

Routing trial traffic through a third country is not, by itself, an international transfer: **transit is not transfer**. Your layer decides where traffic egresses and who can read it.

A transfer arises only where a party in a third country receives or can access the data — but a residency analysis that stops at storage cannot see your layer. **Map egress per market, disclose default backhaul and underlying carriers, evidence end-to-end protection, and issue a routing disclosure.**

THE PICTURE Regulated twice: by telecoms and cyber law, and by the trial on top

Perimeter	What it means for you	Provider action / evidence
Data residency	Routing and egress set where data physically travels; localization rules apply to that.	Map egress points per market; show where data stays or goes.
Cross-border transfer	A transfer arises where a third-country party receives or can access the data — not from routing alone.	Disclose default backhaul and any point where traffic is terminated, decrypted or stored abroad.
Data integrity	Loss or corruption in transit is a data-integrity event in the trial record.	Evidence encryption in transit and link-integrity controls.
Oversight	Whether you are a processor turns on what you do with the content; managed connectivity can make you one.	Name your underlying carriers; provide a routing disclosure the sponsor can assess.

Four bodies of law meet in the connectivity layer: electronic-communications confidentiality and security duties; NIS2 cyber risk-management and incident reporting; GDPR Art. 32 and Chapter V for the trial; and the Cyber Resilience Act for equipment you manufacture.

QOINTA'S POSITION Four facts about your layer that a sponsor will ask you to evidence

Routing is a regulatory decision

Where traffic egresses sets the security, localization and — where a third-country party is involved — transfer position.

You own a layer the sponsor cannot see

A residency analysis that stops at storage never reaches the connectivity layer; what is not mapped is not assessed, by you or anyone else.

Roaming profiles can backhaul abroad

A global eSIM may route via a third country by default; convenience routing quietly crosses borders, and opaque egress points make residency impossible to assure.

Your own equipment may be regulated in its own right

Connectivity hardware and software placed on the EU market is a product with digital elements under the Cyber Resilience Act: reporting since 11 Sept 2026, remaining duties from 11 Dec 2027.

FIVE MOVES TURN AN UNDOCUMENTED DEPENDENCY INTO A DISCLOSURE THE SPONSOR CAN ACT ON

- 1 Map egress per market** — know and document where traffic leaves the country in each deployment region.
- 2 Disclose default backhaul** — where a global eSIM routes by default, and whether traffic is terminated, decrypted or stored on the way.
- 3 Name your underlying carriers** — they shape routing, and a sponsor cannot name what you do not disclose.
- 4 Evidence protection in transit** — end-to-end payload encryption and link-integrity controls along the whole path.
- 5 Issue a routing disclosure** the sponsor can use in its residency analysis and vendor oversight — not a legal opinion on transfer.

Read with care. This edition summarizes QPP-02; the sources and pin-cites are carried there and in the edition's footnotes. It is not legal advice and any specific position should be confirmed with qualified regulatory counsel.

READ NEXT

QPP-00 Regulatory Impact Assessment · QPP-02 Data Residency and Cross-Border Transfer · QPP-05 Cybersecurity · QPP-10 Data Integrity · QPP-12 Vendor Qualification and Oversight

