Centrale Commissie Mensgebonden Onderzoek

Consultation Response CCMO,
The Netherlands
dated 29 October 2026

Consultation Response of the Dutch Committee for Human Research (CCMO) regarding EDPB Guidelines 02/2026

The Dutch Committee for Human Research (CCMO) is responsible for reviewing medical research involving people in the Netherlands and ensuring the protection of research participants. In addition, pursuant to the Medical Research Involving Human Subjects Act (WMO), the CCMO supervises all recognised Medical Research Ethics Committees (MRECs) in the Netherlands and has the statutory authority to establish guidelines governing the review of such research. In this context, the CCMO assesses, among other things, the safeguards in place for the processing of personal data in accordance with the General Data Protection Regulation (GDPR).

The CCMO has reviewed the European Data Protection Board's *Guidelines 02/2026 on Anonymisation* and wishes to bring the following comments to your attention.

Subject: The assessability of anonymity in medical research involving human research participants

In general:

The CCMO is concerned about the practical applicability of the proposed guidelines on anonymity, particularly in the context of the review of medical research involving human subjects. The CCMO also raised this issue in its response to the public consultation on Guidelines 01/2026. Given the importance of this matter, the CCMO wishes to elaborate in this consultation on the specific challenges it anticipates in practice.

In clinical drug trials, research data are processed in pseudonymised form. The coding key that allows the data to be linked to individual participants is stored separately by the participating research centre. The sponsor therefore does not have access to this key.

Furthermore, under the applicable regulations, certain essential documents relating to clinical drug trials must be archived for a minimum of 25 years. The retention period and the precise scope of this obligation vary depending on the type of document and the applicable regulations. As a result, sponsors retain pseudonymised research data and other research documentation for extended periods of time.

In practice, sponsors, which are frequently established outside the European Economic Area (EEA), state that data from research initiated by them are anonymised upon completion of the study and subsequently used for further scientific research. They sometimes argue that the

sponsor does not have access to the coding key, as this is held by the participating research centre. However, the substantiation of the claimed anonymity and the measures taken to prevent re-identification are not always sufficiently transparent to the body responsible for reviewing the subsequent research.

More importantly, however, the fact that the coding key is stored separately does not rule out the possibility of identification by other means. Depending on the nature and level of detail of the data, the availability of additional information (such as DNA data) and the possibilities for data linkage, re-identification may remain possible. The availability of additional data held by other parties involved and developments in technical identification methods may also be relevant. The re-identification capabilities that AI technology may offer in the future further increase the risk that pseudonymised data can be traced back to the individuals from whom they originate. These developments even raise the question of whether data can still be considered anonymous in the long term.

Against this background, it is essential that the MREC reviewing the proposed use of such data for further scientific research is able to assess whether the classification of the data as anonymous is valid and adequately substantiated. The MREC must therefore be informed not only about the categories of data held by the sponsor, but also about any additional information to which the sponsor has access and any other re-identification possibilities that are reasonably relevant to assessing the status of the data (anonymous or otherwise).

A substantive assessment of an anonymity claim may require specialist knowledge of statistics, data science, information security and the technical design of the data processing. An MREC cannot automatically be expected to carry out this assessment entirely independently. The guidelines should therefore provide greater clarity on the substantiation that may be expected from a party claiming that data are anonymous, and on how reviewing bodies can, where necessary, obtain access to appropriate independent expertise.

This is essential because the consequences of an incorrect classification of data (for example, classifying data as anonymous when they are not) can be considerable. In particular, we wish to highlight the situation in which data are wrongly classified as anonymous: in that case, the legal protection afforded by the GDPR ceases to apply, whereas ensuring adequate protection of research participants should always remain the overriding priority.

More specifically

In its response to the public consultation on Guidelines 01/2026, the CCMO already requested that the EDPB:

- provide a clearer description of the conditions under which anonymisation is possible in medical research involving human research participants;
- explore the possibility of an independent certification system for the classification of data as anonymous within the meaning of the GDPR;

- clarify that a party claiming anonymity must be able to substantiate this classification through a documented assessment. Where relevant, this assessment should take into account any remaining identifying characteristics, possibilities for data linkage, available additional information and the means of identification that can reasonably be expected to be available.

In addition, the CCMO requests that the EDPB clarify the following points in the final guidelines.

1. Clarify the responsibilities of the party making the anonymity claim and how reviewing bodies, including MRECs, can obtain access to independent technical expertise where the assessment requires specialist knowledge.
2. Explicitly state that the absence of an identification key held by the party processing the data is not, in itself, decisive in determining whether data qualify as anonymous. Relevant additional information and identification possibilities available to other parties must also be taken into account, insofar as these are relevant under the applicable assessment framework.
3. Clarify the circumstances in which an earlier assessment must be reviewed, for example in the case of long-term data retention, a new purpose of use, new possibilities for data linkage or substantial changes in the available technical capabilities.

In summary: anonymity must not be based solely on a classification assigned to a dataset by the sponsor. Where this classification results in the GDPR no longer applying, it must be based on an adequately substantiated and verifiable assessment. The protection of research participants must not depend on an anonymity claim that the reviewing body concerned is unable to adequately scrutinise.