30 October 2026

EBF_047104

EBF response to the European Data Protection Board's consultation on the draft Guidelines 02/2026 on Anonymisation

The European Banking Federation (EBF) welcomes the opportunity to provide a response to the European Data Protection Board's (EDPB) consultation on the draft Guidelines on Anonymisation, hereinafter – the Guidelines. In particular, we would like to draw the EDPB's attention on a number of points that merit further consideration in the final version of the Guidelines.

- **Ensuring alignment with applicable and future regulatory frameworks**

The Guidelines should form part of a coherent and integrated regulatory frameworks, taking into account both existing and future regulatory instruments, including the Digital Omnibus proposal[1].

Divergences in the interpretation of key concepts, such as anonymisation and pseudonymisation, between the Guidelines and the Digital Omnibus proposal could create significant legal uncertainty for concerned actors and undermine the consistent application of the relevant rules. Given that anonymisation assessments are sensitive to legal and factual developments, it is preferable to avoid finalising guidance that may shortly need to be revisited.

We therefore strongly recommend that the EDPB temporarily refrain from finalising the Guidelines until negotiations on the Digital Omnibus have concluded, or, at a minimum, include an explicit review clause (e.g., within 6 months of the Digital Omnibus being finalised) to ensure that the Guidelines can be reassessed and revised in a timely manner in light of the final legislative text.

- **Simplifying and structuring the Guidelines for greater clarity**

The complexity of the Guidelines risks creating significant legal uncertainty. While anonymization is a technically complex area, the Guidelines would benefit from being formulated in a manner that is directly accessible to the stakeholders concerned: lawyers, compliance officers, engineers and policymakers. The Guidelines, in their current form, do not provide a sufficiently clear and predictable framework on the criteria for anonymisation. It is therefore necessary that **the Guidelines be simplified and structured in a more pedagogical manner.**

- **Preserving a technology-neutral approach**

The Guidelines should reflect the technology-neutral approach of the GPDR, allowing organizations to select and adapt the methods and measures they consider most appropriate to the specific context and nature of their processing activities, thus also promoting innovation. A prescriptive approach could risk locking organisations into specific

[1] Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus).

practices or technologies, limiting their ability to adapt to technological developments and potentially discouraging the emergence and adoption of more efficient and privacy-enhancing solutions.

- **Promoting a predictable framework for innovation**

The Guidelines should avoid creating a framework under which anonymisation would become impossible to achieve. An overly restrictive or overly demanding approach could cripple innovation and reduce incentives to implement anonymization techniques.

Anonymization is an essential lever for reconciling the use of data for purposes, such as the development of artificial intelligence, in the context of a particularly dynamic competitive international landscape while respecting the rights and freedoms of the people concerned. Public authorities should encourage these practices, which would also contribute to European technological and economic sovereignty.

The Guidelines should therefore strike a pragmatic balance: they must set sufficiently robust standards to guarantee effective protection, while avoiding requirements that would make anonymisation inaccessible in practice.

2. Legal analysis

2.2 Identifying the applicable perspective(s)

The principles set out in **Paragraphs 11-15**, their interaction with the *SRB* judgment and the concept of "perspective" require further clarification. In particular, clarification is needed regarding which entity is responsible for identifying the relevant entities and from whose perspective anonymity should be evaluated.

Paragraph 15 states that the relevant perspective depends on who determines the purposes and means of the processing. This **statement**, however, **appears to be at odds with**:

1) **The definition of "perspective" provided by the EDPB in the glossary**[2], which does not consider the criteria of "*who determines the purpose and means of the processing*", but only "*the means reasonably likely to be used by that entity*".
2) **The CJEU *SRB* case**. According to the judgment, the classification of data as personal or not does not depend on the roles of the parties under the GDPR, but on an assessment of the means reasonably likely to be used by an entity. We also note that the Court did not address the qualification of the recipient as a processor, nor did it establish that information which is personal data for the controller must automatically be regarded as personal data for a separate entity acting on the controller's behalf.

Where the recipient has no realistic means of identifying the data subjects, receives no re-identification keys or supplementary information, and is contractually and technically prevented from obtaining them, the mere existence of such information in the hands of the controller should not automatically determine the qualification of the data in the recipient's sphere. If information that is effectively anonymous for the recipient must nevertheless always be regarded as personal data merely because another entity retains

[2] *Perspective: Each entity has a perspective, which will depend on their circumstances and informs the means reasonably likely to be used by that entity. If an entity has or may gain means reasonably likely to be used to identify the natural person to whom the information relates, the information can be said to be personal data from their perspective.*

reidentification capabilities, the practical added value of a perspective-based assessment is significantly reduced. In this regard, **anonymity should be assessed on a case-by-case basis, from the perspective of the entity for which the data is intended to be anonymous.**

This case-by-case assessment should also apply in the case of a controller-processor relationship. The current wording under Paragraph 15 – where the Guidelines assume that data shared with any entity acting on behalf of a controller (e.g., processor) remains personal data at all times, even if the processor cannot identify the individuals in the data set - replaces the factual assessment of identifiability required by Recital 26 with a status-based assumption linked solely to the contractual relationship between the parties. It also raises practical questions regarding the processor's ability to comply with its obligations under the GDPR. If the processor genuinely receives information that does not allow identification of data subjects and has no realistic means of obtaining the missing information, it is unclear how the processor could meaningfully assess the impact of a personal data breach, identify the categories of affected data subjects, support the controller in handling data subject requests, or otherwise perform obligations that presuppose the existence of personal data from the processor's own perspective. These practical implications further support the need for a case-by-case assessment of anonymity, based on the means reasonably likely to be used by the recipient and its actual ability to identify individuals, rather than on a presumption deriving solely from its status as a processor acting on behalf of a controller.

That being said, the assessment of anonymity should be distinguished from the controller's own determination as to the status of the transferred data and compliance with its GDPR obligations. In other words, where the parties disagree on the classification of the data or where the controller decides to continue treating the data as personal data, the controller's determination as to the status of the transferred data should prevail over that of the recipient (including the processor).

Relevant perspective in a chain of processing

Under Paragraph 11, the sentence *"[t]he goal of anonymisation should be to ensure that the resulting data is anonymous for all of the relevant entities concerned by the assessment"* would also benefit from further clarification.

In practice, different entities involved in a **processing chain** may have different means reasonably available to identify individuals. For example, an IT outsourcing arrangement, the customer acting as a controller may retain a key or additional information enabling re-identification of data subjects, whereas the IT supplier and its subcontractors have no access to such information. In this scenario, the data may be effectively anonymous from the perspective of the supplier and its sub-processors, but not from the perspective of the customer.

Following the SRB case, **we recommend that the Guidelines adopt a case-by-case assessment to anonymity in processing chains, taking account of the circumstances and means reasonably available to each relevant entity, rather than requiring the data to be anonymous for all entities collectively**. In particular, the fact that data remain personal data for the controller should not automatically mean that they must also be treated as personal data by an IT supplier that has no reasonable means of re-identification. At the same time, the controller should remain responsible for complying with its own GDPR obligations, including transparency requirements concerning the processing.

Relevant perspective in a group of companies

The Guidelines deal with the issue of "perspective" mainly through bipartite examples (independent controller/third party, manager/subcontractor), but do not provide a framework for enterprise group architectures. As a result, a company structured as a group has no framework to determine whether data anonymized by one entity can be processed as such by another entity of the same group, which complicates the articulation with intra-group processing and creates a risk of divergent interpretations between national supervisory authorities of the different countries of establishment.

We recommend that the Guidelines clarify that, **where several legal entities within the same group act separately/as separate controllers, identifiability is to be assessed for each entity individually**, having regard for the additional information and means of identification that the entity itself may lawfully and realistically access regardless of the existence of a shared group infrastructure. The Guidelines should further clarify that, **where the receiving group entity has no means reasonably likely to be used to re-identify the data** (e.g., legal restrictions via Inter-Company Agreements), **for the receiving party the information received does not constitute personal data**.

We note, however, that if there is a legitimate need later on, the group may share the identifiable data; however, in such circumstances, the recipient would be processing personal data.

To conclude this section on the relevant perspective, we note that there may be situations where the entity conducting the assessment may not have access to all the necessary information and evidence. We would therefore welcome **clarification from the EDPB on how this assessment can be carried out with sufficient certainty in the absence of complete information and evidence**.

2.3 Whether the information "relates" to a natural person

Paragraph 17 appears to conflate the requirement that information "*relates to*" a natural person with the separate requirement that the person be identifiable ("*Information may relate to a person even if it is not readily apparent that it does so,* ***or if some additional processing is necessary to reveal that link****"*). The purpose of this test is to determine whether the information concerns a person – that is, whether there is a substantive link between the information and that person – not whether the person can be identified/singled-out. **We therefore recommend deleting this reference from Paragraph 17**.

Beyond this conflation of distinct requirements, the reference to "*many techniques*" suggests a more absolute approach. It follows from this paragraph that the entity must assess whether a technique capable of revealing information about one or more individuals from aggregate data could be used by a relevant entity. This assessment is particularly difficult to carry out in practice, as the entity may not have access to all the information required to reach a reliable conclusion. Moreover, given the rapid pace of technological development and the increasing availability of such technologies, those could arguably be used in the vast majority of cases, meaning that information may always relate to a natural person. This is an overly restrictive and impractical approach for businesses.

2.4 Whether the natural person is "identified or identifiable"

Paragraphs 20-22 and 26-29 would benefit from further clarification regarding the threshold for indirect identifiability. While the Guidelines recognise that information held by different entities may be combined, they do not sufficiently explain

what degree of practical accessibility to supplementary information should be demonstrated before an individual is considered identifiable from a particular entity's perspective. Specifically, it should not be sufficient that another entity, such as the controller, retains the ability to identify the data subjects. The assessment should establish whether the recipient itself can, either directly or through a realistically plausible chain of actors, access supplementary information and use it effectively for identification purposes.

This distinction is especially important where the controller retains re-identification capabilities while the recipient has no access to the underlying identifiers, keys or source data. In this respect, **the concept of "*means reasonably likely to be used*" should not be interpreted as encompassing any theoretical possibility of obtaining additional information.** Rather, consistent with Recital 26 GDPR and the reasoning in *Breyer*, the assessment should determine whether there is a concrete and credible identification pathway, including a realistic prospect that the relevant steps would actually be taken. The test concerns means reasonably likely to be "used", NOT every means that is technically or theoretically available. **The existence of a purely hypothetical route to identification should not, in itself, be sufficient.**

Recommendations:

The Guidelines should **clarify that indirect identifiability requires a concrete and credible chain of access to supplementary information**, taking into account the legal ability to obtain it, the practical feasibility of doing so, the effectiveness of the identification process and the likelihood that these steps would actually be carried out in practice.

Furthermore, **where the controller deliberately structures the arrangement so that the recipient has no access to identifiers, source data or re-identification keys, and is contractually prohibited from attempting to obtain such information, this should be taken into account when assessing the practical likelihood of identification**. The issue is not whether contractual safeguards alone conclusively determine anonymity, but whether legally enforceable restrictions are given appropriate evidential weight in assessing the means reasonably likely to be used. The possibility that a contract might be later be amended, waived or breached should not negate an effective present restriction; a material weakening of the controls should instead trigger reassessment.

We would also appreciate some **clarification on the scope of Paragraph 21**. Read together with paragraphs 20 and 28, it may be understood that the transfer to a recipient capable of identification forms part of the transferring entity's "means reasonably likely to be used" (or "chain of means"). However, paragraph 21 does not make this reasoning explicit and could also be read as attributing the recipient's identifying capabilities to the transferring entity irrespective of whether those capabilities form part of the latter's means. Therefore, it is unclear from the text whether the assessment is limited to the data transfer between an entity and a third party, or whether the entity should also take into account any subsequent transfer by that third party. In other words, **is a controller expected to assess the entire chain of transfers?** Where would its responsibility end?

In practice, it may be **extremely difficult to determine whether an entity has the means reasonably likely to identify a data subject indirectly**, particularly if the controller is required to assess the means available to every entity in a transfer chain.

Such requirement could severely restrict the ability to transfer anonymized data to third parties.

Recommendation:

We ask the EDPB to **clarify the scope of the controller's assessment and responsibility** and ensure that the standard remains proportionate and workable in practice.

Paragraph 22 (particularly when read in conjunction with Paragraph 35) **raises questions regarding responsibility and the temporal durability of anonymisation**. A level of anonymisation considered sufficient ten years ago may no longer be acceptable twenty years from now.

- Does paragraph 22 require each entity to verify continuously that data remain genuinely anonymous?
- Would an entity be held responsible for failing to notify the original controller that the effectiveness of the anonymisation has deteriorated, for example because the technique used has become obsolete?
- Which entity bears responsibility for ensuring that the data remains anonymous, and for implementing the measures needed to preserve that anonymity? Do those measures meet the standard of technical measures reasonably required to maintain anonymity?

The Guidelines should avoid requiring organisations to assess remote or speculative technological developments. Reassessment should instead be proportionate and triggered by a material change that is reasonably capable of affecting identifiability.

2.4.2 Means reasonably likely to be used

Paragraph 28 introduces the concept of "*chain of means*". The way we understand this test (particularly when read in conjunction with Example 7[3]) is that a means is reasonably likely to be used when the entity could, in theory, call on a competent third party to carry it out in its place. This reasoning, taken to its conclusion, makes almost any anonymised data potentially reidentifiable since there is almost always a technical service provider on the market capable of lifting a pseudonymity with sufficient means or future technologies.

A bank sharing anonymized data with a business partner (insurer, broker, payment platform) can never completely rule out the use of a service provider specializing in re-identification; the anonymization documentation therefore becomes structurally fragile, regardless of the care taken in anonymization, which discourages data sharing that is compliant in practice.

Recommendation:

The Guidelines should **clarify that the possible use of a third party is relevant only where objective facts support a concrete and credible identification pathway and a realistic prospect that the third party would actually be engaged. The**

[3] "*The controller knows that their business partner would not itself be able to perform this re-identification technique. However, **they could easily hire a third party to do it**. That technique therefore still qualifies as a means reasonably likely to be used by the business partner*."

existence of a capable provider in the market should not, by itself, satisfy the Recital 26 test.

We would also like to make the following observations regarding Paragraph 29

- Cost and time are recognised as objective factors when assessing the means reasonably likely to be used to identify an individual. However, Paragraph 92 appears to significantly limit the relevance of those factors by stating that technological identification techniques, including AI-based techniques, are becoming increasingly accessible at a lower cost.
- The requirement to assess the means reasonably likely to be used to identify an individual based on "*reasonably foreseeable technological developments*" appears difficult to implement in practice. We would welcome guidance or examples to assist controllers in respecting this requirement.

The Guidelines would also benefit from further **clarification regarding the circumstances in which an entity should be considered relevant for the anonymity assessment**. While **Paragraph 30** and following refer to a broad range of actors, including private individuals, malicious actors and other third parties, it remains **unclear what objective criteria should be applied to determine whether such actors must actually be taken into account in a specific assessment**.

Organizations should not be expected to consider categories of actors solely on the basis of theoretical possibilities. Rather, an entity should be regarded as relevant where objective elements indicate that it could realistically gain access to the dataset, obtain the supplementary information necessary for identification, or otherwise participate in a credible re-identification scenario.

Recommendation:

We would welcome **additional guidance on the threshold for relevance and on the level of documentation expected from controllers**. This would help promote greater consistency, legal certainty and accountability in the practical application of the Guidelines.

We further highlight that requiring organisations to assess whether cybercriminals or any other malicious actors (such as foreign intelligence agencies or unethical companies) could gain access to a dataset sets an impractical and potentially open-ended standard. Organisations cannot reliably anticipate the capabilities, intentions, or unlawful methods of unknown malicious actors. Without clear and objective parameters, this requirement creates significant legal uncertainty and may lead organisations to treat virtually all datasets as personal data, even where robust security measures are in place. We therefore urge the EDPB to take a pragmatic approach.

More specifically, **the Guidelines should clarify that the mere possibility that a cybercriminal or another unauthorized actor could access the data is not, in itself, sufficient to exclude anonymity from the recipient's perspective**. Such actors should only be taken into account where objective factors demonstrate a realistic likelihood that they could: (i) access the dataset held by the recipient, (ii) obtain the supplementary information retained separately by the controller, and (iii) effectively combine those elements in order to identify the data subjects. This would ensure that the assessment

remains aligned with Recital 26 GDPR, which is based on means reasonably likely to be used and on a realistic rather than purely hypothetical probability of identification.

Additional clarification appears necessary regarding the other categories of actors listed in Paragraph 30, such as friends, relatives, neighbors or other people who may possess supplementary information about the individual. While such actors may theoretically contribute to identification, it is unclear how controllers or recipients could reasonably assess their relevance in practice. In particular, the Guidelines do not explain how an organization should identify such persons, determine what information they possess, or assess their potential role in a re-identification scenario. **An interpretation requiring organizations to consider undefined groups of private individuals would risk creating an assessment that is difficult to apply in practice and highly speculative**.

Furthermore, **the analysis should distinguish between disclosures to independent third parties and processing carried out by a service provider under a contractual arrangement**. In the latter case, the relationship is typically governed by a combination of technical, organisational and contractual measures specifically designed to prevent re-identification. For example, the controller may retain exclusive control over identifiers, source data and re-identification keys, while the recipient is technically unable and contractually prohibited from obtaining supplementary information. While contractual measures alone cannot determine anonymity, such safeguards remain relevant objective factors when assessing whether a chain of identification is realistically available and reasonably likely to be used in practice. The Guidelines could therefore **clarify that the assessment should focus on realistic and objectively substantiated re-identification scenarios**. Otherwise, there is a risk that purely hypothetical possibilities, involving actors who are unlikely to obtain access to both the dataset and the supplementary information required for identification, lead to an overly broad interpretation of identifiability that is difficult to reconcile with Recital 26 GDPR and the requirement that the means be reasonably likely to be used.

Finally, we highlight that controllers should not be required to account for every hypothetical risk arising across an unlimited chain of downstream recipients. Their assessment should be limited to risks that are reasonably foreseeable in the specific context of the data-sharing arrangement.

We note that **Paragraph 33** appears to establish a rebuttable presumption ("*The general assumption that people will follow the law can, therefore, be rebutted if (...)"*), to be assessed in light of (1) the effectiveness and deterrent effect of legal prohibitions; (2) the balance between the expected gains and the costs or risks involved; (3) the vulnerability of the data to unlawful access; and (4) evidence of comparable breaches. **The assessment required under Paragraph 33 appears disproportionate, if not impossible, to carry out in practice**. How can an entity demonstrate that the sanctions applicable under, for instance, French law are sufficiently dissuasive? Shouldn't this issue be addressed through technical security measures instead?

The reasoning provided under **Example 8** ("*Since the media company's out-of-date security measures mean that those third parties could also likely hack into the media company's servers [...] The media company therefore decides that it will upgrade its network security before re-testing the anonymity of the data*") creates a potentially endless loop without a clear resolution. Even where entities have implemented all reasonable

measures to preserve the anonymity of the data, any subsequent reassessment may lead to the same inconclusive outcome.

The position may be different where data have been anonymised solely for the purpose of a transfer, while the underlying non-anonymised data remains accessible on the entity's servers. In that situation, the relevant question is not simply whether the data is anonymous, but from what point in time, from whose perspective and for what purpose they may be regarded as anonymous.

Many entities anonymise data specifically for transfer purposes. The Guidelines should clarify whether the continued availability of the source data in non-anonymised form before or outside the transfer is sufficient to deprive the transferred dataset of its anonymous nature. **Data cannot realistically be expected to be anonymous in absolute terms, at all times and in every possible context. The Guidelines should therefore provide a clear, workable, and context-specific standard for assessing anonymity**.

Paragraph 35 recommends **periodically reassessing the risk of re-identification over time**. While this is presented as good practice, this would **shift anonymisation to an ongoing compliance obligation**. Organisations would be expected to demonstrate, and periodically reassess, that datasets remain anonymous as technologies and re-identification capabilities evolve.

While a forward-looking approach is understandable, particularly from a risk management perspective and in light of technological developments, **the proposed standard creates significant legal uncertainty and a substantial operational burden for businesses**. Effective implementation would require continuous monitoring, dedicated expertise, governance arrangements and additional resources to navigate the different assessment approaches.

Paragraph 35 creates legal uncertainty as to how the classification of data may evolve over time, the expected frequency of reassessments, triggering events requiring reassessment and proportionality considerations based on the nature of the dataset and processing activities. No controller can continuously monitor developments in information and communication technologies. Moreover, any requirement to update the classification of data shared with a partner would place a significant burden and potential liability on the controller, which would be expected to keep pace with technological developments.

This provision would impose a significant operational burden on companies, requiring them to periodically reassess datasets previously considered anonymous and to adapt their compliance processes as re-identification risks evolve. Without clearer, more practical and pragmatic safeguards, this approach risks adding further complexity to GDPR compliance for European organisations.

Recommendation:

Consistent with the principles of accountability and proportionality, the Guidelines should clarify that **reassessments should be performed on a risk-based basis and whenever a material change occurs that may affect identifiability**, such as changes to the dataset or its outputs, access by the recipient to new supplementary information, developments in re-identification techniques, or security incidents.

2.5.1 Datasets containing a mix of anonymous and personal data

With reference to **Paragraph 36**, the Guidelines retain a strict position where datasets contain a mix of anonymous and personal data: "*the dataset as a whole should only be considered anonymous if the anonymisation is effective for all of the included individuals*". This requires the likelihood of re-identification to be insignificant for all of these individuals. However, where a dataset contains some records mixing personal and anonymous data, the entire dataset must be treated as personal data unless the records are separated and can be treated distinctly. **We stress that for large or complex datasets, such record-by-record assessment would create a significant operational burden and may be technically unworkable.**

2.5.2 GDPR compliance and the anonymisation process

Paragraphs 35 and 37-42 could benefit from further clarification regarding the allocation of responsibilities where information remains personal data from the controller's perspective but is anonymous from the recipient's perspective. Where a service provider receives information that is effectively anonymous from its own perspective, the fact that Article 28 GDPR may not apply should not affect the controller's obligations, in relation to the processing activities performed prior to the disclosure of the dataset.

In particular, the controller remains responsible for the selection, extraction, pseudonymization, anonymization and disclosure of personal data and must ensure that such processing is carried out on a valid legal basis and in accordance with the principles of transparency, data minimization, security and data protection by design and by default. The controller should also document, in line with the accountability principle under Article 5(2) GDPR, the reasons why the recipient does not have means reasonably likely to be used to identify the data subjects. Paragraphs 37-41 already recognize that data may remain personal from the controller's perspective while being anonymous for the recipient and that the anonymization process must be lawful, transparent and appropriately documented.

It may therefore be useful to clarify that the non-application of Article 28 GDPR, where information is anonymous from the recipient's perspective, does not limit the controller's obligations in respect of the personal data processing carried out before disclosure. Rather, the controller should remain responsible for documenting the effectiveness of the anonymization measures, demonstrating that the recipient lacks realistic means of identification, and reassessing that conclusion whenever material changes occur. Should the recipient subsequently acquire means reasonably likely to be used to identify data subjects, the relationship could then be re-evaluated and, where appropriate, brought within the scope of Article 28 GDPR.

Paragraph 40 states that, in complying with their transparency obligations regarding the anonymisation process, controllers "*should not use descriptions like "anonymous", "de-identified" or "de-personalised" if individuals are actually still identifiable*". The Guidelines should clarify what terminology controllers should use in such circumstances if not the above.

3. The Technical Analysis of Anonymisation

3.2 Approaches to the assessment

The Guidelines require organizations to consider not only their own capabilities but also the capabilities of third parties and other actors that may access complementary

information. While this **contextual approach** strengthens privacy protection, it also **raises concerns regarding legal certainty and practical implementation**:

- It may fail to provide sufficient legal certainty due to complexity of the assessment and its implementation in practice, and as a result of the acknowledged risk of false positives, which may undermine confidence in the outcome of the assessment.
- It may create legal and operational uncertainty where organizations have limited visibility over external datasets or third-party data practices.

Clarification on the expected level of due diligence and reasonable assessment would help organizations apply this approach more consistently.

We also highlight that **the simplified approach, as described under Paragraph 48, does not appear to be genuinely simplified, but rather based on the entity's available means**. Where an entity cannot verify that the data has been properly anonymised, the lack of means to verify anonymity effectively requires it to treat the data as non-anonymous to ensure compliance with the GDPR. This raises a further question: if the entity cannot determine whether the data is anonymous, why is the data transferred to or processed by that entity if it cannot use them?

Moreover, **footnote 36** appears to attribute a specific evidential value to the simplified approach by stating that it may be used by controllers to demonstrate that information is anonymous, while not allowing third parties to rely on the same approach to demonstrate the opposite. It would be helpful to clarify the legal basis for this distinction and the intended legal effect of the simplified approach, particularly in light of paragraph 48 stating that it is not an alternative legal standard.

3.4.3 No Inference

The Guidelines introduce a particularly **demanding interpretation of the "No Inference" criterion** and a methodology for assessing it that appears significantly more complex than the methodologies proposed for the No Record Isolation and No Linkage criteria. In particular, distinguishing between meaningful and non-meaningful inferences, while also considering secondary or recursive inferences, may prove difficult to apply consistently in practice.

While its objective is understandable, it remains unclear how organizations can practically demonstrate that no information relating to an individual can be inferred from a dataset, especially considering the increasing capabilities of advanced AI models and inference techniques. Moreover, read literally, the recommendation to analyse whether an inference may itself generate further inferences could result in an open-ended or recursive analytical process with no clear stopping point.

Additional guidance, examples, and objective assessment criteria would be welcome to ensure a consistent and proportionate application of this requirement across organizations and sectors. As regards the potentially recursive "no inference" check, the Guidelines should clarify when controllers may reasonably conclude that the assessment is complete, for example by introducing a practical threshold based on the likelihood that further inferences could realistically be generated and used for re-identification.

We would also welcome if the EDPB could provide guidance on how synthetic data should be assessed and, in particular, how organisations can demonstrate that synthetic data generated from personal data has been effectively anonymised.

3.5 Applying the criteria

3.5.2 Assessing the criteria under the contextual approach

Paragraph 92 mentions that "*Most currently documented (re-) identification techniques are becoming increasingly accessible [...]*". We would welcome if the Guidelines could specify which re-identification techniques they are referring to.

3.5.3 Compiling the results

The combined application of the "No Record Isolation", "No Linkage" and "No Inference" criteria may present significant implementation challenges for datasets commonly used in the financial sector.

For example:

- Financial transaction datasets may contain unique behavioural or transactional patterns, making the complete elimination of record isolation difficult without substantially reducing the usefulness of the data
- Financial ecosystems frequently involve interconnected datasets, third-party actors and shared information, which may make the complete exclusion of linkage risks difficult to assess in practice
- Measures required to satisfy anonymisation requirements may, in some cases, reduce data quality to a level that limits legitimate uses such as fraud detection, analytics, model development or innovation activities.

Given the particular characteristics of financial transaction data, **the Guidelines would benefit from additional sector-specific examples illustrating the practical application of "No Record Isolation", "No Linkage", and "No Inference" in banking, payments, fraud prevention, analytics and AI-related use cases**. Such examples would significantly improve legal certainty and facilitate consistent implementation across the financial sector.

We also highlight that **Paragraph 52** states that violating a criterion "*does not necessarily mean*" the data is personal data and that, on any violation, it is necessary to continue the analysis. However, the table under Paragraph 97 appears to treat a No Inference violation as final, and offers a second-chance step only for the No Record Isolation criterion. Annex 1 also shows this difference: a "specific and meaningful inference" leads straight to conclusion of personal data, and No Linkage is dealt earlier in the process (by extending the data and then re-testing) rather than through a separate step. It might be helpful for the Guidelines to make this reasoning explicit in the main text: a specific and meaningful inference is, by definition, already personal data, and the analysis should therefore end at that point.

Paragraph 98 states that "*If the data violates the No Record Isolation criterion, it should be checked if the isolated records allow for singling out that individuals are distinguished from others by matching those records with the individual's corresponding attributes.*" In practice, the isolation or non-individualisation criterion is extremely complex to apply and significantly limits the circumstances in which data may be considered anonymous. The definition of the isolation criterion also lacks clarity. Paragraph 98 adds a requirement to assess whether an isolated data point enables singling out, although this element is not clearly reflected in the initial definition in section 3.4.1. Under that initial definition, the criterion appears to be met as soon as isolation is possible.

Paragraph 99 also acknowledges that a unique record may remain anonymous if it does not enable an individual to be distinguished. Could the EDPB clarify whether the concept of singling out should be assessed under the inference criterion instead?

The purpose of the provision under **Paragraph 100** is unclear. Does the EDPB mean that an entity using the simplified approach may subsequently supplement its assessment with the contextual approach? If so, the Guidelines should clarify whether this additional assessment is optional or necessary, and whether the contextual approach is sufficient on its own.

Annex 1: Flowchart for the technical analysis of anonymity

The practical differences between the simplified and contextual approaches are not clear from the flowchart. The only apparent difference between the two approaches lies in the initial assumption regarding the status of the data:

- Under the contextual approach, the data is initially assessed as anonymous, and their anonymity is then verified; while
- Under the simplified approach, the data is initially regarded as personal and may be treated as anonymous only if each relevant criterion is satisfied.

ENDS

For more information:
Rachele Ceraulo
Policy Adviser – Data & Innovation
r.ceraulo@ebf.eu

About the EBF

The European Banking Federation is the voice of the European banking sector, bringing together 32 national banking associations in Europe that together represent a significantmajority of all banking assets in Europe, with 3,500 banks - large and small, wholesale and retail, local and international – while employing approximately two million people. EBF members represent banks that make available loans to the European economy in excess of €20 trillion and that reliably handle more than 400 million payment transactions per day. Launched in 1960, the EBF is committed to a single market for financial services in the European Union and to supporting policies that foster economic growth

www.ebf.eu @EBFeu