PORTFOLIO BOOK SERIES · No. 78

White Paper

BEYOND BORDER COMPLIANCE

Cross-Border Data Programmes Fail When Geography Is Treated as a Legal Footnote

Building a portfolio case for coordinated action across competing regulatory regimes

Giovanni Leonardi

July 2019

Contents

Cross-Border Data Programmes Fail When Geography Is Treated as a Legal Footnote

Portfolio · No. 78
Originally written July 2019 | Re-edited and re-rendered for the WhereBeyond Edition,

"A cross-border data programme succeeds when geography becomes a portfolio design variable, not a late legal exception."

1. Executive Summary

A programme steering pack can show every regional workstream as green while the enterprise remains unable to answer a basic question: which personal data crosses which border, under whose authority, and with what operational consequence? In 2019, more than a year after the General Data Protection Regulation became applicable, that gap is no longer a technical inconvenience. It is a portfolio risk.

Cross-border data programmes are commonly framed as legal compliance exercises. That framing is too narrow. The law supplies the obligations, but geography determines how those obligations collide with operating reality: shared service centres, outsourced processing, regional platforms, customer access requests, incident escalation, retention rules and onward transfers. Each can be locally defensible and collectively incoherent.

The evidence from complex programmes points to three recurring failures:

- Local interpretation without enterprise visibility. Regions make reasonable decisions in isolation, leaving central leaders unable to see aggregate exposure or duplication.
- Global standards without local authority. A central team issues controls that cannot be executed under local law, contract or market practice.
- Technology-first remediation. Programmes buy discovery, consent or records tools before agreeing data ownership, decision rights and the transfers that matter most.

The recommended response is a federated cross-border data portfolio: one enterprise control architecture, regional accountability for interpretation and execution, and a portfolio office that sequences investment by transfer risk rather than organisational influence. This is neither full centralisation nor loose coordination. It is a deliberate allocation of decisions.

A representative programme described in this paper began with 47 nominal privacy initiatives across eight jurisdictions and a budget request equivalent to £18.6 million. Once overlapping work was exposed and transfers were ranked by consequence, the portfolio was reduced to 19 governed initiatives at £12.9 million. The saving was not achieved by weakening compliance. It came from removing duplicated inventories, consolidating common controls and stopping low-value technology purchases. More importantly, the programme reduced unresolved high-risk transfer routes from 64 to 11 within nine months.

The central recommendation is straightforward: approve the case for change at portfolio level, fund common control capabilities once, and make every material cross-border transfer traceable to an accountable business owner, a lawful mechanism, an operating control and a regional sign-off.

> *A cross-border data programme succeeds when geography becomes a portfolio design variable, not a late legal exception.*

2. Regulation Meets the Operating Map

The organisation chart is a poor guide to the movement of data. A European customer record may be captured in one country, enriched in a second, supported from a third and archived by a supplier in a fourth. The business process appears singular; the legal and operational chain is not.

That distinction matters because cross-border obligations attach to activities rather than reporting lines. The relevant questions are concrete:

- Where is the individual, and which entity determines the purpose of processing?
- Which systems and service providers receive the data, including support and backup environments?
- What transfer mechanism is relied upon, and does the contract reflect the actual chain?
- Which retention, access and deletion rules can the operating process genuinely execute?
- Who decides whether a new use is compatible with the original purpose?
- Which authority leads when an incident crosses several jurisdictions?

In a single-country programme, ambiguities may be contained within one legal interpretation and one management chain. Across borders, each ambiguity is multiplied. A regional privacy lead may approve a transfer on the assumption that a central contract includes the necessary clauses. Procurement may assume the business has completed due diligence. Technology may assume the data owner has defined retention. The business may assume all three functions have resolved the matter. The transfer proceeds because everyone owns a fragment and no one owns the whole.

The portfolio consequence is hidden demand. Similar inventories are commissioned repeatedly. Each region negotiates its own supplier schedules. Several systems are configured to answer access or deletion requests, but none can trace the full customer journey. Budgets are therefore consumed by activity that is locally rational yet incapable of producing enterprise assurance.

3. What the Programme Evidence Reveals

Consider a composite group operating across eight jurisdictions in Europe, the Middle East and Asia. Its initial case for change listed 47 initiatives: regional record-of-processing exercises, contract remediation, customer preference changes, retention projects, supplier reviews and three competing proposals for data discovery software.

The reported position looked reassuring:

Measure	Reported at mobilisation	What validation found
Regional workstreams rated green or amber	43 of 47	Status measured completion of local plans, not reduction of transfer risk
Applications listed in inventories	612	Only 358 had an identified business owner
Supplier processing arrangements reviewed	81%	Review usually covered the direct supplier, not onward processing
Cross-border routes documented	126	64 lacked a confirmed mechanism, current contract or executable control
Deletion processes described as operational	7 of 8 regions	Only 2 could delete across both live and archived records

The decisive moment came during a customer access request. The front office in one jurisdiction found the primary record within three days. A shared service centre held correspondence under a different customer identifier. An outsourced archive contained

scanned forms, but the retrieval request had to pass through procurement because the service owner had left. Twenty-six days into the statutory response window, the group had found five repositories and still could not say whether the search was complete.

Nothing in that sequence was caused by a single negligent team. Each unit had followed its own procedure. The failure arose between procedures.

The portfolio office then traced one high-volume customer process end to end. A single record crossed six systems, three legal entities and two external processors. Four separate projects had budgeted to inventory parts of that path. Two intended to buy similar scanning tools. No initiative funded the reconciliation of identifiers between the shared service centre and the archive. The programme had allocated £1.4 million to finding data and nothing to ensuring that found records could be connected to the same person.

This example exposes the mechanism behind the wider pattern: local compliance produces artefacts; cross-border governance must produce continuity. An inventory has value only if it connects a processing purpose to data, systems, entities, suppliers, transfers, controls and an owner. If those links break at a border or organisational boundary, the artefact records effort rather than assurance.

4. Why the Familiar Responses Fail

Three responses usually compete for executive support. Each contains a serious truth, but each becomes dangerous when treated as a complete answer.

4.1 Leave Compliance to the Regions

The strongest case for regional autonomy is not parochialism. Privacy law is interpreted and enforced locally. Language, employment law, works council expectations, sector rules and regulator practice differ. A distant central team can easily mistake formal consistency for legal adequacy.

That argument is correct as far as it goes. It fails when autonomy is allowed to obscure shared infrastructure and aggregate exposure. A regional officer can judge whether a local notice is appropriate; that officer cannot alone govern a platform used by seven markets or renegotiate an enterprise supplier contract. Nor can eight regional budgets independently decide which common capability should be funded first.

Regional authority is necessary. Regional isolation is not.

4.2 Impose One Global Standard

The case for a single global standard is equally serious. One control baseline simplifies training, contracting, assurance and technology design. Where the strictest practical rule can be applied everywhere, the enterprise may reduce cost and confusion.

The difficulty is the phrase where practical. A universal rule often conceals exceptions until implementation. Data localisation, employment records, consent requirements, retention duties and regulator expectations may prevent identical execution. When the global policy offers no governed way to record deviation, regions either delay the programme or create informal workarounds. Apparent uniformity then drives real inconsistency underground.

A standard should define the minimum control objective and evidence required. It should not pretend every jurisdiction reaches that objective through the same procedure.

4.3 Buy the Missing Capability

Technology can accelerate discovery, preference management, records maintenance and case handling. It cannot decide who owns a transfer, whether a purpose is legitimate, which jurisdiction governs a relationship or how much residual risk the enterprise will accept.

The composite programme's three discovery proposals illustrate the point. Together they sought £3.2 million. A six-week validation found that roughly half the target repositories contained low-risk operational data already governed by existing retention schedules. The urgent gap was not discovery breadth but ownership and linkage across 23 high-consequence routes. Funding all three proposals would have generated more findings than the organisation could adjudicate.

Tools amplify a control system. Where the system is undecided, they amplify uncertainty.

5. The Case for a Federated Portfolio

The right unit of management is not the regional project and not the central policy. It is the material data route: a repeatable movement or access path that connects a business purpose, a population of individuals, one or more jurisdictions, systems, processors and controls.

Managing these routes as a portfolio changes the investment question. Instead of asking, “Which region has completed its plan?” leaders ask, “Which routes create the greatest consequence if their legal or operational basis fails, and what common capabilities reduce

that exposure?"

The recommended model allocates authority at three levels:

Level	Accountable decision	Required evidence
Enterprise	Control objectives, risk appetite, common capabilities, supplier positions	Control standard, investment roadmap, enterprise exceptions register
Regional	Legal interpretation, local execution, regulator engagement, formal deviation	Regional assessment, implementation evidence, sign-off
Route owner	Purpose, data need, operational controls, remediation acceptance	Route record, named systems and processors, control tests, decision log
Portfolio office	Prioritisation, dependency management, benefits and risk reporting	Ranked register, integrated plan, gate papers, outcome measures

This allocation prevents two opposite errors. Central leaders cannot declare a route compliant merely because a common standard exists. Regional teams cannot accept enterprise exposure without visibility or challenge. The route owner, usually the executive responsible for the business process rather than the system custodian, must account for why the movement exists and whether its benefits justify its controls.

6. Building the Case for Change

A credible case for change should not begin with a catalogue of laws. Executives rarely dispute that laws matter; they dispute the scale, urgency and value of coordinated investment. The case must therefore connect regulatory obligations to operational consequence and portfolio economics.

6.1 Establish the Exposure Baseline

The baseline is a rapid, decision-oriented view, not an attempt to perfect the entire data inventory before action begins. It should identify material routes and test whether four essentials are present:

- Authority: a documented purpose, responsible entity and lawful basis for processing and transfer.
- Accountability: a named business route owner and regional approval where required.

- Execution: contracts, access controls, retention, request handling and incident procedures that work across the whole route.
- Evidence: records that can demonstrate the preceding three elements to management, auditors or authorities.

Materiality should reflect more than record count. A small transfer of health, financial or employee information may deserve higher priority than a large flow of routine contact data. The portfolio should score consequence using categories that leaders can understand: harm to individuals, legal exposure, service interruption, contractual failure and loss of strategic freedom.

6.2 Quantify the Cost of Fragmentation

The investment case strengthens when duplication is made visible. In the composite programme, 47 initiatives contained 112 separately costed deliverables. Mapping them against common control needs revealed:

- 21 inventories using five different classifications;
- 14 supplier-review workstreams examining many of the same enterprise processors;
- 9 retention initiatives dependent on two shared archives;
- 6 customer-request improvements, none funding cross-system identity reconciliation;
- 3 data discovery purchases with overlapping scope.

The revised portfolio funded the reusable components once: a common route register, an approved processing and transfer taxonomy, standard supplier schedules, a cross-border request protocol, shared control testing and targeted discovery for the highest-risk repositories. Regional funds remained for local legal analysis, notices, employee consultation, language and implementation.

The gross request fell from £18.6 million to £12.9 million. Of the £5.7 million reduction, £3.1 million came from removing duplicate work, £1.6 million from narrowing technology scope and £1.0 million from sequencing lower-risk remediation beyond the first funding horizon. The programme retained a contingency for changes in interpretation and enforcement. This mattered: a case that assumes regulation will remain static is not prudent; it is merely neat.

6.3 Express Benefits as Decision Capacity

Avoid claiming benefits that cannot be evidenced, such as the abstract value of “trust”. Trust may be real, but it is difficult to manage as a programme outcome. More useful

benefits describe decisions and controls the organisation can perform:

- percentage of material routes with an accountable owner and confirmed mechanism;
- elapsed time to locate records across the route during an access request;
- percentage of strategic suppliers with validated onward-processing chains;
- number and age of unresolved regional deviations;
- time from an incident signal to a coordinated jurisdictional assessment;
- duplicate control costs removed from regional plans.

These measures connect investment to capability. They also prevent the programme from declaring victory because documents have been produced.

7. The Control Architecture

The federated model requires a small set of artefacts, maintained as management instruments rather than compliance decoration.

7.1 The Route Register

Each material route should record the business purpose, categories of individuals and data, originating and receiving entities, systems, processors, jurisdictions, transfer mechanism, retention rule, owner, regional approvals and control-test status. It should link to existing records rather than reproduce them.

The register is not a universal data dictionary. Its purpose is to make a management decision possible. If a field does not help determine authority, consequence, control or accountability, it probably does not belong in the first release.

7.2 The Control Baseline and Deviation Record

The enterprise baseline states the outcome required and the evidence that proves it. A regional deviation then records:

1. the requirement that cannot be applied as written;
2. the local legal or operational reason;
3. the alternative control;
4. the residual risk and approving authority;

5. the review date or trigger.

This turns difference into governed information. It allows leaders to see whether a supposed local exception is unique, shared by several jurisdictions or symptomatic of a poor central standard.

7.3 Transfer and Supplier Assurance

Contract review must follow the actual processing chain. Direct supplier clauses are insufficient if important operations are passed to affiliates or subcontractors. Assurance should reconcile the contractual schedule with the route register, identify onward processing and test whether changes in location or provider are communicated before they occur.

For repeated arrangements, approved positions on standard contractual clauses, audit rights, breach notification, deletion and subcontracting can reduce negotiation effort. But the approved position is a starting point, not evidence that a particular route has been implemented correctly.

7.4 Operational Playbooks

At least three processes require cross-border playbooks: individual rights requests, incidents and material change.

A rights-request playbook should define the coordinating role, identity matching, regional interpretation, search scope, exemptions, response assembly and evidence retention. An incident playbook should connect security investigation with legal assessment across affected jurisdictions; waiting for a technical conclusion before involving regional privacy leads can consume valuable time. A change playbook should trigger review when a new processor, system, purpose, jurisdiction or data category is introduced.

8. Sequencing the Portfolio

The work should progress through decision gates, not through a single mass remediation plan.

1. Mobilise and set authority. Appoint the executive sponsor, regional decision-makers, route owners and portfolio lead. Approve scoring, escalation and exception rules.

2. Build the material-route baseline. Use existing records, architecture diagrams, contracts and process interviews to identify the routes that matter. Accept that the first baseline will be incomplete; record confidence rather than disguising uncertainty.

3. Stabilise immediate exposure. Address routes with no defensible mechanism, no owner, uncontrolled sensitive data, weak supplier chains or an imminent operational event.

4. Fund common controls. Consolidate shared artefacts and capabilities before regions buy separate solutions. Make regional adoption costs explicit.

5. Remediate by route. Complete the chain from purpose to evidence. Do not close a workstream because one component, such as a contract or inventory, is finished.

6. Test through real operations. Use access requests, supplier changes, retention runs and incident exercises to test whether the controls work under time pressure.

7. Transfer to enduring governance. Move route ownership into business management, regional interpretation into local accountability and portfolio oversight into the regular investment and risk cycle.

The composite programme used three gates. At the first, a route required an owner and consequence score before receiving remediation funds. At the second, legal mechanism and target controls had to be agreed before technology configuration. At the third, closure required an operational test witnessed by a regional representative. These gates initially slowed visible activity. Within two quarters, they reduced rework because projects stopped discovering unresolved ownership and legal questions during implementation.

9. Objections, Trade-offs and Limits

A federated portfolio creates overhead. Route records must be maintained, regional leaders must attend decisions, and deviations become visible to executives. A smaller organisation with few jurisdictions and simple supplier arrangements may reasonably choose a lighter model.

There is also a risk of central bureaucracy. A portfolio office can become another review layer, measuring completeness of templates rather than quality of decisions. Its mandate should therefore be narrow: prioritise routes, manage dependencies, enforce gates, expose decisions and measure outcomes. It should not replace the privacy officer, legal counsel, security, procurement or business ownership.

Nor does the model remove uncertainty. In 2019, organisations are operating amid active regulatory interpretation, differing supervisory expectations and continuing debate about international transfer mechanisms. The objective cannot be permanent certainty. It is controlled adaptability: knowing which routes depend on a contested interpretation, which controls would need to change and who has authority to act.

Finally, standardisation has diminishing returns. Common taxonomies, contracts and evidence can reduce cost; forcing identical local procedures can increase it. The economic optimum lies where shared components end and genuine jurisdictional difference begins. That boundary must be decided, not assumed.

10. Recommendation

Executive committees should approve cross-border data work as a single federated portfolio with funding conditional on four commitments:

- Every material route has one accountable business owner.
- Enterprise control objectives are common, while regional deviations are explicit and approved.
- Common capabilities are funded once and adopted through the portfolio.
- Progress is reported as reduction in unresolved route exposure and improvement in operational response, not completion of local documents.

The first 90 days should produce a material-route baseline, a ranked exposure register, named decision rights, immediate containment actions and a consolidated investment proposal. It should not promise a perfect inventory. Perfection delays decisions while data continues to move.

By month nine, the composite programme had reduced unresolved high-risk routes from 64 to 11, assigned owners to 96% of material routes and cut average retrieval time in controlled access-request tests from 21 working days to 8. Four routes remained open because regional legal interpretation and supplier changes were unresolved; they were reported as executive decisions, not hidden as project slippage.

That is the practical standard. Cross-border governance is credible when the organisation can trace a route, explain its authority, operate its controls, expose its uncertainty and make a timely decision about what happens next. Regulation may begin the conversation, but geography turns it into portfolio management.