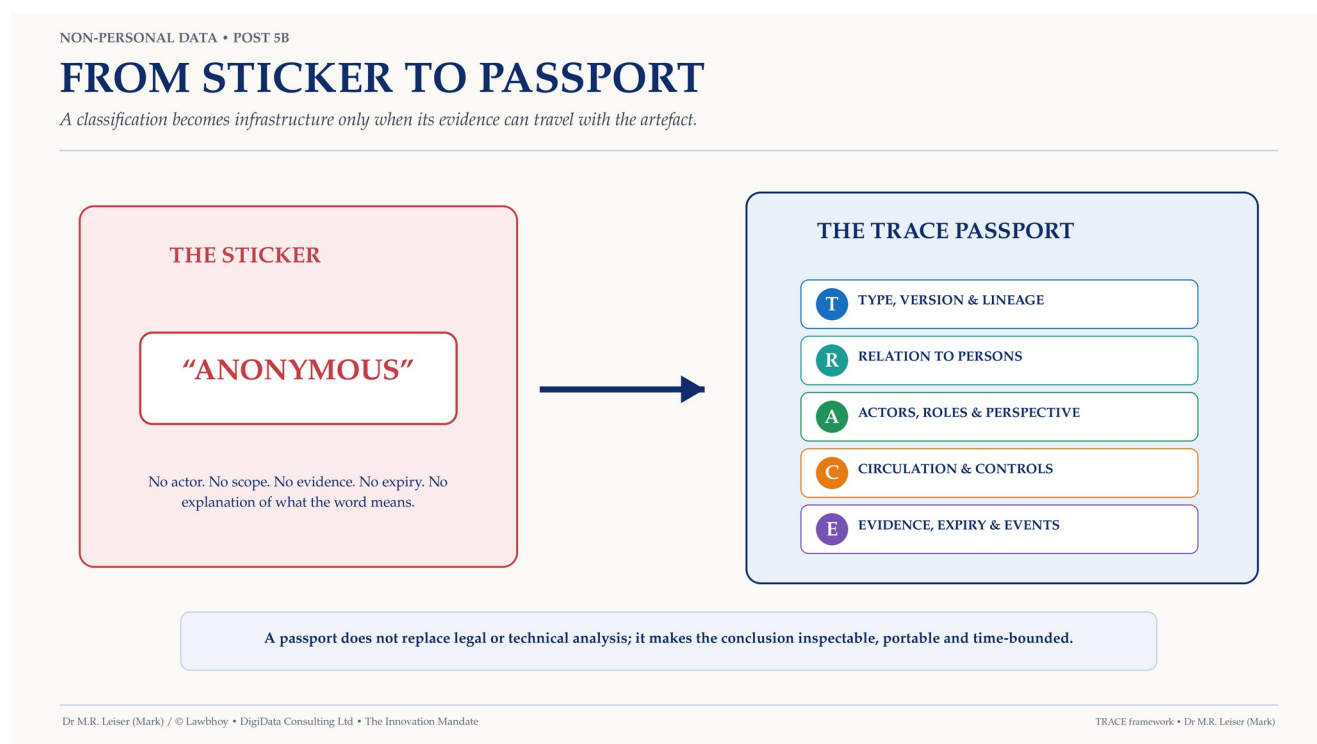


From Sticker to Passport

TRACE and the AUIA can turn contextual anonymisation into a portable, auditable and time-bounded claim.

This is Post 5B, the companion to my repaired taxonomy of non-personal data. Post 5A separates legal status from route, scope, artefact form, circulation and assurance; this essay asks how an organisation can attach that structure to a real dataset, statistic, model or output without reducing the exercise to another label. The answer is a documentation stack in which the EDPB supplies the legal baseline, the Anonymisation and Utility Impact Assessment provides the full evidential dossier, and the TRACE Data Status Passport carries a concise, machine-readable summary with the artefact.

Image 1 — From Sticker to Passport



Caption: A bare “anonymous” sticker conceals the actor, scope, evidence and expiry, while TRACE records each element in a portable passport.

Alt text: A red sticker marked anonymous points towards a structured TRACE passport containing five fields.

Keywords: TRACE passport, data status, anonymisation documentation, portable assurance, evidence, expiry

Designing a taxonomy is easier than preserving its meaning once an artefact begins to circulate. The failure usually begins when the status claim leaves the room in which it was made. A controller writes “anonymous” in a data catalogue, a vendor describes a synthetic dataset as privacy-safe, a clean-room operator refers to de-identified records, or a research consortium passes a transformed table to a new participant without carrying forward the assumptions that supported the original conclusion. The receiving organisation then sees the adjective but not the actor analysis, the route, the intended circulation, the known auxiliary information, the technical tests, the controls or the events that would invalidate the claim. A careful assessment becomes a sticker when the adjective travels but the reasoning, evidence and limits remain behind.

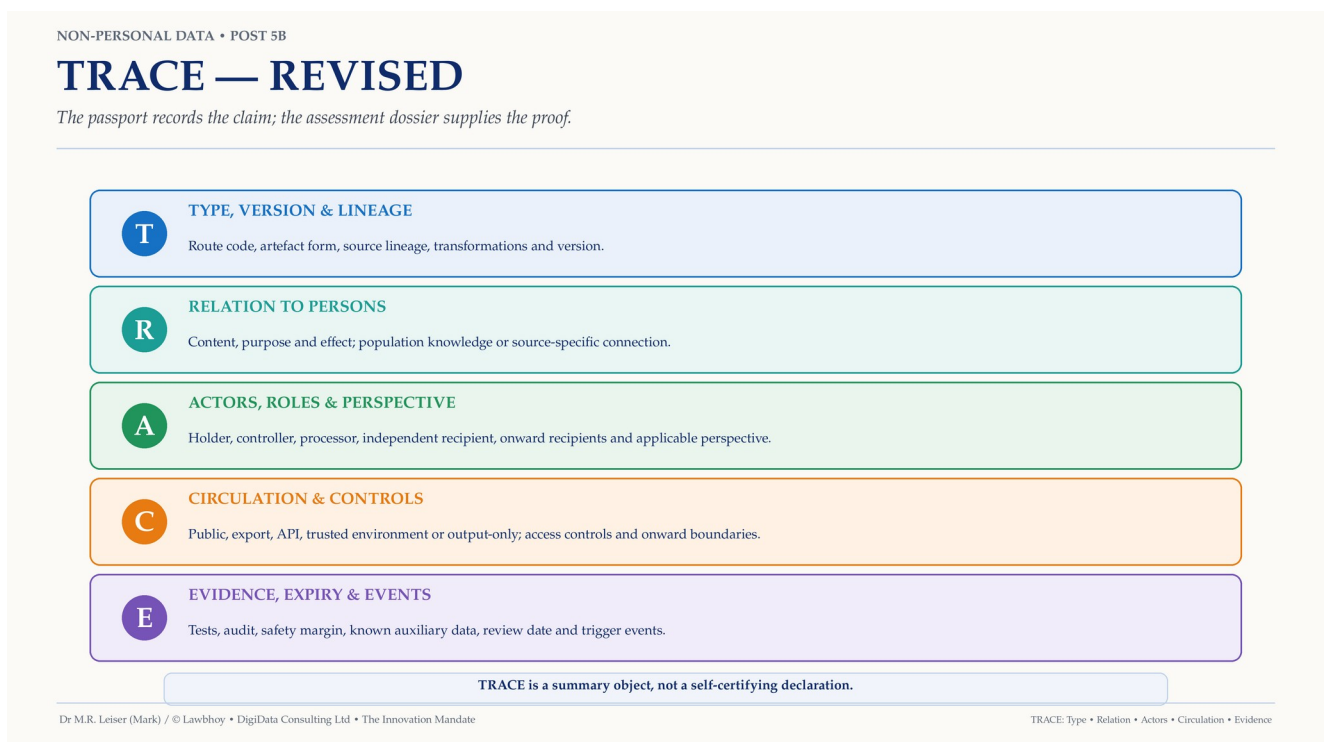
Guidelines 02/2026 already contain the elements of a better approach. The Board asks organisations to map the given data and relevant auxiliary information, identify the relevant entities and applicable perspectives,

apply the criteria of No Record Isolation, No Linkage and No Inference, document the anonymisation process and testing, and revisit the conclusion when the surrounding conditions change. Paragraph 41 expressly requires documentation to survive the anonymisation process, while Annex 1 converts the analysis into a flowchart. The guidelines therefore recognise that anonymity is not a one-off transformation claim; it is an evidenced conclusion about an artefact, an actor, an access environment and a point in time.¹

TRACE records the claim rather than replacing the proof

TRACE should sit above that assessment as a portable summary. The revised acronym stands for Type, version and lineage; Relation to persons; Actors, roles and applicable perspective; Circulation and controls; and Evidence, expiry and events. Each field answers a question that a bare label suppresses, while the structure remains compact enough to travel through a data catalogue, model registry, research environment, procurement pack or regulatory file. TRACE does not certify its own accuracy, and it does not replace a lawyer, engineer or supervisory authority; it creates a common object that those people can inspect and challenge.

Image 2 — TRACE, Revised



Caption: TRACE records type and lineage, relation to persons, actors and perspective, circulation and controls, and the evidence and events governing the claim.

Alt text: Five horizontal rows spell out the revised TRACE fields and the information contained in each one.

Keywords: TRACE, type and lineage, relation to persons, applicable perspective, circulation controls, evidence expiry events

The T field records the artefact's route code, form, version and lineage. An organisation should state whether the artefact followed the native, statistical, transformed or synthetic route; whether it is a dataset, aggregate, model, embedding, feature, benchmark or output; which source materials contributed to it; which transformations occurred; and which version the assessment covers. Separating route from form prevents a model from becoming a legal category and prevents a synthetic label from doing more work than provenance can justify.

The R field records the relationship to natural persons by content, purpose and effect. It should distinguish population-level knowledge from a source-specific connection, record whether the artefact supports evaluation or treatment of an individual, and identify any circumstances in which the use of a technically ordinary artefact could create a personal nexus. A statistic may remain non-personal even when someone

later applies it to a new person; a model or output may remain personal where its behaviour depends on the inclusion or characteristics of someone represented in the source data. The field therefore captures the conceptual distinction at the heart of the EDPB's No Inference analysis.¹

The A field identifies the actors, their roles and the legally applicable perspective. It records the holder, source controller, processors, independent recipients, authorised users, potential onward recipients and any actor whose information or capabilities contribute to identification through means reasonably likely to be used. The processor question belongs here because a technically blind vendor cannot claim its own actor-specific non-personal status where it acts on the controller's instructions and the controller can identify the individuals. A genuinely independent research recipient may stand differently, but the passport must state the role analysis rather than leaving the reader to infer independence from a contract label.¹

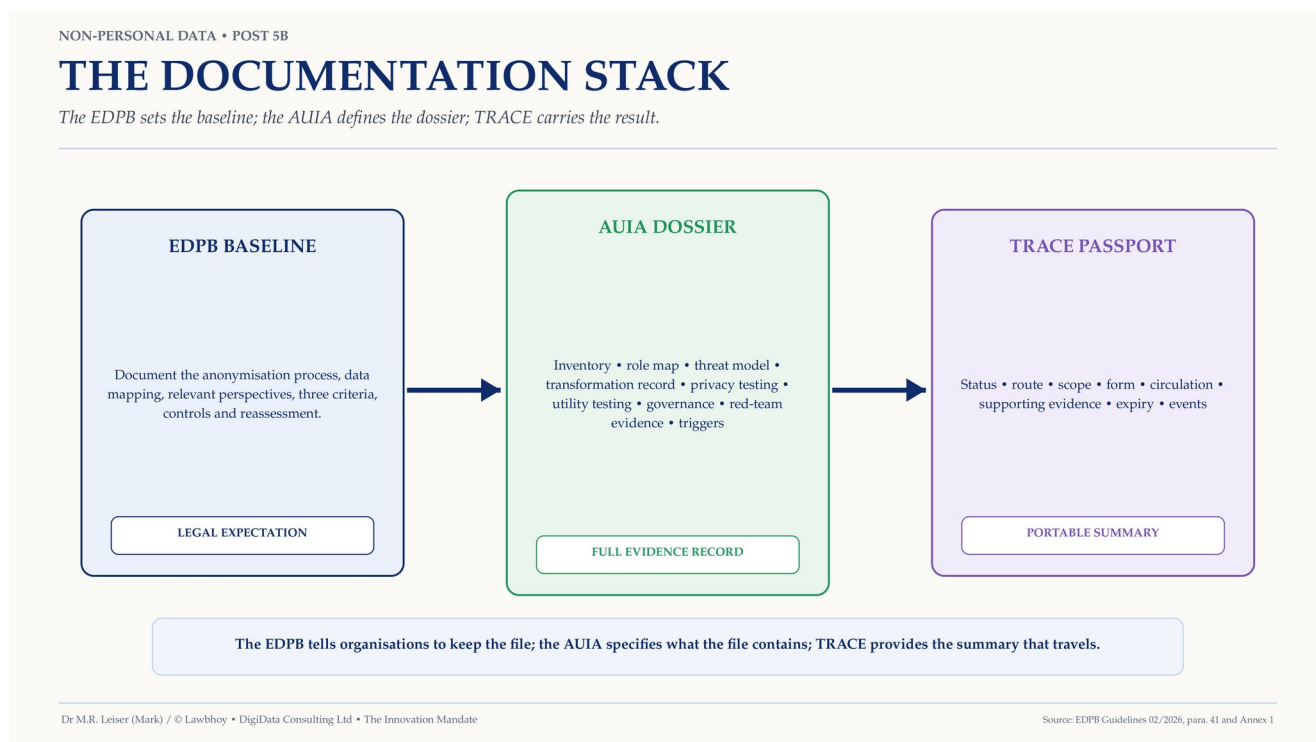
The C field records circulation and controls in the same place while keeping their legal functions distinct. It states whether the artefact will be published, exported, queried through an API, held within a trusted environment or exposed only through output checking. It also records access controls, key separation, contractual restrictions, audit rights, logging, monitoring, retention and onward-transfer boundaries. The field deliberately combines modality and controls because both shape the means reasonably likely to be used, but the passport should also state that neither performs the legal transformation by itself. A clean room may be an excellent way to process personal data safely; it does not make identifiable data anonymous merely by enclosing it.¹²

The E field records evidence, expiry and events so that reliance has both a factual basis and an explicit end point. It identifies the record-isolation, linkage, inference, membership, memorisation, extraction or reconstruction tests that were performed; the assessor, method, date and result; the safety margin; the known auxiliary datasets; the audit or certification evidence; the review date; and the events that require reassessment. The field turns the EDPB's open-ended instruction to reconsider anonymity "where possible and appropriate" into an explicit lifecycle that can support reliance without pretending that a status claim remains eternally true.¹

The AUIA supplies the dossier beneath TRACE

The passport remains only a summary, which means that it requires a full assessment dossier underneath it. My Article 6(11) DMA work proposed an Anonymisation and Utility Impact Assessment, or AUIA, because access remedies often fail when privacy testing and usefulness are treated as sequential afterthoughts. An AUIA records the data inventory, actor and role analysis, threat model, transformation method, technical parameters, privacy tests, utility tests, access controls, contractual and organisational safeguards, red-team evidence, residual risk, approval decision and reassessment triggers. TRACE extracts the portable status claim from that dossier; it does not duplicate the dossier or hide its uncertainty.³

Image 3 — The Documentation Stack



Caption: *The EDPB provides the legal baseline, the AUIA creates the full evidence record, and TRACE carries a portable summary.*

Alt text: Three large boxes labelled EDPB baseline, AUIA dossier and TRACE passport are linked by arrows.

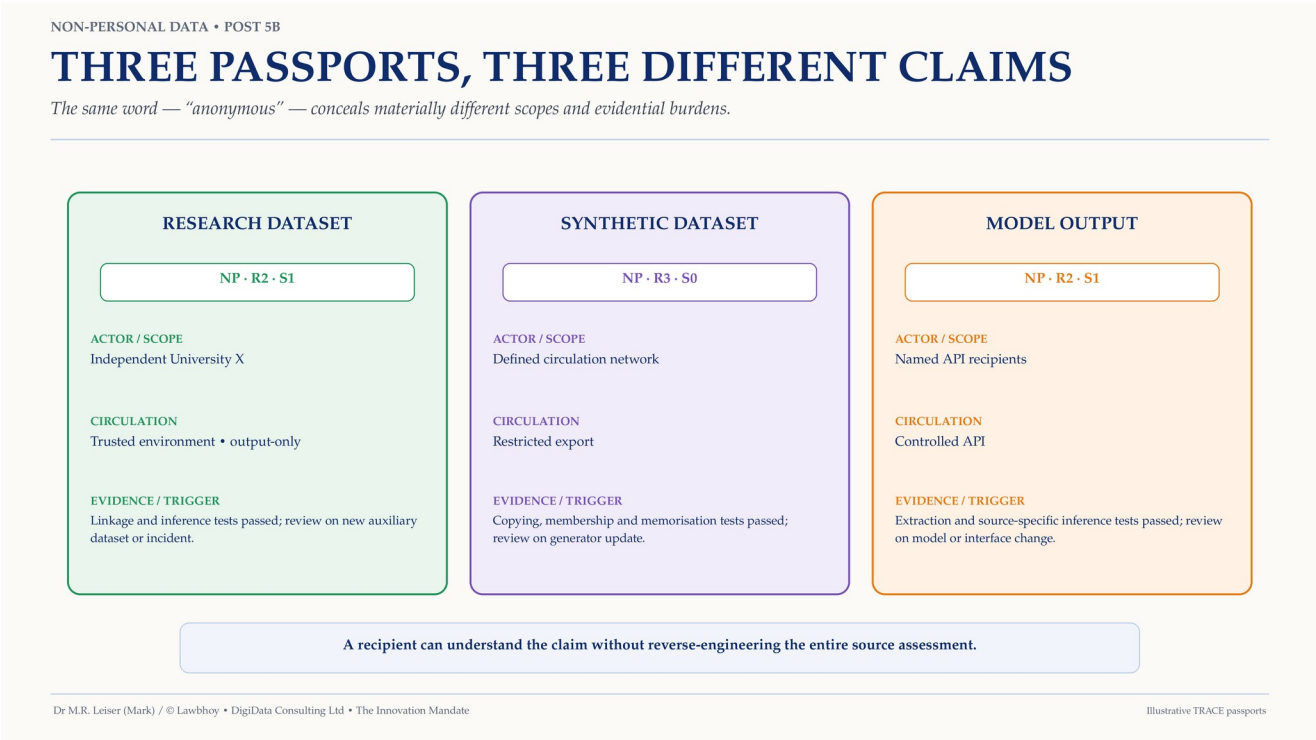
Keywords: EDPB documentation, AUIA, TRACE passport, anonymisation evidence, utility assessment, portable summary

The relationship between the three layers can be stated plainly without flattening their separate functions. The EDPB tells organisations to keep a file; the AUIA defines what the file should contain; TRACE provides the summary that travels. The EDPB baseline includes data mapping, relevant entities, applicable perspectives, the three criteria, controls and reassessment. The AUIA adds the operational detail required to understand how the organisation balanced residual identification risk against the utility needed for research, competition, analytics or AI. TRACE then condenses the decision into a standard form that another organisation can read without reverse-engineering the source controller's entire legal and technical history.

Utility belongs in the assessment because an anonymisation method that destroys the information needed for the lawful purpose may be formally safe but institutionally useless. The AUIA should therefore test whether the transformed artefact preserves the minimum analytical, scientific or competitive function for which it is intended, while recording less intrusive alternatives and stop conditions. That does not create a balancing test in which commercial value overrides identifiability. It ensures that the organisation chooses the least risky lawful artefact capable of delivering the legitimate function, rather than oscillating between raw access and data so degraded that the policy objective disappears.³⁴

Worked passports expose the differences that “anonymous” conceals

Image 4 — Three Passports, Three Different Claims



Caption: A research dataset, synthetic dataset and model output can all be non-personal, but each carries a different route, scope, circulation condition and evidential burden.

Alt text: Three passport cards show recipient-specific research data, circulation-wide synthetic data and a controlled model output.

Keywords: research dataset, synthetic data, AI model output, TRACE examples, recipient-specific scope, circulation

A transformed clinical dataset might carry the label “NP-R2-S1 · DATASET · TRUSTED ENVIRONMENT”. The T field records the source records, transformation and version; the R field explains that the table preserves population-level clinical information without a source-specific route to identity; the A field identifies the hospital as source controller and University X as an independent recipient; the C field limits access to an accredited environment with output checking and no onward export; and the E field records linkage and inference tests, known auxiliary datasets, the assessor, and review triggers tied to a new public dataset or security incident. The passport makes clear that the conclusion does not automatically travel to another university or into public release.

A synthetic dataset might carry the label “NP-R3-S0 · SYNTHETIC DATASET · RESTRICTED EXPORT”. The R3 route records generation rather than transformation, while S0 states that the assessment covers the defined circulation network rather than a single recipient. The evidence should include copying, membership, memorisation, rare-sequence and source-specific inference tests, together with a trigger for any material generator update. A new version may preserve the schema while changing the privacy behaviour, which means that the passport attaches to the version rather than to the product family.

A model output might carry the label “NP-R2-S1 · MODEL OUTPUT · CONTROLLED API”. The form tells the reader that the object is not a row-level dataset; R2 records that the output emerged from transformed personal data rather than synthetic generation; S1 limits the conclusion to named API recipients and the assessed interface; and the evidence records extraction, membership and source-specific inference tests. If the provider changes the prompt interface, retrieval layer, model weights or output controls, the trigger event may invalidate the passport even though the product name remains unchanged.⁵⁶

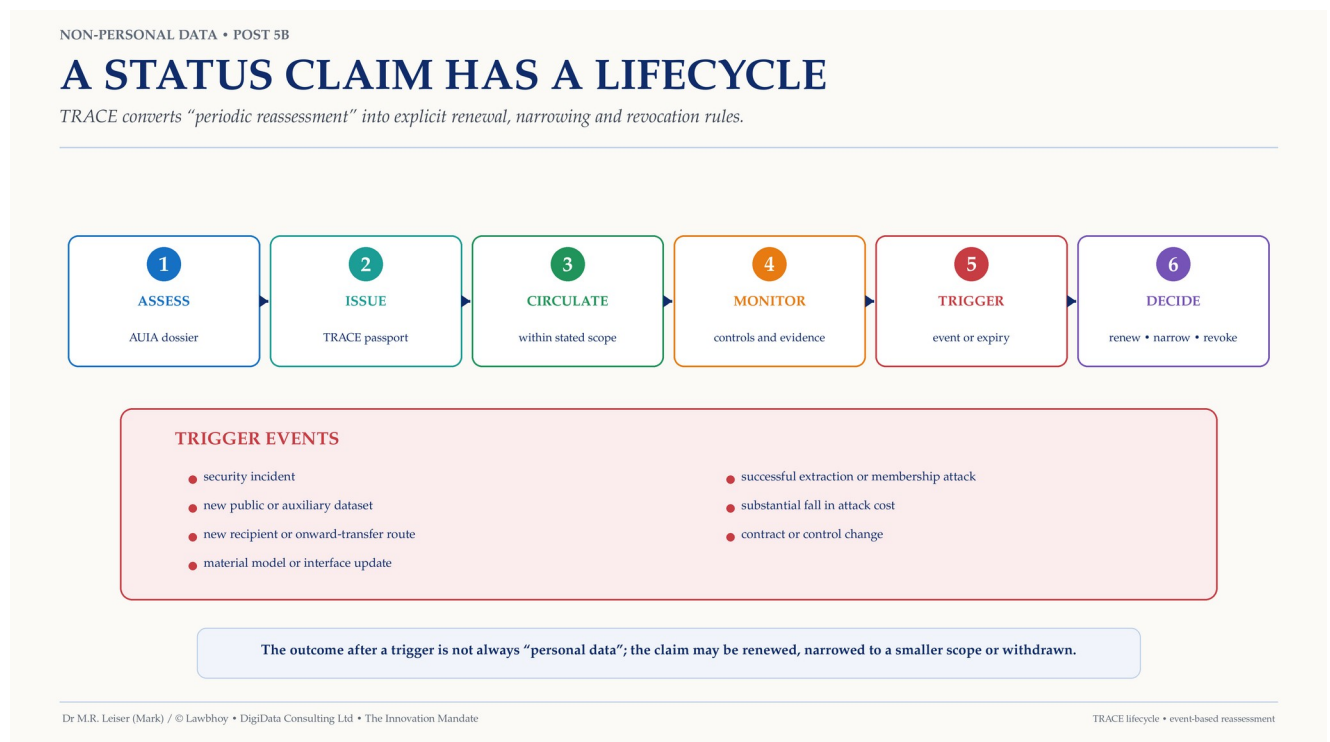
Article 6(11) DMA shows why status and access must remain separate

Article 6(11) of the Digital Markets Act supplies a useful stress test because it requires a gatekeeper operating an online search engine to provide rival search engines with access to ranking, query, click and view data, while requiring personal data in those categories to be anonymised. A privacy-preserving aggregate API may deliver an R1 artefact; an exportable common-tail dataset may follow R2 with S0 or S1 scope; a synthetic sample may follow R3 after membership and memorisation testing; and a model or benchmark must receive the route that describes its actual lineage rather than an obsolete N5 label. Identifiable rare-query data remains personal even inside a clean room, although the clean room may still provide a lawful access modality for governed processing.³⁷

The AUIA determines which artefact and access tier can deliver contestability value through the least risky lawful route. TRACE carries the resulting claim to the recipient and the Commission, stating whether the artefact is exportable, API-mediated, output-only or still governed personal data. That distinction prevents access architecture from silently rewriting the status field, while also avoiding the opposite error of insisting that every useful competitive signal must emerge as a downloadable row-level dataset.

Expiry should follow events rather than administrative superstition

Image 5 — A Status Claim Has a Lifecycle



Caption: TRACE turns periodic reassessment into explicit triggers that lead to renewal, narrowing or revocation.

Alt text: A six-step lifecycle runs from assessment through passport issue and circulation to trigger events and a decision to renew, narrow or revoke.

Keywords: reassessment, lifecycle, security incident, model update, auxiliary data, status revocation, TRACE

The EDPB correctly recognises that re-identification risk changes over time, but “periodic reassessment” is too imprecise to support infrastructure unless organisations know what should cause a fresh analysis. TRACE should record both a review date and event-based triggers: a security incident, a new public or auxiliary dataset, a new recipient or onward-transfer route, a material model or interface update, a successful extraction or membership attack, a substantial fall in the cost of a relevant technique, or a material change in contract or control architecture. The occurrence of a trigger does not predetermine the result; the organisation may renew the passport, narrow its scope, impose additional controls or revoke the claim.¹

This lifecycle also creates a more honest allocation of responsibility. The issuer owns the original assessment and must disclose the conditions that support it; the recipient must remain within the stated scope and notify relevant changes; auditors or certifiers can test the evidence and controls; and regulators can challenge the classification without pretending that the word anonymous proves or disproves itself. A machine-readable passport can preserve the same fields across a data space, model registry or research environment, while the human-readable version supplies the reasons needed for legal scrutiny.

The Omnibus can turn the stack into common infrastructure

The Digital Omnibus should give this documentation stack a legal home. It could require a common minimum passport for actor-specific or certified non-personal claims, empower the EDPB and Commission to develop sectoral AUIA profiles, and connect certification to a rebuttable presumption that the classification was reasonable at the assessment date. The presumption should fall away where the organisation concealed facts, engineered artificial separation, ignored a trigger, permitted uncontrolled onward transfer or relied on a materially changed artefact. Such a system would provide reliance rather than immunity and would give SMEs and research bodies a reusable method instead of forcing them to commission a fresh legal-engineering project for every dataset.⁸⁹

The Innovation Mandate supplies the public-law discipline for that work. When regulators choose the evidence, safety margin, review period or certification threshold that will govern a major class of data use, they shape scientific collaboration, market entry, AI development and the practical protection of rights. They should therefore explain the alternatives, the rights risk, the innovation consequence and the reason why the chosen burden is no more restrictive than the law requires. TRACE makes the decision object visible; the AUIA makes the evidence visible; the mandate requires the supervisory reasoning to become visible as well.⁹

The next step is product development rather than another conceptual layer. The repaired taxonomy can become the classification logic, the AUIA can become a guided assessment and evidence dossier, and TRACE can become the output generated for a defined artefact, actor and circulation plan. A useful tool should never announce that data is anonymous through a black-box model; it should ask structured questions, expose missing evidence, record competing interpretations and generate a candidate passport for professional approval. The architecture is now sufficiently clear to begin that work without embedding the original N5 overlap in software.

Sources and references

1. [European Data Protection Board, Guidelines 02/2026 on Anonymisation, especially paragraphs 35, 41–49, 51–103 and Annex 1.](#)
2. [EDPB, Guidelines 1/2026 on processing of personal data for scientific research purposes, including the discussion of roles, safeguards and research infrastructures.](#)
3. Mark R Leiser, Making Access to Google Search Data Work Without Inventing a Privacy Fiction: Submission to the European Commission, Case DMA.100209 – SP – Alphabet – Article 6(11) DMA, April 2026, including the proposed Anonymisation and Utility Impact Assessment.
4. [Regulation \(EU\) 2022/1925 \(Digital Markets Act\), Article 6\(11\) and Recital 61.](#)
5. [EDPB, Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models.](#)
6. [EDPB, Guidelines 03/2026 on web scraping in the context of generative AI.](#)
7. [European Commission, COM\(2019\) 250 final, Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union.](#)
8. [European Commission, Proposal for a Digital Omnibus, COM\(2025\) 837 final.](#)
9. The Innovation Mandate lecture series, especially slides 3–6, 12–16 and the proposed assurance and supervisory impact machinery.