06 Issue 2026

Legance

EU Data & Cybersecurity Law: New Frameworks for Health Data Research and NIS2 Compliance

Health data and scientific research: EDPB Guidelines paving the way for the European Health Data Space (1/4)

The use of personal data – and in particular **health data** – for scientific research purposes represents one of the most sensitive issues in the current evolution of EU data law. The **new Guidelines** adopted by the **European Data Protection Board** (the "**EDPB**") on the processing of personal data for scientific research purposes, currently under public consultation until 25 June 2026, go beyond mere interpretative clarification and contribute to defining the framework within which a broader circulation of data for scientific purposes may develop. The document — to which the Italian Data Protection Authority also contributed – responds to a long-standing need within the scientific community for practical and harmonized guidance, in an area where the GDPR leaves significant discretion to Member States, resulting in fragmented applications.

Health data and scientific research: EDPB Guidelines paving the way for the European Health Data Space (2/4)

A key aspect of the Guidelines concerns the definition of **"scientific research"**, the EDPB identifies a set of **indicative criteria** – including a **methodical and systematic approach**, **adherence to ethical standards**, **transparency**, and **contribution to the advancement of knowledge** – to assess whether a given activity qualifies as such. Where these criteria are not met, it is for the controller to demonstrate that the processing falls within the relevant notion under the GDPR.

From an operational perspective, the Guidelines confirm that the further use of personal data for scientific research is, in principle, presumed to be compatible with the original purposes of collection, without requiring a new compatibility test, provided that an appropriate legal basis supports the further processing.

Health data and scientific research: EDPB Guidelines paving the way for the European Health Data Space (3/4)

The EDPB also acknowledges the possibility of relying on "**broad consent**" where research purposes cannot be fully specified at the time of data collection. This approach may be complemented by **dynamic consent models**, which allow data subjects to express more granular and evolving choices over time. However, the Guidelines emphasize that such models must be accompanied by **compliance with ethical standards** and the **implementation of additional safeguards**.

The Guidelines also address the particularly sensitive issue of data subject rights, clarifying that rights such as erasure and objection may be subject to limitations where their exercise would render impossible or seriously impair the achievement of research objectives. This requires a **case-by-case balancing** and reflects the specific regime applicable to scientific research under the GDPR.

Health data and scientific research: EDPB Guidelines paving the way for the European Health Data Space (4/4)

The Guidelines also highlight two further key dimensions: on the one hand, the need for a **clear allocation of responsibilities** among the various actors involved in research activities – including universities, public bodies, healthcare institutions and technology partners – with proper qualification of their roles as controller, joint controller or processor; on the other hand, the **central importance of technical and organizational measures**, such as anonymization and pseudonymization, as well as additional safeguards including secure processing environments, independent ethical oversight and restrictions on further use of the data.

NIS2 service categorization: structuring cybersecurity governance through risk (1/4)

The categorization of activities and services introduced under the NIS2 framework represents one of the most significant shifts in the regulatory approach to cybersecurity governance. **Determination No. 155238/2026** adopted by the National Authority for Cybersecurity (the "**ACN**") provides the first concrete implementation of Article 30 of Legislative Decree No. 138/2024, defining the criteria, process and models that NIS entities must follow.

While formally presented as a reporting requirement, the categorization exercise goes beyond a purely administrative obligation. It introduces a structured methodology through which **organizations** are required to **represent their activities and services in terms of their relevance and impact from a cybersecurity perspective**, laying the groundwork for a risk-based governance model.

NIS2 service categorization: structuring cybersecurity governance through risk (2/4)

From 2026 onwards, NIS entities will be required, **between 1 May and 30 June**, to submit via the ACN digital platform a comprehensive and categorized list of all activities performed and services provided, systematically organized within a predefined framework and assigned a corresponding category of relevance.
The model developed by the ACN is based on **ten macro-areas**, each **defined by a specific scope** and **associated with a pre-assigned level of impact**, ranging from minimum to high. Central to the model is the concept of **category of relevance**, understood as the measure of the impact that a potential disruption or compromise of a given activity or service may have on the organization’s ability to perform its NIS-related functions and intended to provide a common reference for calibrating cybersecurity measures proportionately.

NIS2 service categorization: structuring cybersecurity governance through risk (3/4)

Although the model provides pre-assigned relevance levels, organizations may depart from them on the basis of their own assessment, provided that such choices are adequately justified and documented. This interplay between predefined structure and organizational discretion reflects a broader regulatory approach combining harmonization with accountability.

By classifying activities and services according to their relevance, organizations are expected to apply security requirements commensurate with the potential impact of a compromise, enabling a more targeted and efficient use of resources. The Determination also ensures coordination with other frameworks, including those applicable to public sector data classification and to the national cyber perimeter, confirming a systemic approach aimed at building an integrated model of cybersecurity governance.

NIS2 service categorization: structuring cybersecurity governance through risk (4/4)

Overall, the introduction of service categorization reflects a shift from a system-centric to an activity-based perspective on cybersecurity. The upcoming implementation phase marks a key step in the transition towards a more structured and **risk-oriented approach**, where the **ability to map, assess and justify organizational activities** will play a central role in ensuring both regulatory compliance and operational resilience.

Alert Data Law *Alert* Data Law *Alert* Data Law *Alert*

For further information, please contact:

Andrea Fedi
afedi@legance.it

Lucio Scudiero
lscudiero@legance.it