Capsulas

Breaches by the data processor may result in penalties for the sponsor of a clinical study

Spanish Data Protection Authority decisions of 24 and 25 February 2025

The protection of personal data in the context of clinical research has become increasingly important in recent years. The growing digitalisation of studies, the use of technological solutions, and the involvement of multiple stakeholders have increased both the complexity, and the risks associated with the processing of health data.

In this context, the Spanish Data Protection Authority (AEPD) has issued two sanctioning decisions. One decision was against a scientific society, and the other against a group of researchers. Both decisions followed a security breach suffered by a technology service provider engaged by those entities.

These decisions provide valuable practical guidance to help reduce the risk of penalties in similar circumstances.

Deficiencies identified by the AEPD

In both cases, the sanctioned organisations were acting as study sponsors, one for a patient registry and the other for an observational study. To manage the platform where the health data were stored, they had engaged a service provider acting as a data processor. The security breach involved unauthorised access to the processor's information systems. The AEPD found that the processor had failed to implement appropriate technical and organisational measures, such as data encryption, to safeguard the data.

Furthermore, in one of the cases, the AEPD concluded that there was an absence of clear contractual definition regarding the respective roles of data controller and data processor between the sponsor and the participating sites. This lack of clarity contributed to the inadequate handling of the incident. The AEPD also considered the response to the breach insufficient, as affected individuals were notified only through the website and the participating sites, with no direct communication to the study participants.

Proactive responsibility of the sponsor

In clinical research, it is essential to apply the principle of privacy by design. This requires a risk-based and accountability-driven approach, including the careful selection of service providers who can ensure the protection of participants' privacy throughout the study and beyond its conclusion.

In clinical trials and related studies, this proactive responsibility rests with the sponsor, who is regarded as the data controller. Under the General Data Protection Regulation (GDPR), the controller is the entity that determines the purposes and means of the data processing. However, organisations that fund a study may also be considered controllers, even if they are not the formal sponsors, such as in the case of Investigator-Initiated Studies, where access to personal data may occur in the context of the research.

Selection of the processor and oversight measures

The AEPD emphasises that Article 28 of the GDPR requires the data controller to engage only those processors who offer sufficient guarantees to implement appropriate technical and organisational measures that ensure compliance

with the Regulation. A processor's adherence to an approved code of conduct or certification scheme (such as a data protection seal or mark) may support the demonstration of such guarantees.

The same article obliges the controller to put in place appropriate contractual arrangements with the processor and to exercise effective oversight of the technical and organisational measures applied. This oversight also extends to any sub-processors engaged by the processor. Therefore, according to the AEPD, the controller cannot absolve itself of responsibility for the actions of its processors and must ensure both appropriate selection and ongoing supervision.

Further Lessons from the AEPD's Decisions

First, when a data controller appoints a processor, it is not sufficient to rely solely on standard contractual clauses or the processor's reputation. The controller has a duty of diligence, which includes verifying that the processor's measures are appropriate to the specific risks involved and that they are kept up to date through audits, compliance documentation, periodic reviews, checklists, risk reports, and other relevant means.

Second, it is crucial to maintain internal procedures for managing data breaches. These must be clearly communicated, regularly reviewed, and updated as necessary. Such procedures should specify the reporting channels for incidents, the notification obligations towards both the AEPD and affected individuals, and outline the roles, responsibilities, and designated personnel involved in handling the breach.

°°°°°