

International Data Transfers: UK TRA, IDTA and EU SCC Decision Guide



IG-Smart Ltd · Practical Guide Collection · 25 October 2026

General information and original working aids; not legal advice, certification, clinical authorisation or regulatory approval.
NHS identity appearing in retained illustrative artwork does not imply NHS approval or endorsement.

Use this guide to make a better-evidenced decision. This is general information and an original working aid, not a client-specific legal opinion, certification, clinical safety authorisation or regulatory approval. Apply the relevant jurisdiction, current requirements and competent professional review to your circumstances. Examples are illustrative unless expressly attributed.

Your first three steps

1. Map the actual sending and receiving entities, access and jurisdictions.
2. Decide whether a restricted transfer exists and select a valid route.
3. Document the relevant protection test and effective safeguards before data flows.

A practical route from data-flow mapping to documented transfer safeguards for UK, EU and multinational organisations

Executive proposition: A signed transfer agreement is not proof that an international data flow is lawful. First identify whether a restricted transfer exists, who is responsible, whether adequacy applies, which safeguard is appropriate and what assessment and supplementary measures are actually needed.

For: DPOs, General Counsel, privacy officers, global procurement teams, cloud and SaaS buyers, international group data owners and regulated-sector leaders. **Scope:** practical UK GDPR and EU GDPR transfer governance, not country-specific legal advice or a substitute for counsel reviewing the parties' actual flow.

Executive briefing — the five decisions

A board or legal lead should require a transparent record of **(1) the data flow and who initiates it; (2) the applicable legal regime and whether it is a restricted transfer; (3) the adequacy route, safeguard or narrow exception; (4) the level of protection in the destination and the measures actually effective; and (5) the contractual, operational and reassessment owners.**

Current ICO guidance notes that UK legislation now refers to the transfer risk assessment (TRA) as a “**data protection test**”; the ICO continues to use “TRA” in its guidance. The change in terminology does not mean that simply relabelling an old document completes the required evaluation. [S1][S2]

UK and EU requirements are similar in broad purpose but not identical. EU standard contractual clauses (SCCs) should not be assumed to be sufficient on their own for every UK restricted transfer; the UK has the **International Data Transfer Agreement (IDTA)** and **UK Addendum** as relevant Article 46 instruments. [S1]

When relying on appropriate safeguards for a UK restricted transfer, the sender must, acting reasonably and proportionately, decide that the standard of protection for people's information is not materially lower than in the UK. The ICO continues to use ‘transfer risk assessment’ for the statutory data protection test. This is not the same as the EU test and is not a universal assessment requirement for every overseas access or adequacy-covered transfer. Source: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/glossary/>

1. Identify the real flow before choosing a clause

Record the sending and receiving legal entities, their controller/processor roles, the country of each recipient, the storage locations, remote access locations, onward recipients, subcontractors, information categories, sensitivity, purpose, retention, and the technical controls actually used. “Hosted in London” does not necessarily settle remote support from another country. Conversely, an employee travelling abroad does not automatically create the same legal transfer relationship as sending data to a separate overseas controller or processor; apply the ICO's actual restricted-transfer tests. [S1]

The ICO's current three-step restricted-transfer screen

For a potential **UK GDPR** restricted transfer, the ICO's current guidance asks three distinct questions: **(1)** does the UK GDPR apply to the processing; **(2)** is the organisation initiating the transfer of personal information to an organisation outside the UK (including relevant remote access); and **(3)** is the recipient a **separate legal entity**? All three must be established before treating the arrangement as a restricted transfer under that test. The identity of the initiator can differ from the person physically transmitting information. [S5]

Counter-intuitive cases: The same legal entity's employee accessing UK records while abroad is not necessarily a restricted transfer; a separate overseas service provider accessing servers physically in the UK may be. Other security, contract and privacy duties still apply in either case. Apply the EU GDPR's separate approach to EU-governed processing, rather than transplanting the ICO test as EU law. [S5]

Transfer record fields

Field	Decision question
Sender / exporter	Which entity initiates the movement or access?
Recipient / importer	Is it a legally distinct organisation and which role applies?
Processing activity	What precisely is the purpose and lawful basis?
Data and individuals	What information and population are affected?
Destination	Where will recipients or onward parties access data?
Access model	Direct transfer, hosting, support, onward disclosure?
Transfer rule	UK GDPR, EU GDPR or both?
Assessment outcome	Restricted transfer / no restriction / unresolved
Control owner	Who confirms instruments and operational safeguards?

2. The IG-Smart Transfer Legitimacy Decision Chain – seven gates

Gate	Test	Evidence	Outcome if unresolved
T1 Inventory	Can the precise personal-data flow be described?	Transfer map and recipient register	Hold assessment; establish facts
T2 Qualification	Do restricted-transfer rules apply?	ICO/EU regime test and role analysis	Seek appropriate legal view

Gate	Test	Evidence	Outcome if unresolved
T3 Adequacy	Is the destination/recipient covered by a current applicable adequacy arrangement?	Official decision and limits	Move to permitted safeguards analysis
T4 Legal instrument	If needed, is the correct Article 46 safeguard in place?	IDTA / UK Addendum / EU SCC or other permitted mechanism	No unsupported transfer
T5 Protection test	Is effectiveness of the safeguard demonstrated in context?	UK data protection test / EU transfer assessment as appropriate	Additional measures or redesign
T6 Operational controls	Do security, onward transfers and contractual terms work in practice?	Encryption/key access, onward contracts, audits, breach obligations	Remediate and verify
T7 Decision and change	Who authorises and revisits the transfer?	Approval, residual findings, change triggers	Do not assume permanent validity

This is an IG-Smart proposed governance workflow, not a statutory seven-question instrument or regulator endorsement.

3. Choosing the correct legal transfer mechanism

Situation	Potential route	Questions requiring verification
UK personal data to jurisdiction/recipient covered by current UK adequacy regulations	Adequacy, within stated scope	Are the jurisdiction, entity, sector and processing in scope?
EU data to jurisdiction/recipient covered by current EU adequacy decision	EU adequacy, within stated scope	Are recipient and specific transfer covered?
UK restricted transfer without relevant adequacy	UK IDTA or UK Addendum with relevant EU SCCs, or other recognised safeguards	Correct parties, modules, annexes, dates and transfer test?
EU restricted transfer without relevant adequacy	EU SCCs or another applicable Article 46 mechanism	Correct module, onward transfers, local law, supplementary measures?
Intra-group transfers	Group mechanism, BCRs if valid and in scope, or appropriate contracts	Which entities and transfer types are covered?
Exceptional circumstances	Narrow Article 49/UK exceptions when genuinely satisfied	Is the exception applicable and defensible rather than a routine bypass?

Do not assume every non-UK location needs an IDTA or that the UK–EEA arrangements are symmetrical in every respect. Check current UK and EU adequacy decisions separately, including any US-specific recipient certification rules where relied on. A DPA, Article 28 processor agreement and transfer mechanism address related but different obligations.

4. What a defensible UK data protection test evaluates

Identify the specific transfer, the governing safeguard and the factual protection of individuals in the destination. Consider laws and practices relevant to the recipient and the particular access scenario; the likelihood and potential effect of disproportionate access; practical enforceability; technical and organisational measures; and the evidence available for the conclusions. Use the current ICO test, not an invented country score or a one-time tick-box.

An assessment must identify **assumptions and limitations**. Encryption may materially reduce access risk when keys remain effectively outside relevant access channels, but a claim of encryption “at rest and in transit” alone does not settle who can read plaintext or administer keys. Remote administration, provider support processes, supplier subprocessing and log access can matter more than the nominal storage country.

Outcome options: justified transfer with documented control; conditional transfer pending verification; redesign to minimise or localise information; use another service/provider; or do not proceed. Final acceptance belongs to the appropriately accountable organisation and authorised owner, not to the person who completed a spreadsheet.

5. EU transfer-impact assessment and supplementary measures

Where EU GDPR Chapter V requires a transfer tool, evaluate whether the contractual or other safeguard can be effective in the actual recipient context. The European Data Protection Board's Recommendations 01/2020 describe evaluating transfers, tools, relevant laws/practices and possible supplementary measures. **Copying a generic UK TRA into an EU compliance file is not sufficient evidence of an EU assessment without a specific applicability evaluation.** [S3]

Safeguard type	Illustrative measure	Verification question
Technical	Strong encryption and independently controlled keys	Who can access usable content, and under what circumstances?
Technical	Pseudonymisation before export	Can overseas parties reconnect records to individuals?
Contractual	Onward-transfer limits and reporting	Are commitments flowed down and operationally monitored?
Organisational	Restricted support access and documented approval	Are permissions, logs and escalation records inspectable?
Governance	Periodic review and recipient change notice	What triggers reassessment and who will act?

No single generic control eliminates every jurisdictional concern; effectiveness must be tested against the actual transfer.

6. Controller, processor and supplier ownership

The party responsible for restricted-transfer compliance depends on the facts and relationship; a controller should not assume the processor alone has solved onward transfers by signing standard terms. Procurement should identify relevant processing instructions, subprocessor authorisation, transfer locations, access rights, security measures and termination/return processes.

The DPO advises on risk and compliance and monitors the programme within their mandate; operational leaders and the controller/processor retain their respective legal responsibilities. External counsel may need to review complex destination law. Article 27 representative appointments are distinct from DPO appointments and distinct again from transfer safeguards.

7. Illustrative decisions – not client engagements

Example A: UK life sciences sponsor and overseas CRO. Data are pseudonymised in the UK, but the CRO holds the linking key. The analysis must address the real reidentification and onward-access pathways; “coded data” is not sufficient to conclude risk is low.

Example B: UK SaaS provider with overseas support. Production data remain hosted in the UK, while support administrators abroad can view content. Review whether the restricted-transfer test applies to the legal entities and access arrangement, and verify which controls actually prevent exposure.

Example C: EU healthcare exporter using a multinational cloud supplier. Identify the relevant EU controller/processor and SCC module, onward suppliers, local access scenario and measures, rather than applying the UK Addendum as the sole EU safeguard.

Example D: Adequate destination, restricted purpose. Adequacy may address the Chapter V route but does not remove the need for a valid lawful basis, transparency, minimisation, Article 28 arrangements, security and other GDPR duties.

8. Twelve procurement and board questions

1. Which precise processing purpose requires an international flow?
2. Can unnecessary personal information be removed before transfer?
3. Who are all the exporters, recipients and onward recipients?
4. Which roles and legal regimes apply independently?
5. Is there current adequacy for the exact destination and recipient?
6. If not, which permitted safeguard is fully executed?
7. Has the relevant protection test been performed and approved?
8. What destination-law concerns remain material?
9. Who holds encryption keys and administrator privileges?
10. Can subprocessor or remote-support changes occur without reassessment?
11. How will incidents, regulator requests and rights requests be handled?
12. Who can suspend or redesign the transfer if assumptions fail?

9. One-page international-transfer approval briefing

Purpose: __; **Data and people:** __; **Sending and receiving entities:** __; **Recipient country and access sites:** __; **Applicable UK/EU regimes:** __; **Restricted-transfer assessment:** __; **Adequacy or safeguarded route:** __; **Test and supplementary measures:** __; **Material uncertainties:** __; **Authorised decision:** approve / conditional / hold / prohibit; **Owner:** __; **Review trigger:** __.

Does an existing TRA need to be repeated because the terminology changed?

Not automatically. For a UK GDPR restricted transfer relying on Article 46 appropriate safeguards, ICO guidance says a TRA previously completed in line with its guidance meets the new data protection test. Confirm that it remains applicable to the actual transfer and reassess relevant changes. Determine adequacy, derogations, EU GDPR and Part 3 DPA transfers separately. Required safeguards, effective supplementary measures and binding instruments must be established before a restricted transfer starts where applicable. [S2][S4]

A conditional internal decision must identify which conditions are prerequisites to data access. It does not permit a restricted transfer to begin while a required safeguard or test remains incomplete.

10. Frequently asked buyer questions

Is an IDTA needed for every international transfer? No. First decide whether the transfer rules apply, then assess adequacy, safeguards or a genuinely applicable exception.

Are EU SCCs and a UK IDTA interchangeable? No. Different instruments and legal frameworks may require an appropriate UK Addendum or IDTA and the relevant EU arrangement.

Does UK adequacy mean the transfer is automatically lawful overall? No. Other GDPR obligations still apply.

Is a supplier's ISO certificate proof that a transfer is lawful? No. It may support security evidence within scope but is not a Chapter V transfer instrument.

Does a TRA need updating? Yes when relevant circumstances, access, recipient, safeguard, country law or processing changes require reassessment.

Can a global DPO sign away controller accountability? No. The statutory advisory role and management accountability are distinct.

11. Putting the decision into practice

Next step: Submit a Requirement describing the jurisdictions, legal entities, recipient roles and unresolved transfer questions. Do not collect raw personal datasets or confidential data within a public lead form.

Sources

- [S1] ICO, International transfers <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/>
- [S2] ICO, Completing a transfer risk assessment (current guidance) <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/completing-a-transfer-risk-assessment/>
- [S3] EDPB, Recommendations 01/2020: supplementary measures (final June 2021) https://www.edpb.europa.eu/documents/recommendation/recommendations-012020-on-measures-that-supplement-transfer-tools-to_en
- [S4] ICO - What is a transfer risk assessment? <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/completing-a-transfer-risk-assessment/what-s-a-transfer-risk-assessment-tra/>
- [S5] ICO - Are we making a restricted transfer? (current guidance, three-step test). <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/a-guide-to-international-transfers/are-we-making-a-restricted-transfer/>