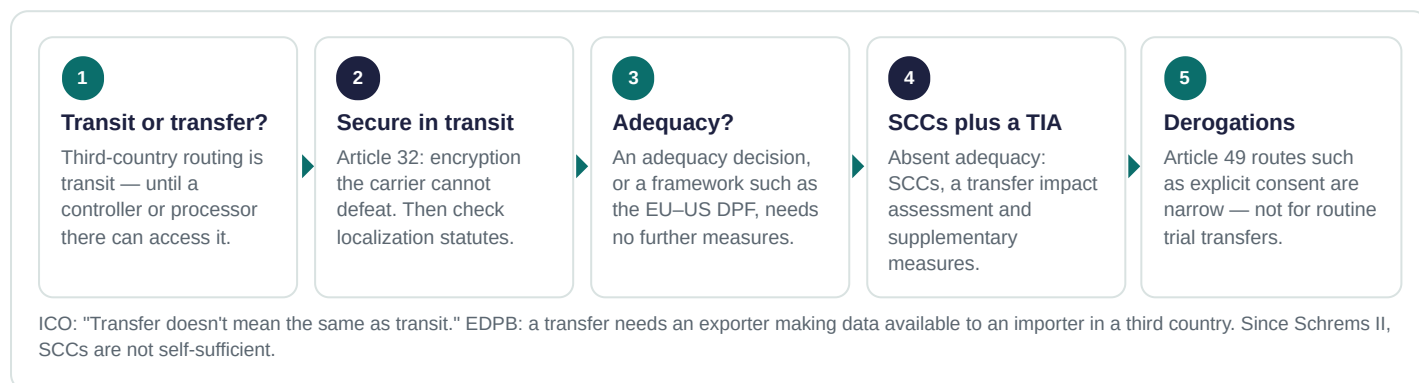


Residency is decided in two layers — where data is stored and where it travels — and the second is **the one nobody assesses**.

The device holds a copy before sync; the eSIM or data plan decides the route. Transit through a third country needs no Chapter V mechanism, but it engages security of transit, localization statutes and — where a third-country party can access the data — a real transfer. **Map both layers before enrollment.**

THE PICTURE Only a transfer needs a Chapter V mechanism, and more than a signature



QOINTA'S POSITION Four distinctions that collapse in most residency assessments

"The data lives in our validated cloud" answers storage only

Storage location says nothing about the route, the legal basis for special-category data, the mechanism a third-country recipient needs, or who is controller.

Health data raises the floor; consent is rarely the basis

Needs an Article 6 basis plus an Article 9(2) condition and, at scale, a DPIA under Article 35(3)(b). Part 11 and EMA/INS/GCP/112288/2023 compliance is a separate perimeter.

Roles are a determination, not a default

The sponsor is usually controller, but sites and some vendors may be controllers or joint controllers. Consent to take part and the lawful basis for processing are two different things.

The device itself makes residency decisions

On-device copies sit in the participant's jurisdiction; sync routing decides whether a border is crossed; an IMEI, MAC or eSIM linked to a participant makes the device a personal-data asset.

SIX DUTIES, ONE PER PARTY IN THE TRANSFER MAP

- 1 Sponsor: own the RIA entry and the DPIA;** decide lawful basis, transfer mechanism and roles; sign off the transfer map.
- 2 eCOA / ePRO vendor: document the storage and sync design,** encrypt at rest, and supply it to the DPIA.
- 3 Connectivity provider: disclose routing, egress regions and payload access;** pin or restrict third-country backhaul.
- 4 Logistics vendor: treat identifier-to-participant linkage as personal data;** secure and reconcile it at decommissioning.
- 5 CRO: disclose sub-processors and their locations** so they enter the transfer map (QPP-12).
- 6 Data-protection function: run TIAs and records of processing;** feed the Trigger Register and reconcile globally.

2

layers decide residency — storage (back-end, on-device) and travel (routing)

7

triggers raise the residency or transfer weight of a deployment and feed the RIA

8 Apr 2025

DOJ Data Security Program (28 CFR Part 202) in effect; clinical investigations exempt

5 Feb 2026

UK Data (Use and Access) Act 2025 "data protection test" applies to transfers

Read with care. Regimes named are illustrative, not exhaustive; adequacy decisions, transfer tools and national rules evolve — the EU-US Data Privacy Framework faces a pending Court of Justice appeal (C-703/25 P). Worked example is a composite.

READ NEXT

QPP-00 Regulatory Impact Assessment · QPP-08 Trigger Register · QPP-12 Vendor Qualification and Oversight · QPP-13 Decommissioning · QPP-23 Global Reconciliation

