Subject: The CED Feedback on the Proposed Digital Omnibus Amendments to GDPR

Introduction

The Council of European Dentists (CED), representing over 340,000 dentists across Europe, welcomes the European Commission's ambition to foster innovation through the "Digital Omnibus" package. However, the healthcare and dental profession is built on a foundation of unwavering patient confidentiality. The proposed shift toward a more contextual or 'subjective' definition of personal data, combined with new derogations for AI development, requires careful consideration. We are deeply concerned that these changes fundamentally alter how health data is protected, identified, and retained. Without a robust and objective framework, there is a clear risk that both health data directly collected in a healthcare setting and health inferences generated through AI systems will be subject to uneven levels of protection, potentially prioritizing technical feasibility over the fundamental right to patient privacy.

A more contextual assessment of identifiability lead to legal uncertainty, where the status of information depends on an entity's technical capabilities rather than the nature of the data itself. Health data is inherently sensitive, regardless of the controller's resources or capacity. Its protection should therefore remain objective and consistent.

The proposed changes open back doors for reclassifying personal data as non-personal. In addition to the obvious example of an entity claiming insufficient means to identify a person, an entity could also establish an intermediate entity of no identifiability means, whose sole purpose would be to acquire the data, render them non-personal (due to its zero identifiability means), and sell the data back to the interested entity, or process the data according to the original intentions.

The addition of the concept of "personal data for a person or entity" is highly problematic. This implies that data can change from personal to non-personal, and vice versa, as they are transmitted from one person, or entity, to another. The implementation of this concept cannot be easily regulated and controlled. Assume an entity of zero identifiability means obtains personal data, then sells the data to another entity (which it can freely do, as the data are not personal for this entity), but rebrands the data as "random data". The receiving entity can freely process and store such "random data", without any legal problems. This scenario highlights several legal uncertainties that the proposed changes may lead to.

The introduction of new derogations for AI systems regarding special categories of data raises questions about the long-term retention of patient information. There is a concern that the use of broad and vague criteria, such as the difficulty of data removal, could lead to health-related information becoming an indelible part of commercial algorithms. Such a framework might prioritize technical feasibility over individual rights, potentially

creating a gap where insights derived from AI operations remain without sufficient safeguards.

To prevent potential vulnerabilities such as discriminatory profiling, it is important that any information allowing for conclusions about an individual's health remains subject to a high and uniform level of protection, regardless of whether it is directly disclosed or inferred through technical means.

The use of legitimate interest for AI development could raise concerns about the consistent application of principles set out in the broader EU legal regulatory framework, particularly in relation to health data. In this context, careful consideration is needed to ensure that any changes do not negatively affect the broader framework established by the European Health Data Space. That framework seeks to enable scientific research in the health sector while preserving a high level of trust in the access to, sharing of, and protection afforded to special categories of health data, including electronic health records. The use of special categories of personal data in AI systems should remain consistent with this regulatory context, ensuring coherence with the wider EU legal framework governing health data use.

The CED therefore urges the European Commission and Parliament to ensure that the digital transition does not undermine the fundamental protections afforded to patient data. It is essential to maintain an objective definition of personal data, ensuring protection whenever identification is possible, and to adopt a consistent, technology-neutral approach so that health inferences do not fall into a less regulated framework.