Privacy operations

Operate the data inventory through access, retention, deletion and request evidence.

Printable workpaper. The detailed guide and all scenario branches are in the Markdown file.

Use synthetic records. Real data-subject requests and sensitive data remain in authorized organizational systems.

Process and expected evidence

1. Trace purpose to system

Purpose–data–system mapping

2. Operationalize retention

Justified retention and copy scope

3. Handle requests safely

Masked request and approval trail

4. Verify deletion and transfer

Copy-specific result and open exception

Work record

Scope / date:
Business / technical owner:
Decision and rationale:
Evidence reference / retest:

Example and closure

Fictional example; not evidence of actual work.

Purpose: Example support record

System / copy: Synthetic archive

Owner: Support data owner

Assessment: Fictional PRV-021

Action: Validate retention decision

Result / exception: Not closed yet

Closure checklist

[ ] Purpose and system match.

[ ] Retention linked to legal assessment.

[ ] Request identity verified proportionately.

[ ] Copies and exceptions reported.

Official sources

KVKK — Silme, yok etme ve anonimleştirme yönetmeliği

https://www.kvkk.gov.tr/Icerik/5441/KISISEL-VERILERIN-SILINMESI-YOK-EDILMESI-VEYA-ANONIM-HALE-GETIRILMESI-HAKKINDA-YONETMELIK

EUR-Lex — Regulation (EU) 2016/679

https://eur-lex.europa.eu/eli/reg/2016/679/oj