noyb – European Center for Digital Rights
Goldschlagstraße 172/4/3/2
1140 Vienna
AUSTRIA

To:
EDPB
Rue Wiertz/Wiertzstraat 60
1047 Bruxelles/Brussel
Belgium

Vienna, 30.10.2026

Subject: Feedback on the EDPB Guidelines 02/2026 on Anonymisation

1. Introduction

1.1. Wide-reaching consequences of these Guidelines

As an initial comment, we want to highlight, that Guidelines 02/2026 are one of the most crucial Guidelines the EDPB has passed in a long time, given that the entire application of the GDPR rests on the findings in these Guidelines.

We therefore urge the EDPB to scrutinise each and every line of the Guidelines before passing a final version. These Guidelines should not be rushed.

1.2. Background on the SRB ruling

Although the SRB judgement has a lot of details that need accounting for, we do not see any groundbreaking results on the nature of anonymous data.

The SRB judgement has a number of distinct elements, including:

(a) the EDPS relying on an overly formalistic argument on Article 4(5) GDPR, that pseudonyms are personal data, even if some of the IDs may be more accurately described as random IDs (e.g. if multiple comments were merged into one ID), that

(b) the case concerned a well-defined and closed environment between SRB and Deloitte, both highly regulated environments with a clear and limited task,

(c) the CJEU essentially affirming that a random string *might* be personal data for one entity but not for another, and

(d) a referral back to the General Court to make an ultimate decision on the individual case (which never happened, because the case was withdrawn).

We want to caution that this very specific fact pattern is massively expanded beyond the individual case and general assumptions are made that are (1) heavily pedalled by the lobby and compliance industry and (2) not in line with the text of the GDPR or indeed CJEU case law.

We are fully aware, that the EDPB is under enormous political pressure to "soften" its approach and *de facto* limit the GDPR, but especially the current debate on the proposed Article 4(1) GDPR has shown, that such an approach does not seem to have a broader political backing beyond the European Commission – and maybe some heavily lobbied Governments like Germany. We urge the EDPB to not pre-empt the political process in this respect, but instead highlight the need for a detailed assessment, as generally foreseen in the Guidelines.

It is clear that an increasingly, subjective or context dependent understanding of personal data is extremely problematic as it primarily hinges on internal information of countless controllers, which would determine not only the enforceability of the GDPR for SAs, but also the fundamental right to data protection for data subjects. The risk of making definitions too easy to manipulate is inherent and would allow entities to operate in a grey area. Every access request and every complaint could be "rerouted" to a debate about the applicability of the GDPR in each specific case – making the law basically unmanageable.

In sum, with the current (industry-friendly) interpretation of the subjective interpretation of anonymous data will almost certainly lead to issues with burden of proof, which in the end will increase legal uncertainty, decrease protections afforded to data subjects, and even serve impractical for most companies.

- → We welcome the EDPB's "contextual" approach instead of any versions of a fully "subjective" approach, as often argued by (extreme) industry voices.
- → We urge that the "contextual" approach must clearly stay the exception to the rule, given that uncertainty about the core definition of "personal data" would likely undermine the effectiveness of the GDPR in practice, and lead to massive caseloads before SAs that concern even just the application of the law.

1.3. Enormous risks of another "*kid in the candy store*" approach

While we recognise the political pressure that the EDPB is under and witness the (often overstretched) claims that are made in light of the SRB ruling, we would like to highlight that any "contextual" or even "subjective" approach leads to massive risks for legal certainty, enforceability of the GDPR, and the protection of data subject's rights.

After all, each controller will independently and internally apply these Guidelines and most controllers and their law firms have a clear incentive to follow the most expansionist and permissive interpretation possible of a "contextual" approach. The SRB ruling has already led to another "kid in the candy shop" approach by many controllers. The existing experiences with the so-called "risk-based approach" or with the assessment of "supplementary measures" for data transfers have shown that an exception can (in practice) quickly swallow the rule.

- → We urge the EDPB to clarify that a "contextual" or "subjective" approach cannot be an exception that swallows the rule and that SAs are determined to enforce against overly expansionists interpretations of the Guidelines.
- → We also urge the EDPB to use utmost precise and clear wording to prevent any legal uncertainty that controllers and their law firms will use to argue that the GDPR does not apply to (often vast) areas of processing.

2. Key Conceptual Elements

While we support many elements of the EDPB's approach in the Guidelines, we would like to encourage the EDPB to sharpen and clarify its approach further. We think that the Guidelines could benefit from linking the existing findings to clearer and more explicit underlying doctrine.

2.1. Purely subjective approach *not* in line with text of the GDPR

We are fully aware that the SRB ruling contains paragraphs that allow for a more "*subjective*" approach. Nevertheless, the text of the GDPR does not contain any subjective elements:

Article 4(1) GDPR follows a purely objective approach when defining personal data, with no mention of the viewpoint of various different people or entities. This is in line with most EU law definitions that typically follow an objective approach in legal definitions.

Also, Recital 26 follows an objective approach by determining that the controller or (any) other person could identify the data subject:

> *"To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly."*

The only element that would lend itself to a "subjective" approach is the (non-binding) wording in Recital 26 that establishes that only *"all the means reasonably likely to be used*" should be considered. This does allow for the consideration of elements which are reasonably likely in any specific situation. However, thi remains a factual question of likeliness and does not support a fully "*subjective approach*".

- → We note that the EDPB seems to follow an underlying legal doctrine that is based on a factual assessment of the likeliness in each case by developing a "contextual" approach. We would very much encourage the EDPB to also explicitly define and highlight in its doctrine that this is a factual approach based on the legal element of the "*likeliness*" in a given situation, making the Guidelines easier to understand and digest.
- → So far, the Guidelines mainly rely on CJEU case law. Given that the EU primarily follows a statutory legal system, we would welcome that the Guidelines clearly refer to the legal text of the GDPR that allow for such a "*contextual*" approach.

2.2. Clear separation between "*pseudonyms*" and "*anonymous data*"

We note that following the SRB ruling many "experts" and indeed the European Commission (deliberately or unknowingly) have confused the concepts of "pseudonyms" (e.g. Social Security Numbers, ID numbers, phone numbers or tracking numbers) and "anonymous data". Recital 26 clearly states that "pseudonymised data" is personal data, which is also reflected in Article 4(7) GDPR:

> *"Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person."*

We welcome that the EDPB did not confuse these concepts in the Guidelines. However, we would encourage the EDPB to maybe make this differentiation more explicit (e.g. in an explanatory text or intro text), to ensure that the Guidelines are not understood as muddying the waters between the concepts in Article 4(1) and 4(5) GDPR.

- → We encourage the EDPB to keep the clear separation between the concepts of "*anonymisation*" and "*pseudonymisation*" that got blurred in the response to the SRB ruling.
- → We would welcome a more explicit section to clarify and highlight the different concepts.

2.3. Factual access to personal data typically *not* a factor under the GDPR

Even if a "subjective" approach is chosen, the CJEU also noted that previous case law still stands. The CJEU has the luxury to stay silent about potential conflicts with other case law, but EDPB Guidelines as well as practitioners must take a wholistic view, which must also include the following considerations:

Data Collecting Controllers

We notice that for example in C-210/16 *Fashion ID,* the CJEU held that a website that included a tracking code of a third party (in this case Facebook), but with no factual access to the personal data, can be a controller. This was the case given that the definition of a controller in Article 4(7) GDPR only refers to the entity that "*determines the purposes and means*", without requiring the factual access to personal data or the possibility of the controller ever gaining such access. A purely "subjective" approach would lead to scenarios of purely "*collecting* controllers" (which include almost all online tracking by third parties, Google Analytics and many other cases) which are not covered by the GDPR if only the "*recipient* controller" is able to identify such data.

Such scenarios are common in other cases, such as Meta Glasses (where Meta may be able to identify a person, but the user does not have the purposes and means to do so), various in-shop Bluetooth or WiFi tracking (where the shop may only track a MAC address, but the provider of the system can re-identify users) or various versions of Google "Street View" (where the collection of street images may be done by a controller other than the controller generating the map).

So far these controllers (often the only entity that an SA can enforce against locally or in the EEA) were covered by the GDPR. Nonetheless, an approach that focuses on the factual access to personal data or the abilities of each controller individually, would allow controllers to claim that they cannot realistically identify a data subject and hence allow the "collection" of personal data for a third party without being subject to the GDPR.

Gap between Article 4(1) and 4(7) GDPR

As noted above, in C-210/16 *Fashion ID*, the CJEU correctly held that the entity that "*determines the purposes and means*" is the controller, no matter whether it has access to personal data or not.

We notice that these cases are only mentioned in Footnote 7 of the EDPB Guidelines. However, these cases seem to be at odds with the approach that focuses on the factual and technical options for each controller to identify a person.

We are fully aware that the "objective" concept of the GDPR (that *noyb* maintains to be the original intention of the legislator) would overcome this problem, but the more a "subjective" approach is taken, the more such conceptional conflicts arise and should be sufficiently highlighted.

- → We strongly encourage the EDPB to cover the conceptual conflicts between the text of Article 4(7) GDPR and the consequent case law (which confirmed that the GDPR is applicable even without *any* access to the data), with case law which makes the possibility of identifying personal data an element to consider for the application of the GDPR.
- → We understand that if a subjective approach is generally followed, the logical option to reconcile such an approach with Article 4(7) GDPR is to consider if in "downstream" processing any controller could identify the data subject – and in such a case, this would have to reflect back on other controllers in the processing chain.

2.4. Limitation of assessment along the various dimensions

When revieing the Guidelines it becomes clear that any contextual assessment quickly becomes a "*4D chess game*". We would therefore suggest that the Guidelines openly suggest to controllers that any contextual assessment can only realistically be undertaken if some of the dimensions are structurally limited by the controller.

This can be for example a clear limitation in relation to the number of entities that have access (see paragraph 29), the possible paths for identifications (see paragraph 30) or the time that such data will be used (see paragraph 35) and new developments must be considered. The combination of such limited dimensions is also very close to the situation in the SRB ruling (one recipient, one purpose, limited time).

While an assessment of all these dimensions is (theoretically) possible, we think that it would be useful and fair to highlight to controllers that realistically there are limits to the assessment that a controller can undertake.

2.5. Number of entities & "open" and "closed" situations

The most relevant such limitation is the number of entities that any contextual approach would have to include:

As mentioned above, the fact pattern in SRB was very specific, as a single recipient in a highly controlled environment got pseudonymised personal data for a limited task and limited time. We understand that the Signal Resolution Board and Deloitte also had clear rules and direct contracts about the use of the data. Conceptually this can be described as a "closed" situation with finite (only one), known recipients.

Recent suggestions by the European Commission in the Digital Omnibus or some of the "expert" commentary on the SRB ruling did not consider the difference between such a "closed" situation as in SRB and an "open" environment (such as e.g. online tracking with 1,000+ recipients). In fact, there is an obvious attempt to expand a ruling for a highly controlled closed situation to any processing operation, involving any number of entities. Basically, an attempt to do a reverse *argumentum a maiori*.

While the EDPB Guidelines already highlight the need to consider the limited distribution of personal data – which is important, we think that a "closed" versus "open" element would provide clearer and more definitive guidance on the level of a clear doctrine. We would therefore urge the EDPB to explicitly highlight a clear differentiation between "closed" and "open" situations.

Logically a "contextual" approach is only possible if there are known, finite contexts. This could serve as a clear, legally accurate and logical determination between a fact pattern as in SRB and other situations (especially data brokerage, online advertisement, device tracking and alike) where data is shared with thousands of recipients.

- → We strongly encourage the EDPB to highlight that in an "open" or "limitless" situation where recipients are not individually known, a controller is not realistically able to engage in an "contextual" assessment, as this would require reviewing limitless "contexts".
- → An assessment of unlimited or not fully known contexts must logically lead to an objective (or in the EDPB wording "simplified") assessment.
- → Consequently, a "contextual" assessment must be logically limited to situations where a finite, known number of entities will have access to personal data.

2.6. Positive knowledge and accountability of the controller

In a recent study, more than 80% of DPOs said, that any risk-assessment often results in a pre-determined outcome that favours the controller.[1] Even if the EDPB Guidelines would be "water tight", the reality is that millions of controllers would apply them without direct oversight and without external review – often under massive economic and internal pressure to declare the GDPR non-applicable. The urge to "look the other way" will be obvious and enormous.

The Guidelines also repeatedly acknowledge (e.g. paragraph 47) that it will be hard to even know about the capabilities of the various players and that controllers will be regularly unaware of the means and options other players have.

Furthermore, due to the uncertain character of the interpretation of "*identification of an individual is being insignificant in reality*", a lot of companies can claim that the GDPR does not apply to them, and engage in opaque processing operations. This, in turn, will give them the ability to operate with impunity until they are challenged and ordered to cease their actions. In order to bring such operations to a halt, the SAs would first have to engage in extensive fact-finding in order to establish the true likelihood that the contracting entity had of obtaining further information that would allow for the identification of data subjects. If this is done on a mass scale (which is likely given the economic incentive) enforcement of the GDPR would be made even more impossible.

One of the elements the GDPR provides to ensure that "biased" or "tilted" assessments are at least easier to discover and punishable is the requirement to keep clear documentation. While the Guidelines highlight the need to have a serious assessment and documentation (e.g. in paragraph 41), we would very much welcome to more explicitly section highlighting that such an assessment must be documented and controllers must be able to provide such an assessment to SAs (and ideally to data subjects, who would lose their rights over any inaccurate assessment).

For example, in paragraph 48 of the Guidelines, the problem is identified as a "risk" but the Guidelines seem to be silent as to where the assessment should default to if such a risk is present. It seems obvious that only the positive knowledge that identification is not realistically possible should allow to evade the GDPR. It seems to us that the Guidelines so far leave open if such knowledge must exist and partly even use wording that suggests that (to the contrary) knowledge that indicates *identifiability* must exist. In a context that often lacks detailed information, this would lead to a default of non-application of the GDPR. Naturally, this would lead to a huge incentive of controllers to try not to know about the detailed options listed in the Guidelines. Such an understanding seems unacceptable from a rule of law perspective.

Without knowing exactly what circumstances of "*identification of an individual is being insignificant in reality*" are, and that this can only happen in very rare cases, the contextual interpretation of the circumstances of a given company will lead to massive issues with burden of proof, which in the end will increase legal uncertainty, and weaken the protections that people are currently afforded under the GDPR.

- → We strongly encourage the EDPB to highlight that in line with the accountability principle (e.g. in Articles 5(2), 24 and 25 GDPR) the controller must be able to demonstrate any assessment that would follow that personal data is sufficiently anonymised. In practice, this requires positive knowledge of these facts, not mere speculation or guessing.
- → We strongly encourage the EDPB to use "negative" wording in the Guidelines (e.g. instead of "*is it possible*" use "*can it be ruled out that*") to underline that only positive knowledge of facts can be considered an element to evade the GDPR.

[1] https://noyb.eu/sites/default/files/2026-03/noyb-Survey_Evidence%20Based%20GDPR-Optimisation.pdf
See Page 8, 4th question.

2.7. Chains of controllers or entities

While a "contextual" approach seems manageable if one or maybe two controllers are at stake, many processing operations involve countless controllers and long chains of data sharing.

Usually, such situations lead to responsibility shifting, finger pointing or a "blame game" between entities. Especially in a situation where multi-factor "contexts" are assessed and if "open" and not only "closed" situations (see above at 2.4) are covered by the Guidelines, there is an enormous risk that the Guidelines will be violated, SAs have little options for enforcement and the data subject has no realistic recourse.

Typically, the law reacts to such situations with joint liability (see e.g. Article 83(4) GDPR). However, given that the "contextual" approach is new, and multi-party situations are inherent in this approach, we would welcome more guidance on the governance, liability and practical protection in (potentially endless) chains of controller.

We understand that the Guidelines foresee that inaccurate assessments would reflect back on a controller, but it seems hard to imagine how in a long chain of controllers the initial controller would e.g. know that the 10th controller down the line had a data breach or has a new technical ability that would allow identification.

- → We would welcome clearer guidance on situations where chains of entities process personal data and some entities within such a chain may be able to identify a data subject.
- → It seems unclear where the accountability and liability starts and ends, if a controller releases personal data under an exemption from the GDPR. Logically a controller making a "contextual" assessment would have to make such an assessment for the entire chain of entities (see above at 2.4 on the "open" and "closed" setting issue).
- → Such chains may not lead to a lack of accountability, especially in contexts that are complex, international or involve controllers with no realistic recourse (such as foreign governments or unlawful actors).

2.8. Lack of consideration of the logical consequences of the EDPB's approach

We note that a subjective approach can lead to logical "chick and egg" issues. The Guidelines seem to touch on this matter e.g. at paragraph 37 to 42, but it seems that many situations are not fully developed in the Guidelines, such as:

- When a third-party claims to not fall under Article 15 GDPR because in a "contextual" approach it wrongly claims to be unable to identify the data subject. In such a situation, it appears that the only recourse that a data subject has is to make access requests to the relevant controller that initially shared the data, however, given that the third-party claims that they cannot identify the data subjects, it would be impossible for the data subject to find any Article 15 GDPR recourse in the context of the aforementioned entity's processing operations. It is important to emphasise that this issue is not limited to access rights, but would logically expand to all rights in Chapter 3 of the GDPR and (in some jurisdictions) could lead to controllers even calling into question the jurisdiction of SAs. It would be crucial to determine that a controller has a duty to document and burden of proof when claiming that personal data was sufficiently anonymised (see e.g. Article 5(2) GDPR).
- Furthermore, it seems unclear how requirements in Article 32 to 34 of the GDPR will be applicable if the Guidelines on the one hand see them as a factors to consider if personal data is sufficiently anonymised (which is naturally an *ex ante* prediction) and on the other hand the application of the law, if *ex post,* such data is in fact leaked making it reasonably likely for hackers or powerful governments to be able to identify such data. Would the GDPR then apply

retroactively? Equally, would the assessment be "dynamic" if new technology, like AI or quantum computing, would make identification realistic?

- Many rules concerning multi-party situations (e.g. joint controllership or the controller – processor situation) could not work anymore. For example, a controller that cannot realistically identify a user, but forwards that information to a processor that has such capabilities could fall outside of the application of the GDPR, which in turn would mean that the processor would not be bound by a contract under Article 28(3) GDPR.
- Furthermore, if data had not been fully anonymised, issues with Chapter 5 would also become relevant. Particularly, as the relevant entities receiving the data are not covered by the GDPR, they are able to make transfers to third-countries, whereas the EDPB itself notes under paragraph 33, there can be evidence that the law would not prohibit re-identification. Although the EDPB does account for this in these Guidelines, further emphasis is needed to stress the severity of this scenario.

We are worried that controllers will overly quickly deploy a "contextual" approach, without taking into account what this would mean for other elements of the GDPR.

→ Especially if a clear difference between an "open" and "closed" situation (see section 2.4 above) would not be established in the Guidelines, the Guidelines would have to expand on how to deal with unavoidable "chicken and egg" problems as described above.
→ The Guidelines seem to lack sufficient explanation concerning what controllers ought to do in a dynamic reality, where assessments turn out to be wrong, where technology rapidly changes or business partners have strong incentives to make inaccurate claims. We would urge the EDPB to ensure that this (dynamic) reality is sufficiently reflected in the Guidelines and clear "fallbacks" towards an application of the GDPR are included.

3. Other individual elements to consider

In addition to the fundamental, conceptual elements highlighted above, we would like to draw your attention to the following individual elements of the Guidelines that may need improvement:

3.1. Paragraph 22 – *"insignificant in reality"*

While the CJEU has ruled repeatedly that the likelihood does not need to be zero, it should just be "*insignificant in reality*" (*OC v the Commission*[2] or *Breyer*[3]) what is noteworthy is that the cited cases the data in question was deemed to be personal data. In practice this means, that while the likeliness must not be zero, it must be – for a lack of another term – very close to zero.

The CJEU was merely stating that such a case – where the likelihood identification is insignificant in reality – can indeed exist. Thus, an exception or a theoretical possibility, rather than a rule.

We think this clear outcome in the case law should be reflected in the Guidelines, given that most controller will have a strong tendency to declare likeliness to be "*insignificant in reality*".

→ Thus, as mentioned in subsection 1.2. of this Feedback, we urge the EDPB to highlight the exceptional nature of the contextual approach in the context of the SRB ruling.
→ We would suggest to highlight that while the likeness must not be ***absolutely*** zero, it must be very close to zero. The current wording suggests more room for controllers than the case law.

3.2. Paragraph 29 ad 30 – *objective factors and relevant entities*

The Guidelines provide a list of objective factors that companies should use to identify the likelihood of identification of individuals. While we largely agree that these factors can be relevant, we would suggest to highlight more clearly (beyond "*including*") that these are merely examples.

We note that in combination of the relevant entities in paragraph 30 (e.g. law enforcement and the technical and financial options of a nation state or cybercriminals with vast technical options) with the objective factors in paragraph 29 would have to lead to a combined conclusion that identification is "*insignificant in reality".*

With these two paragraphs the EDPB is in practice opening up a two-dimensional grid of options where any combination that would make an identification possible would lead to the conclusion that the data is personal. This leads to a situation where a controller must conduct detailed due diligence of an entire supply chain. We note that this again (see above at 2.6) begs the question if positive knowledge and documentation of such facts is required or (as most controllers will choose in practice) mere assumptions or wishful thinking is sufficient.

→ In light of the multiple dimensions to be checked under the Guidelines, the question as to the need to have positive knowledge and documentation of these elements needs to be answered.

[2] Paragraph 51 of the CJEU – C-479/22 P – OC v European Commission.
[3] Paragraph 46 of the CJEU – C-582/14 – Breyer.

3.3. Paragraph 31 – *lack of motivation*

We note that the EDPB explicitly "cautions" against relying on any motivation as a factor in a contextual approach. However, we would suggest to make clear that this is simply not a reliable factor. Motivations change (e.g. when a fraud investigation is suddenly necessary) and motivations may be external or unforeseen (e.g. conflicts with employees, external investigations, new owners of a company). Furthermore the "motivation" of external players (e.g. hackers, governments) in any multi-party situation are basically impossible to capture.

→ We would suggest to make clear(er) that the (often self-declared) "motivation" of a controller or even a third party is not a relevant factor in the assessment.

3.4. Paragraph 33 - *legal limitations*

While we agree, that we should be able to "*generally assume that people will follow the law",* more than 275,000 GDPR complaints were launched the first year of the GDPR's applicability and billions in fines were issued. The law is the ideal outcome of compliance, but naturally people often do not follow the law. While the Draft Guidelines recognise this situation, we would like to point to the fact that, EU legal doctrine typically requires "law *and* practice" for any limitation on the processing of personal data to be relevant. One element that the Guidelines could highlight in paragraph 33 is the difference between serious criminal sanctions (e.g. jail sentences) and rather minor administrative fines (in the realm of a "speeding ticket").

→ We would suggest to clearly adopt the "law and practice" doctrine of the CJEU.
→ We would suggest to add examples of typical cases where law is not a relevant factor (e.g. non-EEA controllers, industry sectors with low compliance, known bypassing of the law [e.g. law firms accessing the government databases on an "honours system"][4] or controllers with a track record of limited compliance) as well as cases where it is a factor (e.g. a government database with strict regulations on access that are enforced by the relevant public body).

3.5. Paragraph 33 – *Example 8*

We note that the "learning" from Example 8 is that compliance with Article 32 GDPR would lead to a chance to argue anonymization. While this attempt to link security with anonymization may be charming, we note that security is typically not absolute and unlawful access it typically not the only way to access data – given that a media company may e.g. come under criminal investigations or be subject to libel lawsuits, which can trigger discovery requirements.

→ We would therefore suggest to adapt Example 8 to better reflect the multi-dimensional options of access.

[4] E.g. in Austria, registered address may only be accessed in case of legal disputes or enforcement actions, however it is generally known that law firms and other providers have access without needing to proof these factors and enforcement is factually almost impossible.

3.6. Paragraph 34 – *contractual limitations*

We welcome that the Guidelines note that purely contractual arrangements are not sufficient for the protection of personal data.

However, we would suggest to add that this conclusion is put a more solid basis, namely that the lack of third-party beneficiary clauses in most contracts makes them structurally unenforceable. Other then e.g. the SCCs, such contracts are not enforceable by the rights-holder (the data subject) and enforceability would hence hinge on a controller to take the risk, cost and effort to sue another business partner. Even if such clauses would be included, data subjects would have to be informed about rights generated via such contracts. The same problem of discretionary enforceability also concerns enforcement by SAs, which cannot directly enforce compliance with a contract.

Lacking such openly disclosed and enforceable third-party beneficiary clauses, contracts seem irrelevant in practice, because protections of data subjects may not be dependent on the various priorities of a controller.

→ We would suggest to add to the Guidelines that the lack of third-party beneficiary clauses and disclose of contracts to data subjects makes them structurally irrelevant.

3.7. Paragraph 35 – *dynamic situations*

We welcome that the Guidelines highlight the need to re-assess assumptions on anonymity. We also note the fast development of AI agents and powerful options that can increasingly combine multiple data sources in a matter of seconds. Many of the options that were so far too labour intensive have quickly become available to controllers, hackers or their parties.

However, the need to have a rather dynamic assessment opens another dimension of options that will be hard for controllers to manage in practice, as the already have to assess the various recipients and their various technical options. Logically also a time dimension is to be considered.

We would therefore suggest that the EDPB highlights the need to potentially also have some type of storage limitation as practical limitation of the dimensions in that an assessment must cover. For example, in the SRB ruling it was clear that the relevant data will only be assessed for a certain period, which did allow for a temporally confined contextual assessment.

→ We would suggest to highlight that a contextual assessment will be simpler if the relevant data is used for a limited time period. Unlimited usage will often make the assessment harder or even impossible as new technology (like AI, quantum computing and alike) will make many current assumptions obsolete.

We hope that this input is useful for your work!