The following feedback on Guidelines 1/2026 is provided by data protection staff of Utrecht University, collected and presented by J.P. Folkers, Chief Privacy Officer of the university.

In paragraph 11, under iv., the criteria around autonomy and independence are rather strict and not realistic when considering the conditions set by research grants, especially the freedom that a research team is supposed to have in regard to publishing the results. Research grants often come with the obligation to publish, disqualifying the research activities as independent research in the current wording of the guidelines. This would seem undesirable given that the research would otherwise be classified as independent.

The current wording and distinction made in the paragraph 17 makes it seem that taking personal data gathered for scientific research and processing it for different scientific research would somehow not qualify it as further processing for scientific research, while selecting personal data that was collected for non-scientific research data and further processing it for scientific research would qualify it as such. This while legally, there would be no such distinction.

The suggestion in paragraph 38 that a single consent for clinical research that would serve both healthcare and scientific research goals conflicts with the requirements of freely given consent the same way as the example relating to the consent to research being a prerequisite to medical treatment. Asking for a *single* combined consent is not free of negative consequences here, since not participating in the research means you will receive no healthcare. The better practice is to ask for separate consent, which would also prevent problems when the single consent would be retracted for one of the purposes, taking the other purpose down with it.

The process of providing research data subject pseudonyms related to their personal data when transferring a pseudonymized dataset to be processed for scientific research by an independent controller, as described in paragraph 94, seems counterproductive and at odds with article 11 of the GDPR.

The receiving controller will have to consider the pseudonymized dataset as anonymous as they cannot reasonably identify the individuals in the dataset, thus falling outside the scope of the GDPR. This consideration has two logical conclusions, one where the GDPR would not be accounted for, and one where the GDPR has been fully accounted for, pretending as if the dataset were personal data. Both these situations lead to undesirable consequences.

The situation that the GDPR will not be accounted for will lead to situations where data subjects identify themselves, making the data processing suddenly fall under GDPR

while legal bases and justifications for processing special categories of personal data will not be in place. This will jeopardize the scientific research as the moment a data subject identifies itself with its identifier, the researcher will have to delete all personal data relating to that subject, as the personal data is being unlawfully processed.

One way to prevent this from the perspective of the researcher is to pretend the pseudonymized dataset contains personal data. This approach is feasible but has the practical implication that researchers will have to do the necessary paperwork to demonstrate compliance and have legal bases in place in case data subjects wish to exercise their rights, a problem they would not have had the provider of the dataset not informed the data subjects about their unique identifier.

This extra measure also seems unnecessary when additional checks are in place for processing for scientific research purposes, as stated in article 89 GDPR. Additionally, this approach will also require the allocation of scarce resources that could be attributed to conducting the research properly and anonymously.

The other way to prevent this from the perspective of the researcher is to pseudonymize the personal data upon receival, making it so that the data subject can no longer identify itself with the unique ID it received from the supplier of the personal data.

Lastly, to touch on article 11: the mechanism to process additional information, when this is not required, purely to facilitate the exercise of data subject rights under GDPR seems to conflict with article 11 (1) GDPR, where it is explicitly stated that controllers that do not need to identify data subjects to achieve their processing goals are not required to maintain, process or receive identifying information solely to comply with GDPR. Carrying out additional data processing solely to make it possible to identify data subjects in a situation where this is not necessary to achieve the goals of the controllers seems at odds with the article.

We hope that you will consider our feedback on the Guidelines.

Kind regards,

J.P. Folkers

Chief Privacy Officer

Utrecht University