Privacy Next's Comments on EDPB Guidelines 02/2026 on Anonymisation and the Ongoing Legislative Process

1. Introduction

Privacy Next wishes to express its reservations about the EDPB's Guidelines 02/2026 on Anonymisation, both in terms of process and substance. Our reservations follow from the previous feedback we provided to the EDPB on its guidelines relating to scientific research. The EU's co-legislators are actively debating these matters through a process mandated by the EU treaties. Therefore, guidance should wait until the legislation is settled.

Article 70 GDPR provides that the Board shall ensure the consistent application of GDPR. As the regulation is being debated, the Board must show institutional restraint; otherwise, the guidance being issued at this time could be perceived as limiting the co-legislators' choices before the democratic process is complete. These guidelines call for organisations to go above existing legal standards but it is unclear how this is a legitimate function for the EDPB.

In the substance of the guidance, the EDPB appears to seek to establish new presumptions, evidential expectations, and continuing duties that neither the legislators nor the CJEU have called for. A recurring feature of the Guidelines is the use of a teleological methodology in which the objective of preserving GDPR protection appears to take precedence over the legal test established by the Regulation and interpreted by the CJEU. Rather than asking whether identification is reasonably likely using objective factors through a risk-based approach, the guidelines adopt an approach that seeks to prevent any situation where data may fall outside GDPR.

Furthermore, the EDPB fails to account for the impact the practical use of the guidelines will have on other GDPR objectives, such as the free movement of data as set out in article 1(3) GDPR, as well as other EU treaty objectives and the policies agreed to by the Commission, Council, and Parliament.

This is highly problematic, as the EDPB is introducing a new regulatory standard that goes beyond existing legal standards, based on the assumption that the motivation for circumvention, let alone the risk of it, is commonplace. Furthermore, by saying that anonymisation requires a GDPR legal basis, thereby ensuring the continued reach of GDPR, the guidelines appear to place further regulatory burdens on organisations engaging in data minimisation efforts.

Accordingly, Privacy Next recommends that the EDPB not finalise the guidance until the Digital Omnibus negotiations have concluded and the will of the EU legislature is known.

Square de Meeûs18 | Brussels Belgium | 1050
www.privacynext.eu | info@privacynext.eu
Transparency Register No. 9833410101750-70

2. Guidance must follow, not pre-empt the legislative process

The EDPB's issuing of guidance on matters the co-legislators are examining raises a fundamental constitutional question of institutional balance in deciding the content of EU legislation. Article 16(2) TFEU assigns to the European Parliament and the Council, through the normal legislative procedure, the task of laying down rules on the protection of individuals and the free movement of personal data. Article 68 GDPR, a secondary law, established the EDPB. The EDPB is not a recognised primary EU institution in Article 13 TEU. Its mandate is specific to the secondary law that created it. Article 70(1)(e) GDPR empowers the EDPB to issue guidelines, recommendations and best practices to encourage consistent application of the Regulation. Article 70 provides a competence to illustrate and support the implementation of existing legislation. The competence does not extend to a role in determining the legislative parameters of matters under consideration by the co-legislators. The EDPB and EDPS have put forth their views on the Digital Omnibus proposal. The EDPB's issuing of guidance for a second time on a matter being discussed by the co-legislators goes beyond its role as set out in the GDPR.

The correct sequence in EU law-making is simple: the Commission proposes, the co-legislators decide, and then the courts interpret. The EDPB is mandated to support consistent implementation of the agreed rules that are in the GDPR. If the legislation is not settled, the EDPB has no role in determining how implementation should occur. Once the Digital Omnibus is agreed, the Board can issue practical guidance anchored in the final settlement. That would be more durable, more legitimate and less confusing than publishing a regulatory framework during the legislative process.

3. The guidelines must account for the EU's full objectives

The guidelines are structurally unbalanced because they are grounded in hypotheticals and appear to envisage widespread circumvention of GDPR obligations, whilst at the same time ignoring normal business practices. Article 1 GDPR protects the personal data of natural persons and also safeguards the free movement of personal data within the Union. Article 1(3) provides that the free movement of personal data must not be restricted or prohibited for reasons connected with data protection. Recital 4 adds that data protection is not an absolute right and must be considered in relation to its function in society and balanced with other fundamental rights in accordance with proportionality.

Data protection is an integral part but not the sole objective of the European Union. Article 3 TEU requires the Union to establish an internal market and pursue Europe's sustainable development based on balanced economic growth, a highly competitive social market

Square de Meeûs18 | Brussels Belgium | 1050
www.privacynext.eu | info@privacynext.eu
Transparency Register No. 9833410101750-70

economy, social progress, and scientific and technological advancement. These objectives ultimately serve the well-being of Europe's people. The Treaties require the EU to create the conditions in which people, businesses, knowledge, and investment can move across borders.

As the European and global economy becomes increasingly data-driven, greater attention must be paid to the free movement of data rather than creating more obstacles to its use. The EU was founded on the free movement of goods, services, people, and capital, and each of these now depends on data to function effectively. The practical impact of the guidelines will be to create further obstacles to the use and free movement of data across the EU. The GDPR regime already suffers from fragmented national and divergent interpretations of regulation, recreating some of the very barriers the Single Market was built to remove. Regulatory guidance in the EU needs to support the effective functioning of the Single Market, which includes upholding the fundamental rights of the Charter. Creating more obstacles for organisations, which in turn negatively affect economic development, cannot be accepted as an EU objective.

Recent political commitments undertaken during the omnibus proposals have reinforced the Treaty objectives. The "One Europe, One Market Roadmap" has been agreed to by the European Parliament, the Council of the European Union, and the European Commission. The roadmap commits the EU to simplifying rules, removing barriers within the Single Market, strengthening trade, and advancing Europe's digital and AI transformation. The Roadmap expressly links a stronger, more integrated economy to Europe's prosperity, security, and independence.

Upholding data protection and other fundamental rights, as set out in the Charter, is also part of realising the roadmap. The EU's regulatory framework is to be interpreted and applied in a manner that reconciles fundamental-rights protection with the functioning of the Single Market, economic development, innovation and social well-being. Economic growth is not an objective pursued solely for businesses' benefit. A competitive economy also creates employment and wealth, supports public services, finances Europe's social model, and enables European societies to maintain high levels of well-being.

The teleological reasoning deployed throughout the guidelines is one-dimensional. The GDPR does not pursue only the protection of personal data. Article 1 GDPR makes clear the regulation seeks to protect natural persons *and* the free movement of personal data, while Recital 4 expressly rejects treating data protection as an absolute right. A purposive interpretation that consistently favours the objective of regulatory protection, while failing to give equal weight to the Regulation's other objectives, risks producing a distorted interpretation of the future legislative settlement adopted by the co-legislators.

Square de Meeûs18 | Brussels Belgium | 1050
www.privacynext.eu | info@privacynext.eu
Transparency Register No. 9833410101750-70

As an institution created under the EU treaty framework, the EDPB must take a more proportionate approach that ensures its guidance supports the lawful use of personal data, while also supporting research, innovation, and cross-border economic activity, all of which contribute to the prosperity and well-being of society. While the EDPB is an independent institution under secondary legislation, independence is not isolation. Agreed EU objectives must inform the interpretation and application of secondary legislation. The EDPB must do more to explicitly account for the EU's other objectives when formulating guidance, as it does not have an autonomous status in the treaties that would allow it to put its data protection concerns above all other legitimate policy objectives.

4. The "Simplified Approach" is neither simple nor supportive of the EU's objectives

The EDPB's proposed simplified approach will produce outcomes where data is treated as personal data throughout the business chain, regardless of the efforts taken to adhere to the existing legal test. The guidelines acknowledge this and recognise that the simplified approach may cause controllers to treat some data as personal even where it may in fact be anonymous from their position. The EDPB states that the simplified approach is not an alternative legal standard and that the contextual approach remains the methodology that most closely reflects the actual legal test under GDPR.

The simplified approach appears designed to produce more conservative outcomes by disregarding differences in entities' capabilities, access to information, and realistic opportunities for re-identification. As a result, organisations will be expected to treat the data as personal data regardless of the practical realities. The guidelines establish a strong presumption in favour of continued GDPR applicability whenever any theoretical re-identification pathway may be identified. The simplified approach appears to substitute a teleological objective for the legal standard set out in Recital 26 GDPR. A methodology that knowingly exceeds the legal standard to maximise regulatory coverage risks replacing the legislature's chosen balance with the regulator's policy preference.

Recital 26 GDPR does not ask whether identification is conceivable or theoretically possible. It asks whether means are reasonably likely to be used, taking into account objective factors such as cost, time, available technology, and technological developments. The phrase "reasonably likely" must perform genuine limiting work. Otherwise, almost every granular dataset remains personal because some actor, somewhere, might obtain additional information at some point in time and deploy a sufficiently capable technique at some point in the future.

Square de Meeûs18 | Brussels Belgium | 1050
www.privacynext.eu | info@privacynext.eu
Transparency Register No. 9833410101750-70

To apply the simplified approach, an organisation must imagine a broad universe of actors, datasets, techniques, and future capabilities. It will be necessary to test **No Record Isolation, No Linkage** and **No Inference** against that universe, record safety margins, monitor technological change, and revisit conclusions as things may evolve. If a theoretical path is found, the organisation must either accept the full GDPR or undertake the contextual analysis. The EDPB presents the simplified approach as a convenient alternative to a detailed contextual assessment. In practice, however, organisations face substantial burdens under either approach, as the guidelines seek to shift focus to any possible threat, regardless of the reality of a situation. Instead of providing the greater legal certainty required by organisations, and supporting them in their lawful activities, the guidelines risk creating a sense of fear about hypothetical contingencies and, perhaps, a fear in the regulatory regime itself that some activities involving data may fall outside GDPR. The guidelines set the foundation standard as being the possibilities and potential capabilities of any "unauthorised and malicious actors." Such motivation cannot be the base presumption guiding legislation. Contractual breach cannot be presumed for every recipient. A future technology cannot be treated as presently available merely because theoretical development may be possible. Cybersecurity incidents are real, but it does not follow that every control will fail or that other legislation requiring action is insufficient. Future developments should be considered where they are reasonably foreseeable within the relevant lifespan of the data and within the realm of justifiable possibilities.

5. The Exclusion of processors from the relative approach lacks a clear legal basis

Paragraph 15 of the Guidelines effectively excludes processors from the relative approach to determining whether information constitutes personal data. Where information remains personal data for a controller, the EDPB considers that a processor must also treat it as personal data when acting on that controller's behalf, regardless of the processor's actual ability to identify the individuals concerned.

Privacy Next questions the legal basis for this interpretation. Article 4(1) GDPR defines personal data by reference to whether an individual is identified or identifiable. Recital 26 requires consideration of the means reasonably likely to be used for identification, including objective factors such as cost, time and available technology. Neither provision establishes a categorical distinction between controllers and processors when assessing identifiability.

The CJEU's judgment in *SRB v EDPS* confirms that the assessment is contextual and that information may be personal data for one entity but not another. The Court did not

Square de Meeûs18 | Brussels Belgium | 1050
www.privacynext.eu | info@privacynext.eu
Transparency Register No. 9833410101750-70

establish an exception for processors. While the judgment does not specifically resolve every question arising under Article 28 GDPR, it provides no apparent basis for automatically attributing a controller's capacity to identify individuals to a processor that lacks such capacity.

The EDPB appears to rely on an interpretation that prioritises maintaining regulatory protection throughout the processing chain. However, such teleological reasoning cannot be a substitute for a legal basis in the Regulation. Article 70 GDPR empowers the EDPB to promote consistent application of existing law, not to introduce additional categories of processing for which the ordinary legal test of identifiability is displaced. Nor can the GDPR's protective objective be invoked in isolation from its equally express objective of facilitating the free movement of personal data.

The consequences are significant. Processors providing cloud infrastructure, AI services, analytics and other specialist capabilities may be denied the benefit of effective anonymisation solely because of their contractual relationship with a controller, even where technical and organisational safeguards prevent identification.

Privacy Next therefore calls on the EDPB to identify the specific legal basis for the exclusion in paragraph 15 or remove it. The classification of information should follow the legal test of identifiability, not a presumption arising from the allocation of processing responsibilities.

6. The guidelines will create more burdens and increase fragmentation

The guidelines seek to shift the regulatory position on anonymisation toward the most feared possible outcomes. In turn, the guidelines discourage data minimisation measures. If organisations perceive that anonymised data may remain subject to GDPR even after significant investments in anonymisation techniques, documentation, and governance measures, commercial and operational incentives to pursue anonymisation will weaken. Organisations are likely to conclude that the regulatory uncertainty around demonstrating anonymity outweighs the effort to make data more usable. This likely outcome runs contrary to how the EU wants Europe's economic and social development to unfold. It also fails to sufficiently recognise the GDPR's dual purposes: to protect personal data and to ensure the free movement of data. The guidelines also claim one objective is to facilitate the safe use and reuse of information while preserving data protection rights. However, a framework that effectively defaults towards continued regulation may discourage innovation in privacy-enhancing technologies rather than encourage it.

Square de Meeûs18 | Brussels Belgium | 1050
www.privacynext.eu | info@privacynext.eu
Transparency Register No. 9833410101750-70

The guidance appears to systematically favour outcomes in which information continues to be treated as personal data. If this becomes the benchmark against which organisations assess anonymisation efforts, they will be reluctant to pursue data minimisation. Proper anonymisation is not a loophole to avoid regulatory compliance. It is a mechanism to reduce risk to individuals through data minimisation while enabling research, public-interest analysis, statistical use, responsible AI development, and cross-border data collaboration. If the threshold is made practically unreachable, organisations lose an incentive to invest in anonymisation and may instead retain identifiable data in closed systems that may not support data protection.

The use of the guidelines will be further complicated by the variance and fragmentation in how national authorities apply the framework for assessing anonymity. One of the EDPB's functions is to promote harmonised interpretation and application of data protection law throughout the EU. Yet the proposed guidance leaves substantial room for divergent supervisory approaches because of the complexities and details that must be examined to ensure all elements of the framework are met. Given eight years of GDPR practice, national authorities will likely place greater emphasis on different aspects of the proposed framework. Businesses operating across multiple Member States may face materially different regulatory expectations despite processing identical datasets. A greater concern is that the guidelines may reverse the regulatory burden. An organisation using the contextual legal standard may be asked by the national authority why it did not choose the method the regulator describes as more cautious. Any disagreement then becomes framed as the organisation seeking to circumvent a particular understanding of GDPR, rather than applying the regulation as it stands.

The EDPB states that this does not formally alter the legal standard, but it will clearly alter the practical use of data and the application of GDPR. The simplified approach may give organisations an easier route to avoid potential regulatory scrutiny, but it will come at a cost because of barriers to data use and ongoing fragmentation in data protection across the EU.

7. Conclusion

Anonymisation must remain a credible legal and technical outcome for organisations to use as a means of data minimisation. The relevant question is not whether identification can be imagined, but whether a specific actor can realistically bring together the data, further information, and technology to successfully identify the data subject. A rigorous, contextual and risk-based test, as explained in the *SRB v EDPS* decision, ensures personal data is protected in the conduct of legitimate activities. That does not weaken

Square de Meeûs18 | Brussels Belgium | 1050
www.privacynext.eu | info@privacynext.eu
Transparency Register No. 9833410101750-70

GDPR. It is a faithful application of the law's full objectives and of the wider values of the European Union.

If the EDPB is to act within its mandate under Article 70 GDPR, and as a body of the EU, the Board should wait for the legislators to agree on the wording of GDPR and then provide practical guidance to support its implementation.

To this end, Privacy Next Recommends that the EDPB should:

- Formally withdraw the proposed guidelines until the current Digital Omnibus process is concluded.

- Unequivocally confirm that the contextual approach is the authoritative legal assessment and that the proposed simplified approach is optional.

- State that national supervisory authorities must not infer that data are personal, or that an infringement has occurred, merely from a failure to use or satisfy the simplified approach.

- Identify the specific legal basis for the exclusion of processors in paragraph 15 or remove it.

Square de Meeûs18 | Brussels Belgium | 1050
www.privacynext.eu | info@privacynext.eu
Transparency Register No. 9833410101750-70