Telefónica comments on EDPB Draft Guidelines 02/2026 on Anonymisation

EU Transparency Register Number: 52431421-12

October 2026

Introductory Comments

Telefónica welcomes the opportunity to respond to the European Data Protection Board's draft Guidelines 02/2026 on Anonymisation and its intention to provide greater clarity on the assessment of anonymous data. Anonymisation is an important tool for protecting individuals while enabling the responsible use of data. Clear and practical guidance can help organisations develop services, conduct research and improve technologies while reducing the need to process personal data.

We believe that anonymisation plays a particularly relevant role in the telecommunications sector, where data can support network planning, service quality, mobility analysis and the development of artificial intelligence. A framework that recognises the effectiveness of appropriate technical measures and the circumstances in which data is used can support these activities while maintaining a high standard of protection for individuals.

In this document, Telefónica expands on four aspects of the draft Guidelines that would benefit from further clarification: 1) the distinction between isolating a record and singling out an individual; 2) the role and perspective of processors; and 3) the recognition of anonymisation as a process that may involve several stages over a significant period of time; and 4) Unlawful means of obtaining additional information for re-identification. We encourage the EDPB to address these aspects through consistent terminology and practical examples that provide useful guidance for supervisory authorities, organisations and individual

1.1.- Clarify the relationship between record isolation, singling out and identifiability

Telefónica recommends that the EDPB further clarify the relationship between **record isolation**, **singling out** and **identification/identifiability**. While these concepts are closely related, the Guidelines appear to treat them as distinct steps in the assessment and they should therefore not be used interchangeably.

This clarification is particularly important in light of the terminology previously used in **WP29 Opinion 05/2014 on Anonymisation Techniques**. That Opinion defined *singling out* as "the possibility to isolate some or all records which identify an individual in the dataset". The draft Guidelines now introduce **"No Record Isolation" as a separate criterion**, while subsequently assessing whether an isolated record may also allow an individual to be *singled out*. The distinction is not entirely clear throughout the Guidelines. Paragraph 54 states that "[a] common

method used to distinguish individuals from others [...] is by singling them out", before introducing record isolation as a distinct concept. This ambiguity is compounded by the fact that the Guidelines appear, in places, to equate identifying a person with distinguishing that person from others, while subsequently presenting singling out as a means of making that distinction. This leaves unclear whether identification and singling out are intended to represent distinct concepts or effectively the same threshold. In turn, paragraphs 98-100 appear to indicate that failure to meet the No Record Isolation criterion does not, in itself, establish that an individual can be singled out. Rather, a further assessment is required to determine whether the isolated record can be matched with corresponding attributes of an individual so as to enable singling out. Telefónica understands this to suggest a conceptual sequence along the following lines:

record isolation → possibility of singling out → identifiability

rather than:

record isolation = singling out = identifiability.

If this understanding is correct, Telefónica recommends that the EDPB states this distinction expressly and consistently throughout the Guidelines. However, this conceptual sequence is not sufficiently clear in the current draft, which at times appears to use these terms interchangeably.

In particular, the Guidelines should clarify whether record isolation refers merely to the technical possibility of isolating a unique record within a dataset, whereas singling out requires an additional ability to relate that record to attributes corresponding to a particular individual. In particular, the Guidelines should clarify whether record isolation refers merely to the technical possibility of isolating a unique record within a dataset, whereas singling out requires an additional ability to relate that record to attributes corresponding to a particular individual, which requires to test another of the three mentioned criteria. If so, this would appear to equate singling out with identification, although the two concepts are not necessarily equivalent. The Guidelines should therefore also clarify what distinguishes singling out from identification.

Also the Guidelines should then explain how singling out relates to the broader legal test of identifiability under Article 4(1) and Recital 26 GDPR, taking into account the EDPB's explanation that identification entails distinguishing an individual from others within a given context in a manner that makes it possible to treat that individual differently.

Paragraph 99 appears particularly important in this respect. It recognises that a record may be unique and therefore fail the No Record Isolation criterion while the data may nevertheless remain anonymous where the isolated record cannot be

related to an individual in a manner enabling singling out or differential treatment. This suggests that **uniqueness or record isolation should not, by itself, be regarded as sufficient to establish identifiability**.

Greater conceptual clarity would be particularly valuable in the telecommunications sector, where datasets routinely contain technically unique records without necessarily providing a realistic means of identifying or acting upon a particular subscriber.

For example, a network-performance dataset may contain a unique record corresponding to a particular combination of timestamp, cell sector, device characteristics and network-performance indicators. That combination may allow the record to be isolated from all other records in the dataset. However, where subscriber identifiers have been removed and the recipient has neither access nor reasonably likely access to the information required to associate that network event with a particular subscriber, the mere uniqueness of the record should not automatically mean that the subscriber has been singled out or is identifiable.

Similarly, an aggregated mobility dataset may contain a unique mobility pattern or sequence of interactions with network cells. The fact that a particular pattern can be distinguished from all other patterns in the dataset establishes technical uniqueness, but does not necessarily establish that the recipient can associate that pattern with a particular natural person or use it to treat that person differently. Whether this amounts to singling out or identifiability should depend on the additional information and means reasonably likely to be available to the relevant entity.

The distinction may also be relevant where anonymised telecommunications data is shared with a third party subject to technical, contractual and organisational restrictions preventing access to subscriber-identification information. A record might remain technically unique within the disclosed dataset, while the recipient has no realistic means of connecting it to the corresponding subscriber. Treating record isolation alone as equivalent to singling out or identifiability could therefore lead to datasets being classified as personal data solely because they contain

unique records, irrespective of whether identification is realistically possible in the circumstances.

Such clarification would improve legal certainty and avoid interpreting technical uniqueness as being automatically equivalent to the legal concept of identifiability under the GDPR.

1.2 The role of processors in the anonymisation process

Telefónica welcomes the contextual approach adopted by the EDPB, under which the same information may be personal data for one entity while being anonymous for another, depending on the means reasonably likely to be used by each entity to identify the individual.

However, Telefónica considers that further clarification is needed regarding the application of this approach to processors.

The Guidelines state that, where an entity processes information on behalf of another entity, the assessment of whether the information constitutes personal data should be made from the perspective of the controlling entity. The EDPB justifies this approach by the need to prevent controllers from avoiding GDPR protections by outsourcing processing activities to third parties.

Telefónica fully agrees with the underlying objective that a controller should not be able to circumvent its obligations under the GDPR merely by outsourcing processing activities. However, this anti-circumvention objective should be distinguished from the separate legal question of whether the information constitutes personal data from the recipient's perspective.

The essential point is that qualification as a processor presupposes the processing of personal data. Under the contextual approach, where a service provider has no means reasonably likely to be used to identify the individuals concerned, the information may be anonymous from its perspective. In Telefónica's view, the provider should therefore be regarded, in respect of that processing activity, as a recipient of non-personal information rather than as a processor under the GDPR, even though it performs the service on behalf of an entity for which the information remains personal data. Acting on another entity's instructions should not, in itself, establish processor status where the information being processed is not personal data from the service provider's perspective.

The assessment should therefore avoid circular reasoning: an entity should not first be classified as a processor merely because it acts on behalf of a controller, and then be deemed to process personal data solely because it has been classified as a processor. Rather, the relevant question should remain whether the recipient has,

taking into account all objective factors and the circumstances of the processing, means reasonably likely to be used to identify the individuals concerned. That assessment should inform whether the recipient qualifies as a processor for the activity in question.

This is particularly relevant where the controller has implemented effective technical and organisational measures before disclosure so that the processor does not receive the additional information necessary to identify the individuals and has no realistic means of obtaining it.

Otherwise, the same dataset could have a different legal character for the same recipient solely because of the legal qualification of the relationship between the parties. For example, a dataset received by an entity acting for its own purposes could potentially be anonymous from that entity's perspective, whereas the identical dataset, subject to the same technical safeguards and identification capabilities, would necessarily constitute personal data where that entity performs the same operation on behalf of a controller.

In such circumstances, neither the content of the dataset nor the recipient's technical capacity to identify individuals has changed. The only difference is the legal role attributed to the recipient.

Telefónica considers that this result requires further justification in light of the contextual approach to identifiability and the Court's case law.

In **EDPS v SRB (C-413/23 P),** the Court confirmed the importance of assessing identifiability having regard to the relevant circumstances and recognised that pseudonymised information does not necessarily constitute personal data in all cases and for every person. The fact that information remains personal data for the disclosing entity should therefore not automatically determine its status in the hands of every recipient.

This does not mean that outsourcing should enable the controller to escape its own GDPR obligations. Those obligations should continue to be assessed from the controller's perspective where appropriate. Rather, the “classification of the data in the hands of the recipient”” should remain conceptually distinct from the question of which obligations continue to apply to the controller.

This distinction would also create appropriate incentives for controllers to apply robust data minimisation and anonymisation measures before making data available to service providers. Where a controller removes identifiers, retains the information necessary for re-identification within its own environment, and implements effective technical, contractual and organisational barriers preventing

the service provider from accessing that information, those safeguards should be relevant to the assessment of identifiability from the recipient's perspective.

A telecommunications operator may engage a specialised provider to analyse network performance. Before transferring the dataset, the operator removes subscriber identifiers such as names, MSISDNs, IMSIs and customer IDs and retains the mapping information exclusively within its own systems.

The service provider receives only technical network information necessary to perform statistical or performance analysis and is technically and contractually prevented from accessing subscriber databases or other information that would enable it to associate the records with individual customers.

From the operator's perspective, the information may remain personal data because the operator retains additional information enabling it to reconnect particular records with subscribers.

However, from the service provider's perspective, identification may be impossible in practice or involve means that are not reasonably likely to be used.

If the same dataset, with the same safeguards, were provided to that company for its own purposes, the contextual approach could potentially lead to the conclusion that the data are anonymous for that recipient. It is therefore unclear why the assessment of identifiability should necessarily produce the opposite result solely because the recipient performs the analysis on behalf of the operator.

Telefónica therefore recommends that the EDPB clarify that performing a service on behalf of a controller does not, in itself, make the service provider a processor under the GDPR. Where the information is anonymous from the provider’s perspective, taking into account its actual means of identification and the effective technical, organisational, contractual and legal barriers preventing access to additional identifying information, the provider should be treated as a recipient of non-personal information for that activity. The objective of preventing circumvention should preserve the controller’s own GDPR obligations without automatically extending processor status to a recipient for whom the information is not personal data.

1.3. Anonymisation as a gradual and iterative process

Telefónica believes that the Guidelines should give greater consideration to the practical implementation of anonymisation as a process that may require several stages and a significant effort. Depending on the characteristics and complexity of the dataset, anonymisation may involve source mapping, data cleaning, removal of identifiers, reduction of granularity, aggregation, testing and successive

adjustments. Its effectiveness may depend on the combined outcome of these steps rather than on a single operation.

We agree that the obligations applicable to personal data must remain in place while individuals are still identifiable. However, the initiation of an anonymisation process should be distinguished from the point at which a specific output has been validated as anonymous for the relevant entity and context. The need for repeated testing or further transformation should be recognised as part of the process, with appropriate safeguards and justified time limits, rather than as an assumption that anonymisation must be achieved immediately.

The reference to immediate anonymisation in paragraph 39 should therefore be complemented by practical guidance for processes that cannot be completed in a single step. An anonymisation process may involve service providers that initially receive identifiable personal data and act as processors at that stage. Once the data have been effectively anonymised, the resulting information may be made available for analysis to another recipient or retained for analysis by the same service provider. In Telefónica's view, where that provider no longer has means reasonably likely to be used to identify the individuals concerned, it should be regarded, for that subsequent analytical activity, as a recipient of anonymous information rather than as a processor of personal data.

Prompt reduction of identifiability should be encouraged, while allowing the time reasonably required to implement and validate effective measures. The retention of original data or intermediate copies should be justified for each stage, limited to what is necessary and subject to access controls. An intention to anonymise should not justify indefinite retention or processing for unrelated purposes.

In the telecommunications sector, datasets containing spatial and temporal observations may require successive reductions in granularity and tests of the combined information available. We encourage the EDPB to include an example explaining how organisations can progressively reduce geographical and temporal detail, suppress groups that are too small and assess whether successive releases allow individual trajectories to be reconstructed. This would help clarify both the point at which an output can be regarded as anonymous and the circumstances requiring further work.

The Guidelines should also allow organisations to describe the measures applied during the process without presenting an intermediate result as anonymous. Terms such as "de-identified" or "data undergoing anonymisation" can communicate a reduction in identifiability while making clear that the data remains subject to the GDPR where individuals are still identifiable. We believe that paragraph 40 should distinguish between descriptions of technical measures and claims that data has ceased to be personal.

Clear labelling would support governance and auditing throughout the process. Organisations should be able to record the stage reached, the transformations applied, the relevant access restrictions and the outstanding validation steps. Such information should describe the actual status of the data and should not create an expectation that the GDPR no longer applies before the required assessment has been completed.

Proportionate documentation and reassessment

Telefónica supports documentation of the anonymisation process and its outcome. We believe that the guidance should help organisations record the dataset or output assessed, the relevant entities, the measures applied, the tests performed and the conditions under which the conclusion remains valid. The level of detail should reflect the complexity of the processing and the risk of identification.

We also encourage the EDPB to distinguish the validation work needed to complete anonymisation from subsequent reassessment of a validated output. Reassessment should be linked to material changes, such as broader access, newly available auxiliary data, relevant security incidents or demonstrated developments in re-identification techniques. Where periodic review is appropriate, its frequency and scope should be proportionate to the characteristics and exposure of the data. This would provide a manageable framework without requiring organisations to demonstrate absolute irreversibility against every conceivable future development.

1.4. Unlawful means of obtaining additional information for re-identification

Telefónica welcomes the recognition in paragraph 32 that, as a general rule, entities can be presumed to comply with the law and that legal prohibitions may exclude certain means from the assessment of identifiability. However, further clarification is needed regarding the exceptions in paragraph 33, under which unlawful means may nevertheless be considered reasonably likely to be used.

This clarification is particularly important in light of Breyer (C-582/14, paragraphs 45–49). In paragraph 46, the Court recognised that identification would not constitute a means reasonably likely to be used where it was prohibited by law or practically impossible because it would require disproportionate effort. The Court's subsequent reasoning relied on the existence, subject to verification by the referring court, of legal channels through which the website operator could involve the competent authority to obtain additional identifying information from the internet service provider. The judgment therefore concerned a lawful route to identification, rather than the possibility of circumventing a legal prohibition. In Telefónica's view, Breyer does not, in itself, support extending the assessment to unlawful means

merely because a prohibition may be breached or insufficiently enforced. To the extent that paragraphs 32–33 contemplate such an extension, the Guidelines should explain its legal basis and limits, rather than present it as following directly from that judgment.

In Telefónica's view, the mere technical possibility of obtaining additional identifying information through unlawful access should not be sufficient to establish that an individual is identifiable. The assessment should distinguish between means that are theoretically conceivable and those that are realistically available and reasonably likely to be used in the specific circumstances. Otherwise, the possibility of a cyberattack, unlawful disclosure or future data leak could prevent information from being considered anonymous even where effective safeguards currently prevent access to the additional information necessary for identification.

This distinction is particularly important because the assessment of identifiability and the assessment of security risks serve different legal purposes. When determining appropriate security measures under Article 32 GDPR, controllers should anticipate threats, including malicious conduct and unlawful access. However, those threats should not automatically determine whether information constitutes personal data under Article 4(1) GDPR. A hypothetical security incident should not, in itself, be treated as making additional identifying information available to a recipient.

Telefónica therefore considers that any exception to the presumption of lawful conduct should be interpreted narrowly and supported by sufficient, objective and context-specific evidence. The factors listed in paragraph 33 should not operate as independent presumptions of identifiability. For example, weaknesses in enforcement or the potential benefits of unlawful conduct should not, without further evidence, establish that a particular entity is reasonably likely to obtain and use the additional information required for re-identification. Similarly, previous incidents in comparable situations should be assessed for their actual relevance to the entities, datasets and safeguards concerned.

The Guidelines should also distinguish clearly between a hypothetical future disclosure and an incident that has actually made additional identifying information accessible. The latter may justify reassessing anonymity in light of changed circumstances; the former should not automatically determine the status of the information at the time of the assessment.

Telefónica recommends that the EDPB clarify the legal basis and limits for considering unlawful means within the identifiability assessment, and explain how paragraphs 32–33 should be applied consistently with the recognition of effective confidentiality and access controls in paragraph 89. In particular, the Guidelines should confirm that the mere possibility of circumventing a legal prohibition or overcoming a security safeguard is insufficient: any departure from the presumption

of lawful conduct must demonstrate a concrete and reasonably foreseeable pathway to obtaining and using the additional information necessary for identification.

Conclusions

Telefónica considers that clear distinctions between record isolation, singling out and identification are essential to the consistent application of the Guidelines. We encourage the EDPB to define these concepts precisely, align the relevant provisions and explain through practical examples why technical uniqueness does not automatically establish contextual identifiability.

We also believe that the Guidelines should recognise the role of processors in carrying out anonymisation and allow a contextual examination of their actual identification capabilities in defined circumstances. This should be accompanied by effective safeguards and should preserve the controller's responsibilities and the obligations applicable to earlier processing of personal data.

Recognising anonymisation as a potentially lengthy and iterative process would help organisations apply the framework in practice. Guidance on intermediate states, temporary retention, validation and proportionate reassessment would support effective implementation while maintaining protection for individuals.

Finally, the Guidelines should clarify the legal basis and limits for considering unlawful means of obtaining additional identifying information. Breyer relied on the availability of lawful channels for identification and does not, in itself, establish a broader exception based on the possibility of circumventing legal prohibitions. Any departure from the presumption of lawful conduct should therefore require sufficient, objective and context-specific evidence of a concrete risk, while clearly distinguishing the assessment of identifiability from the assessment of security threats.

We encourage the EDPB to incorporate these clarifications to provide a balanced framework that supports compliance, responsible innovation and trust in the use of da

*****



www.telefonica.com