

What the recipient holds: a threat model for data you have already shared

Julien Boninfante, Chief Information Security Officer · 2026-10-05

Seven ways a shared record can lead back to a person, and a practical review of what the recipient could infer.

Look at the copy the recipient receives

A data-flow diagram shows where a file goes. Open the file as well. What fields remain, what can be inferred from them and what other information could the recipient use?

For an illustrative case, replace a name in a staff record but leave an unusual job title and a small office location. A colleague may still recognise the person immediately.

Seven routes to review

Route	What to ask
Outside datasets	Could these attributes match a public or other available record?
Free text	Does the narrative identify a role, event or location?
Stable identifiers	Can the recipient connect this record to earlier ones?
Small groups	Is a rare combination enough to single someone out?
Staff access	Who can view, export or copy the information?
Sub-processors	Which other services receive it, and for what purpose?
Retained copies	What remains after the job, contract or retention period ends?

The linked identifiability research illustrates why combinations of ordinary attributes deserve attention. A percentage from a historical population study is not a measurement of your current dataset's risk.

What substitution changes

Replacing direct identifiers removes those original values from the shared copy. It does not remove every possible route to recognition. Synthaveil output is no exception: the product replaces selected identifying details, and it makes no claim that the result is anonymous. Review indirect identifiers and the remaining narrative together.

Test how your configuration handles unusual values, missed matches and new fields before relying on it.

Rotation has a scope

Changing the scope creates different stand-ins. Within a scope, consistency can keep records joinable; across scopes, matching stand-ins directly becomes less useful. Unchanged details can still connect the records. Rotation is therefore one part of the assessment, not a guarantee that a recipient cannot build a profile.

Set the window to support the legitimate task and check whether the recipient needs that much linkage.

Evidence and follow-up

A run record shows what the configured control did; confirming the copy is fit to share, and that no other sharing route exists, stays your decision.

Record the fields shared, the policy and key scope, the reviewer and the recipient's retention terms. Include known gaps. Revisit the assessment when the schema, purpose, provider or access arrangements change.

Keep restoration information separate and protected. While you hold the key or the originals, the output remains personal data in your hands. For a recipient with no reasonable means to re-identify anyone, the position can differ; that is an assessment you make and record, not a default. Retain the purpose, permission and transparency review alongside the technical evidence.

Sources and further reading

1. [Sweeney, L. — Simple Demographics Often Identify People Uniquely \(Carnegie Mellon University, 2000\)](#).
2. [Golle, P. — Revisiting the Uniqueness of Simple Demographics in the US Population \(WPES 2006\)](#).
3. [Sweeney, L. — k-anonymity: a model for protecting privacy \(2002\)](#).
4. [EDPB Guidelines 01/2025 on pseudonymisation](#)
5. [CJEU, EDPS v SRB \(C-413/23 P\), 4 September 2025](#)
6. [ICO — Pseudonymisation guidance \(28 March 2025\)](#).
7. [GDPR Recital 26 — identifiability and pseudonymised data](#)
8. [GDPR Article 5\(2\) — accountability](#).

9. GDPR Article 32 — security of processing

10. OWASP GenAI LLM Top 10 2026 (published 3 August 2026)

Illustrative guidance. Product availability and limits: synthaveil.com/products