knowit

Comments on EDPB Guidelines 1/2026

Jannika Törnqvist
Senior Legal Counsel

Date
25.06.2026

Key Considerations in Clinical Trials

Knowit Cybersecurity & Law provides consultancy services in cybersecurity and IT law, including data protection, and has extensive experience in advising organizations conducting various types of clinical trials. We welcome the enhanced guidance provided in the EDPB Guidelines 1/2026 on the processing of personal data for scientific research purposes ("Guidelines"), recognizing that well-defined and consistent frameworks are essential to promote legal certainty, reduce regulatory fragmentation, and facilitate consistent application. We consider that certain aspects of the Guidelines would benefit from further clarification to avoid ambiguity in interpretation and practical implementation, and that there are compelling grounds for refining these elements in order to support a fair and predictable research environment.

A significant challenge arises in relation to the conduct of scientific research in the context of clinical trials, and particularly where such trials are carried out in third countries by organizations established within the EEA. In these circumstances, controllers may, for the reasons outlined below, be compelled to rely on consent as the legal basis for the processing of personal data. Nevertheless, such reliance may not be appropriate under the applicable legal framework, in particular where the conditions for valid consent cannot be fully satisfied, and may consequently place European organizations at a competitive disadvantage compared to actors operating under less restrictive regulatory regimes.

Against this background, Knowit Cybersecurity & Law has identified the following key issues that we believe warrant further clarification and consideration in the context of the Guidelines.

1. *Definition of vulnerability*

The approach set out in paragraph 37 in the Guidelines risks creating tension with existing guidance[1] on the definition of vulnerable segments of the population requiring special protection as it appears to narrow the concept of vulnerability in a manner that may not fully reflect the legislator's broader intention. We would like to draw attention to the fact that, in other relevant guidance, the concept of vulnerability is not limited to situations where a patient's capacity to provide consent is "severely affected" by a mental or physical medical condition. In this regard, a more restrictive interpretation in the present Guidelines may not fully reflect the broader understanding of vulnerability applied elsewhere, unless it is the explicit intention of EDPB to influence how vulnerability is to be interpreted in other contexts as well.

[1] For example, WP29 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, point 7 page 10.

However, should this reflect the intended approach, additional clarification would be warranted regarding the practical assessment of being severely affected by a mental or physical medical condition. In particular, determining whether a patient's condition severely affects their capacity to provide consent would, in many cases, require a degree of patient-specific knowledge. It remains unclear how such an assessment is expected to be carried out in practice, especially in research settings where personal data are frequently pseudonymized and where the entities conducting the clinical trials may not have access to, and should not have access to, identifiable patient information. We would also like to draw your attention to the fact that, as outlined in Example 7 of the Guidelines, consulting a non-profit organisation may not, in all cases, constitute a viable option, in particular where no such organisations exist in relation to rare disease conditions.

In this context, further guidance would be needed on the extent of the investigatory or due diligence obligations placed on controllers involved in clinical research. Specifically, it should also be clarified whether such actors may rely on assessments made by treating physicians or other healthcare professionals, or whether they are expected to undertake additional independent verification. Absent such clarification, there is a risk of creating legal uncertainty and imposing impracticable obligations on said controllers.

2. Consent as a legal basis in clinical trials

Owing to the inherent imbalance of power between the patient and the treating physician, as well as other entities involved in a clinical trial, consent may not be regarded as freely given. This concern is further reflected in paragraphs 36–38 of the Guidelines, which highlight the challenges associated with ensuring that consent is genuinely freely given in such contexts. In addition, the processing of personal data is often a precondition for participation in the clinical trial itself, rendering consent effectively conditional. In many instances, consent cannot be effectively withdrawn without undermining the integrity of the trial or conflicting with applicable legal retention obligations. Taken together, these factors give rise to significant concerns as to whether the threshold for valid consent under Articles 4(11) and 7 GDPR can be met in such circumstances.

As also previously noted by the EDPB, controllers are required to undertake a particularly thorough assessment of the specific circumstances of a clinical trial before relying on consent as a legal basis for the processing of personal data for research purposes.[2] It is our interpretation that consent should not, as a general rule, be relied upon as the legal basis for processing personal data in the context of clinical trials. Therefore, further guidance is needed on the availability and practical application of alternative legal bases, particularly in cross-border or third-country research contexts (as discussed below), in order to ensure legal certainty and consistent implementation.

[2] Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) (art. 70.1.b), paragraph 21.

3. *Legal basis for clinical trials conducted in third countries*

Clinical trials conducted within the EEA may rely on the legal basis of public interest pursuant to Article 6(3) and Article 9(2)(g), (i) and (j), based on Union or MS law to which the controller is subject. This approach is beneficial, as it may avoid the challenges associated with relying on consent, including issues relating to freely given and separate explicit consents for the processing of personal data, and provides a clearer and more robust legal framework, particularly in relation to vulnerable patient groups.

However, this approach is not available where equivalent studies are conducted in third countries by organizations established within the EEA. In these circumstances, controllers conducting clinical trials (whether acting as sponsors or otherwise) are, in practice, limited to explicit consent under Article 9(2)(a) as the legal basis for processing personal data, given that only Union or MS law is recognized for the purposes of invoking public interest. The challenges associated with relying on consent as the legal basis, particularly in the context of vulnerable groups of data subjects, have been outlined above.

The approach gives rise not only to legal uncertainty, but also to circumstances in which it may be precluded to identify or rely on an appropriate legal basis for the processing, thereby increasing operational complexity and contributing to inconsistencies in the conduct of global clinical research. It may further place European organizations at a competitive disadvantage compared to actors operating under different regulatory frameworks. Accordingly, further clarification, together with a more harmonized approach, is of particular importance.

Example

A controller established in the EEA sets up a clinical trial requiring the participation of severely or terminally ill patients, residing both within and outside the EEA. In such circumstances, the patients' scope for genuine choice may be inherently constrained, as they may have little realistic alternative but to participate in the clinical trial in order to access treatment.

Within the EEA, this issue is comparatively less problematic, as controllers may rely on public interest as the legal basis for the processing personal data. However, the situation differs significantly in third-country contexts where, in practice, the controller may have limited options for lawful processing under Article 9(2) GDPR beyond explicit consent. Nevertheless, the patients' health status raises serious doubts as to whether any consent provided for the processing of their personal data can truly be regarded as freely given and unconditional under the GDPR. Thus, in these global research settings, it may prove difficult and/or burdensome to reconcile the practical realities of clinical trials with the requirements of the GDPR in a lawful and consistent manner.

Concluding Remarks

In conclusion, Knowit Cybersecurity & Law recommends that the Guidelines be further clarified to ensure a consistent and workable approach to consent as a legal basis, vulnerability of data subjects, and other available lawful bases in clinical trials. Particular attention should be given to third-country clinical trials conducted by EEA-based organizations, where the current interpretation may create legal uncertainty and unintended practical consequences. Such clarification would support both strong data subject protection and the effective conduct of responsible scientific research, while also helping to safeguard the competitiveness of European research actors in a global context.