COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

Custodian Abroad: Cross-Border Collection

Data Transfer, Blocking Statutes and Local Law When the Evidence Sits in Another Country

A remote collection inside England is a technical exercise with a data-protection overlay. The moment the custodian or the device is in another country, it becomes a legal exercise first and a technical one second. The data is subject to the local law of where it sits; moving it to England is a restricted international transfer under the UK GDPR; the destination country may have a blocking statute that makes exporting evidence for foreign proceedings a criminal offence; local privacy, secrecy and works-council rules may forbid what English disclosure demands; and a device physically abroad cannot lawfully be imaged simply because an English order says so. Cross-border collection is where the confident assumptions of domestic practice meet a wall of foreign law, and the lawyer who treats it as merely a longer courier journey creates serious risk for their client and their provider. This guide sets out for UK lawyers the legal architecture of collecting from a custodian abroad: the transfer rules, the blocking statutes, the local-law traps, and the routes, cloud-side collection, local agents, letters of request, that get the evidence lawfully.

⏱ Estimated reading time: 25 min read

§ ABOUT THE AUTHOR

PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM

Computer Forensics Lab is a London-based digital forensics and electronic disclosure practice established in 2007. Its eDiscovery arm, **e-discovery.uk**, runs cross-border collections in coordination with local counsel and in-country examiners: cloud-side collection through UK-controlled accounts, in-country imaging where the data must not leave, and transfer mechanisms and blocking-statute analysis built into the plan, so the evidence arrives lawfully and admissibly for CPR Part 35 disclosure.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | CROSS-BORDER COLLECTION | TRANSFER & BLOCKING-STATUTE ANALYSIS | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

THE HEADLINE POINT: A CUSTODIAN ABROAD TURNS COLLECTION INTO A LEGAL EXERCISE BEFORE A TECHNICAL ONE: THE DATA IS UNDER LOCAL LAW, ITS TRANSFER TO ENGLAND IS RESTRICTED, A BLOCKING STATUTE MAY CRIMINALISE EXPORT, AND THE EVIDENCE MUST BE COLLECTED BY A ROUTE THAT SATISFIES ENGLISH DISCLOSURE AND FOREIGN LAW AT ONCE, PLANNED WITH LOCAL COUNSEL FROM THE START

Data transfer (§3): bringing a custodian's data from abroad into England is a restricted international transfer under the UK GDPR, needing a lawful transfer mechanism (adequacy, the International Data Transfer Agreement or Addendum, or a derogation) and a transfer risk assessment: the movement of the evidence a data-protection act in itself, not a neutral logistics step. **Blocking statutes and local law (§4):** some countries make it a criminal offence to gather or export evidence for foreign proceedings otherwise than through official channels (the French blocking statute is the classic example), and many impose privacy, banking-secrecy, state-secrets, labour and works-council constraints that forbid what English disclosure would require: local law can prohibit the very collection English law demands. **The routes (§5):** cloud-side collection through a UK-controlled provider account (which may avoid physically touching anything abroad), in-country collection by a local examiner keeping data in the jurisdiction until transfer is cleared, and formal channels, letters of request and the Hague Evidence Convention, where compulsion or official sanction is needed. **Planning (§6):** local counsel engaged at the outset to map the local-law constraints, the transfer mechanism chosen, the in-country resources arranged, and the sequence designed so no step breaches local law: the plan made before the first byte moves. **Deployment (§7):** the English court's disclosure duty reconciled with foreign law, the court told candidly where foreign law constrains compliance, and proportionate, lawful collection defended, because an English order does not license breaking another country's criminal law, and the court expects the tension surfaced, not ignored.

- **Local law governs the data:** where it sits decides what may be done to it, whatever an English order says.
- **Transfer is restricted:** moving the data to England needs a UK GDPR transfer mechanism and a risk assessment.
- **Blocking statutes can criminalise export:** gathering evidence for foreign proceedings may be an offence abroad.
- **Cloud-side may avoid the border:** a UK-controlled account can sometimes be collected without touching anything abroad.
- **Local counsel first, always:** the plan is legal before it is technical, and made before collection starts.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: the evidence is under someone else's law

English litigation is confident about disclosure: the duty is broad, the court's reach is long, and a party who holds relevant documents must produce them. That confidence is territorial. It stops, more or less, at the coastline. When the custodian and the device are in Germany, France, Switzerland or the United States, the data on that device is subject to the law of that place, and the fact that an English court has ordered its disclosure does not, by itself, make it lawful to collect and export it. A great many things an English lawyer would do without a second thought at home, image the device, ship the drive, upload the mailbox to a UK review platform, can be regulated, restricted or criminal where the data actually sits.

Three layers of foreign law bite. The first is data protection: moving personal data out of its home jurisdiction is a restricted transfer that needs a lawful mechanism, and the UK GDPR is not the only regime in play. The second is the blocking statute: a handful of countries positively prohibit the gathering of evidence on their soil for use in foreign proceedings except through official channels, on pain of criminal penalty. The third is the broader thicket of local privacy, secrecy, labour and works-council law that may forbid searching an employee's device, exporting banking data, or touching anything a works council has not approved. The cross-border collection succeeds only when it satisfies English disclosure and all three foreign layers at once, which is why it begins not with an examiner but with local counsel. This guide sets out that architecture.

§ 03 · INTERNATIONAL DATA TRANSFER

International data transfer under the UK GDPR

- **The restricted transfer:** bringing personal data from abroad into England, or moving it between jurisdictions in the course of collection, is a restricted international transfer under the UK GDPR requiring a lawful basis for the transfer itself, separate from the lawful basis for processing: the movement regulated, not just the holding.
- **The mechanisms:** transfer to or from a jurisdiction with UK adequacy needs no additional mechanism; otherwise the UK International Data Transfer Agreement, or the UK Addendum to the EU Standard Contractual Clauses, or (for one-off litigation transfers) a derogation such as the establishment or defence of legal claims: the mechanism chosen to fit the route and the countries involved.
- **The transfer risk assessment:** where a mechanism other than adequacy is used, an assessment of whether the destination's laws undermine the protection the mechanism promises, with supplementary measures where needed: the post-Schrems discipline applied to the collection.
- **Data minimisation reduces the transfer:** collecting and transferring only the relevant material (targeted cloud-side queries, in-country filtering before transfer) shrinks the personal data crossing the border and the risk it carries (guide 115 §7): minimisation as a cross-border risk-reduction tool, not only a review one.
- **The DUAA 2025 and the evolving landscape:** the UK's data-protection framework continues to develop (the Data (Use and Access) Act 2025 and adequacy decisions evolve): the current position on mechanisms and adequacy verified at the time of collection, not assumed from memory.

§ 04 · BLOCKING STATUTES AND LOCAL LAW

Blocking statutes and local law that forbid what disclosure demands

- **Blocking statutes:** laws that prohibit gathering or communicating evidence located in the country for use in foreign judicial proceedings otherwise than through official channels (the French blocking statute is the paradigm, and others exist), breach of which is a criminal offence: the collection that English disclosure demands potentially a crime where the data sits, requiring the formal-channel route of §5.
- **Banking and professional secrecy:** jurisdictions with strong banking secrecy (and professional-secrecy regimes for lawyers, doctors and others) that criminalise disclosure of protected data: the financial or professional records English disclosure seeks protected by local criminal law.
- **State secrets and data-localisation:** state-secrets laws and data-localisation regimes that forbid the export of categories of data or require data to remain in country: the material lawfully collectable only in place, never exported, in some jurisdictions.
- **Labour law and works councils:** in several European jurisdictions, searching an employee's device or communications requires works-council consultation or agreement and engages strong employee-privacy protections: the employee collection English law treats as routine subject to a co-determination process abroad.
- **Criminal privacy protections:** countries where unauthorised access to another's communications or device is a criminal offence with few of the exceptions English practice relies on: the imaging of a custodian's device potentially unlawful without their genuine consent or a local order.

§ 0 5 · THE ROUTES

The routes: cloud-side, in-country collection and letters of request

- **Cloud-side through a UK-controlled account:** where the custodian's data is held in a corporate cloud account controlled from the UK, collection server-side may reach it without any act physically occurring abroad (guides 111 to 114): frequently the cleanest route, though the local-law analysis still applies to the personal data and the custodian's rights, and the location of the provider's data centres may matter.
- **In-country collection, data kept local:** a local examiner collects the device or accounts within the jurisdiction, the data held in country under local-law-compliant conditions, and only the relevant, filtered material transferred once the mechanism and any blocking-statute clearance are in place: the route that respects local law by not exporting until export is lawful.
- **Formal channels, letters of request:** where compulsion is needed, or a blocking statute requires the official route, the Hague Evidence Convention letter of request (or bilateral mechanisms) through which the foreign court sanctions the evidence-gathering: slower and narrower, but the lawful path where self-help would be a crime.
- **Consent, genuinely given:** a cooperative custodian's genuine, informed, freely given consent to collection and transfer, valid where local law permits consent as a basis: real consent, documented, not the coerced consent of an employee who cannot refuse, which many jurisdictions disregard.
- **The route chosen per country and per data type:** a single matter spanning several jurisdictions may need different routes in each, and different routes for different data types within one country: the collection plan a matrix of country and data type, not a single method (guide 6's jurisdiction-mapping discipline, at collection).

§ 06 · PLANNING WITH LOCAL COUNSEL

Planning the cross-border collection with local counsel

- **Local counsel first:** qualified local counsel in each relevant jurisdiction engaged before any collection step, to map the blocking-statute, secrecy, labour and privacy constraints and confirm what is lawful: the foreign-law analysis obtained from those qualified in it, not guessed from English assumptions.
- **The country-by-data matrix:** for each jurisdiction and each data type, the lawful route, the transfer mechanism, the consents or consultations needed, and the sequence: the plan documenting how each element is collected lawfully before anything begins.
- **In-country resources arranged:** local examiners, review facilities or hosting where data must remain in country until transfer is cleared: the practical capability to keep data local secured in advance.
- **Works-council and employee steps:** where local labour law requires it, the works-council consultation or agreement and the employee-transparency steps completed before collection: the co-determination process run on its own timeline, which the collection plan must accommodate.
- **The English court kept informed:** where foreign law constrains or delays compliance with an English disclosure obligation, the position explained to the English court proactively (§7), with the plan showing the lawful maximum being done: the tension surfaced early, not sprung at trial.

§ 0 7 · DEPLOYMENT

Deployment: reconciling English disclosure duties with foreign law

- **The duty does not evaporate, but it is not absolute:** the English disclosure obligation applies to documents within a party's control wherever located, but the English court recognises that foreign law may constrain compliance, and expects a party to do the lawful maximum and explain any genuine foreign-law impediment, not to hide behind it or ignore it (guide 20's proportionality, meeting comity).
- **Candour with the court:** where a blocking statute or local law genuinely prevents or delays production, the position is put to the court candidly and early, with local-counsel evidence of the constraint and the steps being taken (letters of request, in-country collection): the court far more sympathetic to a surfaced, evidenced constraint than to late-discovered non-compliance.
- **The genuine-versus-tactical line:** the court distinguishes a genuine foreign-law bar from a party sheltering behind an overstated one: the local-counsel evidence and the demonstrated efforts to comply lawfully are what mark the difference, and a party that has planned properly (§6) can show it.
- **Admissibility and integrity preserved:** the evidence collected by a lawful cross-border route still meeting the English integrity and chain-of-custody standards (guides 2, 3), so that lawful collection abroad is also admissible collection at home: the two standards satisfied together.
- **Proportionality across the border:** the cost and delay of formal channels weighed in the proportionality of what is sought, with cloud-side and in-country routes offered as the proportionate alternative where compulsion would be disproportionate: the cross-border collection sized to the dispute, not pursued to the last document regardless of the foreign-law cost.

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: a custodian abroad sits within the same redundant estate as any other, but the layers are distributed across jurisdictions and each layer's collectability depends on where it physically resides and whose law governs it. The device abroad holds the local and deleted material but is the hardest to reach lawfully. The corporate cloud account, if controlled from the UK, may be collectable server-side without a foreign act at all. The provider's data centres may sit in a third country, adding another law. The counterparties, often in yet other jurisdictions, hold their side. The UK entity's own systems may already hold copies of much of the foreign custodian's correspondence and shared documents, collectable domestically without any cross-border step. The prudent cross-border plan asks first what can be collected inside the UK from the domestic side of every communication and shared repository, reducing the foreign collection to what genuinely exists only abroad, and then routes that residue through the lawful mechanism. Redundancy, here, is not just a fallback but the principal tool for minimising the cross-border problem itself.

QUESTION	DEVICE ABROAD	UK-CONTROLLED CLOUD ACCOUNT	UK ENTITY'S OWN SYSTEMS	COUNTERPARTIES (VARIOUS JURISDICTIONS)	PROVIDER DATA CENTRES	FORMAL-CHANNEL ONLY
Correspondence	Local cache (hard to reach)	Y: server-side	Y: the UK side of it	Y: their copy	Underlying storage	Where compulsion needed
Shared documents	Local copies	Y: synced + versioned	Y: shared into UK	Received copies	Underlying storage	n/a
Structured records	n/a	Y: if UK-controlled	Integrated copies	Their view	Localisation may bind	Where secrecy applies
Deleted / local-only	Y: device only	Version history	n/a	n/a	n/a	Often the only route
Lawful to collect where	Local law + transfer	UK, subject to rights	Y: UK, domestic	Their jurisdiction	Their jurisdiction	Via foreign court

Fallback strategy in one line: collect everything the UK side already holds domestically first; reach the UK-controlled cloud server-side; and route only the genuinely foreign-only residue through in-country collection, transfer mechanism or letter of request, with local counsel.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE BLOCKING STATUTE AND THE LETTER OF REQUEST

An English fraud claim needed documents from a custodian and a company office in a jurisdiction with a blocking statute criminalising the gathering of evidence for foreign proceedings outside official channels. The claimant's first instinct, to instruct a local firm to image the office server, was exactly what the statute forbade, and local counsel (§6) stopped it: proceeding would have exposed those involved to criminal penalty. The §5 formal-channel route was taken instead: a Hague Evidence Convention letter of request through which the foreign court sanctioned the evidence-gathering, narrowly scoped to the relevant documents. It was slower and required the English court's cooperation, but it produced admissible evidence lawfully, and the §7 candour with the English court, explaining the constraint and the route with local-counsel evidence, meant the timetable accommodated it. The self-help route would have been a crime; the official one was merely slow, and slow-but-lawful beat fast-but-criminal.

EXAMPLE 2 · THE CLOUD ACCOUNT THAT NEVER LEFT THE UK'S CONTROL

A commercial dispute involved a custodian based in a jurisdiction with strict employee-privacy and works-council law, whose device could not be searched without a co-determination process the timetable could not wait for. But the custodian's work data lived in the corporate Microsoft 365 tenant administered from the London head office. The §5 cloud-side route reached the relevant mailbox and OneDrive content server-side, through the UK-controlled account, without any collection act occurring in the foreign jurisdiction or on the foreign device. The §3 transfer analysis still applied, the custodian's personal data was being processed and the transfer mechanism and minimisation were addressed, and local counsel confirmed the route did not offend local law, but the works-council and device-search problem was avoided entirely by collecting from the UK side of the estate (§8). The lesson is that redundancy is the cross-border lawyer's best friend: the evidence existed in a place English law already controlled.

EXAMPLE 3 · THE IN-COUNTRY COLLECTION THAT WAITED FOR THE TRANSFER MECHANISM

A multi-jurisdiction investigation required imaging devices in three European countries. The temptation was to image them all and ship everything to the London review platform at once. The §6 plan, built with local counsel in each country, imposed discipline instead: local examiners imaged the devices in each jurisdiction, the images were held in country, and only after the §3 transfer mechanism (the UK International Data Transfer Agreement, with a transfer risk assessment) was executed and, in one country, a works-council step completed, was the filtered, relevant material transferred to London. The data minimisation of §3 meant only a fraction of each image crossed a border. The collection took three weeks longer than a ship-it-all approach, but it was lawful in every jurisdiction and admissible in England, and when the other side probed the collection's propriety, the country-by-data matrix and the executed mechanisms answered every question. Lawful, documented and slower beat fast and exposed.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Treating an English order as a global licence:** imaging or exporting data abroad because an English court ordered disclosure, ignoring that local law governs the data: Example 1's near-crime.
- **Skipping local counsel:** the foreign-law constraints guessed from English assumptions rather than obtained from those qualified in the jurisdiction: the single most dangerous omission.
- **Transfer treated as logistics:** data shipped to England with no transfer mechanism or risk assessment, a UK GDPR breach in the collection itself (§3).
- **Blocking statutes unresearched:** a self-help collection run in a jurisdiction where it is a criminal offence, exposing individuals to penalty.
- **Works-council and labour steps ignored:** an employee device searched abroad without the co-determination process local law requires: Example 2's avoided trap.
- **Ship-it-all by default:** Example 3's temptation: whole images exported before minimisation and before the mechanism, multiplying the transferred personal data and the risk.
- **Non-compliance concealed:** a foreign-law bar discovered late and sprung at trial, rather than surfaced candidly to the court early (§7).
- **Domestic redundancy overlooked:** a hard foreign collection pursued while the UK side of the estate already held much of the material collectable at home (§8).

Technical limitations

- **Cloud-side does not dissolve local law:** even server-side collection processes the custodian's personal data and may engage local rights and data-centre-location questions: the analysis still required, not bypassed.
- **Formal channels are slow and narrow:** letters of request take months and yield only what the foreign court sanctions: the timetable and scope planned around them.
- **Consent is often invalid:** employee consent is disregarded in many jurisdictions as not freely given: it cannot be the whole basis where local law rejects it.
- **The law is moving:** adequacy decisions, transfer mechanisms and the UK framework evolve (DUAA 2025 and beyond): the current position verified at the time, not assumed.
- **Multi-jurisdiction means multi-plan:** each country needs its own analysis and route; there is no single cross-border method: the complexity scales with the map.

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- In which countries are the relevant custodians, devices and data, and is any of it already held in UK-controlled cloud accounts or UK systems?
- Are there works councils, secrecy regimes or known blocking statutes in any relevant jurisdiction?
- Which local counsel do we engage in each jurisdiction, and how does their timeline affect ours?

Ask your opponent

- Please identify the jurisdictions in which relevant custodians, devices and data are located, and confirm what is held in UK-controlled accounts or systems and collectable without a cross-border step.
- Please confirm the routes proposed for collecting foreign-located data, the transfer mechanisms to be used, and any foreign-law constraints (blocking statutes, secrecy, labour law) said to affect production, supported by local-counsel evidence.
- Please confirm that any collection abroad will comply with local law and maintain integrity and chain of custody to the standard required for admissibility in these proceedings.

Ask your eDiscovery / forensic provider (and local counsel)

- For each country and data type, what is the lawful route, the transfer mechanism, and the consents or consultations required?
- What can be reached cloud-side through a UK-controlled account or collected domestically from the UK side, reducing the foreign collection?
- How will in-country data be held and filtered before transfer, and how will the whole be documented for the English court?

SUGGESTED WORDING · INSTRUCTION FOR A CROSS-BORDER COLLECTION

> "We instruct you, together with local counsel in each relevant jurisdiction, to plan and conduct the collection of evidence located abroad in respect of the custodians and jurisdictions at Schedule 1. Please: (1) before any collection step, obtain local-counsel confirmation of the applicable blocking-statute, secrecy, labour, works-council and privacy constraints, and produce a country-by-data-type matrix identifying the lawful route for each; (2) identify all relevant material collectable within the UK from UK-controlled cloud accounts or UK systems, and limit foreign collection to material genuinely available only abroad; (3) for foreign-located data, use in-country collection with data held locally, transferring only filtered relevant material once a lawful UK GDPR transfer mechanism and any required consents, consultations or official channels (including letters of request) are in place; (4) complete a transfer risk assessment and apply data minimisation so that only relevant material crosses any border; and (5) maintain integrity and chain of custody to the standard required for admissibility in England, and document the lawful basis of each step. Advise promptly of any foreign-law impediment to compliance so it can be put to the court."

§ 1 2 · QUICK CONTROL

Checklist and red flags · When to involve a digital forensic expert

The cross-border-collection checklist

- ☐ Jurisdictions of custodians, devices and data identified
- ☐ Local counsel engaged in each relevant jurisdiction before any step
- ☐ Blocking-statute, secrecy, labour and privacy constraints mapped
- ☐ Material collectable within the UK identified and collected first
- ☐ Lawful route chosen per country and per data type
- ☐ UK GDPR transfer mechanism selected and executed
- ☐ Transfer risk assessment completed; data minimisation applied
- ☐ Works-council and employee steps completed where required
- ☐ In-country data held locally until transfer is lawful
- ☐ Integrity, chain of custody and English admissibility preserved

Red flags

- An instinct to image or ship a device abroad on the strength of an English order alone: Example 1.
- Any jurisdiction with a known blocking statute or strong secrecy regime.
- Employee-device collection abroad with no works-council step: Example 2's avoided trap.
- Whole images exported before minimisation or a transfer mechanism: Example 3's temptation.
- No local counsel engaged.
- A foreign-law impediment discovered late rather than surfaced early.
- Domestic UK sources of the same material overlooked.

When to involve a digital forensic expert

At the very first indication that a custodian, device or data set is abroad, because the plan is legal before technical and local counsel must be engaged before any collection step (Example 1); at planning, where the country-by-data matrix, the transfer mechanisms and the in-country resources are built with local counsel (Example 3); at collection, where cloud-side, in-country and formal-channel routes are executed lawfully with integrity preserved (Example 2); and at deployment, where the reconciliation of English disclosure with foreign law is put candidly to the court and the collection defended under CPR Part 35. Through **e-discovery.uk**, cross-border collections are run in coordination with local counsel and in-country examiners so the evidence arrives both lawfully and admissibly: because an English order reaches English shores, and everything beyond them is another country's law.

§ 13 · COMMON QUESTIONS

Frequently asked questions

The court has ordered disclosure. Can we just image the custodian's device abroad?

No: an English order does not make it lawful to collect and export data in another country, whose law governs the data (§2). Depending on the jurisdiction, self-help collection may breach data-protection, labour, secrecy or blocking-statute law, and in some places be a criminal offence (§4, Example 1). Engage local counsel first and choose a route lawful where the data sits.

What is a blocking statute and why does it matter so much?

It is a law that criminalises gathering or exporting evidence located in the country for foreign proceedings otherwise than through official channels (the French statute is the classic example, §4). It matters because the ordinary collection English disclosure expects can be a crime where the data sits, and the only lawful route may be a letter of request through the foreign court (§5, Example 1): slow, but lawful.

Is moving the data to England just a logistics question?

No: it is a restricted international transfer under the UK GDPR needing a lawful transfer mechanism (adequacy, the IDTA or Addendum, or a litigation derogation) and usually a transfer risk assessment (§3). Treating it as mere logistics is a data-protection breach in the collection itself. Data minimisation, transferring only relevant material, reduces both the risk and the volume crossing the border.

Can cloud-side collection avoid the whole problem?

It can avoid much of it where the data sits in a UK-controlled corporate account, because collection happens server-side without a foreign act or a foreign-device search (§5, Example 2): but it does not dissolve local law, the custodian's personal data is still processed and their local rights and the provider's data-centre locations may still bite. It is often the cleanest route, but the local-law analysis still applies.

What do we tell the English court if foreign law blocks disclosure?

The truth, early and with evidence: put the constraint to the court candidly, supported by local-counsel evidence, and show the lawful maximum being done, letters of request, in-country collection, cloud-side routes (§7, Example 1). The court distinguishes a genuine, evidenced foreign-law bar from a party sheltering behind an overstated one, and rewards the party that surfaced and planned around the constraint rather than concealing it.

Can the employee just consent to us collecting their device abroad?

Sometimes, but be careful: many jurisdictions treat employee consent as not freely given and disregard it (§5, §10), and works-council or co-determination steps may be required regardless of the individual's agreement (§4). Genuine, informed, documented consent helps where local law accepts it, but it cannot be assumed to be the whole basis, and local counsel must confirm its validity in the jurisdiction.

§ 1 4 · REFERENCE

Glossary

Restricted transfer
Moving personal data outside its jurisdiction, regulated under the UK GDPR.

Blocking statute
A law criminalising evidence-gathering for foreign proceedings.

IDTA
The UK International Data Transfer Agreement, a transfer mechanism.

UK Addendum
The UK addition to the EU Standard Contractual Clauses.

Adequacy
A finding that a country protects data adequately, easing transfer.

Transfer risk assessment
Assessing whether a destination's law undermines the transfer safeguard.

Letter of request
A formal request through a foreign court to gather evidence.

Hague Evidence Convention
The treaty framework for taking evidence abroad.

Works council
An employee body whose consultation local law may require.

Data localisation
A rule requiring data to remain in a country.

Sources and authoritative references

The cross-border disciplines in this guide draw on materials published by our laboratory and e-discovery practice, referenced here as sources:

- e-discovery.uk, EDRM Phase 03 · Preservation and Phase 04 · Collection (cross-border, in-country and cloud-side collection as practised): e-discovery.uk/edrm/preservation · e-discovery.uk/edrm/collection
- cflab.uk, digital forensics services (cross-border collection coordination, integrity and CPR Part 35 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- ICO, international transfers and the IDTA (transfer mechanisms and transfer risk assessments): ico.org.uk, international transfers
- HCCH, Hague Evidence Convention (taking of evidence abroad): hcch.net, Evidence Convention · CPR Part 34 (evidence, including letters of request): justice.gov.uk, Part 34
- PD 57AD: justice.gov.uk, PD 57AD · CPR Part 31: justice.gov.uk, Part 31 · Data (Use and Access) Act 2025: legislation.gov.uk, DUAA 2025 · ISO/IEC 27037: iso.org, 27037

DISCLAIMER

This publication provides general information about cross-border collection from custodians abroad as at August 2026. International data-transfer law, adequacy decisions, blocking statutes and local privacy, secrecy and labour law vary by jurisdiction and change frequently; this guide is not a substitute for qualified local-law advice in each relevant jurisdiction, which must always be obtained before collecting abroad. The worked examples are fictional. This guide is not legal advice, does not create a professional relationship, and should not be relied upon in place of advice on the facts of a specific matter from a qualified lawyer or a suitably qualified forensic practitioner. Links were live at the date of publication.

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

Cross-border collection at **e-discovery.uk** is run as a legal exercise first: local counsel engaged in every relevant jurisdiction before any step, a country-by-data-type matrix built so each element has a lawful route, and the collection sequenced so no act breaches local law. The plan reaches first for what the UK side of the estate already holds, collecting domestically from UK-controlled cloud accounts and UK systems to shrink the foreign problem (Example 2), then routes the genuinely foreign-only residue through in-country collection with data held locally until a UK GDPR transfer mechanism and any works-council or official-channel steps are in place (Example 3), and uses letters of request where a blocking statute or the need for compulsion requires the formal path (Example 1). Every step is documented for the English court, integrity and chain of custody are preserved for admissibility, and data minimisation keeps the personal data crossing any border to the relevant minimum. Reports run under CPR Part 35. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and if a matter has a custodian abroad, the first call is to local counsel, and the second is to a collection team that has done it lawfully before.

INSTRUCT THE LAB

Speak to a forensic examiner, not a salesperson.

Describe your matter in confidence and an examiner will respond the same working day. Conflicts checks and scoping calls with US counsel are routine.

NEW ENQUIRIES
+44 (0)20 7164 6971

EMAIL
info@cflab.uk

E-DISCOVERY
e-discovery.uk

Computer Forensics Lab Ltd · Euro House, 133 Ballards Lane, Finchley, London N3 1LJ, United Kingdom
cflab.uk · Customer service +44 (0)20 7164 6915 · ICO ZB395023 · NPCC · ISO 17025 aligned practice · UK Gov Digital Marketplace