

Where the Data Actually Travels

A companion reading from the connectivity provider seat — what routing and egress do, and do not, do to a trial's data-protection position

Prepared for	eSIM, roaming and data-plan providers, and the sponsors and vendors that rely on them.
Subject	What the connectivity layer's routing and egress do, and do not, do to a trial's data-protection and data-integrity position.
Status / Date	Final — 1 September 2026
Version	1.0
Prepared by	Rudiger Mees

Executive summary

The answer. Routing trial traffic through a third country is not, by itself, an international transfer. The regulators are explicit: transit is not transfer.¹ What your layer does decide is where traffic egresses, who can read it on the way, and which carriers sit beneath you — a security-in-transit and data-localization question, and a transfer question only where a party in a third country receives or can access the data.

Which rules. Four bodies of law meet in the connectivity layer. Your own perimeter — the confidentiality and security duties of an electronic communications provider² and, since NIS2, cyber risk-management and incident-reporting duties.³ The trial's perimeter — security of the data in transit under GDPR Art. 32, Chapter V where a third-country party is involved, and the integrity of the record once it reaches the sponsor's repository.⁴ And, for connectivity equipment you manufacture, the Cyber Resilience Act.

What to do. Map egress per market, disclose default backhaul and your underlying carriers, evidence end-to-end protection of the payload, and issue a routing disclosure the sponsor can use in its residency analysis. In qointa's assessment, that document — not a legal opinion on transfer — is what a sponsor needs from you, and it is the only part of the picture you alone can supply.

¹ ICO, "What is an international transfer of personal information?": "Transfer doesn't mean the same as transit. If personal information is just electronically routed through a country outside the UK, but the transfer is actually from one UK organization to another, then it's not a restricted transfer" — while "you must put in place appropriate security measures to prevent unauthorised access to the personal information while it is in transit". EDPB Guidelines 05/2021 on the interplay between Article 3 and Chapter V (version 2.0, 24 February 2023) set three cumulative criteria for a transfer, the second of which requires the exporter to disclose by transmission, or otherwise make available, personal data to an importer in a third country; mere routing is not addressed. Verified 1 September 2026.

² Directive 2002/58/EC (ePrivacy), Art. 4 (security of services) and Art. 5(1) (confidentiality of communications and the related traffic data). Verified at <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002L0058> on 1 September 2026.

³ Directive (EU) 2022/2555 (NIS2), transposition due 17 October 2024. Providers of public electronic communications networks and of publicly available electronic communications services are in-scope entities (Art. 3(1); Annex I, digital infrastructure). Art. 23(4): early warning without undue delay and in any event within 24 hours, incident notification within 72 hours, final report within one month. In-scope status verified against the Irish NCSC NIS2 FAQ (ncsc.gov.ie/nis2/FAQ) and Art. 23(4) at nis-2-directive.com, 1 September 2026 — see the open items in the change log.

⁴ EMA, Guideline on computerised systems and electronic data in clinical trials, EMA/INS/GCP/112288/2023 (GCP IWG, 7 March 2023), Annex 4 (security) — including protection of data during transfer.

Transit is not a transfer — the question changes when someone abroad can read the data

Routing a packet through a third country raises a security and localization question; a transfer arises when a party in that country receives or can access the data

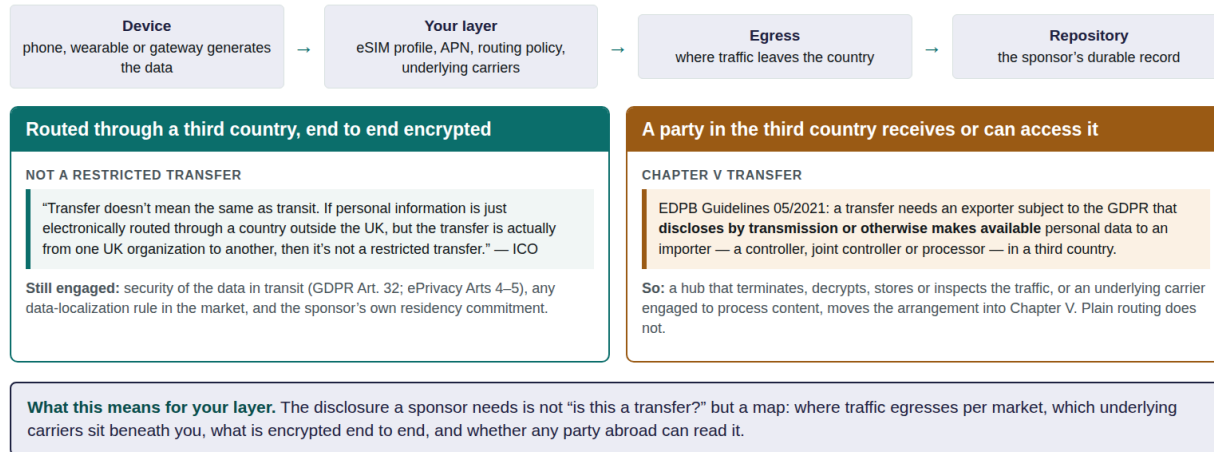


Figure 1 — Transit is not a transfer: the question changes when a party abroad receives or can access the data.

1. Routing and egress are decided in your layer, and the trial inherits them

This is a companion edition of qointa's position-paper series, read from the connectivity provider's seat. **Where traffic routes, and where it leaves a country, is set in your layer** — and the sponsor's residency analysis, which usually stops at storage, cannot see any of it.

It is addressed to connectivity providers — eSIM, roaming and data-plan — and to the trial teams that depend on them. This edition summarizes the position set out in QPP-02 — Data Residency and Cross-Border Transfer; the sources are cited there in full.

How this fits the full framework

This companion is keyed to Section 12 of the Regulatory Impact Assessment (QPP-00 — Regulatory Impact Assessment (RIA)). The numbered papers carry the detail — the ties most relevant to a connectivity provider are:

- **QPP-02 — Data Residency and Cross-Border Transfer.** Your core perimeter: routing and egress decide where data physically travels, and where a third-country party enters the chain.
- **QPP-05 — Cybersecurity.** In-transit protection, and the cyber duties attaching to your own network and equipment.
- **QPP-10 — Data Integrity.** Loss or corruption en route is an integrity event in the trial record, not only a network one.
- **QPP-12 — Vendor Qualification and Oversight.** Whether you sit inside the sponsor's oversight as a processor turns on what you do with the content of the communications, not on the fact that you carry them.

Regulatory basis

The positions in this edition rest on the following sources. Pin-cites are in the footnotes; the full argument is in the numbered papers.

- **ICO**, “What is an international transfer of personal information?” — transit is not transfer; security in transit is still required.
- **EDPB Guidelines 05/2021** (v2.0, 24 February 2023) on the interplay of Art. 3 and Chapter V GDPR — the three cumulative criteria for a transfer.
- **EDPB Guidelines 07/2020** (final, 7 July 2021), para 27 — an electronic communications provider is normally a controller of traffic and billing data, and not a controller of the content of the message.
- **Directive 2002/58/EC (ePrivacy)**, Arts 4 and 5(1) — security of the service; confidentiality of communications and traffic data.
- **Directive (EU) 2022/2555 (NIS2)**, Art. 3(1) and Annex I; Art. 23(4) — 24-hour early warning, 72-hour notification.
- **Regulation (EU) 2024/2847 (Cyber Resilience Act)**, Arts 14 and 71 — reporting since 11 September 2026; remaining obligations from 11 December 2027.
- **EMA/INS/GCP/112288/2023**, Annex 4 — security and protection of clinical-trial data, including during transfer.

2. 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.
- **Roaming profiles can backhaul abroad.** A global eSIM may route via a third country by default.
- **Your behavior is invisible unless you disclose it.** What is not mapped is not assessed — by you, the sponsor or anyone else.

3. Four different questions meet in your layer, and only one of them is a transfer question

Your layer sits beneath the device, yet it determines where data travels. Each question maps to a paper — and to a concrete action or disclosure on your side (Figure 2).

Perimeter / topic	What it means for you	Paper	Provider action / evidence
Data residency	Routing and egress set where data physically travels, and any localization rule applies to that.	2	Map the egress points per market and show data stays in-jurisdiction (or where it goes).
Cross-border transfer	A transfer arises where a party in a third country receives or can access the data — not from routing alone.	2	Disclose default backhaul and any point where traffic is terminated, decrypted or stored abroad.

Perimeter / topic	What it means for you	Paper	Provider action / evidence
Data integrity	Loss or corruption in transit is a data-integrity event in the trial record.	5, 10	Evidence encryption in transit and link-integrity controls.
Oversight	Whether you are a processor turns on what you do with the content; a managed-connectivity contract can make you one.	12	Name your underlying carriers and provide a routing disclosure the sponsor can assess.

Your layer is regulated twice — by the telecoms and cyber law you already live under, and by the trial that rides on it

The sponsor cannot see either set of duties unless you map them; a routing disclosure is how both become assessable

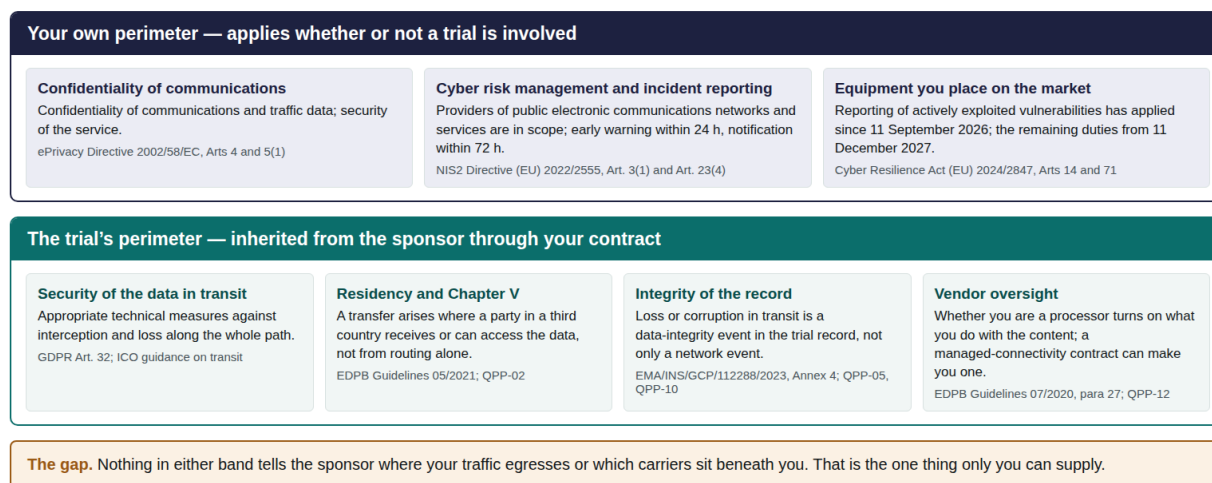


Figure 2 — Your layer is regulated twice: by the telecoms and cyber law you already live under, and by the trial that rides on it.

4. Four things to watch: default routes, opaque egress, underlying carriers and your own equipment

- **Default roaming routes.** Convenience routing can quietly cross borders.
- **Opaque egress points.** If you cannot show where traffic leaves, residency cannot be assured.
- **Underlying carriers.** The carriers beneath you shape routing, and a sponsor cannot name what you do not disclose.
- **Your own equipment may be regulated in its own right.** Connectivity hardware and software you place on the EU market is a product with digital elements under the Cyber Resilience Act: reporting of actively exploited vulnerabilities and severe incidents has applied since 11 September 2026, and the remaining obligations apply from 11 December 2027.⁵

⁵ Regulation (EU) 2024/2847 (Cyber Resilience Act), Art. 14 (reporting obligations, applicable from 11 September 2026) and Art. 71 (main obligations from 11 December 2027); Art. 2(2) excludes devices covered by the MDR and IVDR. The CRA binds manufacturers of products with digital elements placed on the market, not the provision of a connectivity service.

5. Five moves make your routing assessable

Five moves turn an undocumented dependency into a disclosure the sponsor can act on (Figure 1).

- **Map egress per market** — know and document where traffic leaves the country in each deployment region.
- **Disclose default backhaul** — say where a global eSIM routes by default, and whether traffic is terminated, decrypted or stored anywhere on the way.
- **Name your underlying carriers** — the carriers beneath you shape routing and belong in the disclosure.
- **Evidence protection in transit** — encryption of the payload end to end, and link-integrity controls along the whole path (QPP-05 — Cybersecurity; QPP-10 — Data Integrity).
- **Issue a routing disclosure** — a document the sponsor can use in its residency analysis and vendor oversight (QPP-02 — Data Residency and Cross-Border Transfer; QPP-12 — Vendor Qualification and Oversight).

6. Showing where traffic goes is the whole of the ask

The connectivity layer is the part of a trial's data path that no one else can document. **Showing how and where traffic routes, what is encrypted, and who sits beneath you turns an unmapped dependency into an assessable one** — and settles, on the facts rather than by assumption, whether a transfer arises at all.

How qointa can help

qointa maps connectivity paths against the sponsor's residency commitments, drafts the routing disclosure and the processor-role analysis that go with it, and reviews in-transit controls against the trial's data-integrity obligations. info@qointa.com

Scope and status

This is a companion edition summarizing qointa's position-paper series from one stakeholder's perspective, keyed to Section 12 of the Regulatory Impact Assessment (QPP-00 — Regulatory Impact Assessment (RIA)). The sources for the positions taken here are cited in the footnotes and in the Regulatory basis box; the full treatment is in the numbered papers. It is not legal advice, and any specific position should be confirmed with qualified regulatory counsel.