1. Introduction and Scope

Syntonym Limited ("**Syntonym**") welcomes the opportunity to contribute to the public consultation of the European Data Protection Board (the "**Board**") on the draft Guidelines 02/2026 on Anonymisation, adopted on 7 July 2026 (the "**Guidelines**"). We support the Board's objective of enabling the use of effectively anonymised information while protecting individuals' rights and freedoms. Our contribution is offered from the perspective of a developer of privacy-enhancing technology for camera-captured data and is confined to questions arising in the deployment, validation and subsequent use of such technologies.

Syntonym is a developer of privacy-enhancing technology in the visual data domain. We provide anonymisation and pseudonymisation technology to organisations that process image and video data captured by camera systems. Our technology replaces identifying elements, such as faces, bodies and vehicle license plates, with synthetic alternatives while preserving non-identifying visual and behavioural signals, such as gaze direction, blinks, head pose, facial expressions and movement. We also provide conventional redaction techniques such as blurring, pixelation and masking for other identifying elements and indirect identifiers in visual data. Synthetic replacements are designed to preserve signals that are needed for computer vision development, and no mapping between the original and synthetic replacements is retained.

The organisations we support process camera data to develop and validate autonomous driving systems, advanced driver assistance systems, driver and occupant monitoring systems, robotics and human-robot interaction, workplace safety, research, wearables and other camera-based applications. These systems typically require faces, gaze, head pose, expressions and body movement to remain analytically usable, which is why the choice of anonymisation technique has a direct bearing on whether controllers are able to rely on anonymous information or instead retain identifiable footage.

Clear guidance can make effective safeguards easier to adopt. Organisations willing to anonymise footage may nevertheless be uncertain about the evidence required and the legal position of subsequent use, training, validation or sharing. If that uncertainty delays adoption, identifiable visual data may continue to enter AI workflows unnecessarily, increasing opportunities for identification, profiling and surveillance. Against wider concerns about AI safety, practical clarity would help translate advances in privacy-enhancing technology into protection for individuals. We therefore encourage

examples connecting the Guidelines' legal framework to the decisions controllers processing visual data actually face, without reducing the standard of effective anonymisation.

2. General Observations

Syntonym welcomes the Guidelines and supports their objective. The structured assessment offers controllers a coherent and auditable method when assessing whether personal data has been rendered anonymous. We particularly welcome the confirmation that the likelihood of identification must be insignificant rather than zero (paragraph 22); the articulation of the No Record Isolation, No Linkage and No Inference criteria, together with the simplified and contextual approaches; the requirement that an inference be both specific and meaningful; the recognition that anonymisation does not depend on the deletion of the original data (paragraph 10); and the emphasis on documentation, testing, periodic reassessment and the sharing of expertise on the state of the art (paragraphs 35, 41 and 84).

The observations that follow are intended to assist the Board in addressing those questions. In our experience, greater clarity would enable more controllers to adopt anonymisation at an early stage, in line with Articles 5(1)(c) and 25 of the GDPR, and would reduce the unnecessary retention and circulation of identifiable footage in research and AI development workflows.

3. Application of the Framework to Image and Video Data

Our principal observation is that the Guidelines are framed primarily by reference to structured and aggregate data. Visual data nonetheless represents one of the most significant categories of personal data processed for the development of AI systems, and the controllers processing it face distinct questions as to how the three criteria are to be applied in practice.

The concepts of record, record-level data, and attribute are well suited to structured datasets. In visual data, a single individual may appear across many thousands of frames and in several camera streams. Computer vision development usually requires an individual's movements or gaze to remain coherent within a sequence. Example 5 usefully demonstrates that attributes which are individually common may single out an individual when combined. At the same time, treating every visible attribute as identifying would render anonymisation impracticable and would remove the information for which the data is processed. Syntonym would therefore welcome a short passage, or a dedicated example, explaining how these terms apply to image and video data.

4. Anonymisation at the Point of Capture and Anonymisation of Existing Datasets

In our experience, anonymisation of visual data is applied under two principal deployment models, each of which all for different considerations under the Guidelines. The first is anonymisation at the edge, at the point of collection or capture, where raw frames are processed transiently on the device and identifiable footage is not stored or transmitted beyond the collection and anonymisation window. The second is the anonymisation or pseudonymisation of previously collected data through a hosted or on-premise service, before the resulting dataset is used for model training, retraining, validation and testing, shared with research partners or annotation providers, or publicly released.

Where anonymisation takes place at the edge, retrospective comparison of original and processed footage is not normally available, because originals are deliberately not retained. Syntonym would welcome guidance on the combination of evidence that would be appropriate in that setting, which might include controlled pre-deployment testing on representative material, validation on target hardware, runtime checks and operational records that do not require routine storage of identifiable footage. An illustrative scenario would provide an actionable route to data protection by design without requiring routine retention that undermines the benefit of edge processing.

For post-collection processing where anonymisation is applied to existing datasets, controlled access to originals generally permits direct comparison with processed outputs. In that setting, the Guidelines could illustrate a validation process combining re-identification testing by a motivated intruder, linkage testing appropriate to the intended release context, and evaluation of whether the processed data remains fit for its intended purpose.

5. Perspectives and Roles of Technology Providers

Anonymisation technology is supplied under several arrangements: as software operated by the controller on its own devices or infrastructure, where the provider has no access to the data; as a managed service, where the provider processes data on the controller's behalf; and in hybrid arrangements, which may include access to original data for support and validation.

Syntonym respectfully suggests that the Guidelines clarify that a provider that supplies validation methodology, test results or recommended configurations does not thereby determine the purposes and means of the processing, which, together with the resulting

assessment and decisions on use and disclosure, remain the responsibility of the anonymising controller.

Practical adoption would also benefit from encouraging consideration of the state of the art when assessing whether anonymous information can meet a purpose. Whether a controller concludes that its purposes can be fulfilled using anonymous information often depends on the technique it has in mind. For visual data, if the comparison is with blurring, pixelation or masking, many computer vision projects will conclude that anonymous information cannot provide the required utility, because those techniques remove the facial and behavioural signals being studied, and may then rely on retaining identifiable footage. Utility-preserving synthetic replacements that retain gaze, expressions, head pose and movement change that conclusion for many such projects.

6. Concluding Recommendations

Syntonym would like to thank the Board for its work on the Guidelines, which will provide much-needed clarity for organisations seeking to make responsible use of data. Effective and well-understood anonymisation allows innovation to proceed, and clear guidance on visual data would, in our view, encourage more controllers to choose anonymisation over the retention of identifiable footage. The principal opportunity is to connect the principles set out in the Guidelines with a practical path from deployment and validation to confident downstream use. Syntonym would welcome the opportunity to contribute technical experience, should this be of assistance to the Board.