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.

Feedback to Digital Omnibus Package

Calling for credibility of digital regulations in Europe

European doctors are concerned with several amendments proposed by the European Commission in the Digital Omnibus Package,[1] as they seem to considerably reduce safeguards around personal data use and re-use, in particular when processing special categories of data such as health data in AI contexts. While the objective for clarification, coherence and simplification are welcomed, these objectives should not be made at the expense of legal certainty, fundamental rights, and trust in the EU digital rulebook.

For CPME, the digital fitness check should have been concluded first, before proposing substantial changes to the digital rulebook with impact on fundamental rights and core definitions. CPME stresses that deeper analysis is required, advising against any amendments which can have a negative impact on the implementation of the European Health Data Space Regulation, in particular legal definitions (e.g. definition of personal data and of scientific research) and legal basis (e.g. legitimate interest to process personal data for the purposes of AI training, testing and validation, including special categories of data). The European Health Data Space Regulation was negotiated under specific premises, aiming for a high-level of trust in accessing and sharing special categories of data, namely data from electronic health records, genetic data, data from wellness apps, personal data from medical devices, among other.

Notwithstanding the objective of promoting innovation and development in Europe, the rights that EU regulations afford to citizens must not be diluted. Competitiveness and compliance with data protection and privacy laws are compatible.

[1] European Commission Proposal for a Regulation of the European Parliament and of the Council of 19 November 2025 amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI), COM/2025/836 final; and European Commission Proposal for a Regulation of the European Parliament and of the Council of 19 November 2025 amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus), COM/2025/837 final.

From a preliminary analysis, CPME believes that the amendments proposed by the European Commission go beyond simplification, amounting to deregulation with an impact on patient safety and patient's rights. Patients must trust in the confidentiality and legitimate processing of their health data, otherwise they will undermine the availability of their health data for primary and secondary use purposes.

European doctors believe that the effectiveness of the EU digital rulebook would be improved through clearer regulatory guidance, consistent enforcement across Member States, and targeted support for SMEs rather than broad omnibus amendments. The EU should also stimulate European data sovereignty at short notice, supporting European data platforms, cloud service providers, and other digital services.

CPME calls on the European Commission to consider the following:

- **European fundamental rights cannot be weakened.** Support effective enforcement of regulations as it increases trust in the EU regulatory framework.
- An appropriate balance is necessary to continue to **consider companies risk-based activities when processing special categories of data**, despite being SMEs and small mid-cap enterprises.
- The use of electronic health data from electronic health records for **AI development and operation must be in compliance with the European Health Data Space Regulation** (EHDS),[2] where pursuant to Article 51(1)(a) and Article 53(1)(e) of the EHDS, 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. It should also be recalled, during the negotiations of the EHDS, the co-legislators intention of no longer accepting the training, testing and evaluation of AI as a separate permitted purpose, reinforcing that data for AI development and algorithm training to be permitted only when it falls within the scope of scientific research.[3]
- Require providers of high-risk AI systems, including general-purpose AI systems, and deployers of AI systems referred to in Article 50 of the AI Act, to **designate an AI auditor,** who would be responsible, within a company, public entity or body, for examining the internal processes and procedures put in place during the AI life cycle. Similar to auditors

[2] 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).
[3] In this sense, see M5.2 Guideline for Health Data Access Bodies on minimum categories and limitations on the reuse of health data of the Joint Action Toward the European Health Data Space 2, 16 September 2025, p 28, <https://tehdas.eu/wp-content/uploads/2025/09/draft-guideline-for-health-data-access-bodies-on-minimum-categories-and-limitations-on-the-reuse-of-health-data.pdf >, accessed 5 February 2026.

for corporate governance, or data protection officers for GDPR, an AI auditor could monitor compliance of providers and deployers' internal policies with the AI Act, inform and advise those providers and deployers about the obligations pursuant to the AI Act, cooperate with competent authorities and market surveillance authorities, being their point of contact, while at the same time generating more trust in the market.

CPME believes that **designating an AI auditor is a balanced approach to ensure innovation, while respecting trade secrets and promoting public trust**, considering the new conditions which will need to be followed when processing special categories of data for bias detection and correction, for producing AI outputs, for disclosing or for making personal data available to third parties, as well as the difficulty of competent authorities to ascertain whether the controller has effectively avoided the collection and processing of special categories of personal data and if such data has been removed accordingly;

- **Welcome the proposed non-legislative actions** to facilitate the implementation of digital rulebook, including strengthening coordination and cooperation between regulators. These can be more beneficial than amending core legislation for data protection law in Europe.
- **Welcome the reinforced powers of the AI Office** to centralise oversight and ensure a coherent application of rules for AI systems, offering guidance for national authorities who oversee other AI systems.
- **Welcome increasing the availability of notified bodies**, by streamlining the procedure for conformity assessment bodies to apply for and be assessed in order to become notified bodies.
- **Welcome simplifying the incident reporting schemes** (NIS2, GDPR, DORA) into a Single Entry Point at ENISA. However, sufficient assurances need to be made to ensure deterrence from cyberattacks into this single-entry point.

CPME warns against:

- **Amending core definitions of data protection law** (e.g. personal data), introducing subjective criteria for a controller to be subject to the GDPR (e.g. capacity to re-identify natural persons).
- **Removing the general right for the data subject** not to be subject to automated decisions, which seem to legalise data mining on the web and allowing profiling by default.
- **Introducing a new legal basis for AI system** development and operation, where health data processing can occur, using 'legitimate interest', considering the provisions of the EHDS Regulation.

- **Releasing providers and deployers from their obligation to ensure** that their staff and other persons operating and using AI on their behalf, have a **sufficient level of AI literacy**. In healthcare, the user's (healthcare professionals) comprehension of AI systems and perceived difficulty have an impact on the usage of AI. The higher the AI literacy, including comprehending AI strengths and limitations, more easily will be to deploy AI, where users trust their own judgment instead of feeling pressured for complying with AI's recommendations. Therefore, **CPME agrees with the EDPB and EDPS Joint Opinion 1/2026[4] when it addresses AI literacy.** AI literacy should not be seen as a burden, but rather as helping to raise ethical and social awareness on AI benefits and risks.
- **Amending Annex I of the AI Act through the Medical Devices Regulation revision proposed on 16 December 2025,[5] moving the MDR[6] and IVDR[7] from Section A to Section B. This amendment would render important safeguards on high-risk AI systems inapplicable in medical devices, such as Article 14 ensuring human oversight.** The AI Act already foresees simplification in relation to medical devices and IVD MD (Article 8(2) of the AI Act), and the European Commission even published guidance on the interplay between the AI Act and MDR /IVDR.[8] Further guidance should continue to be developed, as stability of EU legislation is necessary.
- The broad **definition of 'scientific research'**. A reference to ethical committees must be included and a discussion on who can (or not) define an ethical standard must be sought.

CPME supports a compromise text in the Digital Omnibus AI in relation to the following:

- Reinstating the **standard of 'strict necessity'** from current Article 10(5) of the AI Act for the processing of special categories of personal data for the purpose of ensuring bias detection and correction.
- Restoring the obligation to **register in an EU database AI system** where the provider self-exempts its AI system as high-risk, despite being referred to in Annex III of the AI Act. CPME agrees with the arguments put forward by EDPB-EDPS Joint Opinion 1/2026 where it argues that the amendment risks of significantly decreasing accountability of providers of AI systems and could lead to undesirable incentive for providers to unduly invoke this

[4] EDPB-EDPS Joint Opinion 1/2026, on the Proposal for a Regulation as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI), 20 January 2026, p 13 and onwards.
[5] European Commission Proposal for a Regulation of the European Parliament and of the Council of 16 December 2025 amending Regulations (EU) 2017/745 and (EU) 2017/746 as regards simplifying and reducing the burden of the rules on medical devices and in vitro diagnostic medical devices, and amending Regulation (EU) 2022/123 as regards the support of the European Medicines Agency for the expert panels on medical devices and Regulation (EU) 2024/1689 as regards the list of Union harmonisation legislation referred to in its Annex I, COM(2025) 1023 Final, 2025/0404(COD).
[6] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices.
[7] Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices.
[8] Please see European Commission's subgroup on the interplay between AI Act and MDR/IVDR to the European Artificial Intelligence Board, Workshop outputs of 2 December 2025, <https://ec.europa.eu/transparency/expert-groups-register/core/api/front/document/120028/download>, accessed 4 February 2026.

exemption without critical analysis. The registration obligation ensures the transparency and traceability of AI systems.

- Establishing **fixed timelines** for the delayed application of Chapter III, sections 1, 2 and 3 for high-risk systems from Annex III for 2 December 2027 and for high-risk systems from Annex I for 2 August 2028.
- Efforts to help industry and ICT suppliers in **applying the digital rulebook**, without undermining patient safety and patient's privacy.

***