Verbraucherzentrale
Bundesverband

Digital Omnibus: Legitimate objectives, inadequate approaches

Amendments by the Federation of German Consumer Organisations (vzbv) to the European Commission's proposals on the simplification of the digital legislative framework (Digital Omnibus) (2025/0360(COD)).

13. April 2026

Content

I. Relevance for consumers

Digital services dominate consumers' everyday lives and shape key areas such as communication, purchasing and access to information. Consumers make decisions about the use of these services under conditions of significant information asymmetry. According to the European Commission's Consumer Conditions Scoreboard 2023, 70 percent of consumers stated that they were concerned about how their personal data is used and shared. In this context, 38 percent reported a decline in their confidence in electronic commerce.[1] Other studies likewise show that concerns regarding data protection is one of the main reasons why consumers avoid certain digital services.[2]

By contrast, a high level of data protection means simplification and debureaucratisation for consumers. Empirical data thus emphasises that consumer confidence is an essential requirement for the use of digital services and for strong brand loyalty. In a recent survey conducted by the Federation of German Consumer Organisations (Verbraucherzentrale Bundesverband e.V – vzbv)[3] 63 percent of the surveyed consumers said that they trust companies complying with the General Data Protection Regulations (GDPR) significantly or somewhat more when it comes to handling their data. At the same time, 87 percent of the people surveyed consider it very or somewhat important to be able to trust companies with the handling of their personal data before using their services.

High data protection standards can therefore directly influence the willingness to use certain digital services and create a location advantage for European companies whose offers are based on a legally guaranteed level of protection. A coherent and reliable data protection framework therefore remains a prerequisite for functional markets, strong consumer rights, and a sustainable digital economy.

[1] European Commission: Consumer Conditions Scoreboard, 2023, p. 20, https://commission.europa.eu/system/files/2023-10/consumer_conditions_scoreboard_2023_v1.1.pdf, 01/10/2025.

[2] Bitkom: Mehr als jeder Dritte hat Hemmungen, digitale Angebote zu nutzen, 2025, https://www.bitkom.org/Presse/Presseinformation/Hemmungen-digitale-Angebote-Digitaltag-2025, 02/10/2025.

[3] Federation of German Consumer Organisations: Jahresendbefragung. Tabellenband, 2025, p. 3f, https://www.vzbv.de/sites/default/files/2025-12/Tabellenbaender_vzbv_Datenschutz.pdf, 12/12/2025.

II. Executive summary

A large part of the objectives of the Digital Omnibus cannot be achieved with the current proposals. Regarding the reform of the GDPR, the proposals do not result in simplification, but instead introduce new vague technical terms, a complex list of exceptions and additional assessment requirements. Legal certainty is weakened rather than strengthened, and diverging interpretations between Member States and courts, accompanied by lengthy proceedings, are to be expected. No tangible relief is provided for small and medium-sized enterprises (SME). Instead, new risks arise due to unclear applicability thresholds and additional compliance uncertainty. The coherence of European digital law is also not improved; on the contrary, new conflicts between legal instruments are likely. Finally, fundamental rights are not reinforced. Key principles such as transparency, purpose limitation and accountability are circumvented. A reform that fails to meet these foundational objectives cannot contribute to a modern, fit-for-purpose and reliable digital regulatory framework.

As a result, significant risks are created for consumers and European companies. Large, predominantly non-EU technology companies stand to benefit in particular, as their global data infrastructures and extensive legal and technical resources enable them to operationalise exceptions and ambiguous legal definitions more easily. Smaller European providers, by contrast, are confronted with legal uncertainty and additional compliance burdens.[4] For consumers, risks arise because data-intensive processing is facilitated while possibilities for control and enforcement are simultaneously reduced. A foreseeable consequence is a further erosion of trust in digital services.

vzbv therefore recommends:[5]

- A reform of the European digital legislature must be based on clear problem definitions, transparent consultation, robust evidence and a comprehensive impact assessment in line with the European Commission's **Better Regulation** standards.
- **The proposed changes to the definition of personal data must be removed (Articles 3(1)(a) and 3(10))**, as they risk undermining the objective criterion of identifiability under Article 4(1) and Recital 26 GDPR. Any clarification must remain consistent with Court of Justice of the European Union (CJEU) case-law and not alter its scope. Instead, the **European Data Protection Board** (EDPB) **should provide guidance** on pseudonymisation and re-identification risks **(Recital 27)**.
- **The proposed definition of scientific research must be removed (Articles 3(1)(b), 3(2) and 3(6); Recitals 28, 29, 32 and 37).** Any clarification requires careful, evidence-based calibration and must preserve purpose limitation, transparency, and the safeguards of Article 89 GDPR. What is needed are clear methodological standards and operationalised guarantees, not broad exemptions. This should be addressed in the Digital Fitness Check, not the Digital Omnibus.

[4] See Schaake, Marietje; Thun, Max von: Europe's Tech Sovereignty Demands More Than Competitiveness, 2025, https://www.project-syndicate.org/commentary/europe-misguided-fixation-on-enhanching-tech-competitiveness-by-marietje-schaake-and-max-von-thun-2025-04, 13.04.2026.

[5] For a more detailed analysis of the European Commission's proposal, see Federation of German Consumer Organisations: Position paper on the Digital Omnibus, 2025, https://www.vzbv.de/sites/default/files/2026-02/25-12-12_Position_vzbv_Digital-Omnibus.pdf, 13.04.2026.

- **The limitation of the right of access must be removed (Article 3(4); Recital 35).** Rather than creating clarity, it would undermine established CJEU case-law, introduce new uncertainty and likely trigger further litigation. The right must remain exercisable without motive assessment or additional requirements.
- **The weakening of information obligations must be removed (Article 3(5); Recital 36).** Transparency must rely on objective criteria, not contextual assumptions. A legal fiction of knowledge is incompatible with the transparency principle and Article 8 of the Charter of Fundamental Rights (CFR) of the European Union. Simplification is possible without amending the GDPR, for example through standardised short notices and pictograms that improve compliance and comprehensibility.
- **The transfer of the cookie provisions to the GDPR must be revised (Article 15, Recitals 44 and 45).** The preventive protection of Article 5(3) ePrivacy Directive should be preserved. At a minimum, exceptions require strict purpose limitation, technical safeguards, a ban on further processing, and – for measuring reach – a right to object. The security exemption must be narrowly defined. Dark patterns must be prevented. Overall, prohibiting tracking and profiling for advertising would be the more effective and proportionate solution.
- **Automated, machine-readable preference signals are the right approach, but the current proposal will not reduce consent banners** in the foreseeable future and **must therefore be improved (Article 15, Recital 46)**. Controller obligations must be clear and binding; the media exemption should be removed. A technical specification is needed to ensure semantic clarity, easy objection, an effective ban on manipulative practices and automatic blocking of tracking upon rejection. All end-user environments should be covered and regulated to prevent gatekeeper power being exercised at the expense of consumers.
- Processing personal data for the **development of artificial intelligence systems (AI) requires an independent legal basis with strict conditions (Article 15; Recitals 30 and 31)**, including subsidiarity vis-à-vis synthetic or anonymised data, prior risk information, an effective right to object, robust safeguards against replication and re-identification as well as a consent requirement for the data of children.
- **The exemption for AI development and operation from the prohibition on processing sensitive data must be removed (Articles 3(3)(a) and 3(3)(b); Recital 33).** Controllers should rely on the existing, narrowly defined exemptions in Article 9(2)(a) to (j) GDPR, which ensure a balanced level of protection.
- **The protection of children's personal data should be strengthened** across the GDPR, in particular in Articles 6(4), 21, and 25. Advertising and profiling based on children's data should be prohibited and the consent framework must reflect evolving capacities while ensuring consistency with the best interests of the child.
- **Manufacturers of digital products and services should be brought within the scope of accountability** under the GDPR by extending data protection by design obligations and introducing corresponding liability mechanisms. This would align responsibility with decision-making power, reduce compliance burdens – especially for SMEs – and strengthen effective protection of data subjects.

III. Amendments

1. Ensuring legal certainty in core definitions

1.1 AMs to the proposed definition of personal data

Text proposed by the European Commission	Amendments
Articles 3(1)(a) and 3(10)	
(a) in point 1, the following sentences are added: 'Information relating to a natural person is not necessarily personal data for every other person or entity, merely because another entity can identify that natural person. Information shall not be personal for a given entity where that entity cannot identify the natural person to whom the information relates, taking into account the means reasonably likely to be used by that entity. Such information does not become personal for that entity merely because a potential subsequent recipient has means reasonably likely to be used to identify the natural person to whom the information relates.'	**deleted**
The following article is added: 'Article 41a (1) 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. (2) For the purpose of paragraph 1 the Commission shall: (a) assess the state of the art of available techniques;	**deleted**

(b) develop criteria and or categories for controllers and recipients to assess the risk of re-identification in relation to typical recipients of data.

(3) 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.

(4) The Commission shall closely involve the EDPB in the preparations of the implementing acts. The EPDB shall issue an opinion on the draft implementing acts within a deadline of 8 weeks as of the receipt of the draft from the Commission.

(5) The Implementing Acts shall be adopted in accordance with the examination procedure referred to in Article 93(3).'

Recital 27	
(27) ***This Regulation proposes a series of targeted amendments to Regulation (EU) 2016/679 for clarification and simplification, whilst preserving the same level of data protection. Article 4 of Regulation (EU) 2016/679 provides that personal data is any information relating to an identified or identifiable natural person.*** In order to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used to identify the natural person directly or indirectly**.** Taking into account the case-law of the Court of Justice of the European Union ***concerning the definition of personal data***, it is ***necessary*** to provide further clarity on when a natural person should be considered to be identifiable. ***The existence of additional information enabling the data subject to be***	(27) In order to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used***, such as singling out, either by the controller or by another person*** to identify the natural person directly or indirectly. Taking into account the case-law of the Court of Justice of the European Union, it is ***important*** *to* provide further clarity on when a natural person should be considered to be identifiable. ***The European Data Protection Board should support controllers by adopting guidelines assessing and specifying the state of the art of available techniques, as well as the technical and organisational measures and criteria to pseudonymise personal data effectively, and clarifying the circumstances in which a natural***

identified does not, in itself, mean that pseudonymised data must be regarded as constituting, in all cases and for every person or entity, personal data for the purposes of the application of Regulation (EU) 2016/679. In particular, it should be clarified that information is not to be considered personal data for a given entity where that entity does not have means reasonably likely to be used to identify the natural person to whom the information relates. A potential subsequent transmission of that information to third parties who have means reasonably allowing them to identify the natural person to whom the information relates, such as cross-checking with other data at their disposal, renders that information personal data only for those third parties who have such means at their disposal. An entity for which the information is not personal data, in principle, does not fall within the scope of application of Regulation (EU) 2016/679. In this respect the Court of Justice of the European Union has held that a means of identifying the data subject is not reasonably likely to be used where the risk of identification appears in reality to be insignificant, in that the identification of that data subject is prohibited by law or impossible in practice, for example because it would involve a disproportionate effort in terms of time, cost and labour. An example of a prohibition against reidentification can be found in the obligations of health data users in Article 61(3) of Regulation (EU) 2025/327 of the European Parliament and of the Council. The Commission, together with the European Data Protection Board, should support person is identifiable and the means reasonably likely to be used to identify a natural person, including means and criteria to assess the risk of re-identification and the effectiveness of pseudonymisation techniques, without affecting the definition of personal data set out in Article 4(1) of Regulation (EU) 2016/679.

While controllers remain fully responsible for determining whether data resulting from pseudonymisation constitute personal data, the guidelines should support controllers in implementing such measures and criteria, and provide practical guidance to demonstrate how pseudonymisation reduces the risk of re-identification of data subjects.

controllers in the application of this updated definition by stipulating technical criteria in an implementing act.	

The amendment addresses the European Commission's proposal to clarify the notion of identifiability and to introduce criteria under which pseudonymised data may no longer constitute personal data. While the objective of providing greater legal clarity is supported, the proposed approach risks creating ambiguity as to the scope of the definition of personal data under the GDPR and may lead to a de facto narrowing of its application.

In particular, suggesting that pseudonymised data could cease to be personal data for certain entities departs from Recital 26 GDPR and the case-law of the CJEU, which require a broad and objective assessment of identifiability, including all means reasonably likely to be used by the controller or by another person. Such a shift would introduce fragmentation across data processing chains, weaken legal certainty, and undermine the effective exercise of data subject rights.

The amendment therefore removes the proposed changes to the definition of personal data and replaces them with a targeted mandate for the EDPB to provide an opinion on the assessment of identifiability and the effective use of pseudonymisation techniques. This approach preserves the existing legal framework while supporting consistent application in practice. The amendment builds on the proposal of the Cypriot Council Presidency[6], with targeted improvements to ensure coherence with the GDPR and the case-law of the CJEU.

For a more detailed analysis of the European Commission's proposal, see page 8ff of vzbv's position paper.[7]

1.2 AMs to the proposed definition of scientific research

Text proposed by the European Commission	Amendments
Articles 3(1)(b), 3(2) and 3(6)	
(b) the following points are added:	**deleted**
(38) "scientific research" means any research which can also support	

[6] WK 3736/2026 ADD 4, 2026, p. 2ff, https://table.media/assets/berlin/digital-omnibus-march-30-gdpr,-p2b,-eprivacy-fr,-ro,-pl-(1).pdf, 13.04.2026.

[7] Federation of German Consumer Organisations: Position paper on the Digital Omnibus, 2025, p. 8ff, https://www.vzbv.de/sites/default/files/2026-02/25-12-12_Position_vzbv_Digital-Omnibus.pdf, 13.04.2026.

innovation, such as technological development and demonstration. These actions shall contribute to existing scientific knowledge or apply existing knowledge in novel ways, be carried out with the aim of contributing to the growth of society´s general knowledge and wellbeing and adhere to ethical standards in the relevant research area. This does not exclude that the research may also aim to further a commercial interest.'	
Article 5 (1)(b) is replaced by the following: '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), be considered to be compatible with the initial purposes, independent of the conditions of Article 6(4) of this Regulation, ('purpose limitation');'	**deleted**
In Article 13, paragraph 5 is added: '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	**deleted**

measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available.'	
Recitals 28, 29, 32 and 37	
(28) In order to assess whether research meets the conditions of scientific research for the purpose of this Regulation, account can be taken of elements such as methodological and systematic approach applied while conducting the research in the specific area. Research and technology development should be conducted in academic, industry and other settings, including small and medium-sized undertakings, (Article 179(2) TFEU) and should be always of a of high quality and should adhere to the principles of principles of reliability, honesty, respect and accountability (verifiability).	**deleted**
(29) It should be reiterated that further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. In such cases it is not necessary to ascertain on the basis of Article 6(4) of this Regulation whether the purpose of the further processing is compatible with the purpose for which the personal data are initially collected.	**deleted**
(32) The processing of personal data for scientific research purposes and the application of the GDPR's provisions on scientific research are conditional on the adoption of appropriate safeguards for the rights and freedoms of data subjects, pursuant to Article 89(1) GDPR. To that end, the GDPR balances the right to protection of personal data,	**deleted**

pursuant to Article 8 CFREU, with the freedom of science, pursuant to Article 13 CFREU. The processing of personal data for the purpose of scientific research therefore pursues a legitimate interest within the meaning of Article 6(1)(f) of Regulation (EU) 2016/679, provided that such research is not contrary to Union or Member State law. This is without prejudice to the obligation of the controller to ensure that all other conditions of Article 6(1)(f) of Regulation (EU) 2016/679 as well as all other requirements and principles of that Regulation are met.	
(37) Where the processing takes place for the purpose of scientific research and the provision of information to the data subject proves to be impossible or would involve a disproportionate effort it should not be necessary to provide the information provided for under Article 13 of this Regulation. The controller should make reasonable efforts to acquire contact details if they are readily available and acquisition would not require a disproportionate effort. The provision of the information would involve a disproportionate effort in particular where the controller at the time of collection of the personal data did not know or anticipate that it would process personal data for scientific research purposes at a later stage, in which case it may not have easily available contact details of the data subjects. In such situations the controller should inform data subjects indirectly, such as by making the information publicly available. The provision of such information should ensure that as many data subjects concerned as possible are reached. Relevant means to make the information publicly available should be determined depending on the	**deleted**

context of the research project and the data subjects involved.

The proposed changes must be removed.

The European Commission's proposal fundamentally alters the concept of scientific research under the GDPR by expanding it into a broad and indeterminate category covering a wide range of data-intensive activities, including those driven by commercial interests. This decouples the research regime from its original justification, which is based on methodical, quality-assured research serving the common good within recognised ethical and institutional frameworks. As a result, the basis for the privileges and derogations in Article 89 GDPR is undermined.

At the same time, the proposal weakens key safeguards. A blanket presumption of purpose compatibility in Article 5 (1)(b) GDPR, combined with broad exceptions from transparency obligations and an expanded notion of legitimate interest, significantly reduces the effectiveness of purpose limitation and transparency. In the absence of clear methodological standards and enforceable oversight, this risks enabling strategic reclassification of data processing as "research", facilitating misuse and eroding data subjects' rights.

While clarifying the notion of scientific research may be desirable, this is a complex issue. The proposal illustrates the risks of addressing it through broad language without adequate safeguards, impact assessment, or alignment with existing frameworks. Such reform requires careful, evidence-based consideration, including a clear delineation of genuine research and operationalised safeguards.

Any clarification should therefore be addressed in the ongoing Digital Fitness Check rather than through the Digital Omnibus. It should also be assessed whether the GDPR is the appropriate instrument, or whether a more suitable, sector-specific framework would better ensure legal certainty and effective protection of fundamental rights.

For a more detailed analysis of the European Commission's proposal, see page 10ff of vzbv's position paper.[8]

[8] Federation of German Consumer Organisations: Position paper on the Digital Omnibus, 2025, p. 10ff, https://www.vzbv.de/sites/default/files/2026-02/25-12-12_Position_vzbv_Digital-Omnibus.pdf, 13.04.2026.

2. Preserving effective rights of access and transparency

2.1 AMs to the proposed limitation of the right to access

Text proposed by the European Commission	Amendments
Article 3(4)	
In Article 12, paragraph 5 is replaced by the following: '5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character or also, for requests under Article 15 because the data subject abuses the rights conferred by this regulation for purposes other than the protection of their data, the controller may either: (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or (b) refuse to act on the request. The controller shall bear the burden of demonstrating that the request is manifestly unfounded or that there are reasonable grounds to believe that it is excessive.'	**deleted**
Recital 35	
(35) Article 15 of Regulation (EU) 2016/679 provides data subjects with the right to obtain from the controller confirmation as to whether or not	**deleted**

personal data concerning him or her are being processed and, where that is the case, access to the personal data and certain additional information. The right of access should allow the data subject to be aware of, and to verify, the lawfulness of the processing and enable him or her to exercise his or her other rights under Regulation (EU) 2016/679. By contrast, it should be clarified in Article 12 of the Regulation that the right of access, which is from the outset favourable to data subjects, should not be abused in the sense that the data subjects abuse them for purposes other than the protection of their data. For example, such an abuse of the right of access would arise where the data subject intends to cause the controller to refuse an access request, in order to subsequently demand the payment of compensation, potentially under the threat of bringing a claim for damages. Other examples of abuse include situations where data subjects make excessive use of the right of access with the only intent of causing damage or harm to the controller or when an individual makes a request, but at the same time offers to withdraw it in return for some form of benefit from the controller. Moreover, in order to keep their burden to a reasonable extent, controllers should bear a lower burden of proof regarding the excessive character of a request than regarding the manifestly unfounded character of a request. The reason is that the manifestly unfounded character of a request depends on facts that lie principally within the controller's sphere of responsibility, whereas the excessive character of a request concerns the possibly abusive conduct of a data subject, which lies primarily outside the controller's sphere of

influence, and therefore the controller may be able to prove such abuse only to a reasonable level. In any event, while requesting access under Article 15 of Regulation (EU) 2016/679 the data subject should be as specific as possible. Overly broad and undifferentiated requests should also be regarded as excessive.

The proposed changes must be removed.

The European Commission's proposal fundamentally alters the function of the right of access by introducing vague and motive-based grounds for refusal, including the notion of "abuse" and a lowered standard of proof. This transforms the right from an objective control instrument into a conditional entitlement subject to discretionary assessment by controllers. Such a purpose-based limitation is foreign to the structure of the GDPR and incompatible with Article 8 CFR and established CJEU case law, which treats the right of access as independent of the data subject's motives.

The use of indeterminate concepts such as "abuse" or "excessive", combined with a reduced evidentiary threshold, significantly expands controllers' discretion and risks facilitating blanket refusals. This is particularly problematic in complex data processing environments, where broad or repeated requests are often necessary because data subjects cannot know in advance how their data are processed.

There is no demonstrated regulatory gap. Article 12 (5) GDPR already allows controllers to refuse manifestly unfounded or excessive requests. For example, recent CJEU case law (C-526/24 Brillen Rottler) confirms that these instruments are sufficient to address abusive practices. The proposal therefore creates additional legal uncertainty without providing added value.

The planned expansion of the grounds for refusal would weaken the effectiveness of the right of access and undermine its role as a key enforcement mechanism. It should therefore be rejected.

For a more detailed analysis of the European Commission's proposal, see page 12ff of vzbv's position paper.[9]

---

[9] Federation of German Consumer Organisations: Position paper on the Digital Omnibus, 2025, p. 12ff, https://www.vzbv.de/sites/default/files/2026-02/25-12-12_Position_vzbv_Digital-Omnibus.pdf, 13.04.2026.

2.2 AMs to the proposed weakening of information obligations

Text proposed by the European Commission	Amendments
Article 3(5)	
In Article 13, paragraph 4 is replaced by the following: '4. Paragraphs 1, 2 and 3 shall not apply where the personal data have been collected in the context of a clear and circumscribed relationship between data subjects and a controller exercising an activity that is not data-intensive and there are reasonable grounds to assume that the data subject already has the information referred to in points (a) and (c) of paragraph 1, unless the controller transmits the data to other recipients or categories of recipients, transfers the data to a third country, carries out automated decision-making, including profiling, referred to in Article 22(1), or the processing is likely to result in a high risk to the rights and freedoms of data subjects within the meaning of Article 35.'	**deleted**
Recital 36	
(36) Article 13 of Regulation (EU) 2016/679 requires the data controller to provide the data subject with certain information on the processing of his or her personal data as well as certain further information necessary to ensure fair and transparent processing, as defined in paragraphs 1, 2 and 3 of that provision. According to paragraph 4 of Article 13 of Regulation (EU) 2016/679, that obligation does not apply where and insofar as the data subject already has the information. To further reduce	**deleted**

the burden of data controllers, without undermining the possibilities of the data subject to exercise his or her rights under Chapter III of the Regulation, this derogation should be extended to situations where the processing is not likely to result in a high risk, within the meaning of Article 35 of the Regulation, 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 in the light of the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller. These should be the situations where the context of the relationship between the controller and the data subject is very clear and circumscribed and the controller's activity is not data-intensive, such as the relationship between a craftsman and their clients, where the scope of processing is limited to the minimum data necessary to perform the service. The controller's activity is not data-intensive where it collects a low amount of personal data and its processing operations are not complex, which is not the case, for example, in the field of employment. In such circumstances, that is to say when the processing is non data-intensive, non-complex and where the controller collects a low amount of personal data, it should be reasonable to expect, for instance, that the data subject has the information on the identity and contact details of the controller as well as on the purpose of the processing when that processing is carried out for the performance of a contract to which a data subject is a party, or when the data subject has given his or her consent to that processing, in accordance with the

requirements laid down in Regulation (EU) 2016/679. The same should apply to associations and sport clubs where the processing of personal data is confined to the management of membership, communication with members and the organisation of activities. Nevertheless, this derogation from the obligations of Article 13 is without prejudice to the independent obligations of the controller under Article 15 of that Regulation, which applies in case the data subject requests access based on the latter provision. Where the derogation from the obligations of Article 13 does not apply, in order to balance the need for completeness and easy understanding by the data subject, controllers may adopt a layered approach when providing the information required, notably by allowing users to navigate to further information.

The proposed changes must be removed.

The European Commission proposal significantly expands the exception to information obligations by introducing vague criteria and a legal fiction of knowledge. It allows controllers to dispense with transparency obligations based on assumptions about the relationship with the data subject, the intensity of processing, and presumed awareness. This replaces objective requirements with discretionary assessments by controllers.

The proposal constitutes a material change to the transparency regime. Transparency is a core element of fair and lawful processing under Article 5 (1)(a) GDPR and a prerequisite for the exercise of data subject rights. It is closely linked to Article 8 CFR and must be based on clear, predictable criteria. The introduction of indeterminate concepts such as "clear and circumscribed relationship", "not data intensive" or "reasonable grounds to assume" creates significant legal uncertainty and risks inconsistent application.

The legal fiction that data subjects are already informed fundamentally contradicts the logic of the GDPR. The framework is based on actual provision of information, not presumed knowledge. This also creates tensions with the requirements for valid consent under Articles 4 (11) and 7 GDPR, which presuppose that data subjects have received the relevant information.

There is no demonstrated regulatory gap. The European Commission has not provided evidence that existing transparency obligations lead to disproportionate

burden. The proposal therefore weakens a key protection mechanism without sufficient justification, while offering no real simplification, as the underlying information must still be available for accountability and access purposes.

Reasonable simplifications of the transparency obligations can be made without material changes to the GDPR: Standardised short texts and pictograms for typical processing procedures could support companies in fulfilling their information obligations and at the same time increase understandability for consumers.

For a more detailed analysis of the European Commission's proposal, see page 13ff of vzbv's position paper.[10]

3. Strengthening tracking protection and user control

3.1 AMs to the proposed transfer of the cookie provisions into the GDPR

Text proposed by the European Commission	Amendments
Article 15	
After Article 88, the following articles are added:	***Access to and storage of information*** in the terminal equipment of ***users***
'Article 88a	(1) Storing of ***information*** or gaining of access to ***information*** already stored, in the terminal equipment of a ***user*** is only allowed when that ***user*** has given his or her consent, in accordance with this Regulation.
Processing of personal data *in the terminal equipment of* ***natural persons***	***(1a) A user shall not be denied access to a service or to a functionality of a service on the grounds that he or she has not given consent under paragraph 1 to the storing of, or gaining of access to, information in terminal equipment that is not strictly necessary for the provision of that service or functionality.***
(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) deleted**
(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	

[10] Federation of German Consumer Organisations: Position paper on the Digital Omnibus, 2025, p. 13ff, https://www.vzbv.de/sites/default/files/2026-02/25-12-12_Position_vzbv_Digital-Omnibus.pdf, 13.04.2026.

Article 6, to safeguard the objectives referred to in Article 23(1).

(3) Storing of ***personal data***, or gaining of access to ***personal data*** already stored, in the terminal equipment of a ***natural person*** without consent, ***and subsequent processing,*** shall be lawful to the extent it is necessary for any of the following:

(a) carrying out the transmission of an electronic communication over an electronic communications network;

(b) providing a service explicitly requested by the ***data subject***;

(c) creating aggregated information about the usage of an online service to measure the audience of such a service, where ***it*** is carried out by the controller of that online service solely for its own use;

(d) ***maintaining or restoring the security*** of a service provided by the controller and requested by the ***data subject or the terminal equipment used for the provision of such service***.

(4) Where storing of ***personal data***, or gaining of access to ***personal data*** already stored, in the terminal equipment of a ***natural person*** is based on consent, the following shall apply:

(a) the ***data subject*** shall be able to refuse requests for consent in an easy and intelligible manner with a single-click button or equivalent means;

(b) if the ***data subject*** gives consent, the controller shall not make a new request for consent for the same purpose for the period during which the controller can lawfully rely on the consent of the ***data subject***;

(c) if the ***data subject*** declines a request for consent, the controller shall not make a new request for consent for

(3) Storing of ***information***, or gaining of access to ***information*** already stored, in the terminal equipment of a ***user*** without consent, shall be lawful ***only*** to the extent it is ***strictly*** necessary for any of the following ***purposes***:

(a) carrying out the transmission of an electronic communication over an electronic communications network;

(b) providing a service explicitly requested by the **user of the terminal equipment**;

(c) creating aggregated and anonymous information about the usage of an online service to measure the audience of such a service, where ***such measurement*** is carried out by the controller of that online service solely for its own use***, is restricted to aggregated statistical counting, does not enable the identification, tracking or profiling of individual users beyond what is strictly necessary for aggregated statistics, does not involve fingerprinting techniques or the creation of persistent identifiers, does not make personal data or other information accessed pursuant to this point accessible to third parties, and provides users with effective means to object without affecting the usability of the service; where such measurement is carried out by a processor on behalf of the controller, the information shall be processed solely on behalf of that controller, kept separate from information collected on behalf of other controllers, and not combined with or used in relation to such information***;

(d) ***ensuring the confidentiality, integrity and availability*** of a service provided by the controller

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 Regulation].

and ***explicitly*** requested by the ***user of the terminal equipment, including measures necessary for the secure provision of that service in accordance with Article 32, provided that such measures are proportionate and limited to what is strictly necessary for that purpose and do not override the fundamental rights and freedoms of the user, and do not serve commercial or analytical purposes.***

Any access pursuant to this paragraph shall be limited in scope, duration and intensity to what is strictly necessary for that purpose. Techniques intended to circumvent the limitations laid down in this paragraph shall be prohibited.

(4) Information accessed pursuant to paragraph 3 shall be processed only insofar as strictly necessary for the purpose justifying the access and shall not be further processed for incompatible purposes. Article 6(4) shall not apply to such processing. Such information shall not be used for the purpose of obtaining consent for unrelated processing activities. Information accessed pursuant to paragraph 3 shall be deleted or rendered anonymous immediately after the purpose justifying the access has been fulfilled.

Subsequent processing based on consent pursuant to paragraph 1 shall remain subject to Articles 6 and 9.

(5) Where storing of ***information,*** or gaining of access to ***information*** already stored, in the terminal equipment of a ***user*** is based on consent, the following shall apply:

	(a) the ***user*** shall be able to refuse requests for consent ***and withdraw consent*** in an easy and intelligible manner with a single-click button or equivalent means; ***it shall be as easy to refuse or withdraw consent as to give it***; (b) if the ***user*** gives consent, the controller 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 ***user***; (c) if the ***user*** 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**;** ***processing of personal data shall be lawful only insofar as strictly necessary for respecting such refusal and shall not justify the creation of persistent identifiers***. This paragraph also applies to the subsequent processing of personal data based on consent. ***(6)*** This Article shall apply from [OP: please insert the date = 6 months following the date of entry into force of this Regulation].
Recitals 44 and 45	
(44) The storing of personal data, or the gaining of access to personal data already stored, in a terminal equipment and the subsequent processing of such data should be regulated under a single legal framework, namely Regulation (EU) 2016/679, where the subscriber of the electronic communications service or the user of the terminal equipment is a natural person. The amendments presented in this Regulation continue to offer the highest levels of protection for personal data, while simplifying the experiences of data subjects in exerting	**deleted**

their rights and expressing their choices online. The amendments concern in particular storage of information in that equipment, accessing or otherwise collecting information from that equipment that entails the processing of personal data through cookies or similar technologies to gain information from the terminal equipment. The relevant rules should also apply regardless of whether the terminal equipment is owned by the natural person or by another legal or natural person.

The storing of personal data, or the gaining of access to personal data already stored, in a terminal equipment should continue to be allowed only on the basis of consent. Similar to the approach in Directive 2002/58/EC, this requirement should not preclude storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person, when that is based on Union or Member State law within the meaning of Article 6 of Regulation (EU) 2016/679 and if it fulfils all conditions of lawfulness laid down in that provision, and is done for the objectives laid down in Article 23(1) of Regulation (EU) 2016/679.

With a view to reducing the compliance burden and providing legal clarity to controllers, and given that certain purposes of processing pose a low risk to the rights and freedoms of data subjects or that such processing may be necessary to provide a service requested by the data subject, it is necessary to define a limitative list of purposes for which the processing should be permitted without consent. As regards storing of personal data, or the gaining of access to personal data already stored, in a terminal

equipment, and subsequent processing that is necessary for those purposes, this Regulation should therefore provide that the processing is lawful. The controller, such as a media service provider, may mandate a processor, such as a market research company, to carry out the processing on its behalf.

For the subsequent processing of personal data for other purpose than those defined in the limitative list, Article 6 and, where relevant, Article 9 of Regulation (EU) 2016/679 should be applied. It is the responsibility of the controller in the light of the principle of accountability to choose the appropriate legal basis for the intended processing. In order to be able to rely on legitimate interest under Article 6(1), point f, of Regulation (EU) 2016/679 as a ground for the subsequent processing of personal data, the controller must show that it pursues the controller's or third parties' legitimate interest, the processing is necessary in order to achieve the purpose of that legitimate interest, and the interests or fundamental rights of the data subject do not override the interests pursued by the controller. In this context, controllers should take outmost account of the following elements: whether the data subject is a child; the reasonable expectations of data subject; the impact on the individual either because of the scale of data processed or the sensitivity of the data processed; the scale of the processing at issue in the sense that the processing cannot be particularly extensive either because of their amount or the range of categories of data; the processing should be based on data limited to what is necessary and cannot be based on monitoring of large parts of the online activity of the

data subjects; and other relevant factors as appropriate. The processing should not give rise to the continuous monitoring of the data subject's private life. Where the controller cannot rely on legitimate interest as a legal ground for the subsequent processing, the processing should be based on another ground in Article 6(1), in particular on consent in accordance with Articles 6 and 7 of Regulation (EU) 2016/679, provided that all principles of Regulation (EU) 2016/679 are met.	
(45) Data subjects that have refused a request for consent are often confronted with a new request to give consent each time they visit the same controller's online service again. This may have detrimental effects to the data subjects which may consent just in order to avoid repeating requests. The controller should therefore be obliged to respect the data subject's choices to refuse a request for consent for at least a certain period.	**deleted**
	Access to and storage of information in the terminal equipment of a user constitutes, in itself, an interference with the private sphere of that user and with the right to respect for private life guaranteed in Article 7 of the Charter of Fundamental Rights of the European Union. Such access may occur irrespective of whether the information concerned qualifies as personal data. Clear, precise and harmonised rules are therefore necessary to ensure a high level of protection of users while safeguarding the functioning of the internal market. ***As a rule, storing of information, or gaining access to information already***

stored, in terminal equipment should be permitted only on the basis of the user's consent. Users should not be denied access to a service or to a functionality of a service on the ground that they refuse consent to access or storage operations that are not strictly necessary for the provision of that service or functionality. Information relating to such access and storage should be provided in a clear and prominent manner and separately from general terms and conditions.

Limited exceptions may be justified where access is strictly necessary for carrying out the transmission of an electronic communication, for providing a service explicitly requested by the user, for first-party audience measurement under conditions ensuring aggregation and the absence of tracking, or for ensuring the confidentiality, integrity and availability of a service explicitly requested by the user in accordance with Article 32 of Regulation (EU) 2016/679. In all cases, such access should be limited in scope, duration and intensity to what is strictly necessary for the purpose pursued.

Such exceptions should be interpreted strictly. In particular, audience measurement should be restricted to aggregated statistical counting, should not enable the identification or tracking of individual users, should not involve device fingerprinting or comparable techniques, and should not result in the monitoring of large parts of a user's online activity. It should not

involve the disclosure of personal data or other information accessed pursuant to the exception to third parties. Where such measurement is carried out by a processor, it should be carried out exclusively on behalf of and under the instructions of the controller of the service concerned, solely for the purposes of that controller, and the information collected on behalf of different controllers should be kept separate. Information accessed under these exceptions should remain strictly limited to the purpose justifying the access, should not be further processed for incompatible purposes, and should be deleted or rendered anonymous immediately after that purpose has been fulfilled.

In order to preserve effective self-determination, refusal of consent should be as easy as granting consent. Measures taken to respect a refusal should not lead to the creation of new persistent identifiers solely for that purpose.

The pervasive use of tracking and profiling for advertising purposes poses significant risks to fundamental rights and has broader negative effects on individuals and society. In particular, large-scale tracking across services enables detailed behavioural profiling, undermines user autonomy, and contributes to opaque and uncontrollable data ecosystems. In practice, the current consent-based model has not provided effective protection, as users are confronted with complex interfaces, asymmetries of information and structural pressure to consent. Making access to a service or functionality conditional on consent to access or storage operations that are not strictly necessary undermines the requirement that consent be freely given. Against this background, a prohibition of tracking and profiling for advertising purposes should be considered the most effective and proportionate means to ensure a high level of protection.

Should the Union legislator nevertheless maintain a consent-based framework, further adjustments to the European Commission's proposal are necessary to ensure effective protection, legal certainty and genuine simplification.

Access to information stored in terminal equipment constitutes, in itself, an interference with the private sphere protected under Article 7 of the Charter of Fundamental Rights of the European Union, irrespective of whether the information qualifies as personal data. Maintaining a preventive end-device protection framework under Directive 2002/58/EC (ePrivacy Directive), which addresses access as such rather than shifting the rule entirely into a data-processing regime, ensures greater coherence, legal certainty and consistency with the established logic of terminal equipment protection. The proposal therefore preserves the principle that consent is required as a rule for access, while subsequent processing remains subject to the general data protection framework. By clearly distinguishing access from subsequent processing, the amendment avoids structural inconsistencies linked to the threshold of "personal data".

At the same time, it supports simplification. A limited and precisely defined set of exceptions permits access without consent where strictly necessary for technical transmission, for providing a service explicitly requested by the user, for first-party audience measurement under strict anti-tracking conditions, or for ensuring the security of a requested service in accordance with Article 32 GDPR. In all cases, such access must be limited in scope, duration and intensity to what is strictly necessary for the purpose pursued. This reduces unnecessary consent interfaces in low-risk situations while preserving a high level of protection.

Audience measurement remains confined to aggregated, first-party use and may be carried out by a processor exclusively on behalf of and under the instructions of the controller. Where such measurement is carried out by a processor, strict limitations are necessary to prevent circumvention. Data must be processed solely on behalf of the controller, kept separate from data processed on behalf of other controllers and must not be combined or reused across services. Identification, tracking, large-scale monitoring, fingerprinting and commercial exploitation or data resale are excluded. Information accessed under these exceptions should remain strictly limited to the purpose justifying the access, should not be further processed for incompatible purposes, and should be deleted or rendered anonymous immediately after that purpose has been fulfilled.

To address consent fatigue, refusal must be as easy as granting consent, and compliance with refusal obligations must not lead to the creation of persistent identifiers.

Overall, the amendment preserves preventive end-device protection, increases legal clarity, reduces unnecessary consent requests, and supports fair competition and innovation within the internal market while maintaining a high level of fundamental rights protection.

For a more detailed analysis of the European Commission's proposal, see page 15ff of vzbv's position paper.[11]

[11] Federation of German Consumer Organisations: Position paper on the Digital Omnibus, 2025, p. 15ff, https://www.vzbv.de/sites/default/files/2026-02/25-12-12_Position_vzbv_Digital-Omnibus.pdf, 13.04.2026.

3.2 AMs to the proposed introduction of automated, machine-readable preference signals

Text proposed by the European Commission	Amendments
Article 15	
Article 88b Automated and machine-readable indications of ***data subject's*** choices with respect to ***processing of personal data*** in the terminal equipment of ***natural persons***	Automated and machine-readable indications of ***user's*** choices with respect to ***storing of, or gaining access to, information*** in the terminal equipment of ***users***
(1) Controllers shall ensure that their online interfaces allow ***data subjects*** to:	(1) Controllers shall ensure that their online interfaces allow ***users, with respect to the storing of, or gaining access to, information in terminal equipment pursuant to [OP: please insert the reference to the Article = "Access to and storage of information in the terminal equipment of users"],*** to:
(a) Give consent through automated and machine-readable means, provided that the conditions for consent laid down in this Regulation are fulfilled;	(a) Give consent through automated and machine-readable means, provided that the conditions for consent laid down in this Regulation are fulfilled;
(b) decline a request for consent and exercise the right to object pursuant to Article 21(2) through automated and machine-readable means.	(b) decline a request for consent**,** ***withdraw 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.	***Such automated and machine-readable means, as made available pursuant to this Article, shall allow users to express their choices for specific purposes and, where applicable, in relation to a specific controller or service context.***
(3) Paragraphs 1 and 2 shall not apply to controllers that are media service providers when providing a media service.	(2) Controllers ***and all parties involved in the generation, transmission or recognition of such indications*** shall ***comply***
(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 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].

with and give effect to the choices made by ***users*** in accordance with paragraph 1.

Where an active refusal signal is present, storing of, or gaining access to, information in terminal equipment shall not take place. A request for consent for the same purposes may be made only through the automated and machine-readable means referred to in paragraph 1, subject to [OP: please insert the reference to the Article = "Access to and storage of information in the terminal equipment of users" (5)(c)].

(3) **deleted**

(4) The Commission shall ***adopt, within 12 months of the entry into force of this Regulation, implementing acts specifying technical requirements and interoperability conditions for automated and machine-readable indications of users' choices referred to*** in paragraph 1.

Those implementing acts shall define in particular:

(a) interoperability requirements for the transmission and recognition of signals;

(b) minimum technical and organisational requirements for ensuring that an active refusal signal prevents the storing of, or gaining access to, information in terminal equipment without requiring further user interaction, without prejudice to paragraph 2;

(c) safeguards to ensure that the implementation of such signals does not result in the creation of new persistent identifiers solely

for the purpose of recognising or storing the user's choice;

(d) that such mechanisms are neutral and do not favour specific services, software or interfaces;

(e) that users are able to rely on software or services of their choice, including third-party tools, to generate and manage such signals.

The Commission shall closely involve the European Data Protection Board in the preparations of the implementing acts. The European Data Protection Board 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).

(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 ***software or systems enabling the storing of, or gaining access to, information in terminal equipment***, which are not SMEs, shall provide the technical means to allow ***users*** to give their consent, ***to withdraw consent,*** 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***, and shall be subject to the obligations laid down in this Regulation in relation to those means***.

(7) Paragraph 6 shall apply from [OP: please insert the date = 48

	months following the date of entry into force of this Regulation].
Recital 46	
(46) ***Data subjects*** should have the possibility to rely on automated and machine-readable indications of their choice to consent ***or*** refuse a consent request or object to the ***processing of data***. Such means should follow the state of the art. They can be implemented in the settings of a web browser or in the EU Digital Identity Wallet as set out by Regulation (EU) 914/2014, or any other adequate means. Rules set out in this Regulation should support the emergence of market-driven solutions with appropriate interfaces. ***The controller*** should be obliged to ***respect*** automated and machine-readable indications of ***data subject's*** choices ***once there are available standards. In light of the importance of independent journalism in a democratic society and in order not to undermine the economic basis for that, media service providers should not be obliged to respect the machine-readable indications of data subject's choices.*** The obligation for providers of web browsers to provide the technical means ***for data subjects to make choices with respect to the processing should not undermine the possibility for media service providers to request consent by data subjects***.	(46) ***Users*** should have the possibility to rely on automated and machine-readable indications of their choice to consent**,** ***withdraw consent,*** refuse a consent request or object to the ***storing of, or gaining access to, information in terminal equipment pursuant to [OP: please insert the reference to the Article = "Access to and storage of information in the terminal equipment of users"]***. Such means should follow the state of the art. They can be implemented in the settings of a web browser***, operating systems, applications*** or in the EU Digital Identity Wallet as set out by Regulation (EU) 914/2014, or any other adequate means. Rules set out in this Regulation should support the emergence of ***interoperable*** market-driven solutions with appropriate interfaces. ***Controllers*** should be obliged to ***comply with and give effect to*** automated and machine-readable indications of ***user's*** choices. ***The use of such mechanisms should not lower the requirements for valid consent. Consent expressed through such mechanisms should relate to specific purposes and identifiable controllers and be based on the prior provision of clear and comprehensive information to the user. Such mechanisms should not rely on default settings or interface designs that steer users towards giving consent, including at the initial configuration or first use of***

a software or service. Withdrawal of consent should be as easy as giving consent and should be possible through the same automated and machine-readable mechanism.

Where an active refusal signal is present, storing of, or gaining access to, information in terminal equipment should not take place. To enable context-specific user choices while avoiding repeated consent requests, a request for consent for the same purposes may be made through such automated and machine-readable means. Where the user declines such a request, no further request should be made for a period of time in accordance with [OP: please insert the reference to the Article = "Access to and storage of information in the terminal equipment of users" (5)(c)]. Requests for consent should not be made through alternative interfaces outside those automated and machine-readable means.

Automated and machine-readable indications that clearly express the user's choice and comply with the requirements of this Regulation should produce legal effects without undue delay.

Implementing acts adopted by the Commission should ensure interoperability and technical effectiveness of such signals, including that an active refusal signal effectively prevents the storing of, or gaining access to, information in terminal equipment without requiring additional user interaction and without creating new persistent identifiers. Those requirements should apply consistently to all

entities involved in the generation, transmission or recognition of such signals, including controllers and providers of software or services enabling their use. The interpretation and application of the requirements applicable to such signals should be guided by the European Data Protection Board, in order to ensure consistency with Union data protection law, including Regulation (EU) 2016/679, and with the Charter of Fundamental Rights of the European Union.

The obligation for providers of web browsers ***and other end-user software environments*** to provide the technical means ***should ensure that users can effectively give consent, withdraw consent, refuse consent requests and exercise their right to object through automated and machine-readable means. Supervisory authorities should be able to effectively exercise their powers in relation to entities involved in the generation, transmission or recognition of such indications.***

Automated and machine-readable preference signals do not address the structural drivers of pervasive tracking and profiling in the online advertising ecosystem. In particular, they do not alter the economic incentives underlying large-scale data collection, cross-service tracking and behavioural profiling. As such, they cannot, in themselves, remedy the fundamental shortcomings of a consent-based model, characterised by complexity, asymmetries of information and structural pressure on users to consent.[12]

Within a framework that continues to rely on consent, preference signals can nevertheless facilitate the exercise of users' choices and reduce repetitive and manipulative interfaces. Their effectiveness depends on a clear legal framework that ensures binding effect, prevents circumvention and preserves the substantive requirements of valid consent under Union law. The amendment clarifies that preference signals function as an effective mechanism for exercising users'

---

[12] See Verbraucherzentrale Bundesverband: Perspectives for the Regulation of Personalised Advertising, 2025, https://www.vzbv.de/sites/default/files/2025-02/25-02-10_Positionpaper_vzbv_Personalised-Advertising.pdf, 13.04.2026.

choices regarding the storing of, or gaining access to, information in terminal equipment pursuant to [OP: please insert the reference to the Article = "Access to and storage of information in the terminal equipment of users" (5)(c)]. By referring to "information" rather than "personal data", the amendment preserves coherence with the preventive end-device protection logic of that Article and avoids inconsistencies linked to the personal data threshold, thereby enhancing legal certainty.

The amendment reinforces the binding nature of such signals. Controllers must comply with and give effect to users' automated indications. Where an active refusal signal is present, storing of, or gaining access to, information in terminal equipment must not take place. To enable context-specific choices while avoiding repeated consent requests, a request for consent for the same purposes may be made through automated and machine-readable means, subject to the limitations laid down in [OP: please insert the reference to the Article = "Access to and storage of information in the terminal equipment of users" (5)(c)]. Requests for consent should not be made through alternative interfaces.

Automated mechanisms must not lower the requirements for valid consent under Union law. Withdrawal must be possible through the same mechanism and be as easy as giving consent, in accordance with Article 7(3) GDPR.

The amendment replaces industry-led standardisation with mandatory implementing acts to be adopted by the European Commission within a defined timeframe and with the involvement of the EDPB. This ensures interoperability, prevents fragmentation and provides predictable compliance conditions. Implementing acts must guarantee that the signals are effective without requiring additional user interaction and without creating new persistent identifiers.

Obligations for providers of web browsers and other relevant end-user software environments ensure that users can effectively give and withdraw consent, refuse consent requests and exercise their right to object through automated and machine-readable means. Such mechanisms should be neutral and allow users to rely on software or services of their choice, including third-party tools.

Overall, the amendment increases legal clarity, reduces compliance complexity, strengthens fundamental rights protection under Article 7 of the Charter and contributes to a level playing field within the internal market.

For a more detailed analysis of the European Commission's proposal, see page 17ff of vzbv's position paper.[13]

[13] Federation of German Consumer Organisations: Position paper on the Digital Omnibus, 2025, p. 17ff, https://www.vzbv.de/sites/default/files/2026-02/25-12-12_Position_vzbv_Digital-Omnibus.pdf, 13.04.2026.

4. Enabling responsible AI development

4.1 AMs to the proposed legal basis for AI development

Text proposed by the European Commission	Amendments
Article 15	
Article 88c Processing in the context of the development and operation of AI Where the processing of personal data is necessary for the interests of the controller in the context of the development and operation of an AI system as defined in Article 3, point (1), of Regulation (EU) 2024/1689 or an AI model, such processing may be pursued for legitimate interests within the meaning of Article 6(1)(f) of Regulation (EU) 2016/679, where appropriate, except where other Union or national laws explicitly require consent, and where such interests are overridden by the interests, or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. Any such processing shall be subject to appropriate organisational, technical measures and safeguards for the rights and freedoms of the data subject, such as to ensure respect of data minimisation during the stage of selection of sources and the training and testing of AI an system or AI model, to protect against non-disclosure of residually retained data in the AI system or AI model to ensure enhanced transparency to data subjects and providing data subjects with an	**deleted**

unconditional right to object to the processing of their personal data.’	
	Article 6a
	Processing for the development of artificial intelligence systems
	(1) For the processing of personal data for the development of artificial intelligence systems, the conditions set out in paragraphs 2 to 6 shall replace point (f) of Article 6(1).
	(2) The processing of personal data for the development of artificial intelligence systems shall be lawful only if the controller demonstrates that the specified, clearly defined processing purposes cannot be achieved through technologies for the protection of personal data available according to the state of the art, such as synthetic or anonymised data.
	(3) The controller shall inform the data subject, at least three months before the processing begins, of the specific risks of that processing for the development of systems under paragraph 1, in particular that
	a) personal data may flow into those systems;
	b) subsequent erasure from those systems is technically impossible or only possible to a limited extent; and
	c) the data used for the development of those systems may be reproduced in the outputs of those systems.
	(4) The controller shall grant the data subject an unconditional right to object. The objection may be declared at any time before the processing under paragraph 1 begins and shall not require any justification.
	(5) The controller shall demonstrate that it processes exclusively personal

	data of data subjects who have been informed in accordance with paragraph 3 and who were able to effectively exercise their right to object under paragraph 4.
	(6) The controller shall, taking into account the state of the art and the costs of implementation, implement appropriate technical and organisational measures to
	a) prevent the reproduction of personal data of a data subject who has been informed in accordance with paragraph 3 and who has not exercised their right to object in the outputs of systems under paragraph 1; and
	b) minimise the identifiability of data subjects in systems under paragraph 1.
	The first sentence shall be without prejudice to other lawful processing of personal data.
	(7) The processing of personal data of children under 18 years of age shall be lawful under paragraph 1 only with the explicit consent of the holders of parental responsibility. Upon reaching the age of majority, data subjects shall have an unconditional right to object to processing under paragraph 1, which they may exercise against the controller within 12 months of reaching the age of majority.
	(8) This Article shall be without prejudice to Article 9.
Recitals 30 and 31	
(30) Trustworthy AI is key in providing for economic growth and supporting innovation with socially beneficial outcomes. The development and use of	**deleted**

AI systems and the underlying models such as large language models and generative video models rely on data, including personal data, in various phases in the AI lifecycle, such as the training, testing and validation phase and may in some instances be retained in the AI system or the AI model. The processing of personal data in this context may therefore be carried out for purposes of a legitimate interest within the meaning of Article 6 of Regulation (EU) 2016/679, where appropriate. This does not affect the obligation of the controller to ensure that the development or use (deployment) of AI in a specific context or for specific purposes complies with other Union or national law, or to ensure compliance where its use is explicitly prohibited by law. It also does not affect its obligation to ensure that all other conditions of Article 6(1)(f) of Regulation (EU) 2016/679 as well as all other requirements and principles of that Regulation are met.	
(31) When the controller, in the light of the risk-based approach which informs the scalability of the obligations under this Regulation, is balancing the legitimate interest pursued by the controller or a third party and the interests, rights and freedoms of the data subject, consideration should be given to whether the interest pursued by the controller is beneficial for the data subject and society at large, which may for instance be the case where the processing of personal data is necessary for detecting and removing bias, thereby protecting data subjects from discrimination, or where the processing of personal data is aiming at ensuring accurate and safe outputs for a beneficial use, such as to improve accessibility to certain services.	**deleted**

Consideration should also, among others, be given to reasonable expectations of the data subject based on their relationship with the controller, appropriate safeguards to minimise the impact on data subjects' rights such as providing enhanced transparency to data subjects, providing an unconditional right to object to the processing of their personal data, respecting technical indications embedded in a service limiting the use of data for AI development by third parties, the use of other state of the art privacy preserving techniques for AI training and appropriate technical measures to effectively minimise risks resulting, for example, from regurgitation, data leakage and other intended or foreseeable actions.		
	(30a) The development of artificial intelligence systems, including in particular the training, fine-tuning, validation and other processing operations aimed at establishing or modifying model parameters, constitutes a distinct regulatory situation that fundamentally differs from conventional processing situations under Article 6(1)(f). Personal data typically flow irreversibly into the model architecture or its parameters; subsequent erasure is technically impossible or only possible to a limited extent, and data processed for the development of such systems may be reproduced in model outputs. Article 6a takes account of these particularities by separating this regulatory situation from the general doctrine of Article 6(1)(f) and by laying down specific conditions.	
	Processing of personal data for the development of artificial intelligence	

systems is lawful only where the processing purpose cannot otherwise be achieved. The mere usefulness of personal data does not suffice, in view of the specific and potentially irreversible risks associated with such processing; the controller must be able to demonstrate that the specified processing purposes cannot be achieved through technologies for the protection of personal data available having regard to the state of the art.

In order to enable the data subject to make an informed decision on the exercise of the right to object, the controller should provide information on the specific consequences of processing for the development of artificial intelligence systems. That information should in particular indicate that personal data may flow irreversibly into the model, that subsequent erasure is technically impossible or only possible to a limited extent, and that data used for the development of such systems may be reproduced in model outputs.

The right to object should be capable of being effectively exercised prior to the commencement of the processing. Legitimate expectations of data subjects can arise only where processing for the development of artificial intelligence systems has been contractually agreed or where the controller has announced the processing within an adequate period. Legitimate expectations cannot be constructed retroactively to legitimise existing data sets. The right to object shall also be available to persons who are not users of the service. The controller should provide

procedures that are easily accessible and do not require registration.

The right to object must not be undermined by the controller pseudonymising the data or otherwise rendering them anonymous and subsequently invoking an inability to identify the data subject. The controller should ensure, through appropriate documentation, that the connection between original data and an objection remains traceable even after transformation of the data. This obligation reflects the accountability principle laid down in Article 5(2).

Technical measures for the protection against reproduction of personal data and for the minimisation of identifiability should be understood in a technology-neutral manner. Examples of currently available techniques include differential privacy, federated learning and machine unlearning. In certain cases, the generation of personal data by the model may be permissible, for example where the data subject has given consent or has manifestly made the data public.

The publication of artificial intelligence models as open source may in principle be desirable, but may entail particular challenges, since a subsequent objection vis-à-vis the original controller may become ineffective in practice if the model already exists in numerous copies. The controller should take this into account when deciding on open-source publication and, where appropriate, take suitable precautions, for example through documentation of the origin of the

training data or contractual binding of downstream users.

Children deserve specific protection in the processing of their personal data, since they typically cannot assess the scope and risks of data processing for the development of artificial intelligence systems. Processing of their personal data for AI development purposes therefore requires the explicit consent of the holders of parental responsibility. This reflects the potentially long-term consequences of such processing. This also applies where the data have been introduced into the dataset by third parties. Upon reaching the age of majority, data subjects should be able to decide for themselves whether their data may continue to be used; they therefore have an unconditional right to object, which they may exercise within twelve months after reaching majority.

The development of AI systems involves structural particularities that distinguish it from conventional processing under Article 6(1)(f) GDPR. Personal data may be irreversibly integrated into model parameters, subsequent erasure is technically limited, and data may reappear in system outputs. In such situations, the general balancing framework of Article 6(1)(f) does not sufficiently ensure the effective protection of data subjects' rights, in particular the right to object.

The structural characteristics of AI development also raise fundamental questions of effective protection under Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. Where personal data are integrated into model parameters in a manner that is difficult or impossible to reverse, the exercise of data subject rights, in particular the right to erasure and the right to object, risks becoming ineffective in practice. This creates a structural imbalance between controllers and data subjects that cannot be adequately addressed through the ex post balancing inherent in Article 6(1)(f) GDPR. A differentiated regulatory approach is therefore necessary to ensure that the use of personal data remains proportionate and subject to meaningful control by data subjects, while providing controllers with clear and predictable conditions for lawful processing.

The amendment therefore introduces a lex specialis within the framework of Article 6 by replacing the conditions of Article 6(1)(f) for this specific processing context. It clarifies that the use of personal data must be strictly necessary and

that less intrusive technologies available according to the state of the art must be considered. To ensure effectiveness, the right to object must be exercisable prior to the commencement of processing, accompanied by clear information on the specific risks involved.

By establishing clear, proportionate and technology-neutral conditions for the development of AI systems, the proposal contributes to simplification and legal certainty. It creates a level playing field across the Union by defining uniform safeguards, while maintaining space for responsible innovation. Strengthening effective safeguards at an early stage enhances trust, reduces litigation risks and supports the sustainable development of AI in the internal market.

For a more detailed analysis of the European Commission's proposal, see page 8ff of the expert opinion commissioned by vzbv.[14]

4.2 AMs to the proposed exception from the ban on processing sensitive data

Text proposed by the European Commission	**Amendments**
Articles 3(3)(a) and 3(3)(b)	
Article 9 is amended as follows: (a) in paragraph 2, the following points are added: '(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.	**deleted**
(b) the following points are added: '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	**deleted**

[14] Hense, Peter; Wagner, David: Proposal for a Legal Basis for the Processing of Personal Data in the Context of the Development and Deployment of AI, 2025, p. 8ff, https://www.vzbv.de/sites/default/files/2026-02/25-12-08_Legal-Opinion_Hense_Wagner_AI-Legal-Bases.pdf, 13.04.2026.

such measures, the controller identifies special categories of personal data in the datasets used for training, testing or validation or in 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.'

Recital 33	
(33) The development of certain AI systems and AI models may involve the collection of large amounts of data, including personal data and special categories thereof. Special categories of personal data may residually exist in the training, testing or validation data sets or be retained in the AI system or the AI model, although the special categories of personal data are not necessary for the purpose of the processing. In order not to disproportionately hinder the development and operation of AI and taking into account the capabilities of the controller to identify and remove special categories of personal data, derogating from the prohibition on processing special categories of personal data under Article 9(2) of Regulation (EU) 2016/679 should be allowed. The derogation should only apply where the controller has implemented appropriate technical and organisational measures in an effective manner to avoid the processing of those data, takes the appropriate measures during the entire lifecycle of an AI system or AI model and, once it identifies such data, effectively remove	**deleted**

them. If removal would require disproportionate effort, notably where the removal of special categories of data memorised in the AI system or AI model would require re-engineering the AI system or AI model, the controller should effectively protect such data from being used to infer outputs, being disclosed or otherwise made available to third parties. This derogation should not apply where the processing of special categories of personal data is necessary for the purpose of the processing. In this case, the controller should rely on the derogations pursuant to Article 9(2)(a) – (j) of Regulation (EU) 2016/679.

The proposed changes must be removed.

The European Commission proposal introduces a new exception allowing the processing of special categories of personal data in the context of AI development, based on the notion of "residual data". This constitutes a structural deviation from Article 9 GDPR, which is designed as a prohibition with narrowly defined exceptions. The proposal shifts this logic towards a broad, activity-based privilege for large-scale data processing.

The draft reverses the risk-based approach of the GDPR. Instead of requiring stricter safeguards for more intrusive processing, it creates privileges precisely where large-scale, opaque and unstructured processing occurs. The acceptance that sensitive data may remain in datasets despite not being necessary for the processing purpose undermines the principles of data minimisation and necessity under Article 5 (1)(c) GDPR.

The proposal is also in tension with established CJEU case law, which consistently treats the presence of special categories of personal data as triggering the application of Article 9 GDPR, irrespective of intent. By privileging the inseparable combination of sensitive and non-sensitive data, the proposal risks lowering the level of protection in a manner incompatible with Union law.

In addition, the shift towards ex post safeguards, such as output filtering, weakens the principle of proactive protection. Data subjects are deprived of effective control and remedies, particularly where the processing itself is deemed lawful under the new exception. This is especially problematic given that individuals are typically unaware of such processing and cannot effectively exercise their rights.

There is no sufficient justification for this structural change. The proposal weakens the protection of special categories of personal data, creates legal uncertainty and departs from the established system of the GDPR. Controllers should instead rely

on the existing, narrowly defined exceptions in Article 9 (2)(a) to (j) GDPR, which ensure a level of protection compatible with fundamental rights.

For a more detailed analysis of the European Commission's proposal, see page 21ff of the expert opinion commissioned by vzbv.[15]

5. Additional targeted amendments

5.1 AMs to strengthen the protection of children's personal data

Text proposed by the European Commission	Amendments
Articles	
	Article 6(4), point (b), is amended as follows:
	(b) the possible consequences of the intended further processing for data subjects, in particular where the personal data of a child are concerned;
	Article (8)(1) is amended as follows:
	1. Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. The processing of a child's personal data for advertising purposes or for the creation of personality or user profiles shall be prohibited. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age

[15] Hense, Peter; Wagner, David: Proposal for a Legal Basis for the Processing of Personal Data in the Context of the Development and Deployment of AI, 2025, p. 21ff, https://www.vzbv.de/sites/default/files/2026-02/25-12-08_Legal-Opinion_Hense_Wagner_AI-Legal-Bases.pdf, 13.04.2026.

	for those purposes provided that such lower age is not below 13 years.
	Article 9(2), point (a), is amended as follows: ***(a) the adult data subject has given explicit consent to the processing of those personal data for one or more specified purposes, either on their own behalf or, where applicable, as the holder of parental responsibility over a child, or a child has, having regard to the child's maturity, given consent to processing which is not manifestly contrary to the child's best interests, except where Union or Member State law provides that the prohibition referred to in paragraph 1 may not be lifted by the data subject;***
	Article (21)(1) is amended as follows: ***1. The data subject shall have the right to object, on grounds relating to his or her particular situation, in particular where the personal data of a child are concerned, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.***
	Article 22(2), point (c), is amended as follows: ***(c) is based on the explicit consent of the adult data subject.***
	In Article 25(1) the following sentence is added:

	Particular regard shall be given to the protection of the rights of children.
	In Article 25(2) the following sentence is added: ***The default settings shall, in particular, take into account the specific vulnerability of children.***

The amendments strengthen the protection of children's personal data by integrating their specific vulnerability more consistently across key provisions of the GDPR.

While Recital 38 GDPR recognises that children merit specific protection, this is only partially reflected in the operative provisions. The amendments therefore clarify that, where children's data are concerned, this must be explicitly taken into account in compatibility assessments under Article 6(4) and in the exercise of the right to object under Article 21. This reinforces the weight of children's interests in proportionality and balancing tests without altering the underlying legal structure.

In addition, the amendments strengthen data protection by design and by default by requiring controllers to give particular regard to the rights of children and to reflect their specific vulnerability in default settings (Article 25). This ensures that protective considerations are embedded at the level of system design and not left solely to ex post assessments.

The introduction of a prohibition on processing children's personal data for advertising and profiling purposes addresses the heightened risks associated with behavioural targeting and commercial exploitation of minors. It establishes a clear and enforceable boundary in an area where case-by-case assessments have proven insufficient to ensure effective protection.

Finally, the clarification in Article 9(2)(a) reflects the need to take into account children's evolving capacities while ensuring that any processing of special categories of personal data is not manifestly contrary to the child's best interests.

Overall, the amendments enhance legal certainty, support more consistent application and enforcement, and ensure that the GDPR more effectively reflects the fundamental rights and protection needs of children in the digital environment.

The amendments mirror the proposal of the German Data Protection Conference (Datenschutzkonferenz, DSK) to operationalise existing principles of child protection within the current regulatory framework.[16]

[16] Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder: Verbesserung des Datenschutzes von Kindern in der Datenschutz-Grundverordnung, 2025, https://datenschutzarchiv.org/detailansicht/Dokumente/2025/ST_DSK_20251120_de.pdf, 13.04.2026.

5.2 AMs to establish manufacturer accountability for data protection by design

Text proposed by the European Commission	Amendments
Articles	
	Article 4 is amended by adding the following point: ***(27) 'manufacturer' means a manufacturer within the meaning of Article 4 of Directive (EU) 2024/2853 of the European Parliament and of the Council. Where a manufacturer determines the purposes and means of the processing of personal data, it shall be considered a controller within the meaning of point (7) of this Article.***
	Article 24 is amended by adding the following paragraph: ***4. The manufacturer shall design and develop its products, services and applications, taking into account the right to the protection of personal data and the state of the art, in such a manner that controllers and processors are able to comply with their obligations under this Regulation without having to make disproportionate modifications to those products, services and applications. The manufacturer shall support controllers and processors in fulfilling their obligations under Articles 30, 33 and 34 by providing, upon request, all information necessary for that purpose.***
	Article 79(2) is amended as follows: ***(2) Proceedings against a controller, processor or manufacturer shall be***

	brought before the courts of the Member State where the controller, processor or manufacturer has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller, processor or manufacturer is a public authority of a Member State acting in the exercise of its public powers.
	Article 82 is amended by adding the following paragraph: ***(7) Where damage is caused wholly or partly by an act or omission of a manufacturer, the manufacturer shall be liable to the data subject in addition to the controller or processor. The manufacturer shall also be liable vis-à-vis the controller and the processor.***

The amendments introduce targeted obligations for manufacturers in order to align data protection responsibilities with actual decision-making power in digital environments.

While the GDPR primarily addresses controllers and processors, key decisions on the architecture, functionalities and default settings of digital products are often taken by manufacturers. This creates a structural imbalance: controllers remain accountable for compliance but frequently lack effective control over the technical conditions of processing. This is particularly evident in Article 25 GDPR, where data protection by design and by default is required, but can in practice only be implemented within the limits set by product design.

The amendments address this gap by requiring manufacturers to design products, services and applications in a way that enables compliance and by introducing corresponding accountability and liability mechanisms. This reduces decentralised compliance burdens, particularly for SMEs, and improves legal certainty.

At the same time, embedding data protection requirements at product level strengthens the protection of data subjects by making privacy-friendly design and default settings the standard rather than the exception.

Overall, the amendments correct a structural imbalance, enhance enforceability and contribute to a more effective and practical application of the GDPR.

The amendments mirror the proposal of the DSK, which identifies a structural gap in the current allocation of responsibilities under the GDPR.[17]

[17] Erfahrungsbericht der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Anwendung der DS-GVO, 2019, p. 15ff, https://www.datenschutzkonferenz-online.de/media/dskb/20191213_erfahrungsbericht_zur_anwendung_der_ds-gvo.pdf, 13.04.2026.

Imprint

Published by:
Verbraucherzentrale Bundesverband e.V.
(Federation of German Consumer Organisations)
Rudi-Dutschke-Straße 17, 10969 Berlin

T +49 30 25800-0
vzbv.de

Publishing date:
April, 2026

The Federation of German Consumer Organisations is registered in the German Lobby Register and the European Transparency Register. You can access the relevant entries here und here.