



Anonymization Reassessment:

Six Changes to Watch

A practical trigger guide for privacy, legal, governance and data teams

Use this guide when an earlier conclusion of anonymity may depend on assumptions that have changed.

A trigger does not mean the data is no longer anonymous. It means an assumption may need to be tested again. Even where one EDPB criterion is affected, further analysis may still be needed before the data is treated as personal.

Before you start

Dataset / data release: _____	Last anonymity assessment: _____
For whom was the data intended to be anonymous? _____	Assessment / version / reference: _____

Ask first: What was assumed to be unavailable, separate, too difficult, too costly or insufficiently revealing and is that assumption still true?

1. The data became richer or more precise

What changed: More fields, finer locations, precise timestamps, longer histories or less aggregation.

Why it matters: More detail can make a record distinctive even without a name.

Example: Year of birth and city become full date of birth, postcode, occupation and exact timestamps.

What to check:

- Compare current fields with the version originally assessed.
- Check whether granularity increased or aggregation decreased.
- Look for attribute combinations that may now be unique.

What to do next: If uniqueness may have increased, test Record Isolation and consider Linkage where outside data could connect the record to a person.

EDPB lens: No Record Isolation; data properties; dimensionality and resolution.

2. New information can now be linked to the data

What changed: A new public, commercial, internal or leaked source overlaps with the anonymized dataset.

Why it matters: A dataset can become easier to identify when another source supplies matching attributes.

Example: Age, general location and profession later overlap with a new public register that also contains names.

What to check:

- Identify new sources that did not exist or were not realistically accessible before.
- Check for overlapping attributes or behavioral patterns.
- Ask whether confidential linking information has been exposed.

What to do next: Where meaningful overlap exists, perform targeted Linkage analysis. Several strong sources or a clear matching route may justify fuller reassessment.

EDPB lens: No Linkage; additional information; chains of means.



3. Who can access the data has changed

What changed: A new recipient, wider internal access, public release, a new vendor, or a breach changes who can reach the data or related information.

Why it matters: Anonymity may differ by perspective because entities have different information and capabilities.

Example: A dataset once restricted to a research institute with no identifying records is later published online.

What to check:

- Who can access or realistically receive the data now?
- What additional information does those entities hold?
- Is the recipient acting independently, or processing on behalf of another entity whose perspective may apply?
- Did a security incident undermine an assumption of restricted access?

What to do next: Reassess the relevant perspective. Public release, major access expansion, or a significant leak may justify fuller reassessment.

EDPB lens: *Relevant entity perspective; access; means reasonably likely to be used.*

4. Re-identification has become cheaper, faster or easier

What changed: Improved search, computing, automated matching, machine learning or LLMs reduce the expertise, time or cost needed.

Why it matters: A method once dismissed as impractical may now fall within the means realistically likely to be used.

Example: Hundreds of pseudonymous posts once needed manual review; an LLM can now extract identity clues automatically.

What to check:

- Review methods previously excluded as too costly, slow or specialized.
- Check whether tools are now readily available.
- Ask whether the task can now be run at much greater scale.

What to do next: Where a key feasibility assumption has changed, carry out targeted re-identification testing.

EDPB lens: *Means reasonably likely to be used; time and cost; available technology.*

5. AI can now search and combine sources that used to stay separate

What changed: An AI system or agent can use web search, APIs, retrieval tools, internal databases, external directories or code in one workflow.

Why it matters: This emerging capability can remove practical separation between information sources. The EDPB specifically notes that AI, especially agentic AI, is likely to reduce the time and cost of re-identification and may make gathering and combining information from multiple sources easier.

Example: A research team receives data that was assessed as anonymous from its perspective because it had no access to identifying customer records. A new AI agent later gives that team access to both the research dataset and systems containing identifiable customer information.

What to check:

- Identify which relevant entities can now use AI or agents to access and combine data, and what systems or datasets those tools can reach.
- Check whether the AI system or agent can retrieve identified and supposedly anonymous information.
- Review new connectors, APIs, permissions and external search capability.

What to do next: If previously separate sources can now realistically be combined, test Linkage and Inference. Broad capability changes may justify fuller reassessment.

EDPB lens: *No Linkage; No Inference; additional information; changing capability.*



6. New inferences can be drawn from the data

What changed: New analytical or AI techniques can derive person-specific information that was not explicitly present, such as likely home/work locations, membership or attributes.

Why it matters: Re-identification can begin with inference. Newly inferred information may help single out or link a person.

Example: A mobility dataset contains no home address. A newer method infers likely home and workplace from recurring movement patterns.

What to check:

- What can current tools infer that older tools could not?
- Is the inference specific to an individual, meaningful, reliant on this data, and capable of affecting that individual's rights or interests?
- Could the inferred information assist singling out or linkage?

What to do next: Conduct targeted Inference analysis. Do not treat every prediction as a failure: the EDPB requires a sufficiently specific and meaningful inference.

EDPB lens: *No Inference; possible downstream Record Isolation or Linkage.*

Small numbers can still matter. A re-identification technique that works for only a small subset - potentially even one individual - can still require further analysis.

What should happen when you identify a change?

DOCUMENT / MONITOR	After preliminary review, there is no credible indication that the change affects re-identification capability. Record what changed, why the earlier assumptions remain reasonable, and when to review again.
TARGETED ANALYSIS / TESTING	A specific assumption may have changed. Test the affected issue: Record Isolation, Linkage, Inference or relevant-entity perspective.
FULLER REASSESSMENT	Several material assumptions changed, access expanded substantially, a credible new re-identification route exists, targeted testing reveals a material vulnerability, or an EDPB anonymity criterion appears not to be met and requires further analysis.

RED FLAG: confirmed re-identification

If a supposedly anonymous record has been connected to an individual, escalate immediately. Where the individual has been identified, the information is not anonymous from that relevant perspective. The question is no longer only whether identification might realistically be possible in the future.

Source basis: EDPB Guidelines 02/2026 on Anonymization (Version 1.0, adopted 7 July 2026 for public consultation) and supporting technical literature on re-identification methods, including record linkage, inference, mobility re-identification, and emerging LLM/agentive techniques.

This guide is a reassessment trigger aid, not a substitute for a legal or technical anonymization assessment. For general information only; not legal advice.