KAROLINSKA UNIVERSITY HOSPITAL

Ärende/D-nr: K 2026-5903

17 June 2026

Comments on EDPB Draft Guidelines 1/2026 on the Application of the GDPR to Scientific Research, with a focus on the attribution of responsibility (controller and processor)

The European Data Protection Board (EDPB) has published the draft Guidelines 1/2026 to provide long-awaited clarity on how the GDPR applies to scientific research. The draft is currently open for public consultation, with a deadline for stakeholder comments on June 25, 2026. On behalf of Karolinska University Hospital, Region Stockholm in Sweden (hereinafter "Karolinska"), this submission is hereby respectfully submitted to the European Data Protection Board (EDPB) in response to the public consultation on Draft Guidelines 1/2026 on the application of the GDPR to scientific research.

Karolinska University Hospital is one of the largest university hospitals in Europe and forms part of the regional public authority Region Stockholm. The hospital provides highly specialized healthcare, clinical research and education, with a mission to improve health and healthcare for present and future patients. Currently, over 1,800 clinical studies are ongoing at Karolinska.

The most debated research scenario: commissioned clinical research

The research scenarios in which questions about the allocation of roles most often arise are commissioned research projects, where one party has initiated, manages and funds the study, and another party (typically a hospital) is invited to participate and acts as the executing party. In clinical trials of medicinal products, the first party is referred to as the "sponsor" and the second party as the "trial site". For other types of studies than clinical trials, there are no legally defined terms, but the same terminology is often used in practice and will also be used in this submission for the sake of simplicity.

It is the role of the trial site that parties often disagree on – specifically whether the trial site acts as a controller or as a processor. Karolinska, like many others, applies the EDPB's method for allocating roles (see below) and, following that approach, reaches the conclusion that the trial site is also a controller in respect of its processing of personal data. The trial site's controllership may be separate for certain processing operations and joint for others (we do not elaborate on this point further here).

Other stakeholders refer to the example of "Clinical trials" in paragraph 68 of the EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR and argue that, where the investigator has not participated in drafting the protocol but has merely accepted a

protocol designed solely by the sponsor, the investigator should be regarded as a processor and the sponsor as the controller for the clinical trial.

The example reads as follows:

*"**Example: Clinical Trials***

A health care provider (the investigator) and a university (the sponsor) decide to launch together a clinical trial with the same purpose. They collaborate together to the drafting of the study protocol (i.e. purpose, methodology/design of the study, data to be collected, subject exclusion/inclusion criteria, database reuse (where relevant) etc.). They may be considered as joint controllers, for this clinical trial as they jointly determine and agree on the same purpose and the essential means of the processing. The collection of personal data from the medical record of the patient for the purpose of research is to be distinguished from the storage and use of the same data for the purpose of patient care, for which the health care provider remains the controller.

In the event that the investigator does not participate to the drafting of the protocol (he just accepts the protocol already elaborated by the sponsor), and the protocol is only designed by the sponsor, the investigator should be considered as a processor and the sponsor as the controller for this clinical trial."

When the EDPB's method is applied – in particular the elements of implicit legal competence and the determination of essential means – the outcome in commissioned clinical research projects is that a substantial part of the site's processing activities cannot be performed as processor tasks. Instead, the hospital has to be seen as an independent controller for those processing activities. This is especially the case where national law attributes to the hospital the power and responsibility to determine whether and under which conditions specific processing activities may take place. These implications, which are further developed below, are difficult to reconcile with an interpretation that the trial site would act as a processor, as stated in the example above.

EDPB's method for determining whether a party acts as a data controller or data processor

EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR provide a framework for allocating roles. In essence, the assessment is based on (i) explicit legal competence, (ii) implicit legal competence, (iii) actual influence over the purpose and (iv) determining essential means of the processing.

1. Explicict legal competence

A first element is whether a party is explicitly designated by law as a data controller. As an example, Section 6, Chapter 2 of the Swedish Patient Data Act (2008:355) designates the healthcare provider as controller for processing carried out in the provision of healthcare. When information obtained in the context of a research study is also relevant for the healthcare of the individual patient, it must be entered in the medical record. For this processing activity, the healthcare provider is designated by law as the controller.

2. Implicit legal competence

Where the law assigns a party a specific task or obligation that requires the collection and processing of personal data, that party will normally be regarded as the controller for the processing necessary to perform that task.

3. Actual influence over purpose

Where the law does not clearly designate a controller, the role is determined by who, in practice, decides why and how the personal data are processed and acts with a significant degree of independence. At this stage of the assessment, it becomes relevant to ask who has drafted the protocol and initiated the study.

4. Determining the essential means

A data controller must determine both the purposes and the essential means of the processing. It is not sufficient to determine the purpose alone. Some margin of discretion may be left to the processor, but only in relation to non-essential means. A party that determines the essential means of a processing operation can never be a data processor for that processing activity.

Examples of essential means are:

- which categories of individuals the data relate to
- which data must be processed in order to perform the task
- whether the processing is lawful
- whether the data will be disclosed and, if so, to which recipients
- how long the personal data will be stored.

A party that determines any of these essential means, is immediately excluded from acting as a data processor for that processing activity.

Request for clarification on “implicit legal competence” and “essential means” in clinical studies

Karolinska submits that the implications of implicit legal competence and determining the essential means are not fully brought out in the current draft of the Guidelines 1/2026. We believe it would be very valuable if this aspect could be addressed more explicitly, as we do not see it being dealt with at present. Clarification on this point would be of great practical help, since it lies at the core of many discussions in the context of clinical studies and contributes to delays in study start-up, among other issues.

The allocation of the roles as controller or processor needs to be carried out with regard to the individual processing activities. Here are examples of key activities in the context of clinical medical research that involve the site’s processing of personal data:

- Collecting and storing informed consent forms from study subjects
- Preparing and storing the code key (key to the pseudonymisation)
- Collecting retrospective patient data
- Collecting prospective patient data
- Recording in the medical record any prospective data collected that is relevant for patient care
- Entering study data into a case report form (CRF), typically in electronic format (eCRF)
- In the case of clinical trials of medicinal products, documenting and reporting safety data (AEs and SAEs) to the sponsor of the trial, in accordance with the relevant provisions of the Clinical Trials Regulation (CTR)
- Archiving the study data.

Implicit legal competence

As regards the processing of personal data that consists of safety reporting from the trial site to the sponsor in clinical trials of medicinal products, this is carried out on the basis of implicit legal competence under Article 41 of the CTR. Archiving in such trials is carried out pursuant to Article 58 of the CTR. In studies other than clinical trials of medicinal products, the hospital's archiving obligations instead follow from national legislation (the Swedish Archives Act and the Archives Ordinance). Since these legal acts designate the investigator/site as responsible for these tasks, this suggests that the site, by virtue of its implicit legal competence, is the controller for these specific processing activities. In addition, Article 47 of the CTR provides that the sponsor and the investigator shall ensure that the clinical trial is conducted in accordance with the protocol and with the principles of good clinical practice. In this context, "good clinical practice" essentially refers to the ICH GCP framework, which contains a detailed set of rules, including separate sections specifying the respective responsibilities of the investigator/site and of the sponsor.

Essential means

Hospitals work within a strict legal framework that gives them independent responsibility regarding the processing of their patient's personal data. For many of the processing activities a hospital performs within a clinical trial or other clinical study, the hospital cannot act purely on instructions from the sponsor as a processor would under Article 28 of the GDPR. In Sweden for example, hospitals are governed by strict patient confidentiality laws (the Swedish Access to Information and Secrecy Act (below "OSL") and the Patient Data Act).

There are several processing activities carried out within the framework of a clinical study where, due to national legislation, the hospital disposes of the essential means. In other words, the hospital determines whether the processing of personal data is lawful and whether, and under which conditions, the processing activity may take place and whether the sponsor may get access to the data. This is the case, for example, for the collection of data from patients participating in the study and the disclosure of such data to an external sponsor, who gains

access to the data through the hospital's entry of it into the electronic case report form (the eCRF). In short, when a member of the study staff enters data and clicks "enter" in the eCRF system, the site discloses pseudonymized patient data to the sponsor. This presupposes that the disclosure has been preceded by a confidentiality assessment under the Swedish patient confidentiality legislation, namely the OSL. Confidentiality applies to the information unless it is clear that the information can be disclosed without causing harm to the patient or to any of his or her close relatives (Chapter 25 Section 1 of the OSL). For prospective data, such an assessment cannot be carried out once and for all in advance, since the data do not yet exist at the start of the study. Instead, the confidentiality assessment must be performed successively, as and when each new item of data is collected and disclosed through the eCRF. It is therefore the site that determines whether and how the disclosure to the sponsor takes place.

Furthermore, disclosure of study data collected from patients presupposes that the circumstances are not such that the hospital has reason to believe that the receiving party (the sponsor) will process the data in breach of the GDPR. The hospital must therefore assess whether the sponsor has a legal basis for processing the personal data in accordance with Article 6 of the GDPR, as well as a legal basis for an exemption from the prohibition on processing special categories of personal data under Article 9 of the GDPR. If there is reason to believe that the recipient lacks a lawful basis under the GDPR for its processing, the data are subject to secrecy under the OSL, and the hospital may not make the data available to the sponsor (Chapter 21 Section 7 of the OSL).

Nor could the sponsor replace the site with, for example, a CRO for collecting or storing consent forms, since only the healthcare provider has access to the patients and may not disclose their identity to any third party. The same applies to the preparation and storage of the code key.

Because the hospital in this way controls the processing of personal data, it cannot act solely on the instructions of an external party. The hospital can therefore not be a data processor for these processing activities; it is a data controller.

Short summary

Karolinska submits that the concepts of "implicit legal competence" and "essential means" require further clarification in the EDPB's Guidelines 1/2026. Due to national legislation, hospitals often determine whether personal data may be processed at all, on what legal basis, under which conditions, and whether data may be disclosed to an external party such as a sponsor. In these situations, it is Karolinska's – and many other hospitals' – assessment that a hospital's position is comparable to, for example, the bank example in paragraph 40 of the EDPB Guidelines 07/2020 and the university example no. 22 in paragraph 137 (page 54) in the EDPB's current draft Guidelines 1/2026. In such cases, the hospital cannot act solely on the instructions of an external sponsor as a processor under Article 28 GDPR.

In the context of clinical trials, the hospital is also assigned a number of specific tasks and obligations that require the collection and processing of personal data, which indicates that, for these processing activities, the hospital acts as a controller.

Karolinska therefore considers that implicit legal competence and the hospital's control over essential means play a more decisive role in the allocation of responsibilities in clinical studies than the current draft appears to suggest. Moreover, given that the EDPB's Guidelines 07/2020 on the concepts of controller and processor in the GDPR include an example that contradicts the outcome of the method set out in the same Guidelines, Karolinska would very much welcome further clarification in the final version of Guidelines 1/2026 on how these elements should be taken into account when allocating roles in clinical trials and other clinical studies.

Yours Sincerely,

Annie Johansson

Legal Counsel
Legal Unit, Legal Department
Karolinska University Hospital
SE-171 76 Stockholm
Sweden