Insurance Europe comments on EDPB guidelines on anonymization

Our reference:	COB-DAT-25-057	Date:	30-10-2026
Referring to:			
Related documents:	EDPB guidelines on anonymisation		
Contact person:	Danilo Gattullo Senior Policy Advisor, Conduct of Business	E-mail:	Gattullo@insuranceeurope.eu
Pages:	5	Transparency Register ID	33213703459-54

Introduction

Insurance Europe welcomes the opportunity to comment on the European Data Protection Board's (EDPB) draft Guidelines on anonymisation.

Insurance Europe supports the EDPB's efforts to provide organisations with practical guidance on when data can be considered anonymous and can therefore fall outside the scope of the GDPR. Anonymisation plays an increasingly important role in enabling innovation, risk assessment, fraud prevention, and the development of AI systems. It is therefore essential that the final guidelines are practical, workable, and provide the necessary legal certainty for organisations. Legal uncertainty regarding when data can be considered anonymous may discourage organisations from investing in anonymisation efforts, ultimately undermining both innovation and consumer trust.

While the guidelines contain useful clarifications, Insurance Europe is concerned that certain elements adopt an overly restrictive interpretation of anonymisation which is not fully aligned with the risk-based approach of the GDPR and recent CJEU case law.

Excessive focus on theoretical risks may undermine the usefulness of anonymisation

Insurance Europe welcomes the EDPB's recognition that anonymisation may be assessed from the perspective of the relevant entity. However, the guidelines place considerable emphasis on theoretical risks and appear to impose disproportionate obligations on data controllers.

For example, paragraph 21 stipulates that personal data is deemed to exist if it *cannot be ruled* out that the third party has the means to identify the data subject. This mention could risk lowering the probability-based standard set out elsewhere in the guidelines to a broader "cannot be ruled out" test.

Furthermore, paragraphs 20 and 28 onwards take into account not only the means available to the direct recipient, but also those available to other parties across a chain of potential identification. This approach appears overly broad and could make effective anonymisation extremely difficult in practice. This is particularly

Insurance Europe aisbl • rue Champ de Mars,23 B-1050 Brussels
Tel: +32 2 894 30 00 • E-mail: info@insuranceeurope.eu
www.insuranceeurope.eu

© Reproduction in whole or in part of the content of this document and the communication thereof are made with the consent of Insurance Europe, must be clearly attributed to Insurance Europe and must include the date of the Insurance Europe document.

problematic for complex data-sharing arrangements, such as those in the insurance and reinsurance sectors, where it may be impossible to exclude the possibility that a subsequent recipient or another party holds additional information that could enable identification. If such information can be combined across a series of hypothetical scenarios, even remote possibilities of identification could ultimately prevent data from being considered anonymous.

In paragraph 30, the EDPB seeks to clarify which "relevant entities" should be considered when assessing the means of identification that may be indirectly available to an individual. According to the guidelines, these relevant entities may include *anybody directly or indirectly receiving the data, including unauthorised and malicious actors.* Such actors could include, among others, rogue employees, foreign intelligence agencies, and cybercriminals.

As a result, it would no longer be sufficient to demonstrate that there are no lawful means of obtaining access to additional information. Organisations would also be required to consider methods that are unlawful, assess the effectiveness of legal prohibitions designed to prevent such access, and evaluate the ability of unauthorised, malicious, or criminal actors to obtain additional information. Such an exercise would inevitably be speculative in nature and would place an unreasonable burden on organisations.

A similar concern arises in paragraph 88, where the EDPB highlights *a data leak* as a potential source of additional data: *"When using the contextual approach, it is important to recognise that the capabilities of different entities may vary over time. For example, a data leak could provide certain entities with access to new datasets which were previously unavailable to them. This would, in turn, allow those entities to link information with means which were, at least from that entity's perspective, previously unavailable but are now reasonably likely to be used".*

This approach extends the assessment beyond what can reasonably be expected from data controllers. Data obtained through a leak is, by definition, *not lawfully processed* and therefore should not be regarded as constituting a reasonable means of identification.

Recipient's perspective where processing is carried out on instructions

According to paragraph 15, in the case of processing on behalf of a controller, information is also to be regarded as personal data by the processor if it is personal data for the controller. This can be understood to mean that, in such scenarios, the controller's means of identification are, as a general rule, also attributed to the processor. This risks overshadowing the importance of privacy enhancing technologies and processing architectures.

In reality, outsourced analytics, cloud, modelling and AI services can be designed so that a provider receives only pseudonymised data and has no realistic means of identification. Relevant safeguards may include effective key separation, restricted outputs and contractual and organisational measures.

Paragraph 15 should be amended to reflect the possibility of context-based assessment of the processor's actual and legal means of identification. Relevant factors may include the processor's access rights, the controller's instructions, available output channels, separation of identifying information or keys, traceability measures, and any realistic possibility of obtaining additional information that would enable identification.

Statutory and contractual prohibitions

Insurance Europe welcomes the recognition in para. 32 that statutory prohibitions can effectively limit the means reasonably available to identify an individual. However, the broad indicators in para 33 for assessing the likelihood of unlawful conduct should be applied with caution. Compliance with applicable legal requirements should generally be presumed unless there are concrete reasons to consider otherwise. Factors such as a potential cost advantage or limited enforcement should not, on their own, be sufficient to assume that legal restrictions may be disregarded.

Contractual prohibitions should similarly be given appropriate weight when assessing whether identification is reasonably likely. In the insurance sector, data is frequently transferred to reinsurers, claims service providers and IT providers within established and monitored contractual relationships. Restrictions on the reuse of data or attempts to re-identify individuals can therefore provide meaningful safeguards, particularly when combined with appropriate technical and organisational measures. Such contractual restrictions should form part of the overall assessment of the means reasonably likely to be used for identification or re-identification.

Mixed datasets

In paragraph 36, the EDPB adopts a particularly stringent position regarding datasets containing multiple records. It states that *"In particular, the dataset as a whole should only be considered anonymous if the anonymisation is effective for all of the included individuals – this does not necessarily require an equal level of protection for all individuals, but does require the likelihood of re-identification to be insignificant for all of these individuals. Where this is not the case, and so a dataset contains a mix of personal and anonymous data, the entire dataset should be treated as containing personal data (and therefore within the scope of the GDPR)". Therefore*, where a dataset contains record level unique data, then the risk of identification for each unique record must be assessed.

A similar position is expressed in paragraph 87, where the EDPB notes that *"a (re)identification technique can be successful even if it only succeeds against a single individual in a larger dataset"*.

In practice, however, demonstrating that the risk of re-identification is insignificant for *every single person* within a large and complex dataset may be extremely difficult, if not impossible. Such a standard creates significant regulatory uncertainty and risks setting a threshold too high for anonymisation. Instead, the assessment should focus on whether the dataset, taken as a whole, has been anonymised to a degree that makes re-identification realistically unlikely. The mere fact that a re-identification technique may succeed in relation to a single individual should not automatically lead to the conclusion that the entire dataset cannot be considered anonymous.

Future benchmark and periodic reassessment

The guidelines mention that the risk of re-identification may evolve over time as a result of technological developments, the availability of additional data sources, security breaches or increased computing power, and therefore identify periodic reassessment as good practice (footnote n.3 and para 35). However, this should not be interpreted as an open-ended obligation to continuously consider all possible future developments. In fact, Recital 26 GDPR refers to the technology available at the time of processing and to technological developments that are reasonably foreseeable.

The decisive factor should be whether a development is reasonably foreseeable in the specific context of the processing and whether it materially increases the likelihood of identification. Reassessment should therefore only be necessary where there is a reasonably foreseeable and significant change in the risk of identification, for example following a relevant security incident, as also envisaged in paragraph 42. Such reassessment should only apply to datasets that are still held or used by the relevant entity.

Importantly, subsequent technological developments that were not reasonably foreseeable should not result in processing that was lawful at the relevant time being considered unlawful retroactively. To ensure legal certainty, the documented assessment based on the circumstances and reasonably foreseeable means of identification at the time of processing should remain the relevant benchmark.

Simplified approach

Insurance Europe welcomes the simplified approach as a practical option for organisations seeking a more precautionary assessment. However, as acknowledged in paragraph 48, this approach may go beyond the applicable legal standard by treating data as personal even where it could qualify as anonymous under a contextual approach.

It is therefore important that the simplified approach remains genuinely voluntary and does not become a de facto benchmark in audits or regulatory reviews. Organisations choosing to apply the context-based legal test should not face an additional burden to justify why they have not followed the more precautionary approach.

This is particularly important given the extensive requirements associated with the "contextual approach". The simplified approach should not result in an absolute concept of personal data becoming the practical standard.

Anonymisation process and legal basis

The guidelines clarify (in para 38) that the GDPR continues to apply for as long as personal data is processed in the course of anonymisation. Accordingly, the processing must have a legal basis under Article 6 GDPR and, where special categories of personal data are involved, meet the requirements of Article 9(2).

However, this should not be understood as requiring a separate legal basis whenever anonymisation is carried out for a further purpose. Where the further purpose is compatible with the original purpose, the compatibility assessment under Article 6(4) GDPR should also be taken into account. The guidelines would therefore benefit from greater clarity on the circumstances in which anonymisation forms part of the original processing and when it may constitute compatible further processing.

Three criteria assessment

Section 3.4 sets out three criteria for assessing anonymity: "No Record Isolation", "No Linkage" and "No Inference". The guidelines clarify that failure to meet one of these criteria does not automatically mean that the data are personal. However, the way the criteria are presented could give the impression that they are separate, cumulative conditions that must all be met for data to be considered anonymous. This should be further clarified. The key question under Article 4(1) and Recital 26 GDPR remains whether a natural person can be identified using means that are reasonably likely to be used.

In particular, a clear distinction should be made between isolating a data record and identifying the person behind it. A record may be unique because it contains a combination of characteristics that appears only once, but this does not necessarily mean that the individual concerned can be identified. Identifiability arises only where the record can be linked to a specific person using additional information that is reasonably available, or where the information otherwise allows that person to be specifically distinguished. This distinction is reflected in paragraphs 98–100 and Example 24 where the three criteria are more correctly presented as indicators of identifiability, rather than separate tests that must each be passed.

Pricing, risk assessment and actuarial models

Insurance Europe welcomes the clarifications set out in paragraphs 67 to 71 and in Example 14. Applying general findings derived from a historical dataset to a new applicant does not breach the "No Inference" criterion where that applicant was not part of the source dataset and the conclusion is based solely on statistical information relating to a comparable group.

This distinction is particularly important for the insurance sector. Insurers rely on anonymous claims statistics and actuarial models for purposes such as pricing, reserving and risk assessment. While the application of such information may result in an assessment or decision relating to an identified policyholder and therefore constitute personal data in that context, this should not, in itself, change the anonymous nature of the underlying source dataset.

The guidelines could further clarify that applying generalised findings derived from anonymous data to an identified individual does not, solely as a result of that use, turn the underlying anonymous dataset into personal data. The reasoning reflected in Example 14 could be incorporated into the main text and expressly extended to statistical, actuarial and AI-based risk models.

Conclusions

Insurance Europe supports the EDPB's objective of providing greater clarity regarding anonymisation. However, the final guidelines should better reflect the risk-based nature of the GDPR, the practical consequences of the CJEU's judgment in *EDPS v SRB*, and the importance of ensuring that anonymisation remains a realistic and usable tool for organisations.

The final text should place greater emphasis on realistic re-identification risks, contextual factors and proportionality. This would improve legal certainty, encourage the use of privacy-enhancing techniques and facilitate responsible innovation while maintaining a high level of protection for individuals.