

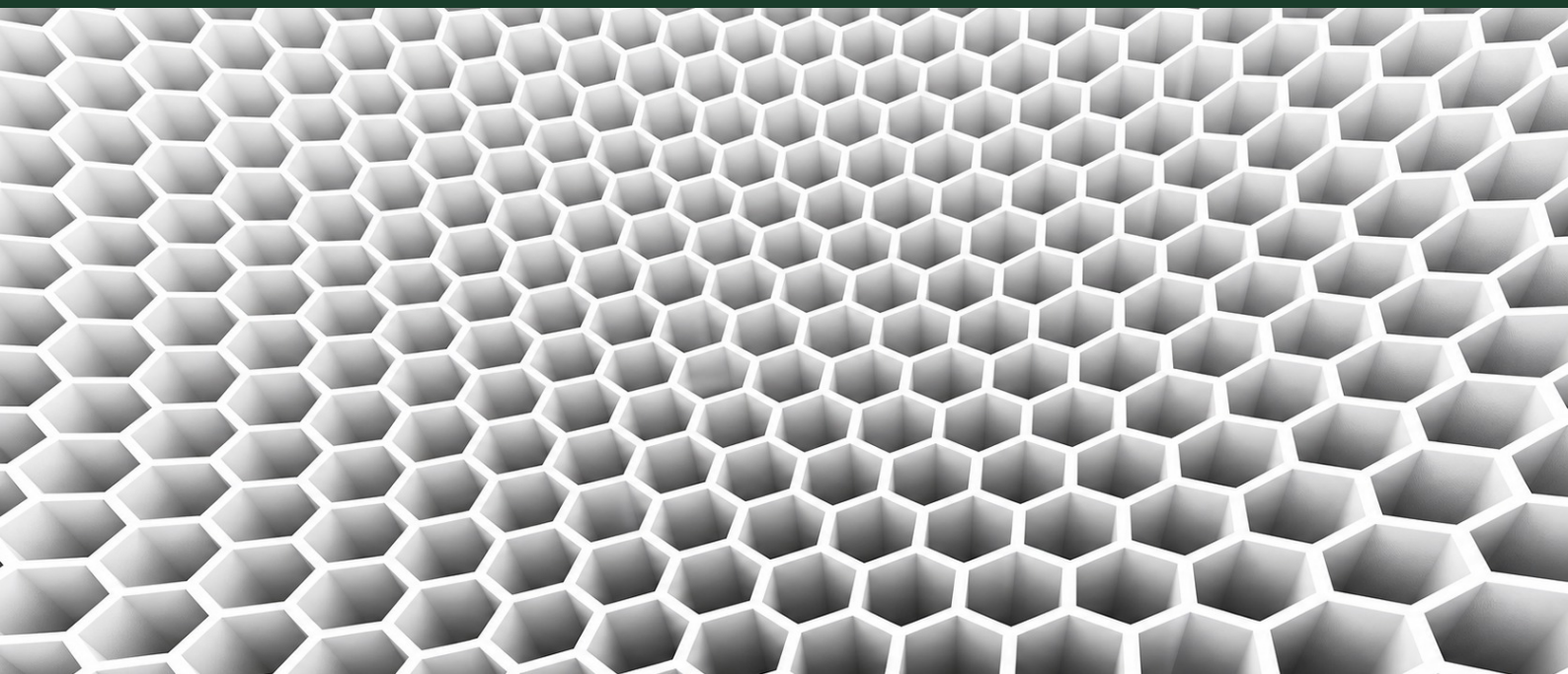
BEYOND THE JURISDICTION

Cross-Border Data Programmes — When Regulation Meets Geography and Nobody Owns the Answer

A Practitioner's Perspective on Multi-Jurisdiction Data Governance Programmes During the GDPR Era

Giovanni Leonardi

February 2019



Cross-Border Data Programmes — When Regulation Meets Geography and Nobody Owns the Answer

Programme · No. 205

Originally written February 2019 | Re-edited and re-rendered for the WhereBeyond Edition, 2025

*“The programme that looked simple in one country
became ungovernable in three.”*

The Problem Nobody Wanted to Own

The pattern became visible almost immediately after GDPR took effect in May 2018. Organisations operating across multiple European jurisdictions — and particularly those with operations spanning the EU, the UK, and regulated markets in Asia-Pacific — discovered that their data programmes had been designed as if regulation were uniform and geography irrelevant. They were neither.

In my experience, the most common failure mode was not ignorance of the regulations themselves. Most organisations had competent legal teams who understood GDPR, understood the local implementations in Germany, France, and the Nordics, and understood the distinct requirements emerging in markets like Singapore and Australia. The failure was structural: nobody had designed a programme governance model capable of reconciling these competing requirements into a coherent set of delivery decisions.

The data programme that had been scoped, funded, and governed as a single entity — with a single set of requirements, a single delivery timeline, and a single accountable executive — fractured the moment it encountered a second jurisdiction with materially different expectations about consent, data residency, or cross-border transfer.

What Actually Went Wrong

The structural problem had several layers, each reinforcing the others.

First, programme governance assumed a single regulatory context. The standard programme structure — a steering committee, a programme board, a set of workstreams reporting to a single SRO — was designed for programmes that operate within one set of rules. Cross-border data programmes operate within many. The consent model that satisfied the Irish Data Protection Commission did not satisfy the Bavarian equivalent. The data residency architecture that worked for the UK required fundamental redesign for Germany. Each jurisdiction introduced not just additional requirements but additional

decision-makers, additional approval gates, and additional interpretive uncertainty.

Second, the legal function and the delivery function operated on different timescales. Legal teams needed time to analyse, interpret, and advise. Delivery teams needed decisions now. In a single-jurisdiction programme, this tension is manageable — one legal team, one set of advice, one decision. In a multi-jurisdiction programme, the legal analysis multiplied while the delivery timeline did not. The result was paralysis: workstreams waiting for legal guidance that was itself waiting for regulatory clarity that might not arrive for months.

Third, data architecture had been designed for efficiency, not for jurisdictional boundaries. The centralised data lake, the single customer view, the consolidated reporting platform — all of these architectural patterns assume that data can move freely within the organisation. GDPR, and particularly the divergent national implementations of GDPR, challenged that assumption directly. Organisations discovered that their elegant, consolidated architectures needed to be partitioned, replicated, or redesigned — and that the programme plan had not accounted for this.

The Deeper Pattern

What cross-border data programmes revealed was not a regulatory problem but a governance design problem. The programme management discipline, as practised in most large organisations, assumes a degree of environmental stability that multi-jurisdiction regulatory compliance does not provide. It assumes that requirements can be baselined, that scope can be controlled, and that the rules of the game will not change materially during delivery.

None of these assumptions held. Requirements shifted as regulators issued new guidance. Scope expanded as each jurisdiction surfaced new constraints. And the rules themselves were being written in real time — the first enforcement actions under GDPR were only beginning to establish the practical boundaries of compliance.

The organisations that navigated this most effectively were those that abandoned the pretence of a single, unified programme and instead adopted a federated model: a common architecture and a shared set of principles, but with local delivery teams empowered to make jurisdictional decisions within those guardrails. This was not elegant. It was messy, duplicative, and expensive. But it was honest about the problem — and honesty about the problem is the first condition of solving it.

The programme that tried to govern cross-border data compliance as a single, centrally controlled initiative was not being ambitious. It was being naive about the nature of the problem it faced.

The lesson for programme leaders is uncomfortable but clear. When the regulatory environment is fragmented, the programme governance model must be capable of operating within that fragmentation rather than pretending it does not exist. This means accepting distributed decision-making, accepting that different jurisdictions will move at different speeds, and accepting that the programme plan is a living negotiation rather

than a fixed contract.

The organisations that learned this during 2018 and early 2019 paid a high price in replanning, rearchitecting, and restructuring their programmes. Those that have not yet learned it will pay the same price later, compounded by the additional jurisdictional complexity that shows no sign of diminishing.