Getting Data Protection Right in the Digital Omnibus

The Digital Omnibus Package is a necessary and welcomed proposal to ensure the General Data Protection Regulation (GDPR) supports Europe's digital transformation without weakening protections. The Commission's clarifications on personal data, AI training, automated decision making, breach notifications and terminal equipment data rightly improve legal certainty and enable innovation that benefits consumers. To make the package truly effective, targeted fixes are now essential.

Key elements of the proposal supported by the European insurance and reinsurance sector

✓ Clarification of solely automated decision making

Why: The proposal successfully clarifies when providers can rely on the contractual exception under Art. 22. This exception has frequently been interpreted restrictively or inconsistently by national data protection authorities, making it difficult to rely on.

✓ Legal basis for AI training, including with sensitive data

Why: The proposed new Article 88c and Article 9(2)(k) introduce much needed clarity on the use of legitimate interest for AI training with sensitive data, subject to robust safeguards. Enabling lawful AI use can improve service efficiency, for example by accelerating claims handling and allowing human experts to focus on complex cases.

Recommendation: The reference to an "unconditional" right to object in Article 88c(2) should be deleted as unconditional objections would be technically unworkable in the context of trained AI models. Similarly, the obligation under proposed Article 9(5) should be clarified. As currently drafted, the provision appears to require the unconditional avoidance of processing sensitive data during AI training and operation. To ensure a proportionate and operationally feasible framework, we recommend clarifying that sensitive data processing should be avoided as far as reasonably possible.

✓ Clarification of the concept of personal data

Why: The new definition provides more clarity by confirming that information is not personal data for an entity that has no reasonably likely means of identification. It moves away from an "absolute" interpretation of personal data, restoring legal certainty and enabling wider use of pseudonymisation and privacy enhancing techniques without lowering data protection standards.

✓ More effective data breach reporting

Why: Extending the breach notification deadline to 96 hours and limiting reporting to high risk incidents will improve the quality of notifications, reduce unnecessary reporting, and allow supervisory authorities to focus on genuinely serious incidents.

✓ Safeguards against abusive access requests

Why: Access requests are increasingly being used for purposes unrelated to data protection such as to support litigation strategy, to identify fraud-detection methods, or to place pressure on organisations through repetitive or excessive requests.

Recommendation: The Digital Omnibus clarifications on data access requests are a step towards the right direction, however they may not be enough, as the burden of proof still rests with the controller to demonstrate that a request is abusive. In practice, this is difficult to meet, as data subjects are not required to justify their requests and controllers often lack the evidence needed to establish abusive intent. An additional exemption should be considered where disclosure would seriously prejudice fraud investigations, litigation or the defence of legal claims, building on the "rights or freedoms of others" exception in Recital 63 GDPR.

✓ Access to terminal equipment data for requested services

Why: Innovative insurance offerings, such as telematics motor insurance policies, increasingly rely on the processing of data obtained directly from terminal equipment, such as connected cars. Under the existing e-Privacy framework, however, consent serves as the primary lawful basis for accessing and utilising data from terminal equipment. This reliance on consent as the sole basis can present challenges for both insurers and policyholders. For example, to be valid, consent must be "freely given". However, if consent is a necessary condition to enter an insurance contract, it can be interpreted as not "freely given". Introducing a legal basis for accessing data from terminal equipment for a service requested by the data subject is a positive and overdue update to the current e-Privacy Framework.

What is missing for insurers

✗ More legal certainty on special categories of data in (re)insurance

Why: The processing of health data is essential for underwriting, claims handling and reinsurance. However, there is currently no clear legal basis across the EU. In practice, insurers are often left to rely on consent, which is not a reliable or effective legal basis. Obtaining explicit consent can be burdensome, especially for beneficiaries, injured parties and in reinsurance, i.e. where no direct relationship with the data subject exists. In addition, the validity of consent in insurance contexts could be put into question because health data processing is indispensable for concluding, performing, and managing certain insurance contracts, including claims handling: since such processing is essential to provide insurance services, consent may be regarded as not "freely given". Diverging national interpretations further complicate cross-border cooperation, notably for reinsurers.

Recommendation: The current situation highlights the need for a clarification of an **appropriate legal basis** that could be relied upon at EU level for the **conclusion and performance of (re)insurance contracts including claims handling**. It would be appropriate to clarify that such processing may be covered by one of the derogations under Article 9 GDPR, such as the establishment of **legal claims (Article 9(2)(f))**.

April 2026

insurance europe
www.insuranceeurope.eu
Insurance Europe
Rue du Champ de Mars 23
B-1050 Brussels - Belgium