD in some cases)	Commission's proposal	Council's General Approach	EDRi position
			Regulation]	*relating to the subscriber or user's past or future activity, including activity across sites or services. Data collected for such measurement shall be pseudonymised after collection and shall not be processed for another purpose.* *The subscriber or user shall be able to refuse requests for consent in an easy and intelligible manner with a single-click button or equivalent means. If the subscriber or user gives consent, the provider shall not make a new request for consent for the same purpose for the period during which the controller can lawfully rely on the consent of the subscriber or user. If the subscriber or user refuses a request for consent, the provider shall not make a new request for consent for the same purpose for a period of at least four months.*	subsequent processing of personal data for the same purpose 'lawful'. This must not be interpreted as overriding the separate requirements of Arts. 5, 6 and 9 GDPR. Recital 44g discusses additional GDPR bases for other purposes, which makes the omission of a clear same-purpose safeguard particularly concerning. EDRi therefore requires an express provision that an ePrivacy device-access exemption never itself supplies a GDPR lawful basis or displaces GDPR data-subject rights. Point (c) permits creating aggregated, anonymous audience statistics, including through a third party acting for the provider. That is safer than individual behavioural profiling, but aggregation of the final report does not establish that raw device events or identifiers were anonymous at collection, and therefore the text needs enforceable first-party limits, aggregation as early as

GDPR Articles (ePD in some cases)	Digital Omnibus Proposal	Current text of the GDPR (ePD in some cases)	Commission's proposal	Council's General Approach	EDRi position
					technically possible, short retention, a ban on fingerprinting and persistent cross-context identifiers, and meaningful verification of the 'no reuse or combination' restrictions. Point (d) creates a distinct media audience-measurement exception linked to Art. 24 of the European Media Freedom Act: the data only have to be pseudonymised after collection and joint-controller arrangements remain possible. As mentioned above, pseudonymisation does not remove personal-data protection, and the rule could normalise device-level monitoring by measurement providers. The media-law reference does not itself justify waiving ePrivacy consent. If accepted, this new exception should be at least restricted to genuinely anonymous measurement with strict technical and institutional controls.

GDPR Articles (ePD in some cases)	Digital Omnibus Proposal	Current text of the GDPR (ePD in some cases)	Commission's proposal	Council's General Approach	EDRi position
					Point (f) is the most problematic: it exempts measuring contextual-ad display and performance, a rule that doesn't belong (if at all) under ePrivacy because contextual advertisement shouldn't require access to device or terminal. In addition to that, it specifically includes advertising keyed to a single search query: such queries can reveal health issues, debt, religion or political views. The clause excludes personal-data processing and profiling but then requires collected data to be pseudonymised after collection. These formulations are difficult to reconcile and may invite controllers to define tracking data as 'non-personal' while using identifiers for impression, conversion or frequency measurement. Recital 44g explicitly mentions capping and measurement cookies, and its suggestion that measuring contextual ads requires device access deserves scrutiny. The

GDPR Articles (ePD in some cases)	Digital Omnibus Proposal	Current text of the GDPR (ePD in some cases)	Commission's proposal	Council's General Approach	EDRi position
					point also allows measurements 'jointly with others', widening the scope for commercial intermediaries. Point (e) covers technical security and this is understandable, but it needs narrow interpretation to prevent security and fraud labels becoming a route for persistent tracking. The single-click refusal rule is welcome, yet allowing renewed requests four months after refusal will not prevent repeated pressure, especially across services. Recitals 44b–44g and 45 must be aligned with a tightly limited operative text.
NEW: ePrivacy Articles 15a and 17 **Supervision and impleme**	**Council Art. 5(2a)–(2b)**	(ePrivacy is enforced through national arrangements under the Directive)	**No corresponding provision**	*2a. In Article 15a, the following paragraph is added:* *5. Member States shall designate the competent supervisory authority under Regulation (EU) 2016/679 for the supervision and enforcement of the rules under this Article 5, paragraph 3, of this Directive. 2b. In Article 17, the following paragraph is added:*	EDRi supports the **Council's General Approach 's** assignation of supervision of revised ePD Article 5(3) to GDPR supervisory authorities, which could offer more consistent interpretation and stronger cross-border enforcement of device access,

GDPR Articles (ePD in some cases)	Digital Omnibus Proposal	Current text of the GDPR (ePD in some cases)	Commission's proposal	Council's General Approach	EDRi position
ntation				***3. Member States shall adopt and publish, by [24 months after the adoption of this Regulation] the laws, regulations and administrative provisions necessary to comply with Article 5(3). They shall immediately communicate the text of those measures to the Commission. They should apply those measures from [24 months after the adoption of this Regulation].***	especially where tracking involves personal data. The allocation must preserve the independent Art. 7 Charter confidentiality protection even when a controller argues that device data are not personal. Authorities also need sufficient resources and cooperation with telecom and consumer authorities. The revised Directive requires national implementing measures within 24 months, which creates an avoidable delay and possible variation in the operation of new exemptions.
new Art. 88b Automated, machine-readable consent/ objection signals	**Art. 3, Point 15** **Recitals 45 and 46**		***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-***	**Deletion**	EDRi fully 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

GDPR Articles (ePD in some cases)	Digital Omnibus Proposal	Current text of the GDPR (ePD in some cases)	Commission's proposal	Council's General Approach	EDRi position
			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 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*		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 refusal of non-essential tracking practices. The **Council's General Approach** deletes the entire proposed GDPR Article 88b on machine-readable signals and supplies no equivalent in its ePrivacy changes, thus rejecting the only rights-respecting simplification

GDPR Articles (ePD in some cases)	Digital Omnibus Proposal	Current text of the GDPR (ePD in some cases)	Commission's proposal	Council's General Approach	EDRi position
			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].*		measure proposed by the Commission: legally binding and interoperable refusal can reduce repeated consent demands while protecting the ability to refuse tracking. Deletion abandons one of the few concrete ways to simplify people's experience without stripping them of choice. Recital 45's concern about consent fatigue cannot justify deleting this solution.

GDPR Articles (ePD in some cases)	Digital Omnibus Proposal	Current text of the GDPR (ePD in some cases)	Commission's proposal	Council's General Approach	EDRi position
NEW: GDPR Article 97(5a) Review of Chapter IV	**Council Art. 3(16) and Recital 40a**	**No equivalent**	**No equivalent**	***5a. By [six months after entry into force of this amending Regulation], the Commission shall issue a dedicated report with recommendations on Chapter IV on controller and processor, with particular regard to the proportionality of the obligations for small and medium enterprises and non-commercial organisations undertaking low risk processing activities and whether such obligations should be amended taking into account the level of risk for data subjects.***	The **Council's General Approach** asks the Commission to report within 6 months on GDPR Chapter IV obligations, with particular attention to SMEs, non-commercial organisations and purportedly low-risk processing. This represents a new accelerated route towards reopening controller and processor accountability before the current Omnibus has been implemented or assessed. Recital 40a's emphasis on consistency should not be used to presume that rules themselves are disproportionate. Organisation size is an unreliable proxy for processing risk: small suppliers can operate intrusive advertising, AI or data-broker infrastructure, while large organisations may conduct routine low-risk processing.
New ePrivacy	**Council Art. 5(2c)**	**No equivalent**	**No equivalent**	***The Commission shall submit to the European Parliament and the***	The **Council's General Approach** requires a report on

GDPR Articles (ePD in some cases)	Digital Omnibus Proposal	Current text of the GDPR (ePD in some cases)	Commission's proposal	Council's General Approach	EDRi position
Article 18 Review of privacy-enhancing technologies	**and Recitals 43a–44a**			*Council, no later than [12 months after the adoption of this Regulation], a report reviewing and assessing the use of privacy-enhancing technologies, including in relation to the storing of, or gaining access to information on terminal equipment, taking into account the state of the art, and with a view to provide incentives and legal certainty for service providers in deploying such technologies. Where appropriate, the Commission shall submit proposals to update the applicable legal framework, taking account of the results of that report, any sectoral developments and any other proposal it may deem necessary in order to improve the effectiveness of the rules on the storing of, or gaining access to information on terminal equipment.*	privacy-enhancing technologies within 12 months and explicitly invites further legislative proposals. PETs can support data minimisation, security and confidentiality, but the ability to pseudonymise data or use privacy-preserving measurement does not establish that device access is harmless, nor does it automatically make the information non-personal. The proposed review could become a second route for expanding Article 5(3) exemptions after adoption, especially alongside Recitals 43a–44g and the consent-free measurement clauses.
Recital-only issue Article 49 GDPR	**Council's new Recital 40b**	Current Article 49 contains specific requirements and safeguards for derogations in the absence of an adequacy decision or appropriate safeguards: (d) concerns important reasons of public interest,	No proposed amendment	*Further, for the purpose of the consistent application of that Regulation, it is recalled that data transfers to a third country or an international organisation where one of the derogations of Article 49(1), points (d) and (f) to (g), of Regulation (EU) 2016/679 applies*	The **Council's General Approach** newly inserted recital (40b) says that transfers under Article 49(1)(d), (f) and (g) need not be non-repetitive. The express 'not repetitive' condition in Article 49 is

GDPR Articles (ePD in some cases)	Digital Omnibus Proposal	Current text of the GDPR (ePD in some cases)	Commission's proposal	Council's General Approach	EDRi position
Transfers		(f) legal claims and (g) vital interests.		***are not required to be non-repetitive. Thus, for example, the derogation in point (d) allows such data transfers where necessary for important reasons of public interest, including international data exchange between tax administrations, even where those transfers are repetitive, if that is necessary to achieve the public interest at issue.***	attached to the final compelling-legitimate-interests derogation, not automatically to every ground cited here. However, repetition does not remove the specific necessity and safeguard requirements for the listed derogations or convert them into routine substitutes for Arts. 45–46 GDPR. This could allow facilitating systematic, large-scale transfers without safeguards, whereas each transfer must be independently necessary and proportionate under the applicable ground, and cannot be justified by a general appeal to administrative convenience. Moreover, there is pending CJEU decision on the matter.