



eu-LISA Industry Roundtable · Strasbourg · 9–10 September 2026

Engineering Trust into Data

High-assurance data for identity & border systems

Georgios Stavropoulos Project Coordinator

Eleftheria Katsoura Project Manager



From discipline to deployment

How high-assurance data is built, protected and governed — and how EINSTEIN handled it at the border.

PART 1 · PRINCIPLES

-  The data-management lifecycle
-  Collection & quality
-  Biometrics: the hardest case
-  Security & access
-  Processing & the AI Act
-  Privacy-enhancing technologies
-  Retention & governance

PART 2 · EINSTEIN

-  EINSTEIN in context
-  Data-protection challenges & responses
-  The AI Act lens
-  Looking ahead — steps & risks

● WHY NOW

Data management is now regulated

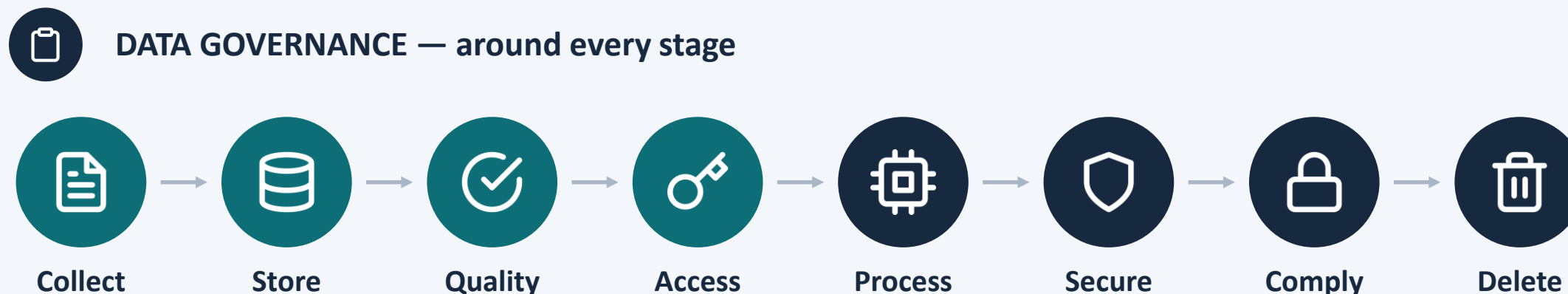
At the border, three forces converge: sensitive data, real-time decisions, and a fast-evolving legal stack.



Design for the obligation, not the date. Five regimes govern one border data flow — and the AI-Act high-risk deadline just moved to Dec 2027.

The data-management lifecycle

One connected cycle, wrapped by governance — its strength set by the weakest link.



A weakness in one stage undermines all the others — trust is earned end-to-end.

Quality at the point of capture

Minimise by architecture

Capture on-device; what you never centralise cannot leak.

Quality as a control

Score biometric quality at capture; record provenance.

Monitor for drift

People, documents and attacks evolve — quality is continuous.



Biometrics: the hardest case

You can reset a password; you cannot reissue a face.

A higher legal bar

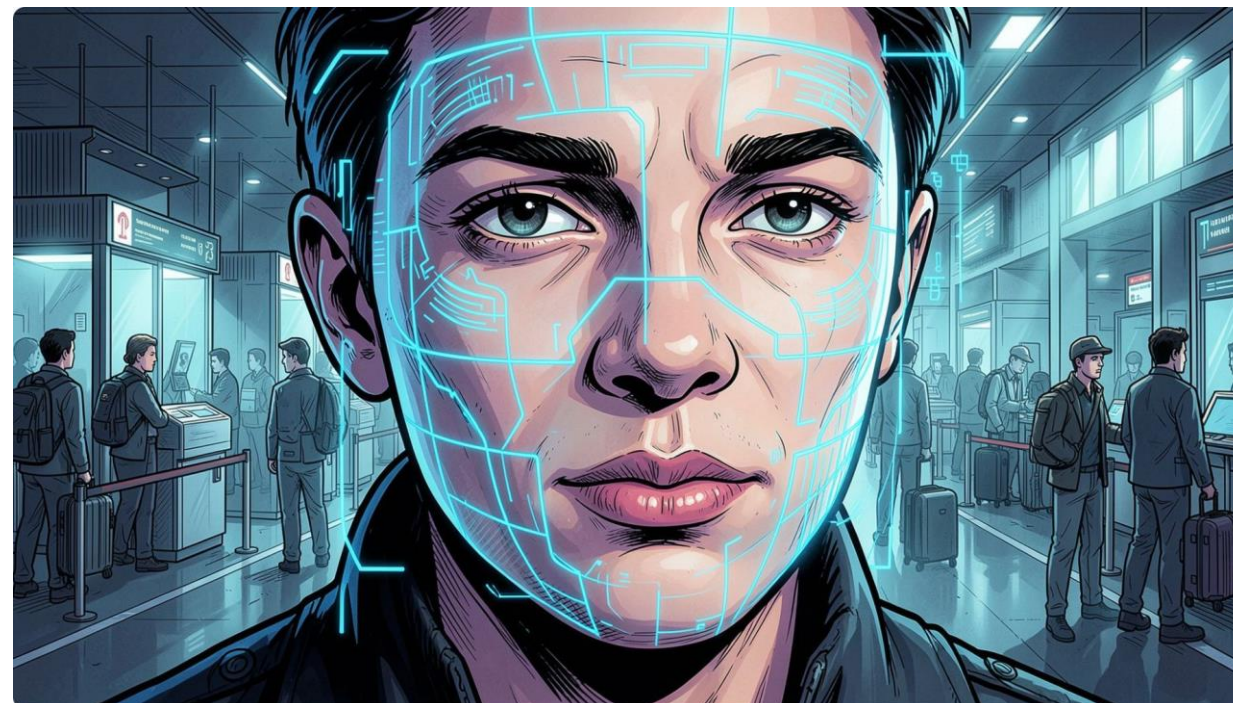
Special-category data — needs an Article 9 basis (explicit consent).

Protect the template

Store irreversible, revocable references — not the raw image.

Integrity against attack

Detect presentation and morphing attacks at capture.



Zero-trust by construction

Protect the data even from the systems and people that process it.



Encrypt everywhere

At rest, in transit and in use —
with real key management.



Resilience by design

Defence in depth and
rehearsed incident response.



Least-privilege access

Fine-grained access,
segregation of duties, audit
trails.



AI multiplies value — and risk

Accuracy, robustness, explainability and human oversight are engineering requirements.



EU AI Act — a risk-based ladder



Humans decide

Scores advise; detection escalates to an expert — never auto-rejects.



Bias & robustness, tested

Across demographics; hardened against spoofing and morphing.

Deadline moved: high-risk duties + the FRIA now apply from Dec 2027.

Privacy-enhancing technologies

Techniques that unlock value from data while minimising exposure — privacy by design.



Federated learning

Train a shared model — data never leaves a site.



Homomorphic encryption

Compute directly on encrypted data.



Secure computation (MPC)

A joint result; each input stays secret.



Differential privacy

Provable limits on what analytics reveal.



Template protection

Irreversible, revocable biometric references.



Self-sovereign identity

User-held credentials, selective disclosure.

Where each technique fits

The right privacy-enhancing technology depends on the job at the border.



Federated learning

Improve a fraud model across countries without sharing raw documents.

Cost: coordination



Homomorphic encryption

Match a biometric while it stays encrypted — the server never sees it.

Cost: compute & latency



Template protection

Store a revocable reference — a breached template can be reissued.

Standards maturing



Self-sovereign identity

The traveller holds the credential and discloses only what's needed.

Enabled by eIDAS 2

Retention, deletion & governance

Keep only what the purpose needs; reuse under safeguards; and prove it, end-to-end.



Purpose-bound retention

Erase across copies — or destroy the key.
Erasure by default.



Lawful research reuse

Longer storage only with a reason, a period
and a prior DPIA.



Provable accountability

A living plan, records, DPIA — and, for high-risk AI, a FRIA.

The assurance instruments

DPIA

Data Protection Impact Assessment

FRIA

Fundamental Rights Impact Assessment

DMP

Living Data Management Plan

RoPA

Records of Processing Activities

EINSTEIN in context

Six interoperable applications, assessed for data protection across three cycles of live testing.

€6M

Budget

36 mo

2024 – 2026

21

Partners · 11 countries

TRL 7+

Operational

Six applications across the identity & document journey



APP1 · Online ID issuance



APP2 · Mobile checks



APP3 · Document authentication



APP4 · Pre-registration



APP5 · EES kiosk



APP6 · Fast-track corridor

The principles, demonstrated

A few concrete results from EINSTEIN that show the approach at work.



Federated, not pooled

APP3 improves one shared model across sites — only model updates travel, never raw documents.



On the device, end to end

APP4 runs MRZ, NFC, liveness and the 1:1 face match on the phone — no central store.



Verifiable offline

A Digital Travel Credential in an on-device wallet, checkable even without connectivity.



The human decides

Attack-detection scores never auto-reject — they escalate to a human expert.

The AI Act, applied to EINSTEIN

How the applications sit under the AI Act — and how we assessed it.



Verification, not mass identification

1:1 verification; where identification is needed, 1-to-few — never 1-to-many remote identification.



Humans decide

Biometric scores are advisory; the officer decides — outside GDPR Article 22.



Designed for integration

EU-system checks (SIS, VIS, EES, ETIAS) are simulated — built for lawful integration, not connected to live databases.



Assessed every cycle

A DPIA and a FRIA per application, reviewed across three rounds — developers, end-users and the ethics lead.

Designing & assessing systems like this

Three lenses for any high-assurance identity or border system.



Regulation

- GDPR — Art 5, 9, 25, 32, 35
- AI Act — Annex III, Art 22, 27
- Law-Enforcement Directive
- EES · eIDAS 2



Technique

- Minimise & process on-device
- PETs — federated, template, SSI
- Human-in-the-loop by design
- Encryption & zero-trust



Open challenges

- A biometric breach is permanent
- Keep verification from drifting to ID
- Template protection & wallets to mature
- Regulation & technology, aligned

Thank you

Engineering trust into data — from principle to the border.

Georgios Stavropoulos Project Coordinator · stavrop@iti.gr

Eleftheria Katsoura Project Manager · el_katsoura@iti.gr

