



BioMed Alliance position on the Digital Omnibus Proposals

How to balance innovation and privacy protection in the healthcare sector

1. Introduction

Recently, the European Commission presented its Digital Package, including the proposals for the Digital Omnibus (2025/0360 (COD))¹ and the Digital Omnibus on AI (2025/0359 (COD))², which aim to simplify digital rules across sector. While BioMed Alliance believes that certain aspects of the proposals might reduce some of the barriers to data driven health research, and quality assurance of AI-based software tools implemented in clinical practice, others may open the door for potential misuse and reidentification of patients based on sensitive health data. The right balance must be found that facilitates essential research and innovation, while ensuring sufficiently strong safeguards are in place to protect the privacy of patients.

The Alliance represents 34 European medical and research societies across Europe, which generate, collect and share health data to advance clinical research, maintain registries, improve patient care, and support healthcare professionals and researchers. The healthcare and biomedical research sectors are currently burdened by numerous overlapping regulatory frameworks, and in certain cases such as for the GDPR also differential implementation. It is therefore key that legislative change considers the specificities of the health sector and supports a sustainable, inclusive and safe digital transition.

Summary of our position:

- Simplifications in the Digital Omnibus must not jeopardise current and future **patient privacy**, especially in healthcare, where protecting **sensitive data** is essential. We acknowledge that the reduced scope of personal data defined in the proposal (GDPR Article 4(1)) could be of benefit to ethical and legitimate health research and specifically bias detection and post-market surveillance of AI tools in clinical practice to prevent the realistic risk of discrimination. However, we remain concerned about legal clarity of the provisions, and unanticipated consequences, resulting in the possible singling out of certain patients or patient groups and of the broader potential for malicious use.
- Clarity should be provided upfront on the means and criteria to determine whether data resulting from pseudonymisation no longer constitutes **personal data** for certain entities, and include feedback from the healthcare sector.
- **Sector-specific guidance** for the application of GDPR for health research remains necessary, to contribute to a more uniform understanding and interpretation of the requirements and facilitate health data sharing.
- While supporting including a **definition of scientific research** under Art 4 (38), we call for further elaboration of the principles of scientific research.

¹ For more information see e.g.: [Digital Omnibus Regulation Proposal | Shaping Europe's digital future](#)

² For more information see e.g.: [Digital Omnibus on AI Regulation Proposal | Shaping Europe's digital future](#)



Biomedical Alliance in Europe

- Additional information on the practical application of Recital 33 (Omnibus) and Article 9.5 (GDPR) for **personal data processing for the development and operation of AI** is needed to ensure a harmonised implementation and sufficient safety standards in the health sector.
- Removing the **template for post-market monitoring plans** should not lead to different practices and insufficient safety standards, thereby putting patient safety at risk. As the performance of AI tools varies across subgroups and is known to degrade over time, certain groups may become disproportionately disadvantaged. It is therefore strictly necessary that this is systematically monitored through robust post-market surveillance.
- A clear division of **responsibilities and sufficient investment for promoting AI literacy** is key.
- Clear regulations are needed for **general-purpose AI systems** in healthcare to ensure safe integration into clinical practice.

Digital Omnibus

Changes to the General Data Protection Regulation (GDPR)

Even though the General Data Protection Regulation (GDPR) has applied since 2018, there are still differences in interpretation and implementation in the health research sector across countries, regions, health institutions, and even within departments of the same organisation. This fragmentation is perhaps greatest in health research as the provisions for scientific research (including but not limited to Art 89) create barriers to data use and sharing in healthcare and research, particularly considering that healthcare institutions often adopt a risk-averse approach. In some cases, they hesitate to share data for research or innovation, or are reluctant to approve data-driven research activities, fearing potential legal consequences. Nonetheless, these activities are often permissible under GDPR and could greatly benefit patients, but due to misinterpretation they sometimes do not take place. Sector specific guidance on the implementation of GDPR for health research would help to take away uncertainty, and facilitate a more harmonised interoperation across the EU. The European Health Data Space (EHDS) has provided a level of legal clarity on the processing and interoperability of electronic health data for scientific research, regulatory decision making and evidence-based policy making (secondary purposes). However, EU Member States may apply stricter measures for genetic data, molecular data, wellness data and data from biobanks. The EHDS itself only applies to electronic data shared through the EHDS framework, and excludes other forms of data such as paper-based or physical health data. We therefore believe pragmatic and authoritative guidance based on input from health science experts across all EU member states is necessary.

- **Provide sector-specific guidance** on the application of GDPR in health research, to contribute to a more harmonised implementation and interpretation of the requirements and facilitate health data sharing, particularly among academic researchers, hospitals and other healthcare providers. This guidance should take into account the views of patients, healthcare professionals and scientific researchers.



Biomedical Alliance in Europe

Definition of scientific research in the Digital Omnibus

In order to provide legal clarity, it is important that a comprehensive definition of scientific research is included in the legislative framework. We welcome the Commission's proposed addition to GDPR article 4 (33) which proposes a definition for scientific research. However, some changes are necessary to ensure that the principles of scientific research are well defined and clear and match the reality in the sector.

- Taking into account the opinion of the European Data Protection Board and the European Data Protection Supervisor³, we believe that the definition of scientific research should be further clarified under the proposed article 4 (38):
Scientific research should be conducted following a methodological and systematic approach of the relevant scientific research field based on accepted scientific principles. In addition, scientific research should be conducted in an autonomous and independent manner and lead to verifiable and transparent results. 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.

Data use for AI development

Health data are increasingly used to develop AI models that improve patient care and advance medical research. AI is helping to analyse clinical data (including diagnostic data), identify patterns, predict disease progression, and personalise treatment plans, across the health sector and particularly in fields like oncology, radiology, genomics, radiation oncology, and pathology. However, due to the sensitive nature of health data it is essential that sufficient privacy standards are in place for the use of such data in the development and operation of AI.

Under the proposed changes to **GDPR Article 88c**, personal data processing for the development and operation of AI would be allowed under legitimate interest, unless national laws require consent. However, the wording of **Article 9**, which restricts the use of special categories of data (including health data), may leave room for uncertainty. The proposed change in **Article 9.2K** permits health data processing for AI development, but the wording in **Recital 33** (Omnibus) and **Article 9.5** (GDPR) demand safeguards to prevent the unauthorised collection or processing of sensitive personal data. The wording of these provisions leaves room for differential implementation, e.g. recital 33 (Omnibus) mentions that 'Special categories of personal data may residually exist in the training, testing or validation data sets or be retained in the AI system..' and it needs to be clarified how this would be applied in practice. To prevent misuse, appropriate enforcement measures, including fines, should apply to responsible parties.

- **Clarify the practical application of Recital 33 (Omnibus) and Article 9.5 (GDPR) for personal data processing for the development and operation of AI** to ensure a

³ See: EDPB-EDPS Joint opinion 2/2026 on the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus) | European Data Protection Board:
https://www.edpb.europa.eu/our-work-tools/our-documents/edpb-edps-joint-opinion/edpb-edps-joint-opinion-22026-proposal_en



Biomedical Alliance in Europe

harmonised implementation and sufficient safety standards in the health sector.
Ensure transparency on what data is used for the development and operation of AI.

Changes to the definition of Personal data

Health data can provide a wealth of information that can benefit research, but protecting personal data in healthcare is essential to maintaining patient trust, privacy and prevent potential abuse. Health data are highly sensitive, and any misuse or unauthorised access can have serious consequences, undermining the confidence patients need to share their information. Robust data protection enables patients to share their medical details with confidence, which is critical for accurate diagnosis, treatment, and research.

Under the amendment to **GDPR Article 4(1)**, information is no longer considered personal if it is shared in a pseudonymised format and the receiving entity cannot re-identify the individual using ‘means reasonably likely to be used’ by that entity. The proposal also states that “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”. This change follows a recent European Court of Justice ruling (EDPS v SRB ruling), and while it could facilitate the sharing of pseudonymised data for health research, it also may lead to a higher risk of abuse, particularly for actors who do not operate under the same ethical and regulatory checks and balances and principles that take place in scientific research. Especially, combining pseudonymised data with publicly accessible or diverse datasets increases the risk of re-identification. For instance, a rich dataset containing medical information alongside a fingerprint could allow for complete unravelling of an individual's identity. Special attention with stricter access requirements is needed when creating large, diverse datasets.

We believe the proposed changes leave room for differential application and thus the healthcare sector faces the risk of inconsistent implementation. As the proposed changes are not fully consistent with EDPS v SRB ruling, or with other CJEU caselaw, we are concerned this will not provide the legal clarity it intends, and could actually add to increased confusion in health sector implementation.

To ensure healthcare data is shared responsibly while enabling innovation, clear guidelines are needed to define how this term will be assessed and applied consistently across the healthcare sector, including contexts where clinical and diagnostic datasets are reused for research and quality assurance purposes. In ‘Article 41a (1) the Commission is giving the possibility to develop implementing acts to specify means and criteria to determine whether data resulting from pseudonymisation no longer constitutes personal data for certain entities. This seems a considerable mandate for an implementing act, with potential for significant interpretive possibilities, which would essentially define the scope of personal data. We would like to recommend that these means and criteria are clarified already during the co-decision process, and involve public feedback, including from patients, healthcare professionals and scientific researchers. We would also recommend that this provision should take into account the scope of scientific research defined in Art 4(38) (taking into account our suggested changes to this definition outlined above). Art 41a(3) then goes on to say the implementing act may then be “used as an element to demonstrate that data cannot lead to reidentification of the data subject” (41a(3)). These means and criteria could be used as the legislative test on which data are



Biomedical Alliance in Europe

considered pseudonymised and by which entities. However, 41a(3) introduces legal unclarity by suggesting that these means and criteria may only be an element, alongside possible other considerations which are not clarified. This appears to leave a considerable amount of legal unclarity. Also, what is pseudo-anonymised now might be traceable in the future when more data become available, which posed a risk of easier re-identification.

- **Clarify the means and criteria** to determine whether data resulting from pseudonymisation no longer constitute personal data for certain entities in the proposal, with public consultation, including by patients, healthcare professionals and scientific researchers. The size and richness of datasets should also be considered to minimise the risk of re-identification, particularly in large or highly granular datasets.

Digital Omnibus on AI

AI in healthcare

As Artificial Intelligence becomes more integrated in clinical settings and health research, it brings new benefits but also responsibilities and risks for healthcare professionals, who must provide oversight and validate AI generated outcomes. This makes it crucial for AI frameworks to uphold privacy and guarantee the accuracy, inclusiveness, and quality of results, to ensure the safe use of AI tools aligns with the demands of clinical practice.

Post-market monitoring for AI systems

Once AI systems are deployed in healthcare settings, ongoing monitoring becomes essential to ensure their safety, reliability, and effectiveness and detect potential bias. Post-market monitoring allows for the early identification of any issues that may arise during real-world use, ensuring that systems continue to meet regulatory standards and provide safe outcomes for patients.

The removal of the Commission's empowerment to create a template for post-market monitoring plans, as outlined in **Article 72.3 (AI Act)**, is intended to offer more flexibility for providers of high-risk AI systems. However, guidance needs to be put in place to ensure that this simplification does not provide too much leeway leading to different practices across the sector. Sufficiently high standards of post-market surveillance and monitoring should be maintained to enable the evaluation of the safety and reliability of AI systems, particularly in healthcare settings where the risks of unreliable systems can affect diagnostic decision-making and patient safety.

- **Ensure clear and consistent guidance** for post-market monitoring of AI systems in healthcare to ensure homogeneous safety standards across the sector.

Addressing bias

It is essential that AI algorithms and systems that are used in healthcare are developed on the basis of complete and/or augmented datasets with a wide representation of patients and conditions, that take into account underlying factors such as social determinants of health. Bias in such systems may have serious consequences for healthcare and research, and may lead to misdiagnosis, propagation of subconscious preconceived notions, and inefficient treatment. While prevention is important, certain risks may only become visible once AI



Biomedical Alliance in Europe

systems are used at scale and over extended periods of deployment. Existing systems already show that safeguards are often insufficient to prevent the emergence or persistence of discriminatory effects. We must therefore be able to detect and correct bias post-deployment, otherwise undetected harms can occur and / or persist in real-world use. A lifecycle assessment approach is necessary to prevent, identify and correct bias both in a pre-market and post-market setting.

- **Bias detection is indispensable, both in high-risk and non-high risk AI medical devices.** Processing of special-category data pseudonymised data for bias detection should be permissible, with the necessary safeguards in place. Data processing should be subject to the “strictly necessary” threshold and appropriate safeguards (IMCO-LIBE amendment 8) and be consistent with the AI Act’s data-governance framework. An explicit legal basis under the GDPR (substantial public interest), combined with robust pseudonymisation, security measures and transparency, strengthens legal certainty and supports more uniform application across the EU.
- In practice, hospitals and auditors often work with **pseudonymised datasets that are useful for bias audits** but not re-identifiable by the recipient. In case of potential serious harm, controlled re-identification should be made possible to direct necessary clinical actions. Clear EU level guidance on when such data are sufficiently shielded for the recipient would enable low risk, high value audits consistently across Member States.

AI literacy

As AI technologies become more embedded in healthcare and clinicians are responsible for oversight, the need for enhancing AI literacy within the sector is increasing. Previously, under article 4 of the AI act, providers and deployers of AI systems were supposed to take measures to ensure a sufficient level of AI literacy. It was therefore the responsibility of AI providers and deployers to ensure that healthcare professionals had sufficient knowledge to safely and effectively use AI systems, to allow them to fulfil their responsibilities under the AI act. However, under the proposed amendment in the Omnibus to **Article 4 of the AI Act**, the wording is changed and the responsibility of ‘encouraging literacy’ is instead put on the Commission and Member States. More clarity needs to be provided on the roles and responsibilities of different actors, to ensure that there is sufficient support for training and enhancing AI literacy.

- **Provide clarity on the roles and responsibilities of different actors to ensure that there is sufficient support for training and enhancing AI literacy**, so healthcare professionals and researchers can effectively and safely integrate AI into clinical practice and research.

General-purpose AI in Healthcare

General-purpose AI (GPAI) models are becoming increasingly popular, and they are used on a widespread basis across different sectors. As they are not specifically intended to be used in healthcare, they do not automatically have to comply with Chapter III requirements of the AI Act



Biomedical Alliance in Europe

for high-risk AI systems. Nonetheless, patients and even healthcare professionals use them on an individual basis (including shadow use) to gain insights and assist in the diagnosis and treatment of different health conditions. It is therefore essential that the regulatory framework considers the risks of using such GPAI in a healthcare setting.

- **Provide specific rules and requirements for the use of General Purpose AI in healthcare**, accompanied with support for training, to mitigate the risks for patients' health.

Conclusion

BioMed Alliance supports the intention to streamline digital legislation through the Digital Omnibus Package, but the right balance must be found to uphold privacy protection while supporting research, quality control in clinical practice and innovation. Clear, sector-specific guidelines and transparent regulatory frameworks are essential for facilitating health data sharing and supporting the digital transformation of healthcare and research.