German Association of the Automotive Industry (VDA) Position Paper on EDPB Guidelines on the Anonymisation of Personal Data

Overall assessment of the Guidelines from the perspective of the automotive industry

The German Association of the Automotive Industry (VDA) welcomes the revision of the Guidelines on anonymisation by the European Data Protection Board (EDPB). Legal certainty regarding anonymisation is of central importance for data-driven innovation, in particular for automated and connected driving functions as well as cybersecurity and road safety.

The recognition of the contextual approach is particularly welcome: whether data is anonymous may depend on the actual means of identification available to the respective entity. This is consistent with the case law of the Court of Justice of the European Union and with the reality of collaborative data ecosystems involving different datasets and different identification capabilities.

At the same time, it remains questionable whether the Guidelines establish sufficiently practical and legally certain criteria. In addition to the contextual approach, they provide for a simplified approach that disregards differences between the identification capabilities of individual entities. There is a risk that, in practice, this approach could become the de facto expected standard.

The scope of the re-identification risks to be taken into account also creates practical uncertainty. Additional information held by other entities, external datasets, technological developments, AI techniques, data leaks and chains of entities may become relevant. The assessment therefore risks shifting away from concrete identification capabilities towards scenarios that are difficult to foresee.

Moreover, it remains unclear how much weight should be given to technical and organisational measures and closed industrial data spaces. Clear criteria are needed to determine when such measures reduce a re-identification risk to a level where it is insignificant in reality.

The broad scope of re-identification risks also affects documentation and reassessment. Companies should not, in practice, be required to prove that future re-identification risks are excluded.

From the VDA's perspective, the Guidelines should therefore in particular:

- ensure that the contextual approach remains the applicable standard for assessing anonymity;
- limit re-identification risks to realistic and objectively foreseeable scenarios;
- clarify the relevance of technical and organisational measures and secured industrial data spaces in the assessment of anonymity;
- ensure that documentation and reassessment requirements are risk-based and practicable;
- and, overall, ensure that the requirements for anonymisation do not result in a de facto zero-risk standard.

Key comments on the Guidelines and need for adjustment from the perspective of the automotive industry

1. Unclear practical role of the simplified approach – the contextual approach must remain the standard for assessing anonymity

The EDPB recognises that anonymity must be assessed from the perspective of the relevant entity in the specific processing context ("contextual approach"). The entity's actual capabilities, access possibilities and additional information are decisive. Accordingly, not every theoretical possibility of identification is relevant.

This reflects the reality of the automotive industry: vehicle manufacturers, suppliers, fleet operators, research institutions and technical service providers regularly have access to different datasets and different identification capabilities. For processors, however, the Guidelines state that the controller's perspective is decisive; the differentiation therefore requires careful qualification of the respective roles.

The practical role of the "simplified approach" is critical. It disregards differences between entities regarding access to data, additional information and other resources for re-identification. As a result, the same dataset may be treated as not anonymous as a precaution even though the contextual assessment leads to a different result for the specific entity.

The practical relevance can be illustrated by the transfer of vehicle data within a collaborative development chain: if an OEM transfers driving and sensor data to a supplier acting as an independent controller for the further development of a driver assistance system, that supplier may have no access to driver or vehicle owner data, contractual information or other attribution data. Under the contextual approach, the assessment would determine whether the supplier can identify a natural person using the means actually available to it. If the necessary additional information is unavailable and there are no other means of identification reasonably likely to be used, the data may be anonymous from the supplier's perspective. Under a simplified assessment, these differences in actual identification capabilities are initially disregarded. The dataset may therefore be treated as not anonymous solely because of theoretical possibilities of re-identification, even though the supplier's actual identification capabilities have not changed.

This potential divergence in results raises the question of the precise function of the simplified approach within the assessment process envisaged by the EDPB. On the one hand, the Guidelines clarify that the contextual approach reflects the legal standard and that the simplified approach is not an alternative legal standard. On the other hand, the simplified approach appears in the flowchart as a distinct possible assessment path, without making sufficiently clear whether it constitutes an alternative assessment or merely a preliminary screening function. Paragraph 49 could be understood as meaning that the simplified approach serves, in particular, as a preliminary assessment: if this simplified assessment already shows that re-identification is theoretically impossible, the assessment may end. If theoretical means of re-identification are identified, the contextual approach may subsequently be used to assess whether those means are actually reasonably likely to be used from the perspective of the relevant entities.

Such an understanding would be methodologically comparable to a preliminary threshold assessment: a preliminary simplified assessment determines whether an in-depth assessment is required, but does not replace it. However, the Guidelines do not make sufficiently clear whether the EDPB actually intends the simplified approach to perform this function.

If the simplified approach is intended to serve as a voluntary preliminary assessment in this sense, this should be expressly clarified in the Guidelines and, in particular, in the flowchart. The Guidelines should clearly distinguish between a preliminary assessment and the legally relevant assessment of anonymity and transparently specify the function of the simplified approach, when a contextual assessment is required and that the simplified approach does not impose separate additional requirements for anonymity. Otherwise, there is a risk that companies or supervisory authorities will in practice treat the stricter simplified approach as a separate minimum or expected standard.

From the VDA's perspective, there is a particular need for clarification and adjustment regarding:

- clarification of the function and sequence of the simplified and contextual approaches; if the simplified approach is intended merely as a voluntary preliminary assessment, this should be expressly reflected in the flowchart and the transition to the contextual assessment should be clearly defined;

- clarification that the simplified approach does not constitute a separate legal assessment standard or impose additional requirements for anonymity and, in particular, must not become a de facto minimum or expected standard in corporate or supervisory practice.

2. Extension of the anonymity assessment to theoretical re-identification scenarios – re-identification risks must be limited to realistic and objectively foreseeable cases

The Guidelines specify which identification capabilities are to be taken into account through the concept of “means reasonably likely to be used”. Relevant means may include not only an entity’s own means, but also additional information, data sources or means available from other entities where their use is reasonably likely.

An individual may therefore also be identifiable where datasets, additional information or technical capabilities are distributed across several entities and can reasonably be brought together.

Against this background, “No Record Isolation”, “No Linkage” and “No Inference” assess whether the dataset withstands potential risks of re-identification.

A systematic assessment framework is useful. However, the combination of a broad interpretation of the relevant means of identification with the technical criteria must not lead to excessive requirements for demonstrating effective anonymisation.

“No Record Isolation” requires that no unique combination of attribute values allows an individual record to be singled out. Vehicle and sensor data may be technically unique because of driving manoeuvres, measurements, timestamps or vehicle states without enabling the recipient to identify the driver.

It should therefore be clarified that technical uniqueness alone is insufficient; the decisive question must remain whether it actually results in the identifiability of a natural person in the specific processing context.

“No Linkage” requires that linkage with further information does not result in identifiability. In collaborative data ecosystems, this may involve combining information held by several entities. It would be problematic if merely theoretical fleet, workshop, contractual or mobility data were considered to preclude anonymity even though the specific recipient can neither access nor realistically use such data.

It should therefore be clarified that realistic access and linkage capabilities of the relevant entity remain decisive and that purely theoretical linkages outside that entity’s scope of access do not, on their own, preclude anonymity.

“No Inference” requires that no specific and meaningful inference can be drawn from the given data. With vehicle and usage data, new AI-based analytical techniques may in future enable additional inferences about driving behaviour or usage patterns.

However, companies cannot reliably foresee what additional insights future analytical techniques may derive from today’s data.

Accordingly, only inferences that can actually be expected based on the known state of the art and realistically available analytical techniques should be taken into account; purely speculative future inference possibilities should not be sufficient.

The range of potentially relevant entities is also particularly broad: depending on the context, investigative journalists, acquaintances, intelligence agencies, cybercriminals or other external actors may be taken into account. Companies face difficulty in foreseeing which information or capabilities of such actors are objectively relevant.

Such entities should therefore only be included where there are concrete indications that their additional information or capabilities may realistically become relevant in the specific processing context.

Technical and organisational measures are relevant, but their weight remains unclear. Vehicle-related development data are regularly processed in closed environments with access restrictions, role-based access models and encryption. Nevertheless, data leaks, unauthorised access and future identification capabilities are still to be taken into account.

The Guidelines should therefore specify when effective safeguards and closed industrial data spaces sufficiently reduce re-identification risks.

Overall, the assessment of anonymity risks becoming dependent on factors that companies can neither control nor reliably foresee. The broader the range of risks to be considered, the more difficult it becomes to carry out a reliable assessment of anonymity.

For the automotive industry, this risks creating a de facto excessive standard: vehicle data that are essential for automated and connected driving functions as well as cybersecurity and road safety could regularly fail to qualify as anonymous despite the absence of realistic identification capabilities.

The Guidelines should therefore clearly distinguish between theoretically conceivable and objectively foreseeable re-identification risks in order to ensure legal certainty and innovation-friendly use of data.

From the VDA's perspective, there is a particular need for clarification and adjustment regarding:

- clarification that the application of the "No Record Isolation", "No Linkage" and "No Inference" criteria must be based on objectively foreseeable and realistic identification capabilities and must not result in a de facto zero-risk standard;
- clarification that additional knowledge of third parties, external data sources, future technologies and misuse scenarios should only be included in the assessment where there are concrete indications of their relevance;
- clarification of the relevance of technical and organisational measures and secured industrial data spaces in assessing re-identification risks and their appropriate consideration in the assessment of anonymity.

3. Risk of excessive documentation requirements – documentation requirements must be practicable

The Guidelines require documentation of the anonymisation process, including testing of supposedly anonymous datasets, in order to demonstrate compliance with the GDPR and the effectiveness of the anonymisation. Changes in re-identification risks may also trigger a subsequent reassessment.

Documentation can, in principle, contribute to the traceability of anonymisation decisions, provided that its scope and requirements remain proportionate.

The broad re-identification risks inevitably increase the documentation burden: in addition to the recipient's capabilities, relevant factors may include third-party knowledge, external datasets, technological developments, AI techniques or unauthorised access.

This risks turning documentation from a traceable justification of an anonymisation decision into a de facto requirement to prove that re-identification is excluded. Such proof cannot reliably be provided with regard to future data sources, technologies or AI capabilities.

This is particularly apparent for vehicle and sensor data used over longer periods: it is hardly possible to document with sufficient certainty that new external datasets, additional information held by third parties or future analytical techniques will never create new re-identification risks.

Documentation should therefore serve to make the anonymisation decision traceable, rather than to prove absolute non-re-identifiability. For standardised or recurring anonymisation procedures, concise documentation should generally be sufficient. This could, for example, take the form of an appropriate entry in the record of processing activities, documenting the anonymisation method applied, the outcome and date of the assessment and, where necessary, a reference to a more detailed assessment. Separate additional documentation should only be required where warranted by the specific re-identification risk.

Reassessment should also be clearly circumscribed. A reassessment in the event of a material change in the risk environment is understandable; however, it remains unclear when it is required and what relevance should be attributed to future technologies.

For legal certainty, effectiveness should generally be assessed on the basis of the facts known and the state of the art at the time of the assessment. A risk-based distinction is required between the ex ante assessment, event-driven reassessment and merely recommended periodic review.

From the VDA's perspective, there is a particular need for clarification and adjustment regarding:

- clarification that documentation serves to make the anonymisation decision traceable and does not require proof of non-re-identifiability under every theoretically conceivable or future circumstance;
- recognition of concise and risk-based forms of documentation, in particular an entry in the record of processing activities for standardised or recurring anonymisation procedures;
- clarification that the effectiveness of anonymisation is to be assessed on the basis of the facts known and the state of the art at the time of the assessment, and that reassessment is required only in the event of concrete and objectively verifiable changes in the level of risk.

Conclusion

- The VDA welcomes the further clarification of the requirements for anonymisation. In the consultation process, further clarification should in particular be provided on the relationship and practical application of the contextual and simplified approaches, limiting the re-identification assessment to realistic and objectively foreseeable scenarios, the weight to be given to effective access restrictions, and a risk-based and practicable design of documentation and reassessment requirements. This would strengthen legal certainty for data-driven industries and help to ensure that anonymised data remain responsibly available for innovation, research, cybersecurity and road safety.

Contact persons

Jürgen Mindel

Managing Director
juergen.mindel@vda.de

Dr. Ricarda Leffler

Head of Department & In-House Counsel
ricarda.leffler@vda.de

Susanne Jonetzko

In-House Counsel, Legal and Compliance, DPO
susanne.jonetzko@vda.de

The German Association of the Automotive Industry (VDA) consolidates around 620 manufacturers and suppliers under one roof. The members develop and produce cars and trucks, software, trailers, superstructures, buses, parts and accessories as well as new mobility offers.

We represent the interests of the automotive industry and stand for modern, future-oriented multimodal mobility on the way to climate neutrality. The VDA represents the interests of its members in politics, the media, and social groups.

We work for electric mobility, climate-neutral drives, the implementation of climate targets, securing raw materials, digitization and networking as well as German engineering. We are committed to a competitive business and innovation location. Our industry ensures prosperity in Germany: More than 730,000 (2025) people are directly employed in the German automotive industry.

The VDA is the organizer of the largest international mobility platform IAA MOBILITY and of IAA TRANSPORTATION, the world's most important platform for the future of the commercial vehicle industry.

Publisher	German Association of the Automotive Industry Behrenstraße 35, 10117 Berlin www.vda.de/en German Bundestag Lobby Register No.: R001243 EU Transparency Register No.: 9557 4664 768-90
Copyright	German Association of the Automotive Industry Reprint, also in extracts, is only permitted, if the source is stated.
Version	October 2026