Digital Omnibus Consultation

MedTech Europe's response to the public consultation

MedTech Europe welcomes the opportunity to provide feedback on the Digital Simplification Package (Digital Omnibus) which represents a timely initiative to enhance regulatory coherence and support Europe's competitiveness. MedTech Europe represents the medical technology sector, whose members develop and deploy innovative medical devices, including connected devices, diagnostic software, and AI-enabled technologies, within a highly regulated framework designed to ensure patient safety, quality, and trust.

Digital medical technologies play an increasingly important role in improving healthcare outcomes by enabling earlier diagnosis, more personalised and preventative care, and better clinical decision-making. In this context, simplifying and aligning horizontal digital legislation is not only a matter of compliance. A coherent and fit-for-purpose digital regulatory framework is essential to ensure that innovation can be translated efficiently into safe and effective medical technologies that benefit patients and healthcare systems across Europe.

MedTech Europe supports the overarching objective of streamlining and aligning EU digital legislation and underlines the need for concrete actions to ensure that the Digital Omnibus delivers tangible improvements in legal clarity, operational certainty, and regulatory alignment in practice.

MedTech Europe
from diagnosis to cure

Table of content

Digital Omnibus on AI

The Digital Omnibus on AI Proposal represents an important and timely update to support the effective implementation of the AI Act. For the medical technology sector, the proposal offers an opportunity to address practical challenges arising from the interaction between AI-specific requirements and existing sectoral legislation, notably the Medical Devices Regulation (MDR)[1] and the *In Vitro* Diagnostic Medical Devices Regulation (IVDR)[2] in a context where implementation timelines are approaching and harmonised standards are still under development.

For manufacturers of AI-enabled medical technologies, legal clarity, regulatory coherence, and operational stability are essential to support innovation while safeguarding patient safety and maintaining trust. MedTech Europe therefore emphasises the importance of active stakeholder engagement to ensure that the Digital Omnibus on AI delivers proportionate and workable solutions that are aligned with the objectives of the AI Act and can be implemented effectively in practice.

Given the complexity of the EU digital regulatory landscape, the Digital Omnibus on AI has the potential to play a pivotal role in aligning AI-related obligations with existing medical device and digital legislation. By addressing identified implementation challenges, the proposal can help support Europe's leadership in digital health innovation while ensuring timely access to safe and effective medical technologies for patients.

1. Extension of the AI Act application date

Recommendation: The application of high-risk AI obligations should be postponed until two years after the system is formally declared ready, meaning that harmonised standards, notified body capacity and all required guidance have been finalised and made available to ensure effective implementation and notified body preparedness.

The medical technology sector faces significant challenges due to uneven readiness across notified bodies, delays in standards development, and unclear regulatory guidance. These issues disrupt investment planning, complicate resource allocation, and hinder the safe deployment of AI-enabled medical technologies. A predictable regulatory framework is essential to reduce compliance risks and maintain incentives for innovation.

The Digital Omnibus on AI takes an important step by delaying obligations for high-risk AI systems, acknowledging the difficulties faced by the medical technology sector. We welcome the "stop the clock" measure, which recognises the challenges that complicate long-term planning and innovation cycles for developers and manufacturers. According to the Commission proposal, the obligations in Chapter III, Sections 1, 2 and 3 will only apply once the Commission adopts a decision confirming that adequate compliance-support measures are available. Following such a decision, Annex III obligations would apply after six months, with a fallback date of 2 August 2027, and Annex I obligations after twelve months, with a fallback date of 2 August 2028.

[1] Medical Devices Regulation (EU) 2017/745
[2] *In Vitro* Diagnostic Medical Devices Regulation (EU) 2017/746

However, neither the current application date of 2 August 2027 nor the proposed extension to 2 August 2028 provides a realistic timeframe for the medical technology sector to comply with the AI Act alongside existing MDR and IVDR obligations. The industry, notified bodies, and national authorities are still in a transition phase, with many Member States yet to appoint Notifying Authorities and with competent authorities not fully established across the EU. These ongoing gaps reinforce the need for a longer transition period.

To ensure an orderly transition, the date of application should be postponed to two years after the system has been formally declared ready, including the completion of notified body capacity and required guidance. The readiness assessment should formally involve the Stakeholder Forum and AI Board and be based on clear evidence of sufficient notified body capacity and the availability of harmonised standards that are fit-for-purpose. These elements are critical to supporting compliance and fostering innovation in the medical technology sector, particularly for high-risk AI systems.

Finally, the six-month extension of the application date of Article 50(2) is welcomed. Building on this positive step, targeted adjustments could further improve its implementation. We recommend aligning Article 50(2) with the timelines proposed for high-risk AI obligations. As medical devices are not explicitly excluded from the scope, manufacturers face legal uncertainty and inconsistent interpretations. Moreover, with guidance and a Code of Practice not expected before mid-2026, the current August 2026 deadline appears unrealistic in practice.

Without sector-specific clarification, manufacturers may undertake unnecessary interpretation efforts, adjust processes prematurely, or implement measures that do not meaningfully contribute to patient safety. Accordingly, aligning the application of Article 50(2) with the recommended timelines for high-risk AI obligations is necessary to ensure coherent and feasible implementation.

2. Ensure a harmonised designation pathway for notified bodies

Recommendation: To achieve a harmonised designation pathway as envisaged in the Digital Omnibus on AI, policymakers should ensure a streamlined single-application procedure for dual designation of notified bodies under the AI Act and relevant sectoral legislation, including the MDR and IVDR.

Sufficient and predictable notified body capacity is essential to ensure timely market access for AI-enabled medical technologies. In the absence of a coordinated designation framework and aligned risk requirements, manufacturers face delays, bottlenecks, and duplicative conformity assessment procedures. These systemic challenges slow innovation, increase compliance complexity, and may ultimately delay patient access to safe and effective AI-enabled medical devices.

The Digital Omnibus on AI takes an important step by allowing notified bodies to submit a single application and undergo a unified assessment procedure for designation under both the AI Act and the Union harmonisation legislation listed in Annex I, including the MDR and IVDR. This approach can help reduce unnecessary duplication and build on existing designation processes under sector-specific legislation. However, because formal designation under the AI Act and under sectoral legislation continues to be governed by separate legal acts, notified bodies must still meet additional requirements and develop specific expertise related to AI risk management, data governance, human oversight, and lifecycle management. Developing and maintaining this level of specialised expertise may prove challenging, given the limited availability of highly qualified AI professionals and the increasing demand for such expertise across multiple sectors. This structural capacity constraint risks placing additional pressure on notified bodies, potentially affecting the timely expansion of designation and the effective implementation of AI-related conformity assessment obligations.

Without a clearly harmonised and efficient designation pathway, there is a risk that notified body capacity will remain constrained, leading to continued uncertainty and delays in the conformity assessment of AI-enabled medical technologies. A streamlined and predictable designation framework is therefore essential to support effective implementation of the AI Act, strengthen notified body preparedness, and ensure timely patient access to innovative medical technologies.

To fully realise this objective, policymakers should move medical technologies from Annex I Section A to Section B of the AI Act. This shift would ensure that AI-related obligations for medical devices are applied within the MDR/IVDR framework rather than through parallel designation procedures. AI-enabled medical technologies would still remain fully subject to the AI Act's requirements, including AI risk management, data governance, transparency and human oversight, but these obligations would be implemented coherently through the existing sectoral pathway. This approach reduces duplication of obligations and addresses the incoherence currently observed in the interaction between the AI Act and sector-specific frameworks, while also supporting notified body capacity and ensuring patients can access safe and effective AI-enabled medical technologies without unnecessary regulatory delays.

3. Align AI Act definitions with other sectoral legislation

Recommendation: The definition of "substantial modification" under the AI Act should be clearly aligned with the concepts of "substantial change" and "significant change" as established under the MDR/IVDR, and their associated guidance. Additional clarification is also required regarding the AI Act's use of the term ''safety component'' which does not correspond to any established concept under MDR/IVDR.

The AI Act introduces both "substantial modification," and ''safety component'' as decisive concepts for determining when an AI system is considered high-risk and when notified body involvement is required. However, neither term aligns with existing MDR/IVDR definitions and associated guidance. This misalignment in definitions creates regulatory uncertainty for manufacturers of AI-enabled medical technologies, particularly in cases involving software updates, algorithmic improvements, or adaptive learning cycles.

While MDR/IVDR do not contain a statutory definition of 'significant change,' long-standing Medical Device Coordination Group (MDCG) guidance provides the accepted EU framework for determining when device modifications require notified body involvement. The AI Act's concept of 'substantial modification' should explicitly align with this established framework to avoid the creation of parallel, inconsistent change-control regimes.

Clarification is therefore required not only on the concept of "substantial modification" but also across several obligations in Section 3 of the AI Act, which rely on vague, open-ended legal terms requiring further interpretation to ensure consistent and predictable application. For medium- and long-term projects, early guidance (through FAQs, delegated acts, or other interpretative documents) is preferable in comparison to reliance on future case law, as delayed clarity risks locking organisations into design choices, system architectures, or training-data decisions that may later prove difficult to reverse.

Without harmonised definitions and timely guidance, manufacturers may face inconsistent interpretations, unnecessary re-certification demands, fragmented notified body decisions, and slowed innovation. To avoid duplication and ensure predictable management of adaptive AI within existing medical device frameworks, definitions such as "substantial modification" and "safety component" should be aligned with MDR/IVDR

terminology and supported by coordinated guidance developed with sectoral expert groups, including the MDCG.

4. Clarify that investigational devices and performance study devices are not considered "placed on the market" under the AI Act

Recommendation: Investigational medical devices under the MDR and devices used in performance studies under the IVDR should be explicitly excluded from being considered "placed on the market" or "put into service" for the purposes of the AI Act.

The AI Act does not explicitly exempt investigational devices or devices used in performance studies from being considered "placed on the market" or "put into service," despite these activities being clearly regulated and restricted under the MDR and IVDR. This omission creates legal uncertainty. AI-enabled medical devices undergoing clinical investigations or performance studies are used in strictly controlled settings to generate the evidence required to demonstrate safety and performance. They cannot bear the CE marking prior to the completion of such studies and are not commercially available. Nevertheless, they could fall within the full scope of AI Act obligations.

While Real World Testing (RWT) provisions offer an important pathway for pre-market evaluation, they do not replace the need for an explicit exemption for investigational and performance-study devices. These devices remain governed by MDR/IVDR provisions, and any RWT extension for Annex I products must be aligned accordingly to avoid double application of AI Act and MDR/IVDR obligations.

The Digital Omnibus proposal introduces improvements by allowing medical devices to be tested under real-world conditions and thus provides a pathway for clinical evaluation. However, this does not fully resolve the underlying legal ambiguity. In practice, there remain differing interpretations as to whether investigational devices and performance study devices fall within the AI Act's concepts of placing on the market or putting into service.

MDCG guidance has helped address this misalignment in practice, however the absence of explicit legal clarity remains problematic. Uncertainty at the pre-market stage risks complicating evidence generation, increasing administrative burden, and discouraging clinical research involving AI-enabled medical technologies. Although this proposal introduces improvements by expanding real-world testing provisions and committing them to further guidance, an explicit exemption is still needed to ensure that pre-market research and clinical investigations under the MDR and IVDR are not hindered. Clear alignment would foster innovation, uphold high standards of patient safety, and ensure that clinical evidence generation for AI-enabled medical devices proceeds efficiently and predictably. To achieve this, sector-specific expert groups (such as the MDCG) should be closely involved in developing joint implementation guidance that promotes coherence, prevents duplication, and supports agile innovation in AI-driven medical technologies.

5. Ensure alignment between AI Act risk-management requirements and existing MDR/IVDR frameworks

Recommendation: Harmonised standards supporting the AI Act's risk-management requirements should be developed in close coordination with existing MDR and IVDR risk-management standards, and compliance with established sectoral risk-management frameworks should be recognised as satisfying corresponding AI Act obligations where appropriate.

Manufacturers of medical technologies are already subject to comprehensive, lifecycle-based risk-management obligations under the MDR and IVDR, supported by well-established standards such as ISO 14971 and extensive sectoral guidance. The introduction of additional horizontal risk-management requirements under the AI Act creates a risk of overlap, duplication and divergence, particularly if forthcoming AI harmonised standards (to be developed by CEN-CENELEC) are developed without sufficient alignment with existing sector-specific frameworks.

Although the Digital Omnibus on AI proposal signals an intention to support coherence by requiring AI Act obligations to be taken into account in the adoption of delegated or implementing acts under other EU legislation, this does not yet provide sufficient clarity to avoid overlapping or conflicting risk-management requirements in practice. Without explicit alignment, manufacturers may face parallel compliance processes, increased complexity, and uncertainty in conformity assessment, potentially delaying market access for AI-enabled medical technologies. Coordinated standardisation efforts and clear recognition of established sectoral risk-management systems would support regulatory predictability, reduce unnecessary duplication, and ensure that patient safety and innovation are both effectively safeguarded.

6. Ensure proportionate and GDPR-aligned safeguards under the proposed Article 4a AI Act

Recommendation: The proposed Article 4a's safeguards for bias mitigation processing should remain proportionate, risk-based, and aligned with the General Data Protection Regulation (GDPR)[3]'s existing framework, avoiding duplication or prescriptive requirements that undermine established compliance structures.

MedTech Europe strongly supports the introduction of Article 4a under the AI Act, which enables the use of special categories of personal data for the purpose of detecting and correcting bias in AI systems. At the same time, some adjustments are necessary to ensure that the measure remains proportionate, risk-based, and fully aligned with the GDPR.

As drafted, Article 4a(1)(a-f) sets out a list of safeguards that must be implemented before processing such data. While safeguards are essential, several of the proposed requirements go beyond those established under Article 9 GDPR and other GDPR provisions, despite the fact that the GDPR already provides a comprehensive, risk-based framework for processing special categories of personal data. Introducing parallel or stricter safeguards risks creating inconsistencies, duplicative obligations, and unintended divergences between GDPR and the AI Act framework.

Such inconsistencies are illustrated in particular by the following provisions:

- **Article 4a(1)(b)** requires *state-of-the-art security and privacy-preserving measures*. Under the GDPR, the appropriateness of security measures must be assessed in the light of nature, scope, context and purposes of processing, as well as the likelihood and severity of risks to individuals, not on the basis of a blanket *state-of-the-art* standard.
- **Article 4a(1)(d)** prohibits access to the special categories of personal data for third parties. However, companies should be allowed to work with processors and subprocessors, as long as this is done in compliance with the GDPR.

[3] General Data Protection Regulation (EU) 2016/679

- **Article 4a(1)(f)** requires companies to include in the GDPR records of processing activities the reasoning as to why processing of special categories of personal data was necessary to detect and correct biases. Under the GDPR, the register of processing activities (RoPA) required by Article 30 is intended to be a factual inventory of processing operations, documenting who processes what categories of personal data, for what purposes, with which safeguards, and not as a vehicle for normative justification or legal reasoning. Expanding RoPA to demand detailed justification for the necessity of special category data would effectively convert it into a quasi-impact assessment tool, conflating distinct compliance instruments (documentation under Article 30, necessity/proportionality under Article 9, and risk-based evaluation under Article 35). This conflation undermines the structural clarity GDPR deliberately establishes, duplicates analysis already required in Data Protection Impact Assessments (DPIAs), and risks administrative overload, inconsistent documentation and blurred compliance responsibilities.

To avoid fragmentation and maintain internal coherence between the GDPR and the AI Act, Article 4a should therefore be refined to ensure that required safeguards build on the GDPR's existing, well-established principles rather than introducing new or more prescriptive criteria that disrupt compliance structures already widely implemented across the EU.

Digital Omnibus on the Data Acquis

Regarding the Digital Omnibus on the data acquis proposal, MedTech Europe welcomes the inclusion of targeted adjustments to the GDPR as an important step toward greater coherence in the EU digital framework. The medical technology sector supports efforts to uphold robust data protection while enabling responsible, innovation-driven use of health data in a way that maintains trust and safeguards individuals' rights.

At the same time, persistent challenges remain due to fragmented interpretations, overlapping frameworks, and inconsistent terminology across existing data legislation. For a highly regulated sector such as healthcare, genuine simplification requires a regulatory framework that is coherent, predictable, and fit-for-purpose, including for vertically regulated sectors.

MedTech Europe therefore underlines that, to deliver meaningful simplification, the Digital Omnibus on the data acquis must go beyond incremental adjustments. A proportionate and thoughtful approach is needed that fully takes into account the specific characteristics of health data, the regulatory environment in which medical technologies operate, and the need to safeguard patient interests, including patient safety.

1. Ensure a more practical and context-based definition of personal data

Recommendation: The proposed amendments to the definition of personal data are critically important to enhance legal certainty. These amendments should be complemented by high-level, non-prescriptive guidance to ensure harmonised and practical application of that definition.

MedTech Europe welcomes the European Commission's proposal to revise the definition of *personal data* in Article 4(1) of the GDPR to reflect established Court of Justice of the European Union (CJEU) case law.[4] In line with CJEU case law, we advocate for an explicit endorsement of the *relative approach* (or *whose hands* approach), under which identifiability is assessed in relation to the means reasonably likely to be used by the specific entity processing the data. This principle is also applied by other data protection authorities outside the EU, such as the UK Information Commissioner's Office (ICO) in its guidance on anonymisation and pseudonymisation,[5] and will now be embedded in EU law to ensure greater legal certainty.

Although this revision strengthens legal certainty, we also recognise that it may lead to different interpretations among data protection authorities across the EU. Clarifying when pseudonymised data ceases to be personal data is essential to ensure consistent interpretation. However, implementing acts, as the proposed Article 41a GDPR suggests, that attempt to define technical means and criteria too prescriptively may fail to accommodate diverse use cases. Flexibility is essential to allow controllers to apply risk-based assessments tailored to their operations.

To promote consistency and harmonisation while preserving necessary flexibility, we believe that implementing acts should offer high-level and non-prescriptive guidance, enabling controllers to justify and document their approach, while maintaining accountability. MedTech Europe remains available to support the development of such guidance to ensure a practical and effective framework for our sector.

[4] See cases C-413/23 P (EDPS v SRB) and C-582/14 (Breyer)
[5] Anonymisation | ICO

2. Support a broad and innovation-friendly definition of scientific research

Recommendation: Implementation should remain flexible, innovation friendly, and consistently interpreted across Member States, reflecting the realities of research and development in the medical technology sector.

Adding a definition of *scientific research* in Article 4(38) GDPR that includes innovation, technological development and demonstration is a positive step that supports secondary use of data for improving medical technologies and ultimately benefiting end users and patients. This change aligns with Recital 159 GDPR, which supports a broad interpretation of scientific research, and will help stimulate innovation, while being accompanied by the GDPR's solid safeguards.

While the new definition refers to contributions to *knowledge* and *wellbeing*, this should be understood as illustrative rather than limiting. The key criterion should be a broader positive impact on society, including examples such as product development and performance studies. To maximise societal benefit, it is important that the interpretation of the definition remains sufficiently flexible and does not introduce overly narrow criteria that could inadvertently exclude legitimate forms of industrial research. The revised wording, including the clarification that research *may also aim to further a commercial interest*, appropriately reflects the reality that innovation in medical technologies is often industry led while still serving public interest objectives.

Finally, additional high-level, nonprescriptive guidance is needed to promote consistency in interpreting terms across Member States. Such guidance could include practical examples relevant to the medical technology sector, while preserving the broad and futureproof approach intended by both the revised Article 4(38) and Recital 159. MedTech Europe remains available to support this work and help ensure that the framework is coherent, practical and effective for our industry.

3. Enable responsible AI-related processing of personal data

Recommendation: The proposed Articles 9(2)(k), 9(5) and 88c GDPR should remain proportionate, risk-based and fully aligned with the GDPR framework, avoiding additional prescriptive requirements and ensuring coherence with the terminology and safeguards of the AI Act.

MedTech Europe supports the introduction of a new derogation under Article 9(2)(k) GDPR for processing special categories of personal data in the context of AI systems and models, as this represents an important step toward enabling innovation in medical technologies. However, we are concerned that the conditions introduced in the new paragraph (5) go beyond the existing requirements of Article 9 GDPR and other GDPR provisions, despite the fact that the GDPR already provides a robust and comprehensive risk-based framework for processing special categories of personal data.

The new conditions in Article 9(5) may be challenging to implement in practice and risk hindering the use of special categories of personal data in training datasets - both their unintentional and intentional uses - even when such data is necessary to develop accurate and representative AI systems and models. This could create legal uncertainty for entities developing, training, or deploying AI systems and models in the EU, particularly in the healthcare sector. The organisational and technical measures referred to in Article 9(5) should remain proportionate and aligned with existing GDPR safeguards, avoiding additional or overly prescriptive requirements that would hinder practical application.

We also welcome the introduction of Article 88c GDPR, which clarifies that processing personal data for the development and operation of AI systems may rely on the legitimate interest basis under Article 6(1)(f) GDPR. This clarification is important to support innovation and is consistent with existing guidance issued by certain

authorities.[6] To ensure alignment with the terminology used in the EU AI Act,[7] we recommend replacing the term *operation* with *deployment*.

To further enhance clarity and ensure coherence with the GDPR's existing structure, we recommend that Article 88c be amended as follows:

- **Remove the exception referring to *national laws*,** as this risks undermining harmonisation and introducing fragmentation;
- **Avoid enumerating specific technical and organisational measures** in the legal text. The GDPR already sets out comprehensive requirements and principles that ensure appropriate safeguards for data subjects, and duplicating or prescribing them in Article 88c could lead to inconsistencies and reduce flexibility.

4. Ensure a proportionate and coherent EU framework for personal data breach and incident reporting

Recommendation: The requirements of Article 33 GDPR and the Single-Entry-Point should operate proportionately and coherently, supporting effective risk assessment without unnecessary burden.

MedTech Europe welcomes the proposed changes to Article 33 GDPR, including the alignment of notification thresholds to personal data breaches likely to result in a high risk to individuals and the introduction of a common EU notification template. These improvements will help reduce unnecessary notifications and lower administrative burden, especially for controllers operating under multiple regulatory frameworks.

To ensure coherence across EU legislation, notification timelines should be proportionate and workable. Excessively short timelines, such as the Network and Information Systems Directive 2 (NIS2)[8]'s 24-hour first notification, risk forcing organisations to file premature or incomplete reports while still managing active incidents. The GDPR's proposed deadline for notifying personal data breaches *without undue delay and, where feasible, not later than 96 hours* strikes a more balanced approach, enabling entities to prioritise mitigation and provide more accurate, meaningful information once an initial risk assessment has been conducted. The extension of the personal data breach notification deadline from 72 to 96 hours is a helpful step but may still be insufficient for carrying out a thorough and accurate risk assessment in complex environments such as healthcare.

We also welcome the move toward a Single-Entry Point for incident notifications, which is aligned with broader digital-legislation reforms aimed at reducing duplication and promoting efficient cross-regime reporting. Medical technology manufacturers are currently subject to multiple incident-reporting obligations under EU and national frameworks, often involving different authorities, formats, timelines, and languages. This fragmentation increases administrative burden and creates inefficiencies without improving security or patient protection.

A well-implemented Single-Entry Point, operated according to the "*report once, share many*" principle,[9] could significantly streamline compliance by allowing controllers to meet multiple reporting obligations simultaneously. However, further clarity is needed on the operational details, including how notifications will

[6] See, e.g., CNIL guidance on the "legitimate interest" basis to develop AI systems.
[7] Regulation (EU) 2024/1689 (Artificial Intelligence Act)
[8] Directive (EU) 2022/2555 (NIS 2 Directive)
[9] See Proposal for Digital Omnibus, page 8.

be routed to competent authorities and whether the European Union Agency for Cybersecurity (ENISA) will have sufficient capacity to coordinate both cybersecurity- and data-protection-related incidents.

5. Provide additional clarity on the definition of a 'significant incident' across different legislations

Recommendation: The Digital Omnibus proposal needs to introduce a harmonised threshold for determining when an incident qualifies as significant for reporting purposes.

A unified threshold would promote consistency across EU legislation while allowing flexibility to adapt to the objectives and scope of each regulatory instrument.

The NIS2 Directive's definition of a 'significant incident', which is marked by severe operational disruption or significant material damage, provides a suitable baseline. Aligning reporting thresholds with this definition would strengthen legal certainty, coherence, and proportionality across the regulatory framework.

6. Further adjustments needed for a coherent and workable GDPR framework

Recommendation: The GDPR amendments should be applied in a way that remains proportionate, coherent with existing safeguards, and consistently interpreted across Member States, with clear guidance in areas where divergent interpretation or disproportionate obligations may arise.

MedTech Europe provides the following comments on a number of additional GDPR amendments where further clarification or adjustment would improve coherence and practical implementation:

- **Article 9(2)** - We invite the Commission to further adjust the requirements under points (i) and (j), particularly the need for processing to be based on specific Member State or Union law. In practice, controllers often cannot identify explicit legal provisions enabling the envisaged processing, and safeguards are instead provided through soft-law guidance. Referring exclusively to the safeguards under Article 89 GDPR would resolve this issue and promote greater harmonisation.
- **Article 12(5)** - We support the clarification that controllers may refuse manifestly unfounded or excessive requests, as this helps prevent misuse of rights. Guidance with practical examples would help ensure consistent application across Member States.
- **Article 13(5)** - The proposed flexibility to provide information indirectly where direct communication would involve disproportionate effort is a welcome improvement, particularly in research contexts. For consistency, the same exception should apply under Article 14(5). Additional guidance on what constitutes *disproportionate effort* and acceptable transparency measures, such as public notices, would further support harmonised implementation.
- **Article 35** - Harmonising Data Protection Impact Assessment (DPIA) processes could simplify compliance and improve predictability. However, a mandatory EU-level template or methodology would be overly prescriptive, undermine flexibility, and create unnecessary rework for organisations with established DPIA frameworks. Any template should remain optional and serve as an accountability support tool rather than a binding obligation.
- **Article 88b** - Enabling automated and machine readable consent signals could enhance transparency and user control. However, requiring controllers and browser providers to implement new European standards may significantly increase compliance burden, especially for globally operating organisations. Broad stakeholder involvement in the standard setting process and phased implementation will be essential to ensure feasibility and avoid disproportionate impact.

7. Ensure an appropriate scope of Data Act data-access obligations for medical technologies

Recommendation: The data-access obligations set out in Chapter II of the Data Act[10] should be made voluntary for medical devices, electronic health record (EHR) systems, and related services.

Medical technologies operate within a highly regulated framework designed to ensure patient safety, clinical performance, and security. The Data Act's mandatory data-access obligations do not sufficiently reflect the sensitivity and contextual nature of health data generated by medical devices and EHR systems. Requiring access to raw, pre-processed, or uninterpreted data outside sector-specific safeguards risks misinterpretation, loss of clinical context, and unintended safety consequences in healthcare settings.

At the same time, the European Health Data Space (EHDS)[11] is establishing a dedicated, sector-specific framework for secure access, sharing, and interoperability of health data, applying to both EHR systems and interoperable medical devices. Introducing parallel mandatory data-access obligations under the Data Act risks duplication, inconsistency, and regulatory fragmentation. Making Data Act data-access obligations voluntary for medical technologies would preserve flexibility, respect existing sectoral safeguards, and ensure that data sharing in healthcare is governed by frameworks specifically designed to protect patients and support safe clinical use.

8. Enhance safeguards to prevent data sharing that could compromise safety or performance

Recommendation: For products and services that remain in scope of the Data Act, the "security handbrake" should be strengthened to explicitly allow data holders to limit access where sharing raw or uninterpreted data could compromise patient safety, product performance, or security.

The Data Act includes a "security handbrake" provision designed to prevent serious adverse effects on the health, safety, or security of individuals. However, in the context of medical technologies, this mechanism is difficult to apply in practice, as demonstrating such risks often requires specialised sectoral expertise and clinical context. Raw or pre-processed data generated by medical devices may contain embedded assumptions or limitations that, if accessed or interpreted without appropriate safeguards, could lead to incorrect conclusions or unsafe use.

Without tailored protections, mandatory data sharing risks undermining the integrity and safe functioning of medical technologies. Strengthening the security handbrake to explicitly prioritise patient safety and device performance would provide legal clarity, reduce uncertainty for manufacturers, and ensure that data-sharing obligations do not inadvertently compromise clinical outcomes or trust in medical technologies.

9. Provide legal certainty by excluding legacy medical technologies from Data Act obligations

Recommendation: The definition of "placement on the market" under Article 2(22) of the Data Act should be clarified to explicitly exclude legacy medical devices, software, and related products developed or certified prior to the application of the Regulation.

---

[10] Regulation (EU) 2023/2854 (Data Act)
[11] Regulation (EU) 2025/327 (European Health Data Space)

Medical technologies often have long development and certification cycles, with products placed on the market years after initial design or approval. The current definition of "placement on the market" does not clearly exclude legacy products, creating a risk that devices developed under previous regulatory regimes could be retroactively subject to new Data Act obligations.

With this lack of clarity, manufacturers may face unintended consequences, such as the need to implement design changes to meet Data Act requirements, potentially triggering re-certification under the MDR and IVDR. Such outcomes would impose unnecessary regulatory burdens, disrupt market entry timelines, and divert resources away from innovation. Explicitly excluding legacy products would uphold legal certainty, support predictable investment planning, and ensure that patients continue to benefit from timely access to safe and effective medical technologies.

10. Ensure effective protection of trade secrets as grounds to withhold data access

Recommendation: The Data Act should provide more robust and practicable protections for trade secrets by recognising them as clear legal grounds to withhold data access where disclosure would risk unlawful use, loss of proprietary know-how, or safety concerns.

Current Data Act provisions allow data holders to refuse access to trade-secret-protected information only under narrow and highly evidentiary thresholds. Demonstrating a likelihood of "serious economic damage" on a case-by-case basis is difficult in practice and creates legal uncertainty, particularly in the absence of clear guidance. This exposes companies to increased risks of reverse engineering, misuse of proprietary information, and uneven international competition.

While the Digital Omnibus introduces additional safeguards relating to third-country risks, these measures do not fully address the structural challenges of protecting trade secrets under the Data Act. Insufficient protection of proprietary know-how may discourage investment in innovation and raise safety concerns if complex medical technologies are replicated or used outside regulated environments. Strengthening trade-secret protections would support innovation, legal certainty, and patient safety, while maintaining Europe's competitiveness in medical technologies.

Conclusion

The Digital Omnibus proposals on AI and the data acquis represent crucial opportunities to address the regulatory challenges facing the medical technology sector. By fostering legal clarity, regulatory coherence, and operational stability, these initiatives can enable innovation while safeguarding patient safety and trust. Their success will depend on delivering practical and proportionate solutions that account for the specific complexities of AI-enabled medical technologies and health data. MedTech Europe calls for active stakeholder engagement and a thoughtful, sector-specific approach to ensure that these proposals not only align with broader EU objectives but also support the timely delivery of safe, effective, and innovative medical technologies to patients across Europe.

MedTech Europe and our members look forward to contributing to a more coherent, simplified framework that supports efficient healthcare data access and sharing, safeguards patient interests, and enables the medical technology industry to continue advancing Europe's health and digital ambitions.

About MedTech Europe

MedTech Europe is the European trade association for the medical technology industry including diagnostics, medical devices and digital health. Our members are national, European and multinational companies as well as a network of national medical technology associations that research, develop, manufacture, distribute and supply health-related technologies, services and solutions.
www.medtecheurope.org.

For more information, please contact:
Alexander Olbrechts
Director Digital Health & Medtech Value
a.olbrechts@medtecheurope.org