DSR PROTOCOL · TEKNOPARK İZMIR · DATA RESIDENCY NOTE

Where the data lives: a Turkish company, EU-resident passport data

Turkish company. EU-resident data. Residency, not sovereignty.

IF THE PANEL ASKS “WHERE DOES THE DATA LIVE?” — THE 20-SECOND ANSWER

The company and its R&D sit in Türkiye, at Teknopark İzmir. The production passport data of brands selling into the EU sits in the EU — an EU-region deployment with EU-jurisdiction object storage — because that is what EU customers, regulators and GDPR expect. A passport is product data, not personal data, and our scan path is PII-free by design. We say data residency, not sovereignty — and we can explain the difference.

Why a Turkish entity

Teknopark İzmir gives us the R&D incentives under Law 4691, access to Turkish engineering talent and a home for the intellectual property — developed and held in Türkiye. The Turkish entity owns and operates the technology.

Why EU-resident data

The passports are for products placed on the EU market, so the buyers and regulators are in the EU. Holding their data in an EU region satisfies GDPR and enterprise procurement (with a DPA and standard clauses). Türkiye does not hold an EU adequacy decision, so pulling EU personal data into Türkiye would need transfer mechanisms — we avoid the problem by design: the data stays in the EU and personal data is minimised.

What is personal data here — and what is not

A Digital Product Passport is product data: GTIN, materials, certificates, repair and recycling information. The scan path is PII-free by design — cookie-free pseudonymous sessions, one-way fingerprints, PII-free logs — with strict tenant isolation and an append-only audit ledger. The only personal data is operator account data for the dashboard, held in the same EU cell.

Residency is not sovereignty — say it before they do

Residency means the data physically sits in the EU: achievable with an EU-region deployment and EU-jurisdiction object storage. Sovereignty means immunity from foreign jurisdiction: our edge and hosting providers are US-incorporated, so we do not claim it. If a buyer requires sovereignty, the same containerised codebase redeploys onto an EU-owned provider as a separate residency cell — no rewrite.

Honest status today

DSR runs today as a single deployment, with storage and database wherever provisioned. The EU-resident production cell is a configuration — an EU region plus an EU-jurisdiction bucket — that we switch on for the first EU brand going live. Until then our word is “targeted”, not “enabled”. For Turkish exporters, DSR acts as the processor, not the controller, under KVKK; EU-market passport data is held in the EU cell and any cross-border element is handled under KVKK Article 9 mechanisms — to be confirmed with counsel per contract.

Who holds what, where

WHAT	WHERE	WHY
Company, R&D team, intellectual property	**Türkiye — Teknopark İzmir**	Law 4691 incentives, Turkish talent, IP held in Türkiye
Passport data for EU-market brands (product data)	**EU region — EU-jurisdiction storage**	GDPR, EU procurement, no adequacy gap to bridge
Operator accounts (the only personal data)	**Same EU cell**	Minimised; role-gated; audit-logged
Scan path (shoppers, customs, recyclers)	**Served from the edge, in-perimeter**	PII-free by design: no cookies, pseudonymous, no PII in logs
Signing keys and proofs (Ed25519 VC, RFC 3161)	**In the owning cell**	Proof of custody stays with the data it signs

Not legal advice. Jurisdiction-specific exposure is confirmed with counsel per deal. “Residency” is claimed only for a deployment that is actually configured for it.