Spolek pro ochranu osobních údajů

Comments on the EDPB draft of Guidelines 02/2026 on Anonymisation

We welcome the opportunity to provide feedback on the recently published EDPB draft of Guidelines 02/2026 on Anonymisation.

We appreciate the considerable work undertaken and the effort to harmonise the concept of anonymisation across EU.

We would like to submit comments on these Guidelines.

As a general point, we would like to highlight that excessively stringent requirements for the quality of dataset anonymisation may completely undermine the ability of European businesses to work with large volumes of data. They may also undermine the EU legislature's plans to create a European data space and facilitate data sharing, as set out, for example, in the DGA. Particularly today, when the widespread deployment of AI makes it possible to find previously unimaginable links between diverse data, there is a need to provide greater protection for personal data, while also applying the GDPR realistically in light of its objectives. In particular, as we explain below, we believe that in certain cases greater account will need to be taken of the intentions and motivations of potential controllers.

Below, we set out several points which, in our view, should be considered before the Guidelines are finally adopted.

1. We fully understand the EDPB's conclusion in paragraph 15 concerning processors and the reasons behind it. While this conclusion does not follow directly from EDPS v SRB, we note that the Council mandate on the Digital Omnibus takes the same position. The Guidelines should nevertheless state at what point an entity that initially processed the data on behalf of the controller is assessed from its own perspective, for example where a former processor continues to use the data for its own purposes after the controller's engagement has ended. Example 4 covers only an entity that was independent from the outset.

2. In our view, the Guidelines do not take sufficient account of the context of the processing concerned.
   This is apparent, for example, in Example 5, where whether "the person in a black suit who is also walking a dog" constitutes sufficiently identifying information will in fact depend on the context of the processing concerned. In certain circumstances, that person will be identifiable where further personal data are linked to their unusual behaviour in the CCTV footage concerned or to footage of their face, or where the dataset being processed (e.g. the CCTV footage itself) is supplemented with other information (e.g. a police enquiry about

Spolek pro ochranu osobních údajů / Data Protection Association
with its registered seat at the address Hellichova 458/1, Malá Strana, 118 00 Praha 1 / Prague 1,
registration with public register: Municipal Court in Prague, file No. L 61299
Business ID No.: 03493679, e-mail: spolek@ochranaudaju.cz, tel.: +420 730 677 644

that person). However, the person may not be identifiable if his/her face is not recognisable and his/her behaviour is in no way distinctive (i.e. it is simply a person walking down the street). The concept of singling out within the meaning of rec. 26 GDPR could apply here, but it too must be applied in context: if there is no behaviour for which the person should be singled out from the group, there is no point in applying the concept of singling out. The Guidelines themselves accept this in paragraph 99 and Example 24, where a record that is unique within a dataset is nevertheless not personal data if its attributes cannot be matched to any other data available to the relevant entity, and in paragraph 19, which requires that the individual be distinguished in a way that makes it possible to treat them differently. In Example 5 that condition is met where the footage shows neither the face nor any distinctive conduct. Example 5 should be aligned with those passages.

The example of an IP address as an identifier in paragraph 23 is also somewhat unclear. Here again, the context of the data subject's activities will determine whether the principle of singling out should apply. In other cases (not covered by singling out), it will depend, for example, on whether the Member State concerned imposes a data retention obligation. This has a fundamental bearing on the classification of an IP address as a qualified identifier: in particular, once the data retention period has expired, it will be very difficult to regard an IP address as an identifier (for entities other than those that can benefit from singling out). This is consistent with Breyer (paragraphs 46 to 49), on which the Guidelines themselves rely in paragraph 29 and footnote 23. The dynamic IP address was personal data for the website operator only because of a legal route to additional information held by the access provider. Once that information is no longer retained, identification through the access provider becomes practically impossible within the meaning of paragraph 46 of Breyer, and the IP address ceases, in most cases, to be an identifier for entities that do not hold the link themselves.

3. This is an issue that has long been unclear and subject to debate. Paragraph 31 cautions against using lack of motivation as a factor, yet the same paragraph asks for the value of the re-identified data to the re-identifying entity to be weighed against the cost and effort involved, and paragraph 33 looks at whether the gains from breaking the law outweigh its costs. Paragraph 31 thus excludes lack of motivation even where it is objectively substantiated by the purpose and legal basis of the transfer, a statutory or contractual prohibition of re-identification or the recipient's business model. The EDPB should explain why such verifiable circumstances, unlike the value of the data under paragraph 31, may not be weighed under paragraph 29(b) and paragraph 34, and how the risk that motivation changes over time is addressed where the data are deleted or access ends. This is not limited to the economic balance of value and cost. The actual purpose and likely conduct of the entity are also relevant. A bare statement that an entity does not intend to identify anyone is not sufficient, but sufficiently substantiated intentions should be capable of being taken into account alongside the objective circumstances. Motivation is a factor that should now be given greater prominence, as technological advances and big data processing (including the development of AI) will make it increasingly easy to uncover potential personal data (at least indirectly identifying data) by cross-matching datasets. In our view, in the actual

practice of personal data processing it will not be possible in the long term to avoid taking account of factors relating to the intentions of the person concerned (the potential controller), at least in some cases. Failing to take this factor into account will further extend the reach of the GDPR and further restrict the ability to process large datasets in the EU. Example 7 illustrates a situation in which the intention of the person concerned will in fact need to be taken into account. It could also play a significant role in the assessment of the individual persons referred to in paragraph 30 of the opinion. To some extent, paragraph 33 points in this direction; however, it is unclear what conclusions the EDPB draws from this. Example 8, in particular, is very unclear, since it concerns a situation in which the media company concerned will in any event be able to identify the data subjects concerned (regardless of whether or not it secures its servers), and malicious third parties that breach the security of those servers will in any event obtain all the information necessary for identification.

Paragraph 32 and Example 8 treat external attackers as entities not restrained by a legal prohibition. In Example 22 a research institute with state-of-the-art security nevertheless includes, out of caution, hackers among the relevant entities. Their inclusion did not change the outcome there, but the Guidelines do not say on what basis such entities are to be included or excluded. If their inclusion is automatic, any dataset whose protection depends on the holder's security measures becomes personal. We ask the EDPB to state the threshold for including external attackers as relevant entities under paragraph 30, and how the level of security under paragraph 29(b) is to be weighed in that assessment.

4. Although we are aware of the long-standing debate on the need (or otherwise) for a legal basis or an exception under Article 9 GDPR (or, for example, consent under the ePrivacy Directive) to carry out anonymisation, we would nevertheless recommend explaining the EDPB's position in paragraphs 38 and 39 in greater detail through practical examples. In many cases, the use of anonymised data may be highly beneficial to society, even if the intended purpose differs from that for which the data were originally collected. Reference may be made here, for example, to the situations covered by Article 17 et seq. of the Data Act. Article 18(4) of the Data Act obliges the data holder to anonymise personal data falling within a request or, where disclosure of personal data is required, to pseudonymise them. Such an obligation under Union law can serve as a legal basis under Article 6(1)(c) GDPR for the anonymisation step. The Guidelines should say how paragraph 38 applies where anonymisation is required by law for a purpose other than that of the original processing, including which Article 9(2) exemption may be relied on where that law does not itself provide one.

5. As regards paragraph 40, we must point out, based on our practical experience, that, when data are collected, it is often impossible to anticipate the purposes for which anonymised data (particularly in aggregated form) will be used. Complying with the transparency obligation will therefore often be difficult in practice. One example is the use of aggregated data during the pandemic, for instance to monitor trends in population movements between

regions. Here again, we refer to the Data Act and its rules on B2G data sharing, under which these requirements would also apply in the cases covered by Article 18 of the Data Act.

6. The requirement to document the anonymisation process (paragraph 41), although proportionate for large datasets, is also expressed too categorically. For smaller datasets, there is no reason to insist on documentation of the same depth. The scope of the documentation should follow Article 24(1) GDPR and reflect the nature, scope and risks of the processing, and the Guidelines should say expressly that "adequate" in paragraph 41 scales with that risk.

7. Example 11 should also be given further consideration and discussed. Ultimately, it could lead to the absurd interpretation that any data holder with a dataset at their disposal would be required to test it extensively against publicly available data to verify that it does not contain potential personal data. The Guidelines should make clear that the assessment under paragraph 61 is limited to additional information that the relevant entities can realistically be expected to hold or obtain, and does not require a general search of external sources. The intention and business model of the data holder should also be taken into account here.

8. While we agree with the conclusion in paragraph 36 that a dataset containing both anonymous data and personal data should be protected as a whole under the GDPR, a reasonable approach is nevertheless needed in cases where it is highly likely that the dataset contains only a few items of indirectly identifying information. In such cases, it would be appropriate to apply the obligations under the GDPR to a reasonable extent. The risk-based approach of the GDPR, reflected in Articles 24, 25 and 32, allows the measures applied to such a dataset to be proportionate to the residual risk. Paragraph 36 already implies that separate parts of a dataset may be treated separately, and the Guidelines should say expressly that the controller may suppress or separate the records that remain identifiable and assess the remainder on its own against the three criteria. Separating records known to be identifiable does not, however, address personal data whose presence the holder cannot readily recognise, and it is there that a proportionate, risk-based response is needed.

9. Paragraph 22 requires the likelihood of identification to be insignificant in reality. Paragraph 21 then treats the data as personal for the transfer, for the recipient and indirectly for the transferring entity whenever an onward transfer is reasonably likely and it cannot be ruled out that the recipient can identify the individuals. The phrase "cannot be ruled out" is taken from paragraph 85 of EDPS v SRB, where it qualifies whether third parties have means reasonably allowing identification. Point (b) refers to means reasonably likely to be used, but the words "cannot be ruled out" require the transferring entity to exclude a possibility rather than to assess its likelihood. For recipients that are not known at the time of the assessment this amounts to proof of a negative, which paragraph 22 does not require. Point (a) compounds this, because it asks whether it is reasonably likely that the entity can transfer the data, and almost any entity can. This is the usual situation in patient registries, data spaces and the secondary use of health data. Example 4 recognises that the

perspective of an independent research institute is its own. Where the research project envisages onward sharing with collaborating institutions, the institute will rarely be able to rule out that one of those institutions has means reasonably likely to be used for identification, and the data would then be personal for the institute as well. We suggest clarifying that point (a) concerns transfers that are intended or reasonably foreseeable, not any transfer the entity is technically able to make, and rewording point (b) so that it requires an assessment of likelihood, for example "the transferring entity has not established that the receiving entity is unlikely to have the means to identify the individual through means reasonably likely to be used". Paragraph 32 answers this only where a legal prohibition of re-identification applies, and paragraph 34 treats contractual prohibitions as a complement to technical measures only, so for ordinary research collaborations the result described above remains.

10. Under paragraph 35, data that become identifiable again are to be treated as personal and the controller is accountable for processing them. Yet paragraph 35 and footnote 3 present periodic reassessment only as good practice. An entity that lawfully received the data as anonymous is not a controller under the GDPR and has no obligation under the GDPR to monitor them. Paragraph 35 also refers to "the controller" without saying whether this is the anonymising controller or the entity processing the formerly anonymous data, while the rest of the paragraph speaks of entities processing anonymised data. Footnote 30 relies on Deutsche Wohnen (paragraphs 76 and 78), under which a fine presupposes an intentional or negligent infringement, which in turn presupposes, under paragraph 76 of that judgment, that the entity could not be unaware of the infringing nature of its conduct, here of the personal nature of the data. The Guidelines should say when, short of a fine, the obligations of such an entity arise, what care is expected of it and how it is expected to react to a change in identifiability that it is able to detect. For an anonymising controller that retains the original data or continues to make the dataset available, they should also say whether reassessment remains good practice or forms part of accountability under Article 5(2) GDPR. The Guidelines also do not say what is expected of an entity that receives data represented to it as anonymous, whether as a result of anonymisation or because the data never contained personal data. Read with paragraphs 11, 12 and 30, they could be understood as requiring every recipient to run its own assessment before using the data. We ask the EDPB to confirm that a recipient without indications to the contrary is not expected to carry out its own re-identification testing before using the data, and that its obligations arise from the point at which it knows, or could not be unaware, that the data are identifiable. The Guidelines should distinguish the position of the anonymising controller, of a recipient that knows it is receiving anonymised data and of a recipient that reasonably understands the data to have been non-personal from the outset, and should say what verification, if any, is expected in each case and which concrete indications should trigger further examination.

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

Spolek pro ochranu osobních údajů

processing of personal data. We hope that our comments will help in formulating the final version of the guidelines.

Prague, 29.10.2026

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

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