The Standing Committee of European Doctors (CPME) represents national medical associations across Europe. We are committed to contributing the medical profession's point of view to EU and European policy-making through pro-active cooperation on a wide range of health and healthcare related issues.

Proposed amendments to the Commission's Digital Omnibus on Data

Proposed amendments

The CPME feedback on the Digital Omnibus Package can be accessed here.

European doctors emphasise the importance of ensuring robust protections for personal data, in particular for data concerning health. Several proposals from the European Commission in the Digital Omnibus have weakened these safeguards which, if adopted, will have a significant impact on sensitive data processed in the context of digital healthcare platforms and online medicine sales.

As key risks resulting from this weakened protections, European doctors highlight:

i) Easier profiling of patients in situations of particular vulnerability by digital platforms;
ii) Unethical reuse of health-related data for commercial or advertising purposes;
iii) Expanded tracking of users' devices, undermining confidentiality;
iv) Misuse of health data by online pharmacies and marketplaces;
v) Processing or inference of special categories of data (e.g., health status) without sufficient justification or safeguards.

These risks highlight the need for preserving strong definitions in the General Data Protection Regulation and robust safeguards to ensure ethical and privacy preserving digital medicine supply.

CPME's proposed amendments are indicated in ***bold italics and underlined font***.

Amendments to the General Data Protection Regulation (GDPR)

Amendment 1

Proposal for a regulation
Article 3 – paragraph 1 – point a
Regulation (EU) 2016/679
Article 4(1)(a)

Amendments to Regulation (EU) 2016/679 (GDPR)	
Definition of personal data	
Text proposed by the Commission	*CPME proposed amendment*
Article 4 is amended as follows: (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	***delete***

because a potential subsequent recipient has means reasonably likely to be used to identify the natural person to whom the information relates.'	

Justification

The text proposed by the Commission narrows the concept of personal data, severely weakening the fundamental right to personal data protection. This change is not a technical adjustment but goes far beyond a targeted modification of the GDPR. The attempt to codify the ruling of the Court of Justice of the European Union (CJEU) with regard to pseudonymisation of personal data (C-413/23)[1] is misinterpreted. The text proposed by the Commission risks undermining the implementation of the European Health Data Space Regulation in relation to trust on accessing and sharing of personal electronic health data. Weakening the definition of personal data erodes the foundation of trust between doctors and patients — a relationship that ensures clinical data are accurate, complete, and valid. The integrity of the treatment relationship is critical to generating reliable data for safe digital solutions. European values and the principles of confidentiality demand that trust in this relationship is upheld. Weakening the definition does not drive innovation but risks undermining the quality and safety of digital health initiatives. The deletion of this text is also recommended by the EDPB-EDPS Joint Opinion 2/2026 of 10 February.[2]

[1] Judgment of the Court of Justice of 4 September 2025, EDPS v SRB, C-413/23 P, ECLI:EU:C:2025:645. The CJEU rules that pseudonymised data must not be regarded as constituting, in all cases and for every person, personal data, since depending on the circumstances of the case, pseudonymised data may prevent other persons from identifying the data subject in a way that for them the data subject is not or is no longer identifiable (paragraph 86). The text proposed by the Commission fails by referring to 'information relating to a natural person', which is a step before undergoing pseudonymisation. For further detail please see paragraphs 72 to 77, 85 and 86 of the CJEU decision.

[2] See point 21 of the EDPB-EDPS Joint Opinion 2/2026 of 10 February 2026 on the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus).

Amendment 2

New Amendment
Proposal for a regulation
Regulation (EU) 2016/679
Article 4(5)

Amendments to Regulation (EU) 2016/679 (GDPR)	
Definition of pseudonymisation	
Text proposed by the Commission	*CPME proposed amendment*
-	(5) 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person; ***pseudonymised data shall not be personal data for a given recipient where that recipient cannot identify the natural person to whom the information relates, taking into account the means reasonably allowing them to attribute the information to the data subject.***"
Justification	
This amendment is proposed should the codification of the ruling of the CJEU in case C-413/23, with regard to pseudonymisation of personal data, be desired by co-legislators. This amendment can bring more awareness as to when pseudonymised data is personal data for third parties.	

Amendment 3

Proposal for a regulation
Article 3 – paragraph 1 – point b
Regulation (EU) 2016/679
Article 4(38)

Amendments to Regulation (EU) 2016/679 (GDPR)	
Definition of scientific research	
Text proposed by the Commission	*CPME proposed amendment*
(b) the following points are added: (38) "scientific research" means any research which can also support innovation, such as technological development and demonstration. These actions shall contribute to existing scientific knowledge or apply existing knowledge in novel ways, be carried out with the aim of contributing to the growth of society´s general knowledge and wellbeing and adhere to ethical standards in the relevant research area. This does not exclude that the research may also aim to further a commercial interest.'	(b) the following points are added: (38) "scientific research" means ~~**any**~~ research **conducted following a methodological and systematic approach of the relevant research area and in adherence to the highest ethical and professional standards of such research area. Scientific research shall be conducted freely and lead to verifiable and transparent results.** ~~which can **also** support innovation, such as technological development and demonstration. These actions shall contribute to existing scientific knowledge or apply existing knowledge in novel ways, be carried out with the aim of contributing to the growth of society´s general knowledge and wellbeing and adhere to ethical standards in the relevant research area. This does not exclude that the research may also aim to further a commercial interest~~.'
Justification	
The definition of scientific research needs to be narrowed by making reference to the scientific method as well as to the highest ethical and professional standards of the relevant research area. In addition, considering the Council Recommendation (EU)	

2021/2122 on a Pact for Research and Innovation in Europe,[3] reference should be made to the 'freedom of scientific research' as a value to uphold, to ensure that scientific research can be conducted in an autonomous and independent manner. CPME supports the EDPB-EDPS recommendation in its Joint Opinion 2/2026 of 10 February 2026 to move the sentences addressing innovation, contributing to existing scientific knowledge and wellbeing, and commercial interest to a recital, as these sentences provide context and guidance but do not constitute criteria for an activity to qualify as scientific research.[4]

Amendment 4

Proposal for a regulation
Article 3 – paragraph 3
Regulation (EU) 2016/679
Article 9(2)(k) and (l)

Amendments to Regulation (EU) 2016/679 (GDPR)	
Exemption to process special categories of data	
Text proposed by the Commission	*CPME proposed amendment*
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. (l) processing of biometric data is necessary for the purpose of confirming the identity of a data subject	Article 9 is amended as follows: (a) in paragraph 2, the following ***points~~ is ~~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.~~ (l) processing of biometric data is necessary for the purpose of confirming the identity of a data subject

[3] See value I, paragraph 1, point b, of the Council Recommendation (EU) 2021/2122 of 21 November 2021 on a Pact for Research and Innovation in Europe, <https://eur-lex.europa.eu/eli/reco/2021/2122/oj/eng>.
[4] Please see in this sense point 29 of EDPB-EDPS Joint Opinion 2/2026 of 10 February 2026 on the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus).

(verification), where the biometric data or the means needed for the verification is under the sole control of the data subject.'	(verification), where the biometric data or the means needed for the verification is under the sole control of the data subject.'
Justification	
The EDPB Opinion 28/2024 on AI models[5] confirmed that, under the GDPR, legitimate interests can be used as a legal basis to develop and deploy AI models and systems. It is not necessary to add a specific provision in the operative part of the GDPR, avoiding the introduction of an undefined legal term, such as 'operation of AI'. CPME supports the EDPB-EDPS Opinion 2/2026 which recommends explaining the situations where 'legitimate interest' can be used as valid legal basis in a recital instead.[6] Regulators must also explain in a recital whether training AI models on personal data scraped on the web satisfies a lawful purpose, in particular if it concerns health data. CPME recalls that the training of datasets in healthcare must be carried out on validated datasets specifically tailored to healthcare. Using non-validated internet content can lead to incorrect information in clinical decision-making system process.[7] Finally, specific limitations exist in relation to the use of electronic health data for AI development and deployment which were put in place to ensure trust in electronic health data sharing for secondary use purposes. Pursuant to Article 51(1)(a) and Article 53(1)(e) of the European Health Data Space Regulation (EHDS),[8] the training, testing and evaluation of algorithms, including medical devices, *in vitro* diagnostic medical devices, AI systems and digital health applications are only allowed when part of scientific research related to health or care sectors. Article 9(2)(k) needs to be deleted to also ensure compliance with the EHDS Regulation.	

[5] EDPB Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models, adopted on 17 December 2024.
[6] See point 39 and footnote 47 of EDPB-EDPS Joint Opinion 2/2026 of 10 February 2026.
[7] See points 45 and 46 of CPME policy on the deployment of artificial intelligence in healthcare – sector-specific challenges and accelerators, CPME 2024/073 Final, adopted on 9 November 2024.
[8] Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 (Text with EEA relevance).

Amendment 5

Proposal for a regulation
Article 3 – paragraph 3
Regulation (EU) 2016/679
Article 9(5)

Amendments to Regulation (EU) 2016/679 (GDPR)	
Exemption to process special categories of data	
Text proposed by the Commission	*CPME proposed amendment*
Article 9 is amended as follows: (…) (b) the following paragraph is 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 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.'	Article 9 is amended as follows: (…) (b) the following paragraph is added: '5. ***When processing personal data leads to residual and incidental processing of special categories of data,*** ~~For processing referred to in point (k) of paragraph 2, appropriate organisational and technical measures shall be implemented to avoid v the collection and otherwise processing of special categories of personal data. Where, despite the implementation of such measures, the controller identifies special categories of personal data in the datasets used for training, testing or validation or in the AI system or AI model~~, the controller shall ***implement appropriate organisational and technical measures to avoid such processing and shall*** remove such data. If removal of those ***personal*** data ***is impossible or*** requires disproportionate effort, the controller shall in any event effectively protect without undue delay such data from being used ***or re-used for***

	***other purposes*, in particular** to produce AI outputs ***or actions, and*,** from being disclosed or otherwise made available to third parties.'
Justification	
The text proposed by the European Commission weakens the data minimisation principle under Article 5(1)(b) of the GDPR and increases the risk that special categories of data are processed more easily without a real effort from controllers to delete such data. The CPME proposed amendment is necessary to clarify the scope of the derogation for processing special categories of data and ensuring safeguards throughout the personal data lifecycle. Nonetheless, CPME notes that it will still be very difficult for competent authorities to determine whether the controller has effectively avoided the collection and processing of special categories of personal data and if such data is removed accordingly, in particular when developing and deploying AI. Concerning the latter, CPME strongly recommends that the controller designates an 'AI officer' for these conditions to function correctly.[9]	

Amendment 6

Proposal for a regulation
Article 3 – paragraph 4
Regulation (EU) 2016/679
Article 12(5)

Amendments to Regulation (EU) 2016/679 (GDPR)	
Transparent information, communication and modalities for the exercise of the rights of the data subject	
Text proposed by the Commission	*CPME proposed amendment*
In Article 12, paragraph 5 is replaced by the following:	In Article 12, paragraph 5 is replaced by the following:

[9] The designation of an AI system officer is advocated by CPME in its position on the Digital Omnibus on AI (CPME 2026/016), March 2026 and on the CPME Feedback to the Digital Omnibus Package – Calling for credibility of digital regulations in Europe (CPME 2026/003), February 2026. The AI system officer could ensure internal compliance of companies with the AI Act, in particular when processing special categories of data for bias detection and correction, or for producing AI outputs, or for disclosing or making personal data available to third parties. This officer could facilitate the work of the market surveillance authorities at several instances, being the point of contact for competent authorities, creating more trust in the market environment.

'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.'	'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 ***of an abusive intention by the*** data subject ***to cause harm*** ~~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 ***or that request has an abusive intention***.'
Justification	
This CPME proposed amendment provides legal clarity to controllers in situations where there is an abuse of rights by the data subject with intention to harm the data controller. This is in line with the EDPB-EDPS Joint Opinion 2/2026 and the CJEU judgements related to the right of access by data subjects.[10]	

[10] See points 53 to 57 and footnote 62 of EDPB-EDPS Joint Opinion 2/2026.

Amendment 7

Proposal for a regulation
Article 3 – paragraph 7
Regulation (EU) 2016/679
Article 22(1) and (2)

Amendments to Regulation (EU) 2016/679 (GDPR)	
Automated individual decision-making process, including profiling	
Text proposed by the Commission	*CPME proposed amendment*
In Article 22, paragraphs 1 and 2 are replaced by the following: '1. A decision which produces legal effects for a data subject or similarly significantly affects him or her may be based solely on automated processing, including profiling, only where that decision: (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller regardless of whether the decision could be taken otherwise than by solely automated means; (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or (c) is based on the data subject's explicit consent.'	***delete***
Justification	
The text proposed by the European Commission changes from a 'right not to be subject to' automated decision-making, that is a prohibition in principle unless certain conditions apply, to the situation of being allowed provided that certain conditions apply.	

The text proposed by the European Commission would legalise data mining on the web and allow profiling by default. The text weakens data subjects' rights and should therefore be rejected. The text proposed by the European Commission would also require renumbering the remaining paragraphs of Article 22.

Amendment 8

Proposal for a regulation
Article 3 – paragraph 10
Regulation (EU) 2016/679
Article 41a

Amendments to Regulation (EU) 2016/679 (GDPR)	
Implementing acts to clarify whether data from pseudonymisation constitutes personal data	
Text proposed by the Commission	*CPME proposed amendment*
'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; (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	***delete***

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).'	
Justification	
Determining what constitutes or not personal data directly affects the application of EU data protection law. An implementing act in this area would modify the material scope of EU data protection law, redefining when and for whom information is considered personal data. Since it is desirable for recipients to understand how the definition of personal data should be applied and their respective compliance obligations, CPME supports the EDPB-EDPS Joint Opinion 2/2026 for supervisory authorities, under the control of competent courts, to apply the definitions of the GDPR, and for the EDPB to ensure consistent application on this matter. Guidelines should be developed in this sense by EDPB.	

Amendment 9

Proposal for a regulation
Article 3 – paragraph 15
Regulation (EU) 2016/679
New Article 88a

Amendments to Regulation (EU) 2016/679 (GDPR)	
Processing of personal data in the terminal equipment of natural persons	
Text proposed by the Commission	*CPME proposed amendment*
After Article 88, the following articles are added: 'Article 88a *Processing of personal data in the terminal equipment of natural persons* (1) Storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person is only allowed when that person has given his or her consent, in accordance with this Regulation. (2) Paragraph 1 does not preclude storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person, based on Union or Member State law within the meaning of, and subject to the conditions of Article 6, to safeguard the objectives referred to in Article 23(1). (3) Storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person without consent, and subsequent	After Article 88, the following articles are added: 'Article 88a *Processing of personal data in the terminal equipment of natural persons* (1) Storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person is only allowed when that person has given his or her consent, in accordance with this Regulation. (2) Paragraph 1 does not preclude storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person, based on Union or Member State law within the meaning of, and subject to the conditions of Articles 6 ***and 9,*** ***including professional secrecy***, 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

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. (…)	person without consent, and subsequent processing, shall be lawful to the extent it is 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 data subject; (c) creating ***anonymous*** 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. ***This information shall not be further processed for another purpose***; (d) maintaining or restoring the ***strictly necessary IT*** security ***and data protection 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, ***without changing the functionality of the software on the terminal equipement and informing the user in advance with the possibility to turn-off automatic updates***. (…)
Justification	
The CPME proposed amendments expresses the concern that there will be more room for tracking behaviours, measure usage and analyse interactions directly on user's devices. In the healthcare sector, hospitals networks or devices of healthcare professionals	

need to be appropriately safeguarded due to their obligations of professional secrecy. The CPME proposed amendments also addresses the concern that 'subsequent processing' is limited to specific purposes, and follows several recommendations of the EDPB-EDPS Joint Opinion 2/2026 on the protection of information stored and accessed in terminal equipment.

Amendment 10

Proposal for a regulation
Article 3 – paragraph 15
Regulation (EU) 2016/679
New Article 88c

Amendments to Regulation (EU) 2016/679 (GDPR)	
Processing in the context of the development and operation of AI	
Text proposed by the Commission	*CPME proposed amendment*
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	***delete***

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 unconditional right to object to the processing of their personal data.'	
Justification	
This provision must be deleted since allowing manufacturers to process personal data for AI development and operation based on 'legitimate interest,' raises serious concerns. Such provision creates a legal loophole that undermines shared accountability and clarity in data governance. CPME calls for a clear and shared framework of responsibility across all stakeholders in the healthcare ecosystem, including citizens, patients, clinicians, policymakers, and developers. A governance blueprint that ensures shared accountability is required, as well as stronger involvement of physicians and patients in the development of AI models to ensure these models contribute meaningfully to health outcomes while safeguarding data integrity.	

Amendment 11

New Amendment
Proposal for a regulation
Regulation (EU) 2016/679
Article 89(1)

Amendments to Regulation (EU) 2016/679 (GDPR)	
Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes	
Text proposed by the Commission	*CPME proposed amendment*
Article 89 1. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.	Article 89 1. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ***include ethical oversight and review mechanisms, public engagement and participation, and*** ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.
Justification	

This amendment provides further clarity and guidance on what should be considered 'appropriate safeguards', referring to the need of including ethical oversight and review mechanisms as well as public engagement and participation. This amendment is necessary considering the progress in data-intensive health research and the processing of personal electronic health data without consent.

***