Spolek pro ochranu osobních údajů

# Comments on the EDPB's draft of Guidelines 1/2026 on processing of personal data for scientific research purposes

We welcome the opportunity to provide feedback on the recently published EDPB draft of Guidelines 1/2026 on processing of personal data for scientific research purposes ("proposal of Guidelines").

We greatly appreciate the EDPB for preparing this proposal and addressing a very interesting question concerning the protection of personal data. Nevertheless, we would like to draw attention to a number of problems and ambiguities associated with this proposal.

First, we would like to point out that the issue of scientific research is of fundamental importance for the EU. Due to an excessive degree of regulation, the EU is losing its position in the digital economy and industry. It is therefore important to keep in the EU at least that part of science and research which is still carried out here and, where appropriate, to encourage other research projects to return, since research (whether basic or applied) is a prerequisite for the further development of many scientific and industrial sectors in the EU.

## General comments

### On the issue of industrial and applied research

The possibility of carrying out scientific research in the full range of activities as understood by rec. 159 GDPR is, in our view, a fundamental public interest[1]. Therefore, we consider it a significant shortcoming of the draft Guidelines that, in principle, they do not address issues of this type of research at all and, by their wording and conditions, clearly declare that only scientific research in the narrow sense is considered research. Industrial and applied research (which may include, for example, research in the area of data processing, artificial intelligence, autonomous control systems, robotics, cybersecurity including the use of Big Data, etc.) is, from the perspective of the EU's future competitiveness, entirely essential (alongside, for example, medical research) and should also be supported at the level of EDPB guidelines. Conducting research in these areas is not incompatible with the protection of personal data.

Given that the research-related derogations provided for in the GDPR are rather "soft" in nature and are moreover subject to the restrictions under Article 89 GDPR, there is therefore no reason why industrial and applied research could not be included within the concept of scientific research (as is indeed envisaged by rec. 159, which expressly refers to technological development and to a broad understanding of the concept of research). We believe that an explicit statement to this effect, together with examples of cases in which certain derogations from the GDPR rules may be relied upon for these purposes as well, could significantly encourage all actors in the field of research not to relocate their research activities outside the EU, which is more than desirable in the current situation. The

[1] See, e.g., Communication from the Commission COM(2025) 30 final, A Competitiveness Compass for the EU

requirement of “genuinely scientific” research in point 9 of the draft Guidelines illustrates a failure to understand the current needs of the EU economy.

The boundaries of the concept of scientific research should therefore be set relatively broadly, for example on the basis that stricter requirements may be imposed, compared with classical scientific research, for the use of the derogations provided for in the GDPR for riskier forms of research (which, however, is very often not the case with industrial research). It is therefore necessary to move away from the “black-and-white” approach used in the draft Guidelines.

**On the status of healthcare providers as research organisations**

The narrow approach in points 9 to 12 can cause problems even for more “traditional” research organisations and overlooks that the EU legal order already contains an objective concept of a research organisation. Article 2(83) of Commission Regulation (EU) No 651/2014 defines a “research and knowledge-dissemination organisation” by reference to its primary goal of independently conducting fundamental, industrial or experimental research or widely disseminating the results, irrespective of legal status or way of financing, and lists universities and research institutes among the typical examples. University hospitals ordinarily have research among the statutory objectives set out in their founding charters and are entered in the national register of research organisations maintained by the competent ministry, entry in which is conditioned on meeting the criteria of Article 2(83) (in the Czech Republic, the list of research organisations kept under Act No 130/2002 Coll.). Such entities, alongside universities, higher-education institutions and public research institutions recognised under the law of the Member State concerned, are thereby recognised as research organisations by their constitution and registration. Status of this kind is a more objective indicator of a scientific research purpose than the subjective factors in point 11 and should be given corresponding weight. This is a sufficient positive indicator, not a necessary condition.

Consistent with our general remarks on industrial and applied research, and with recital 159 GDPR and the EDPB’s own acknowledgement that research may be carried out on a commercial basis (point 11 factor v and point 61), the absence of such institutional status does not exclude an activity from the concept of scientific research.

The EDPB should also bear in mind the typical position of a hospital. A hospital most often takes part in retrospective research, in clinical trials of medicinal products and clinical investigations of medical devices, and in patient registries used for research. In each setting the input is the medical documentation the hospital maintains, and the data are processed for research in pseudonymised form. Whether such pseudonymised data constitute personal data should not be assessed in the abstract. As against an absolute approach, under which data are personal whenever anyone might identify the person, the Court of Justice has confirmed a relative approach, under which identifiability turns on the means reasonably likely to be used by the specific actor handling the data, within the meaning of recital 26 GDPR (Breyer, C-582/14, and EDPS v SRB, C-413/23 P) – see also next point. Without resolving that wider debate here, the guidelines could usefully take this relative approach, pseudonymised data assessed from the perspective of each actor, as the starting point for the secondary use of health data in research.

Medical research has become one of the most important fields of research in the EU, with implications for the pharmaceutical industry as a key sector of technological development, and any—even unintended—interference with its principles can cause serious problems.

**On the concept of personal data**

The Guidelines also address only to a very limited extent the question of when data processed by a research organisation carrying out research on the basis of pseudonymised data provided to it by a third party will no longer be personal data (within the meaning of the CJEU judgment in the SRB case). If the EDPB could provide examples of situations in which it would not consider such data processed for research purposes to be personal data, this could greatly assist the development of research and remove uncertainty among research entities.

**On the interplay between the GDPR and the Data Governance Act**

The Guidelines could also devote considerably more attention to the interplay between the GDPR and the Data Governance Act, one of whose objectives is precisely to support the further use of personal data for scientific research.

**Comments on individual points:**

**Point 9**

We consider the narrow understanding of the concept of scientific research, as suggested for example in this point, to be the greatest weakness of the draft Guidelines. In the current situation, it is necessary to support all forms of research in the EU. The derogations and exemptions for research purposes introduced by the GDPR are not fundamental in nature, do not significantly restrict data subjects, and there is therefore no reason to focus them narrowly only on scientific research in the strict sense.

**Chapter 2.1**

We consider the entire approach of this chapter to be inappropriate and excessively narrow. The requirements for "autonomy and independence", the limitation regarding "further commercial interest" in the requirement concerning the "objectives of the research", or the requirements for "assessment, review or approval by independent experts or committees" in principle exclude commercial research. As stated above, we consider this to be a fundamental problem of the entire draft Guidelines. Example 1 also appears misleading. For example, the sentence "The pharmaceutical company hires a team of academically qualified and vetted researchers to carry out the scientific research activities necessary to conduct the trial. This corresponds to factor iv (independence and autonomy)" suggests that research should always be carried out by independent academic researchers. We consider this to be a wholly unrealistic requirement. Similarly, another sentence from this example completely disqualifies commercial research: "The research activities are expected to generate new scientific knowledge, and the results of the trial will be published in a scientific journal." Similar restrictive requirements can also be found in other examples and other points.

**Points 12 and 15**

Neither Article 5(1)(b) nor recital 159 GDPR establishes a closed, six-factor test for the concept of scientific research. Recital 159 requires that the concept be interpreted broadly. Point 12 nonetheless turns the six key-indicative factors into a presumption that operates against the controller, which must "justify and be able to demonstrate" why an activity is scientific research whenever a single factor is absent. This reverses the broad interpretation mandated by recital 159 and creates, by way of

guidance, a quasi-normative admissibility test that the GDPR does not contain. For a research organisation relying on the clinical records it already holds, several of the factors (in particular peer review, publication and the academic qualification of the persons handling the data) cannot be met for substantial parts of the processing, even where the underlying research is genuine. The factors should operate as indicia supporting a broad interpretation, not as cumulative conditions whose absence shifts the burden onto the controller.

This concern is acute for point 15. The ancillary operations listed in point 14 are, by their nature, preparatory data-management tasks. They include identifying potential research subjects such as patients from existing records, together with data extraction, filtering, grouping, curation, categorisation and pseudonymisation. These are the operations on which research re-use of clinical records depends, and they are usually carried out by data-management or IT staff, without peer review or publication. Requiring each of them to be assessed "in light of the factors listed at para. 11" imposes criteria they cannot satisfy and risks excluding routine, low-risk data preparation from the scientific-research regime. For ancillary processing, a clear link to a scientific-research objective is enough, and the research-quality factors need not be re-applied.

**Chapter 3.1.1 Presumption of purpose compatibility**

Point 21 correctly states that the presumption of compatibility under Article 5(1)(b) GDPR concerns the purpose and does not dispense with the assessment of lawfulness, and point 22 notes that the initial legal basis cannot always be relied on for the further processing, in particular where it was consent or a legal obligation. For a hospital, the input for scientific research is, as a rule, medical documentation processed for the provision of healthcare on the basis of a legal obligation (Article 6(1)(c) in conjunction with Article 9(2)(h) GDPR and national healthcare legislation). It follows from point 22 that this basis cannot be carried over to the research, yet the guidelines do not identify which basis applies in this paradigmatic case of secondary use. To prevent the presumption of compatibility from being misread as removing the need for a lawfulness assessment, the guidelines should state expressly that, where personal data collected under a legal obligation are further processed for scientific research purposes, the controller must identify a fresh legal basis under Article 6(1) GDPR (typically Article 6(1)(e) in conjunction with Union or national law) and the applicable derogation under Article 9(2) GDPR.

**Chapter 3.2 Storage limitation**

The first sentence of point 27 correctly reflects Articles 13(2)(a) and 14(2)(a) GDPR, under which the controller states either the storage period or, where that is not possible, the criteria used to determine it. The later statement that "the storage period must be determined by the controller before the personal data are processed", resting only on Article 25(1) GDPR, is inconsistent with that alternative and finds no support in the text of the GDPR. In longitudinal or registry-based research, where verification, reproducibility and successor projects are foreseeable but not datable in advance, a fixed period frequently cannot be set, which is the very situation for which the GDPR provides the criteria alternative. Deleting or qualifying this sentence would keep the use of determinable criteria, rather than a fixed period, expressly available.

**Chapter 4.1.1. "Freely given consent".**

We believe that, in cases of scientific research, in most cases it will not be possible to speak of an "imbalance of power", see points 36 and 39. In particular, we do not consider the example involving "unemployed or disenfranchised persons" to be appropriate. Moreover, in this context the draft

Guidelines identify a problem but do not offer a solution (how consent should be replaced in such cases; or it is not apparent to us how other possible solutions - the use of another legal basis for processing - would contribute to a greater level of protection for data subjects).

**Chapter 4.1.3. – Consent not stemming from GDPR**

Here we miss a clear and more detailed opinion of the EDPB on a pressing practical issue, namely, where consent is granted under special legislation, in which specific cases processing may be based, from the GDPR perspective, on another legal basis. This is relevant in particular where the special legislation on the basis of which consent is required does not allow its unrestricted withdrawal. The use of "consent" as a legal basis under the GDPR would negate that limitation on withdrawal.

**Chapter 4.4. "Processing special categories of personal data"**

As regards the scope of special categories of personal data (point 64), we are aware of the CJEU case-law. The sentence "The notion of special categories of personal data covers not only data that directly reveal sensitive information about a data subject, but also personal data that can be used to collate or deduce such information, and sensitive information inferred from the data processed." is therefore consistent with that case-law. Nevertheless, we must point out that such a broadly formulated scope of special categories of personal data, which also covers cases where the controller concerned does not intend to infer any special categories of personal data and does not in fact infer them, will represent an increasing problem for European research and European controllers. This became apparent, for example, in the preparation of the Digital Omnibus and in the debates on the processing of such categories of personal data for AI training. In the future, a much more pragmatic approach will need to be adopted, taking greater account also of the intention of the controller concerned and its actual steps.

The same problem arises when processing posts from social media (see point 70). In some cases, verifying the terms and settings of services is possible; however, when processing Big Data collected on a large scale from the internet, this can pose a significant problem. Again, it would be appropriate to adopt a pragmatic solution that differentiates more between individual methods and types of processing.

**Chapter 5.1 Obligation to inform**

**Point 77**

Where processing is anticipated over longer periods, point 77 invites controllers to give data subjects the opportunity to provide contact details "even if the purposes for processing personal data do not require the processing of contact details". On the EDPB's own wording this means soliciting and keeping data that are unnecessary for the purpose, which is difficult to reconcile with the principle of data minimisation (Article 5(1)(c) GDPR). In the secondary use of medical documentation the research data are typically held in pseudonymised form precisely in order to minimise, and an added expectation to gather and maintain contact channels works against that design. The transparency objective can be met by the indirect and public means that the EDPB itself endorses (points 79 and 89). Point 77 would be better framed as one option among several, not as an expectation to collect data that are not necessary for the purpose.

**Example 13**

It is not clear to us why a special ticking of a check-box should be required where consent can be obtained by the very act of downloading the application concerned (provided that proper information is given about the purpose of the application and the fact that, by using it, consent to processing is being given). In practice, this method of obtaining consent is common and does not in any way disadvantage data subjects.

**Point 87**

We respectfully disagree with the conclusion that a controller could not erase the contact details of data subjects where it intends to continue processing personal data for scientific research purposes - in particular if it has already informed the data subjects of this intention at least in general terms. Such a prohibition is contrary to the basic principles of the GDPR, and the principle of transparency, as presented by the EDPB, would then come into conflict with the principles of data minimisation and integrity and confidentiality. This is therefore a case of conflict between principles of equal weight, which cannot be resolved in such a simple manner; the circumstances of the specific case must always be taken into account.

As regards the requirement to obtain contact details subsequently in point 88 (and point 100), we consider this appropriate only in very limited cases where the interests of data subjects could be otherwise seriously affected, because such an effort will require the controller concerned to expend considerable effort and financial resources (for example, in the Czech Republic the sending of messages from data boxes is usually subject to a fee). Likewise, the requirement to provide information by means of advertisements (points 89 and 99) seems disproportionate to us for most cases in the context of the purpose of scientific research.

**Point 91**

Under point 91, all personal data generated during research (a diagnosis derived from the data subject's own records, a pseudonym, or an added data point such as gender) fall within Article 14 GDPR and are treated as data "not considered as collected directly from data subjects". This follows the reasoning in case C-169/23. The point does not, however, acknowledge that, where the source data came directly from the same person, as they do when medical documentation is re-used, the exceptions in Article 14(5) GDPR may apply to such derivations, in particular Article 14(5)(a) (the data subject already has the information) and Article 14(5)(b) (disproportionate effort). For routine derivations from data the controller already holds, the point therefore risks creating a duplicative information obligation. A cross-reference in point 91 to the Article 14(5) exceptions for derived data would resolve this.

**Example 15**

Here again we recommend assessing whether, always and for both entities concerned, the data will constitute personal data from the perspective of the CJEU judgment in the case Single Resolution Board.

**Point 108**

We consider the requirement to provide information on "Changes to the identity of the controller – for example if a research laboratory merges with another laboratory, forming a new entity;" to be excessive. If the consequence of the "merge" is the creation of a new entity as a universal legal

successor (which will need to be assessed under the law of the Member State concerned), then in our opinion there is no reason to require special information to be provided to data subjects (unless required by the law of the Member State concerned for other reasons), because such information will be ascertainable from the relevant register.

**Chapter 6.2 – Right to erasure**

**Point 119** states that necessity in the first sub-sentence of Article 17(3) GDPR "must be interpreted restrictively" and that the controller must show the processing to be "strictly necessary". The qualifier "strictly" does not appear in Article 17(3) GDPR, as condition the exceptions on the processing being necessary. Adding a heightened standard of strict necessity narrows a research safeguard that the legislature deliberately placed in Article 17(3)(d) GDPR.

We draw particular attention to the reasoning **in point 120**, under which the availability of the research exception decreases as the number of data subjects increases ("if a controller processes personal data from a large number of data subjects, requests […] for erasure […] may not make it impossible or seriously impair […] the scientific research purposes"). In practice this means that the large patient registries and population datasets that recital 157 GDPR expressly commends, which are the characteristic product of the secondary use of hospital documentation, are the least able to resist erasure requests, to the detriment of data integrity and the reproducibility of results. It would be preferable to treat dataset size as one circumstance among several, rather than as a factor that systematically disables Article 17(3)(d) GDPR for large-scale research.

**Chapter 6.3 – Right to object**

**Point 126**

We point out here that the requirement that processing be "strictly necessary" does not follow from the text of the GDPR. Any further restriction of the necessity principle, already interpreted disproportionately strictly by the Court of Justice of the EU, may fundamentally damage European science and research.

We fundamentally disagree with the approach set out in **point 127**, from which, in our view, it follows that the EDPB expects that, in the event of every objection, there will first be an overall reassessment of whether the processing complies with the requirements of the GDPR ("Moreover, the controller should verify whether the processing of personal data related to the specific objection remains necessary for the performance of a task carried out for reasons of public interest at the time when the request is made") and only subsequently, as a further step, will there be an additional assessment of whether the specific circumstances stated in the objection preclude that processing. Such an approach would be utterly destructive for several controllers, who would have to carry out extensive assessments again upon every objection, even though those assessments had already been carried out at the start of the processing. Applied to cases of legitimate interest (although the point in question concerns public interest), this would mean re-performing the entire balancing test (or DPIA). However, no such requirement follows from the text of the GDPR; on the contrary, the controller concerned should take into account only the special circumstances on the side of the data subject stated in the

objection and balance them against the processing carried out. The original balancing tests and assessments are not affected.

This sentence in **point 128** is also too categorical: “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 sometimes the particular situation may be obvious from the context of processing“. If the specific individual situation of the data subject is completely apparent from the objection, even if it was not clearly expressed, the controller certainly has a duty to handle that objection properly. However, the controller should not be required to search actively for circumstances on the side of data subjects. The principle “vigilantibus iura” should be fully applied here.

**Chapter 7.1 Controller**

In **Example 20**, we would welcome a closer statement of the EDPB’s view on what legal basis “Rapid Survey” should apply to the actual disclosure of contact details. We would also welcome a closer assessment of this situation in terms of the possible application of the Data Governance Act.

**Chapter 7.3 Joint controllers**

We acknowledge that **points 134 and 142** correctly limit controllership. The provision of funding or consultation on a protocol does not in itself confer the role of controller (point 134), and mere adherence to an established protocol may indicate a controller-processor relationship rather than joint controllership (point 142). Point 141, however, provides that joint participation in drafting a protocol that determines the purposes and essential means “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”. Read literally, this confers joint controllership over the entire project on every entity that co-drafted the protocol, whatever the specific processing operation. That is hard to reconcile with the operation- and stage-specific approach required by the Court of Justice, under which the responsibility of each entity must be assessed for each processing operation and stage in light of all the circumstances (IAB Europe, C-604/22, para. 58, which the EDPB itself cites at point 144, and Fashion ID, C-40/17). Example 25 applies that nuance, allocating joint controllership only within the respective constellations and treating the hospitals as independent controllers for healthcare processing, whereas the broad wording of point 141 does not. In a multicentric study a hospital that co-drafts a common protocol should be a joint controller only for the operations whose purposes and essential means it actually co-determines, not for operations such as a central database or a sub-project in which it has no involvement. Aligning point 141 with point 144 and Example 25 would remove that risk.

**Chapter 8.2. Risk analysis and data protection impact assessment (DPIA)**

Point 151 states that “the starting point for adopting appropriate safeguards, pursuant to Article 89(1) GDPR, is conducting a risk analysis or – when required – a DPIA”. Article 89(1) GDPR calls for appropriate technical and organisational measures, in particular data minimisation. It does not make a separate, documented risk analysis a precondition for every processing operation that benefits from the research regime. Treating a risk analysis as the mandatory starting point for all Article 89(1) processing, regardless of the Article 35 GDPR threshold for a DPIA, adds a procedural step that the

text does not require and burdens routine, low-risk re-use of clinical records for research. It would help to clarify in point 151 that the depth of any risk assessment is commensurate with the risk and that a formal risk analysis is not needed where the processing does not meet the threshold for a DPIA.

**Chapter 8.3. Anonymisation and pseudonymisation of personal data**

**Point 156**

Here we would welcome the EDPB expressing its view on which legal basis is appropriate for the anonymisation process itself.

**Points 156 and 157**

Point 156 directs that personal data processed for research should "in the first place be anonymised", by reference to the Article 29 Working Party Opinion 05/2014 on Anonymisation Techniques (WP216). For most biomedical research the input is record-level clinical documentation, and the research design itself, whether longitudinal follow-up, linkage across sources or genetic analysis, requires data that remain attributable to the individual record. Applied to such data, the WP216 standard of resistance to singling out, linkability and inference can be met only through generalisation, suppression or perturbation that strips the dataset of its analytical value. Point 157 already accepts that, where anonymised data would not serve the study, pseudonymisation is used instead. We ask the EDPB to make explicit in point 156 that, for record-level, longitudinal or linkage-dependent research, anonymisation is by design incompatible with the analysis, so that pseudonymisation with appropriate Article 89(1) safeguards is the lawful baseline rather than an exception the controller must justify dataset by dataset. Otherwise the "anonymise first" default, combined with the high WP216 threshold and the ongoing verification required by point 161, pushes controllers either to over-anonymise and forfeit research validity or to face challenge that pseudonymised data are insufficiently minimised.

For rare and ultra-rare diseases this limitation is structural. The number of patients who can enter a given study is by definition very small, in some conditions only a handful across the whole of the EU collaborating through the European Reference Networks. As the enrollable cohort shrinks, the risk of re-identification rises, because the diagnosis together with a few routine attributes such as age, sex and region already identifies the individual. Point 165 recognises this for genetic data, which can be regarded as anonymous only in exceptional circumstances, and the same applies to rare-disease data more broadly. Here anonymisation is foreclosed by the size of the population, not by any choice the controller makes.

**Point 163**

We consider the requirement concerning the possibility of obtaining contact details under point 163 to be a significant problem requiring further verification and discussion: "Therefore, contractual 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." This requirement effectively prevents the applicability of the conclusions

on the absence of identifiability under the CJEU judgment in the SRB case. This would in fact exclude the possibility of relying on that judgment.

**We are grateful for the opportunity to provide our comments on the draft Guidelines. We would like to thank the EDPB very much for its efforts to clarify various issues related to the processing of personal data. We hope that our comments will help in formulating the final version of the Guidelines.**

Prague, 22.06.2026

**JUDr. Vladan Rámiš, Ph.D.**
Chairman of the Committee
**Data Protection Association**

**Mgr. Radek Knop**
Chairman of the Healthcare Committee
**Data Protection Association**