1. Assessment of individual-level anonymisation risk (Paragraph 35)
Paragraph 35 states that anonymisation must be effective for every individual and that a low overall risk across a dataset is insufficient if some individuals remain identifiable. We would welcome further guidance on how controllers are expected to assess this requirement in practice without undertaking additional processing of personal data that goes beyond what is necessary for the original purpose. Assessing whether particular individuals remain identifiable, for example because they are statistical outliers or have rare combinations of attributes, may require more detailed analysis of individual-level records and, potentially, consideration of external datasets that were not relevant to the original processing activity.

We therefore ask the EDPB to clarify:

- How far controllers are expected to go in identifying and assessing outliers or other individuals who may face a higher risk of re-identification.
- What level of additional processing would be considered proportionate and reasonable for the purpose of assessing anonymisation risk.
- Whether any such assessment constitutes a separate processing activity requiring its own legal basis and compliance with data protection principles such as data minimisation.
- How these expectations should be applied in practice, particularly where extensive additional analysis may itself increase the amount of personal data being processed.

Worked examples and detailed case studies illustrating proportionate approaches in different scenarios would be particularly helpful.

2. Status of data shared between controllers and processors
We would welcome greater clarity on how the concept of anonymisation applies where data is shared between different parties, particularly joint controllers, controllers and processors, and processors acting on behalf of controllers.

In particular, we would welcome clarification of whether the status of a dataset should be assessed from the perspective of each recipient, or whether data that constitutes personal data for one party must necessarily be treated as personal data by all parties involved in the processing arrangement.

We would ask the EDPB to specify:

- Can a dataset be considered anonymous with respect to a recipient that has no reasonable means of re-identifying individuals, even where another party retains information that would enable re-identification?
- Does the answer differ in the context of joint controllership arrangements?

- Does the answer differ where a processor anonymises data on behalf of a controller and returns the resulting dataset to the controller?
- How should the availability of keys, mapping tables, or other supplementary information held by only one party be taken into account when determining whether data is anonymous?

Worked examples would be particularly valuable. For example:

- Two joint controllers where only one party retains the key or additional information required to re-identify individuals.
- A processor carrying out anonymisation on behalf of a controller and returning an anonymised dataset to the controller while not retaining the means of re-identification itself.

These examples would help organisations understand how the relativity of identifiability should be assessed in multi-party processing arrangements.