Contribution to the Public Consultation on EDPB Guidelines 02/2026 on Anonymisation

Introduction We welcome the European Data Protection Board's (EDPB) efforts to clarify the concepts of anonymisation. However, we must express our profound concern that the proposed "contextual approach" introduces far too many exceptions and loopholes into the European data protection framework. By making anonymity relative, the Guidelines risk severely diluting the objective standards of data protection, creating dangerous "safe havens" for data exploitation under the guise of anonymity. We respectfully submit the following critical observations.

1. The Slippery Slope of Relative Anonymity: The "Unrecognized Face" Paradox The fundamental flaw of the contextual approach is that it encourages subjective assessments of identifiability. If anonymity is judged solely from the perspective of the recipient's immediate capabilities, it opens the door to dangerous misinterpretations. Take the example of a photograph containing a human face. Under a strictly relative interpretation, a controller or a recipient might argue: "I do not know this person, and I do not have the immediate tools to identify them; therefore, this is not personal data *to me*." This is a highly dangerous precedent. A recognizable human face is inherently and globally identifiable by its very nature. Allowing entities to treat such data as "non-personal" simply because they personally lack the background knowledge ignores the objective reality of the digital age, where facial recognition and public databases are omnipresent. Anonymity must remain an objective, absolute standard to prevent such systemic loopholes.

2. The Illusion of "Anonymous" Research Data The Guidelines suggest that sharing rich, pseudonymised datasets (e.g., patient records or clinical trials) with independent researchers can render the data "anonymous" for the recipient if they lack the decryption key and are contractually prohibited from re-identifying the subjects. This is a dangerously naïve assumption. In the era of Big Data, it is practically unimaginable that datasets rich enough for meaningful scientific or market research do not contain enough unique data points to allow for linkage and profiling. Behavioral patterns, rare attributes, or cross-referenced prescription data inevitably lead to unique profiles. Claiming that a dataset is "anonymous" simply because a contract forbids re-identification is merely "security by obscurity." It removes these highly sensitive datasets from the protective scope of the GDPR precisely when data subjects are most vulnerable to profiling.

3. Penalizing Data Minimization: Anonymisation as a Legal Hurdle The Guidelines maintain that the act of anonymisation itself constitutes "further processing" and therefore requires a valid legal basis. This creates a counterproductive regulatory paradox. Data minimization and storage limitation are core principles of the GDPR. When a controller decides to permanently strip personal data of its identifiable elements—effectively relinquishing control and terminating the privacy risks for the data subject—regulatory authorities should welcome and encourage this action. Instead, treating the technical act of deletion or anonymisation as a heavily regulated "further processing" step forces controllers to jump through administrative hoops (e.g., establishing a new legal basis, updating privacy notices). We should not restrict or penalize controllers who want to proactively eliminate personal data. Anonymisation should be viewed as a compliance measure and a security safeguard, not as a new processing activity that requires independent justification.

Conclusion

The proposed Guidelines introduce too many exceptions that will be inevitably exploited. We urge the EDPB to abandon the overly permissive contextual loopholes and return to a robust, objective standard of anonymity. Furthermore, the act of anonymising data should be deregulated and promoted as a fundamental privacy-enhancing mechanism, rather than hindered by unnecessary bureaucratic requirements.