Biomedical Research Center of the Slovak Academy of Sciences, public research institution
Comments on the draft EDPB Guidelines 1/2026 on processing of personal data for scientific research purposes

	PROVISION	ORIGINAL WORDING	SUGGESTED CHANGE	REASONING
1.	**cl. 2.1 (13)** *new*		**13.** For public universities, national academies of sciences, and accredited public research institutions, the presence of factors indicated in para. 11 shall be institutionally presumed. Such public entities shall not be required to compile ad hoc compliance files to demonstrate the scientific nature of individual internal projects, provided they operate under institutional ethical oversight.	The overall goal of research institutions is to conduct research that benefits society; the administrative burden shall not be disproportionately increased. Public funding, peer-review grant systems, and statutory research mandates already guarantee the scientific integrity of these bodies.
2.	**cl. 2.3 (15)**	**15.** Ancillary processing operations should have a clear scientific research objective, which must be assessed on a case-by-case basis in light of the factors listed at para. 11, in order for those processing operations to be considered motivated by scientific research purposes.	**15.** Preliminary ancillary operations, including data screening, curation, and feasibility assessments conducted internally within a public research institution, university, or national academy of sciences to determine the viability of a future project, are fundamentally exempt from the case-to-case verification of the six factors, provided the data remains within the institution's secured technical environment.	Requiring researchers to pass a complex regulatory gate before they can even look at internal data to formulate a hypothesis is structurally paralyzing. Feasibility testing is a core element of freedom of research and must be protected from administrative pre-clearance.
3.	**cl. 3.1.1 (22)**	**22.** In many cases controllers will be able to rely on the same legal basis, for example where a controller initially processed personal data on the basis of public or legitimate interest. It is, however, not always possible to rely on the same legal basis when further processing	**22.** Public research institutions, universities and national academies of sciences shall be explicitly permitted to retain and further process historical pseudonymized datasets originally collected via consent, relying on public interest (Article 6(1)(e)) or legitimate interest (Article 6(1)(f)) for long-term	Scientific data is a public good. Requiring the destruction or absolute anonymization (which often destroys data utility) of high-value bio-samples and medical registries simply because a grant cycle ended or because patients cannot be re-contacted decades later is

		personal data for scientific research purposes. This applies in particular if the initial legal basis for the primary processing is consent or a legal obligation.	preservation, replication, and secondary discovery, provided that identity keys are structurally segregated from the active research environment.	unreasonable. Technical pseudonymization plus ethical governance provides more than enough protection, allowing society to benefit from long-term data preservation.
4.	**cl. 4.1.2.1 (46)**	**46.** When controllers obtain broad consent, they should ensure that data subjects understand the consequence of their choice that their personal data will be processed in research projects within the area of scientific research that was communicated to them. Thereafter, when the purposes of processing for individual research projects (or stages thereof) become known and before the processing is initiated, the controller should consider if the processing of personal data in those projects will be undertaken inside the boundaries of the broad consent. When doing so, controllers should evaluate if the processing of personal data correlates with the reasonable expectations of the data subjects, in line with the principle of fairness and the autonomy of data subjects67. If possible, controllers should consult with groups representing the data subjects to get a better understanding of the data subjects' wishes and expectations. If a controller determines that the processing of personal data in an individual research project (or part thereof) would fall outside the scope of a	**46.** When controllers obtain broad consent, they should ensure that data subjects understand the consequence of their choice that their personal data will be processed in research projects within the area of scientific research that was communicated to them. Thereafter, when the purposes of processing for individual research projects (or stages thereof) become known and before the processing is initiated, the controller should consider whether the processing of personal data in those projects will be undertaken within the boundaries of the broad consent. Where a data subject has granted broad consent encompassing a specific area of research, the legal and fair boundaries of the processing are defined exclusively by the objective text of the consent and the approval of an independent ethics committee. Controllers shall not be required to conduct separate sociological or subjective assessments of 'data subjects' expectations' or engage in mandatory consultations with external representative groups before initiating subsequent project phases.	Introducing an ambiguous, subjective baseline such as 'the reasonable expectations of data subjects' as an independent hurdle—even when a project strictly operates within the textually defined boundaries of an obtained broad consent—creates prohibitive legal uncertainty for public research institutions. In long-term biobanking and molecular biology, scientific techniques evolve rapidly. If researchers must constantly second-guess whether an innovative method or sub-discourse complies with the unwritten, shifting expectations of past participants, or conduct mandatory external consultations with interest groups, crucial research will stall. Legal certainty must prevail: if the broad consent textually circumscribes the research field (e.g., oncology, genetics) and an independent ethics committee verifies the protocol's ethical integrity, this dual framework must objectively satisfy the requirements of fairness, transparency, and data subject autonomy

		broad consent, then it should ask the data subjects to consent to that individual research project (or stage thereof) – i.e. rely on dynamic consent.		
5.	**cl. 5.3 (86, 87, 88)**	**86.** It may be challenging for controllers to inform data subjects of further processing for scientific research purposes if they have not retained the contact details of the data subjects, for example due to pseudonymisation of the personal data where identifiers or a table of correspondence are not accessible for the controller. To that end, if the controller knows at the time of collection (or when contact details are deleted because they are not necessary to process) that the personal data will be processed for scientific purposes at a later stage, then the controller should make sure that data subjects can stay informed, in accordance with Articles 12 and 13 GDPR. **87.** Controllers should not knowingly delete contact details if they intend to or anticipate that they will further process personal data for scientific research purposes. If a controller knowingly deletes contact details and then fails to inform data subjects directly when further processing personal data for scientific research purposes, this may lead to a breach of the principle of transparency,	**86.** Where a public or academic research institution processes personal data for further scientific research purposes and has deleted or separated direct contact details in line with the principle of data minimization, individual retrospective notification under Article 13(3) and Article 14 GDPR shall not be required. **87.** In such scenarios, the obligation to provide information shall be deemed fully satisfied by indirect transparency measures, provided that the following cumulative safeguards are met: (a) the institution maintains a centralized, permanently accessible Registry of Research Projects on its official website, updated at least quarterly, which details ongoing research areas, collaborating partners, categories of data, and retention periods; (b) the underlying research datasets are structurally protected via pseudonymization. **88.** Public and academic research institutions operating under the safeguards listed in paragraph 87 are explicitly exempt from any obligation to actively acquire or re-verify data subjects' contact details through public	The current sequential logic of paragraphs 86 to 89 introduces an unsustainable regulatory friction between data minimization and transparency. Paragraph 87 penalizes controllers for destroying direct identifiers, while paragraphs 88 and 89 mandate that public entities either strain public registers to reconstruct identity links or drain vital scientific budgets on redundant public advertising campaigns (TV, radio, local press), Requiring clinical research center to re-identify individuals or buy media space for minor protocol shifts defeats the purpose of privacy-by-design. The guidelines should establish a cohesive, criterion-based 'Safe Harbour' for public research.

		pursuant to Article 5(1)(a) GDPR, as well as Article 13(3). 88. If the controller at the time of collection of the personal data did not know or anticipate that it would process personal data for scientific research purposes at a later stage, it may not have contact details of the data subjects. If the controller has identifiers, such as a name or administrative identification number137, it should make reasonable efforts to acquire contact details if they are readily available and acquisition would not require a disproportionate effort. **89.** If public registries or other viable means are not available, if their use would require a disproportionate effort,139 or if a data subject is not listed in any of the available sources, then the controller should inform data subjects indirectly140. The provision of such information should ensure that as many data subjects concerned as possible are reached. Relevant means to make the information publicly available, which need to be adjusted depending on the context of the research project and the data subjects involved, include: • Providing information on a website, as detailed above141; • Posting information in localities where the relevant data subjects are present	registries, and are not required to engage in disproportionate public advertising campaigns (such as television, radio, or print media notices). **89.** – to be deleted -	

		regularly (e.g. schools, universities, correctional facilities, medical care facilities, pharmacies, etc); • Advertising in public spaces, on the television or radio, in newspapers – in particular local media or online; and • Providing information through associations representing research subjects (e.g. patient organisations, trade unions, non-profit organisations etc).		
6.	**cl. 6.3 (128)**	**128.** If a controller determines that it is necessary to process the personal data in question for scientific research purposes, it should nonetheless consider the particular situation of the data subject who objected to the processing186. To that end, data subjects should be enabled to present their particular situation, including personal, social or professional circumstances, which distinguishes them from other data subjects. Such circumstances could, for example, be suffering from a rare disease, which may render a data subject identifiable even if their data are pseudonymised, or being in a family relation with a researcher, which could enable unwarranted identification of the data subject187. However, the fact that a data subject did not elaborate much on their particular situation in the objection is not sufficient for a controller to dismiss an objection per se and	**128.** If a controller determines that it is necessary to process the personal data in question for scientific research purposes, it should nonetheless consider the particular situation of the data subject who objected to the processing. To that end, data subjects should be enabled to present their particular situation, including personal, social, or professional circumstances, which distinguishes them from other data subjects. Such circumstances could, for example, be suffering from a rare disease, which may render a data subject identifiable even if their data are pseudonymized, or being in a family relation with a researcher, which could enable unwarranted identification of the data subject. If the research controller operates entirely on pseudonymized datasets within an encapsulated environment where the identity keys are legally and technically inaccessible to the active research staff, individual objections based on specific social	Mandating that a scientific research institution actively investigate and document the highly specific personal, social, or professional circumstances of an objecting individual (such as family ties to staff or socio-professional configurations) creates an operational loop. To evaluate such specific individual traits, the institution's data protection staff would be forced to collect additional sensitive background context about the person, effectively reversing the benefits of core pseudonymization and expanding the volume of processed identification data. If a public research institution relies on absolute technical firewalls where the researchers operate blindly on coded data strands with zero possibility of linking them to real-world identities, these systemic safeguards objectively override any context-based identification risks. The guidelines

		sometimes the particular situation may be obvious from the context of processing. If the controller has doubts as to the particular situation of a data subject, it may ask the data subject to further specify their request.	or professional circumstances shall be considered systemically mitigated, and the processing shall continue in the public interest of preserving dataset integrity. However, the fact that a data subject did not elaborate much on their particular situation in the objection is not, in itself, sufficient for a controller to dismiss the objection, and sometimes the particular situation may be obvious from the context of the processing. If the controller has doubts about the specific situation of a data subject, it may ask the data subject to further specify their request.	should explicitly state that strong, provable technical encapsulation of data absolves the controller from conducting granular, highly subjective sociological evaluations of an individual's personal environment.
7.	**cl. 7.1 (141, 142)**	**141.** If several parties participate jointly in the drafting of a research protocol that determines the purposes and essential means of processing of personal data, this may suffice for all the entities involved to be considered joint controllers, even if the actual research and the processing of personal data is only carried out by one or some of the entities involved. In such a context of processing, it is not necessary for all the entities involved to have an equally active participation in the determination of the purpose and essential elements of the means in order to qualify as joint controllers. **142.** Agreeing to and consequently adhering to an already established research protocol or study, without	**141.** If several parties participate jointly in the drafting of a research protocol that determines the purposes and essential means of processing of personal data, this may suffice for all the entities involved to be considered joint controllers, even if the actual research and the processing of personal data is only carried out by one or some of the entities involved. However, to ensure that data protection compliance remains proportionate and does not impede academic freedom, joint authorship of a scientific methodology or research protocol shall not automatically create a situation of joint controllership. Where distinct project partners execute separate operational phases of the protocol in full independence (such as one entity performing clinical data collection and another performing subsequent blind	The current presentation of Section 7 establishes an overextended, rigid interpretation of joint controllership that creates a severe, non-proportionate barrier to academic research. Scientific research must remain free from unreasonable constraint. REquiring academic consortia, public research academies, and healthcare facilities to conduct complex joint-governance agreements simply because they co-designed a high-level scientific methodology introduces prohibitive transactional and legal delays. A clear distinction should be maintained between the shared intellectual design of a study and the operational control of data. If an academic institution performs

		participating in the determination of the purposes and means of processing, is not always sufficient to create a situation of joint controllership within the meaning of Article 26(1) GDPR. Instead, this situation may be indicative of a relationship between a controller and processor.	statistical analysis), they shall be regarded as independent, separate controllers for their respective phases, rather than joint controllers. **142.** Agreeing to and consequently adhering to an already established research protocol or study, without participating in the determination of the purposes and means of processing, is not always sufficient to create a situation of joint controllership within the meaning of Article 26(1) GDPR. Instead, this situation may be indicative of a relationship between a controller and processor. Similarly, a joint-controllership relationship shall be excluded where partners split the research workflow into separate, linear processing chains, provided that the entity handling subsequent analytical stages has no legal right or technical capability to access the identity keys managed in the primary stages.	subsequent, blind statistical evaluations on a detached data stream without ever touching or managing patient identity links, it operates as an independent controller of its own research phase. The guidelines must realign with the principle of proportionality, ensuring that administrative data protection frameworks serve to secure privacy, not to structurally delay societal advancements derived from public science.
8.	**cl. 8.3n (161)**	**161.** To ensure the proper effectiveness of anonymisation or pseudonymisation, controllers must use state-of-the-art anonymisation or pseudonymisation methods, taking into account the most current assessment of effectiveness, risks of re-identification, threats to security, etc. The EDPB's guidelines on pseudonymisation provide further guidance on how to assess effectiveness239. There should also be an	**161.** To ensure the proper effectiveness of anonymisation or pseudonymisation, controllers must use state-of-the-art anonymisation or pseudonymisation methods, taking into account the most current assessment of effectiveness, risks of re-identification, threats to security, etc. The EDPB's guidelines on pseudonymisation provide further guidance on how to assess effectiveness. There should also be an ongoing process of verification that the	Public research entities operate on strict state budgets meant to finance biomedical equipment and discovery, not high-level commercial cryptography auditing. If a research archive was securely encrypted according to baseline institutional standards, forcing scientists to engage in continuous, high-cost software overhauls simply because commercial encryption standards evolved elsewhere is highly

		ongoing process of verification that the measures implemented to ensure anonymisation or pseudonymisation are effective over the course of a research project, or as long as the data is otherwise retained, in particular if data sets are combined, which may increase the risk for re-identification.	measures implemented to ensure anonymisation or pseudonymisation are effective over the course of a research project, or as long as the data is otherwise retained, in particular if data sets are combined, which may increase the risk for re-identification. However, for public and academic research institutions, the evaluation of 'state-of-the-art' methods and the frequency of the ongoing verification process must be balanced against the institution's available public resources and the objective likelihood of a security breach. Where technical encryption updates are restricted by public budget limitations, robust organizational safeguards—such as strict internal access logs, legally binding non-reidentification clauses for staff, and physical isolation of repositories—shall be deemed fully sufficient to maintain the required level of effectiveness.	disproportionate. It channels public funds away from critical societal research. Organizational isolation of data (who has keys, who can enter the server room, strict background checks) is an incredibly effective and cost-efficient shield that must be formally recognized as an alternative equal to continuous technical state-of-the-art upgrades.
9.	**cl. 8.3 (163)**	**163.** Legal or contractual obligations that prohibit the re-identification of individuals can, as organisational measures, complement technical anonymisation or pseudonymisation, in particular when data sets are shared between research partners or other recipients. Contractual obligations should also facilitate requests from data subjects exercising their rights in relation to pseudonymised personal data240. Therefore, contractual	**163.** Legal or contractual obligations that prohibit the re-identification of individuals can, as organizational measures, complement technical anonymization or pseudonymization, in particular when data sets are shared between research partners or other recipients. Where a receiving research institution processes a dataset without holding the decryption key, and is bound by strict contractual or statutory prohibitions against any re-identification attempts, the	There is a critical operational boundary between absolute pseudonymization and data that is effectively non-identifiable to a specific recipient. Public research institutions often receive statistical or coded medical data from hospitals, where the key is protected by medical secrecy laws. For the researchers, these data fields are functionally anonymous, as they have no intent, legal right, or technical

		obligations should ensure that – following a request from a data subject that exercises his or her rights – the controller that pseudonymised the personal data can provide the information that is necessary to re-identify a data subject to controllers or processors that process the pseudonymised data for scientific research purposes.241 Alternatively, contractual obligations could ensure that the original controller enables the practical exercise of data subjects' rights.	processing of such data by that specific recipient shall be evaluated with regard to the low risk of re-identification. If the recipient has no reasonably foreseeable means to access the identification keys held by the originator, the data may be treated as non-identifiable from the receiving controller's sole perspective.	capability to identify the patients. The guidelines should explicitly recognize this asymmetric nature of data identifiability. If a contract or law legally and technically bars the researcher from ever accessing the identity keys, the regulatory burden under GDPR regarding the legal bases for further use should be significantly lower and proportionate to the recipient's actual capability, in line with the CJEU jurisprudence on reasonable means of identification.