Financial Innovation for Impact

Cambridge Centre for Alternative Finance

UNIVERSITY OF CAMBRIDGE Judge Business School



Joined-Up Regulation

Coordination Between Data Protection and Financial Authorities in Emerging Markets

Data protection and financial services oversight in ten emerging markets: evidence, obstacles, and a way forward

With the support of

Gates Foundation

October 2026



Suggested Citation

CCAF and Fii (2026). Joined-Up Regulation: Coordination Between Data Protection and Financial Authorities in Emerging Markets

'Gates Foundation' is a registered trademark of the Gates Foundation in the United States and is used with permission.

Cover image: Mumbai skyline

Foreword 4
Acknowledgements 9
Executive summary 10

1. Introduction 15
1.1 About the programme 16
1.2 Audience 16
1.3 Research approach 17
1.4 Limitations 19
1.5 Report structure 20

2. Why joined-up regulation matters 22
2.1 Background and context 23
2.2 The case for joined-up regulation 26
2.3 What we mean by coordination 32
2.4 Five high-impact thematic areas 35
2.5 Regulatory landscape 37

3. Coordination today: Where it is happening 40
3.1 International and regional architecture 41
3.2 National architecture 47

4. Gaps in coordination across the five thematic areas 57
4.1 Digital identity, KYC and AML/CFT 59
4.2 Fraud 65
4.3 Open finance 70
4.4 Credit underwriting and AI 74
4.5 Cross-border data flows and localisation 80

5. Measuring coordination and what it is worth 85
5.1 Why measurement matters 86
5.2 The regulatory coordination index 89
5.3 What the index shows 92
5.4 What coordination is worth 97
5.5 Limitations and future of the framework 99

6. Key findings 100

7. Impediments to coordination 104
7.1 The five impediments 106
7.2 The coordination ‘anti-flywheel’ 110
7.3 How the impediments play out: three patterns 111

8. Recommendations 114

9. Conclusion 123

Appendix 125
Detailed country evidence tables 125

Foreword

Foreword from Fii and CCAF

The technologies reshaping finance do not respect regulatory boundaries. Open finance, AI-driven credit, digital identity and instant payments each sit across several mandates at once, from financial stability and conduct to competition, telecommunications and data protection. Increasingly, the quality of regulation depends on the strength of the bridges between authorities. Among the most consequential is the bridge between financial authorities and data protection authorities. As emerging markets rapidly adopt digital financial services, the data powering them increasingly fall under both.

Where these authorities work together, each brings capacity the other lacks, and coordination reinforces both mandates. Where they do not, risks and harms can propagate: fraud victims may not know where to turn, firms face burdensome uncertainty, and digital public infrastructure can fall short of its promise. Yet how these institutions coordinate in practice has received little sustained, systematic examination, especially with respect to emerging markets.

To address this gap, Financial Innovation for Impact (Fii), together with the Cambridge Centre for Alternative Finance (CCAF) at the University of Cambridge Judge Business School and with the support of the Gates Foundation, has produced Joined-Up Regulation: Coordination Between Data Protection and Financial Authorities in Emerging Markets. It examines ten emerging markets and developing economies (EMDEs): Brazil, Ethiopia, India, Indonesia, Kenya, Nigeria, Pakistan, the Philippines, South Africa and Uganda. It does so across five thematic areas: fraud prevention, open finance, AI in credit underwriting, cross-border data flows, and digital identity and KYC. It draws on desk research, interviews, cross-regulatory workshops, and review by experts and stakeholders.

We find that statutory frameworks broadly permit these authorities to cooperate, and in some countries require it, although specific legal gateways for sharing information still matter. What is missing are working, systematic channels; instead, collaboration is too often ad hoc, fragmentary, and fleeting. While there is no one-size-fits-all model, we observe that coordination takes firmest root when cultivated to address shared problems, with fraud the most consistent catalyst, and that effective, productive collaboration can blossom quickly once authorities convene around a problem and a forum.

The costs of the gap are concrete. Data protection authorities are largely absent from the committees and networks where financial coordination happens, leaving firms to navigate uncertainty and consumers to fall between mandates. And where no data protection authority is yet operating, or no handover between authorities has been agreed, protection can stop at the edge of the financial regulator's perimeter, just as data increasingly moves beyond it.

The report also develops a model Regulatory Coordination Index (RCI), with illustrative and provisional country results. We envision this tool as the starting point of a systematic, cross-jurisdictional effort to treat coordination as something worth measuring. Measurement lets authorities see where they stand, track progress over time and learn from peers, turning coordination from a matter of goodwill into a practice of good governance. That is a critical step towards making joined-up regulation an essential part of how policymakers approach their mandates and challenges. We hope this report helps authorities build these bridges by design, rather than discover their absence after harm has occurred.

We thank the Gates Foundation, in particular Aneth Kasebele and Ariadne Plaitakis, for their support, and the many authorities, institutions and reviewers who gave their time and insight.

Bryan Zhang

Co-Founder and Executive Director, Cambridge Centre for Alternative Finance

Co-Founder & Executive Chair, Financial Innovation for Impact

Pavle Avramovic

Director of Research and Policy, Financial Innovation for Impact

Foreword from Douglas W. Arner

Until recently, financial regulation and data protection developed as separate fields. They rested on different principles, were run by different institutions and belonged to different international networks. Today, however, digitisation has bound them together. When finance runs on data, decisions about data are financial decisions, and the governance of financial data becomes a problem no authority can solve alone.

Much of the legal scholarship on this intersection has asked whether the rules conflict: customer due diligence against data minimisation, record-keeping against erasure, localisation against cross-border flows. Those tensions are real. But the evidence in this report, drawn from ten EMDEs, points elsewhere. In most of the countries studied, rules can be made workable and interoperable. The harder question is not whether the rules collide but whether the institutions ever meet: the authorities responsible for data protection and those responsible for the financial system have few systematic channels for working together. That distinction matters for reform. An institutional gap cannot be closed by drafting alone. It needs deliberate design of how authorities consult, refer, share information and act jointly, adapted to each country's institutional setting.

The international dimension makes this more pressing. EMDEs are developing and deploying digital identity systems, fast payment rails and open finance frameworks at speed. Their data protection authorities are, in most cases, recent creations: in the focus countries the typical data protection authority is around five years old, against around seventy for the typical central bank. The global bodies through which financial authorities coordinate were largely built before these authorities existed.

There are signs of change at both national and international level, and a broad appetite among stakeholders for more and better regulatory collaboration. The open question is whether effective coordination becomes standard practice while national and international frameworks are still being designed, or must be retrofitted later, at greater cost and after years of squandered opportunity.

For scholars, the report shifts the debate from colliding rules to the design of institutions. It documents how coordination works, and where it fails, across a diverse set of jurisdictions, and its Regulatory Coordination Index offers something this literature has largely lacked: a common yardstick for institutional practice across borders. The research agenda that follows, on which designs work, under what conditions and at what cost, deserves sustained attention. I hope policymakers and scholars alike will read it as a basis for financial data governance that is coherent, trusted and fit for an increasingly data-driven financial system.

Douglas W. Arner

Sir Roy Goode Chair, Centre for Commercial Law Studies

Kerry Holdings Professor in Law, University of Hong Kong

Associate Director – Research Programmes, Cambridge Centre for Alternative Finance

Foreword from Aneth Kasebele

By now, the word "digital" has become all but redundant in discussing "digital financial services". Consumers globally are predominantly banking, paying, and borrowing with their phones, including and especially in developing countries. Four-fifths of the world now has a core financial account, whether with a traditional provider or a digital innovator, a figure that sat at one-half just fifteen years ago.[1] This progress is worth recognising. It also gives us a strong foundation to build on as we work towards financial systems that support livelihoods, reduce poverty and create opportunities for people who have historically been excluded.

But this engine of inclusion has an essential source of fuel, without which progress could stall, even threatening already achieved gains: trust. For consumers to adopt and productively use digital financial services, they must be able to trust providers to have their mutual best interests in mind, and governments to defend their rights and ensure fair and transparent conduct. Providers and governments also rely on trust, the former to invest in competition- and growth-enhancing offerings, the latter to develop and implement regulatory frameworks that achieve core goals of consumer protection, innovation, and sustainable growth.

We stand at an inflection point for trust in digital financial services. Many countries have implemented national data protection schemes with regulators empowered to enforce them, or are in the process of doing so. This is a vital step in building the regulatory layer essential to tackling the new global challenges of digital technology, including and especially in digital finance. But this creates a new layer of challenge for trust—between regulators, between government and markets, and between government and consumers, even as accelerating innovations in data movement, money movement, and artificial intelligence engender great positive potential as well as serious looming risks. To take just one example, what regulators and stakeholders do today may determine whether AI in credit underwriting supercharges a new wave of fair, transparent, and inclusive credit for the previously excluded and underserved—or the erosion of privacy and dignity and a burgeoning of surveillance, opacity, and discrimination.

1. World Bank, "Global Findex 2025"

This report sets that stage in detail, and accounts forthrightly for both the potential and the risks. It concludes on a note of optimism that I share. Across most of the national and international landscape, most of the components necessary for good governance of a rapidly evolving financial-technology nexus are in place. The needed laws, institutions, and people are largely in place, and stakeholders largely agree on what needs to be accomplished; what is needed is a roadmap of how to do it, and the capacity and energy to act on it. This report lays out the key steps to building lasting, effective regulatory bridges that ensure joined-up regulation furthers competition, innovation, and inclusive growth.

The findings point to several areas for further consideration at the national and international levels, including knowledge sharing, systematic convening and partnership, and meaningful measurement of efforts and outcomes. They can help inform future discussions on where targeted support may be most effective in advancing financial inclusion, competition, innovation, and sustainable growth.

Aneth Kasebele

Senior Program Officer – Payments Regulation, Inclusive Financial Systems

Acknowledgements

Research team

Cambridge Centre for Alternative Finance (CCAF)

Yue Wu, Data Scientist

Abdulrahman Adebayo, Johanan Awah, Csaba Dosa, Shibhangi Ghose, Mark Farrell, Caroline Macharia, Milicent Malau, Tony Oche, Research Interns

Financial Innovation for Impact (Fii)

Pavle Avramovic, Director of Research & Policy
Max Bentovim, Data Protection Lead
Tanya Ghuman, Research Associate
Sarah Ombija, Senior Research Associate

Dr Michelle Frasher, PhD, CAMS and Steve Wood, Director and Founder, PrivacyX Consulting and former UK Deputy Information Commissioner, also contributed to the underlying research and informed its conceptual framing and foundations.

Reviewers

Vivienne Artz, Eric Duflos (CGAP), Dr Michelle Frasher, PhD, CAMS, Ivo Jeník (CGAP), Sanya Juneja (Fii), Aneth Kasebele (The Gates Foundation), Prof. Louis de Koker (La Trobe Law School), David Medine, Brooke Patterson (The Gates Foundation), Ariadne Plaitakis (The Gates Foundation), Steve Wood, Director and Founder, PrivacyX Consulting and former UK Deputy Information Commissioner

Other individuals reviewed drafts of this report in whole or in part and provided feedback but asked not to be named individually or institutionally; we acknowledge them anonymously and express our gratitude for their contributions as well.

Acknowledgements and disclaimer

This report was prepared by Financial Innovation for Impact (Fii) and the Cambridge Centre for Alternative Finance (CCAF), with funding from the Gates Foundation.

The authors are grateful to the officials of data protection and financial-sector authorities, international bodies, firms and civil society organisations who gave their time to interviews, the Cross-Regulatory workshop held in Kigali, Rwanda, the June 2026 regulators' roundtable and the July 2026 stakeholder workshop. In keeping with the Chatham House Rule, they are not named.

Artificial intelligence (AI) tools were used to support selected aspects of the research and preparation of this publication, including the organisation and analysis of interview material, generation of summaries, and drafting, editing and refinement of text. These tools served a supporting role within a research process led by the research team. The research design, substantive interpretation of the evidence, development of key insights, and formulation of the findings and conclusions were informed by the team's expertise, professional judgement and direct engagement with the research. All AI-assisted outputs were critically reviewed, verified and refined by the team, which retains responsibility for the accuracy, integrity and final content of this publication.

We are grateful to Mike Green for designing the report and Jo Barr for proofreading it. The research team also thanks David Allen, Clare Bannister, Vinish Bhuva, Jack Elliott, Jaimie Mingming, and Katherine Selby for their support.

Full responsibility for the content, and for any errors, rests with the authors. The views expressed do not necessarily reflect those of reviewers and informants, or their institutions.

Executive summary

The problem

Financial markets in emerging markets and developing economies (EMDEs) are changing rapidly. Digital financial services, including mobile money, digital credit and instant payment systems have proliferated, extending financial access to many people previously excluded. Digital finance depends heavily on collecting, transmitting and using personal data at scale, which supports inclusion but raises new regulatory concerns. This is bringing together two domains that have largely developed through distinct institutional structures: financial services regulation and data protection. How financial data are acquired, shared, secured, used, retained and governed is now a central question for both.

This raises a central question: how well do the regulators responsible for these respective domains work together? Where they cooperate well, the benefits can be considerable: safer and more inclusive digital financial services, clearer expectations for market participants and stronger defences against fraud and financial crime. Where cooperation is limited, risks to consumers, markets and societies grow, and fall hardest on the most vulnerable. Given the speed at which digital finance continues to expand, and the sensitivity of the data on which it depends, it is timely to examine how regulatory coordination works and how it might be strengthened.

This report assesses the state of cooperation, coordination, harmonisation and integration[2] between data protection (DP) and financial services (FS) regulators in ten EMDEs[3] ('the focus countries'), with an emphasis on five 'thematic areas'.[4] The report also examines regional and global initiatives that aim, or could help, to improve DP–FS coordination more generally.

The report distinguishes two problems that are easily conflated. The first is overlap: as financial services have become data-intensive, the two regimes bear on the same activities and often on the same records. Overlap is structural and generates unavoidable questions, such as what may be collected for due diligence and for how long, or which authority answers when an automated credit decision goes wrong. The second is the coordination gap: in practice, those questions largely go unanswered, because no forum exists in which to ask them, no authority is obliged to ask them, or the authority that should have asked was brought in after the answer had been settled. Where overlap produces requirements that genuinely cannot both be met, the remedy may need to be legislative. But the coordination gap is the more common problem, and its remedy lies mostly within the authorities' own reach.

2. Rather than repeat all four of these overlapping but distinct terms for DP–FS interaction, the report uses "coordination" throughout to cover all four.
3. The focus countries are Brazil, Ethiopia, India, Indonesia, Kenya, Nigeria, Pakistan, the Philippines, South Africa and Uganda.
4. The five thematic areas are: (1) digital identity, KYC and AML/CFT, (2) fraud, (3) open finance, including open banking, (4) credit underwriting and AI, and (5) cross-border data flows and localisation (Section 2.4).

Key findings

Coordination is growing, but it is improvised. DP–FS coordination has not kept pace with the rise of digital financial services in consumer markets. Questions of data protection are becoming central to financial regulation, while the sensitivity and value of financial data lend it particular significance for data protection authorities. Closer coordination could bring substantial gains: faster and better-designed deployment of digital public infrastructure (DPI), efficiencies for regulators and market participants from greater clarity and certainty, and reduced fraud alongside strengthened **anti-money laundering and countering the financing of terrorism (AML/CFT)** efforts. These gains benefit consumers, responsible market participants and, ultimately, inclusive economic growth. Yet cooperation between the two sets of regulators is usually ad hoc, reactive and limited in effect, where it happens at all.

The gap is institutional rather than legal. Where a data protection statute and an operational authority both exist, the coordination gaps this research found are mostly institutional rather than legal: regulators generally have the power to consult one another and to cooperate. The power to disclose is narrower. Confidentiality duties on supervisory information, the absence of a gateway for sharing personal data between authorities, or a specific conflicting obligation can require legal change, and a memorandum of understanding (MoU) can only implement powers the law already provides; it cannot create them. Half of the focus countries have data protection statutes that either direct the authority to coordinate or collaborate with other regulators (Brazil, Nigeria and the Philippines) or make explicit provision for delegation or sectoral codes (Kenya and South Africa).[5] Nor do DP and FS regulators generally resist coordination: at both institutional and individual level, most say they would value closer engagement with other domestic regulators and with counterparts abroad.

5. For details, see each focus country's individual profile at Annex A. The provisions are: Brazil, Lei Geral de Proteção de Dados Pessoais (Law No. 13,709/2018), art. 55-J(XXIII) and secs. 3–4 (the ANPD and sector regulators must coordinate their activities, and the ANPD must maintain a permanent forum with them); Nigeria, Nigeria Data Protection Act, 2023, sec. 5(h) (the Commission "shall… collaborate with any relevant ministry, department, agency…"); the Philippines, Data Privacy Act of 2012, sec. 7(f) (among the Commission's functions, to "coordinate with other government agencies…"); Kenya, Data Protection Act, 2019, sec. 10 (delegation of powers to a regulator established by an Act of Parliament); South Africa, Protection of Personal Information Act 4 of 2013, ch. 7 (secs. 60–68). Indonesia's Law 27 of 2022 contains no duty to coordinate with sectoral regulators. Its implementing regulation, Government Regulation 33 of 2026 (in force from 16 January 2027), requires a ministry or agency that designates additional categories of specific personal data to coordinate with the data protection authority (art. 6(3)). This is an issue-specific link at regulation level rather than a general coordination duty and is not counted here. The same regulation lets the authority give input when sector regulations exempting financial-sector supervision from data-subject rights and controller duties are drafted (arts. 148(3) and 149(3)), and to coordinate with ministries and agencies in supervision and sanctions (arts. 180(3) and 184(5)). These provisions are permissive, sit at regulation level and depend on an authority not yet established; they are not counted either. Uganda's Data Protection and Privacy Act, Cap. 97, contains no express coordination duty, although regulation 44 of the 2021 Regulations lets the PDPO seek the assistance of any person or authority in an investigation. The Data Protection and Privacy Regulations 2021 require the Personal Data Protection Office to cooperate with government ministries, departments and agencies, and require them to assist it (reg. 6). Separately, the National Payment Systems Act 2020 requires the Bank of Uganda to "cooperate with Government agencies whose functions are relevant to payment systems" (sec. 71(1)). Ethiopia's Personal Data Protection Proclamation 1321/2024 requires every person, including the National Bank of Ethiopia, to cooperate with the Ethiopian Communications Authority (art. 66); the duty runs one way only and is not counted. South Africa's POPIA also provides for consultation on the referral of complaints that fall within another regulator's remit (sec. 78); this is complaint-specific and is not counted separately, since South Africa is counted for its sectoral codes. Draft provisions, such as those in Pakistan's Personal Data Protection Bill, are not counted.

The constraint is capacity and asymmetry, not willingness. It lies mainly in capacity gaps, asymmetries in expertise, and the relative absence of roadmaps, leadership, and shared working tools such as common taxonomies, referral protocols and model agreements. This is encouraging, because these obstacles can be addressed. Stakeholders expect the coordination they want to deliver benefits that exceed its costs. The evidence gathered for this report is consistent with that expectation, and the report sets out methods that would help regulators and others build better evidence going forward.

Where there is no operating data protection authority, there is a window to build coordination in. A major caveat is whether a data protection regulator exists at all. At the report's 30 September 2026 cut-off, three of the ten focus countries lacked a confirmed, fully operational dedicated authority: India and Indonesia were still standing up data protection regulators provided for in law, and Pakistan had no comprehensive data protection statute. For now, this limits what coordination can achieve in those countries, but it also gives them an opportunity to build coordination in from the start.[6]

Five impediments reinforce one another. Five factors explain why coordination falls short (Section 7.1): capacity constraints and asymmetries between authorities; under-prioritisation in goal-setting, since coordination is almost never a measure against which either authority is judged; under-prioritisation in workstreams, so that the data protection authority arrives after the main design decisions; silos and institutional culture; and the absence of shared frameworks, such as common taxonomies and procedures. They reinforce one another in an 'anti-flywheel' that sustains the coordination gap. Coordination attempted without adequate preparation disappoints, and disappointment teaches both authorities to invest less next time.

The impediments play out in three patterns. In co-active jurisdictions (Brazil, Nigeria, the Philippines and South Africa), two active authorities address overlapping issues through separate channels, and the priority is alignment and de-confliction. In uneven jurisdictions (Kenya and Uganda), the financial regulator leads policy in areas of overlap and data protection input is occasional or case-by-case; the priority is to make it systematic. In emergent jurisdictions (Ethiopia, India, Indonesia and Pakistan), the data protection architecture is still forming, which creates uncertainty but also the chance to build coordination in from the start.

The data protection authority usually arrives late, and the international architecture reproduces the gap. Financial-sector frameworks for open finance, fraud and AML/CFT were typically designed before the data protection authority was involved; internationally, financial standard-setters assess while data protection bodies convene, and the early bridges between them are mostly convened from the financial side.

6. In a fourth, Ethiopia, the data protection function has been assigned to an existing regulator, the Ethiopian Communications Authority (ECA), which is now an operating authority with a young data protection mandate; the remaining six focus countries have dedicated data protection regulators.

Across the five thematic areas, the findings can be summarised briefly.

1. **Digital identity, know your customer (KYC) and AML/CFT**. The two regimes govern the same identity and transaction records. In Nigeria, an AML-driven data requirement reached the courts after the two authorities disagreed publicly, with no forum identified in which they could settle it; in India, a comparable mandate was decided in the courts when there was no data protection authority at all.
2. **Fraud**. Financial authorities, financial intelligence units and law enforcement coordinate more with one another than any of them does with the data protection authority, which is rarely present where fraud controls decide what happens to people's data.
3. **Open finance**. Frameworks were often designed before a data protection counterpart could weigh in, so reconciliation happens after launch, and protection can stop where the financial regulator's perimeter does.
4. **Credit underwriting and AI**. Data protection rules on profiling and automated decisions often apply before financial-sector expectations on AI exist, reversing the usual sequence; the vendors that supply data and models sit between the two regulators.
5. **Cross-border data flows and localisation**. Four distinct obligations (transfer permission, local storage, supervisory access, and information that must travel with payments) come from different authorities and are rarely reconciled before they reach firms.

A single example shows what is at stake. In Kenya, digital lenders that required access to borrowers' phone contacts and then messaged those contacts on default engaged three authorities: the data protection authority, which can fine a lender but cannot revoke its licence; the Central Bank, which licenses lenders but publishes no enforcement data on collection conduct; and the competition authority, which handles consumer complaints. Each holds part of the remedy (Box 2).



Recommendations

The report makes seven recommendations (Section 8). They are parallel workstreams rather than a sequence, and most can begin under powers the authorities already hold.

1. **Start with one shared problem and make the result visible**. Agree an anchor problem, such as fraud-data sharing, credit underwriting or open finance, and a joint lead in each authority within a quarter, and deliver a first output within a year.
2. **Designate counterparts and referral routes**. Name contact points within a quarter, audit existing instruments within six months, and adopt a referral protocol that says which authority answers the consumer.
3. **Bring the data protection authority in at the design stage**. Identify the frameworks now being designed, such as open finance, digital identity and payment-system reforms, and secure a data protection role in each.
4. **Develop joint guidance**. Make a joint guidance note on the anchor problem the first deliverable, adapting existing templates.
5. **Build each authority's understanding of the other's domain**. Complete one attachment in each direction and one joint scenario exercise within a year.
6. **Measure and report on coordination**. Name a senior sponsor in each authority, put one coordination objective in each annual plan, and record baseline indicators.
7. **Connect national coordination to regional and international standard-setting**. Submit a coordinated national position to the next relevant international consultation.

Coordination has costs and risks of its own: staff time, governance overhead, slower decisions, blurred accountability and, where capacity is unequal, drift towards the stronger authority's priorities. The recommendations therefore begin with lightweight, reversible measures, leave each authority's statutory decisions with that authority, and judge each mechanism by whether it operates rather than whether it exists.

Trust recurs throughout the research. Consumers need to trust that their data will be handled fairly and that someone will act when it is not; firms need to trust that the rules they must follow are coherent; and each authority needs to trust that its counterpart will consult before acting rather than after. Coordination directly builds the third kind of trust, and through it supports the first two.

Chapter 1

Introduction



1.1 About the programme

This report is the main output of a research and engagement programme on data protection and financial regulation, led by Financial Innovation for Impact (Fii) and the Cambridge Centre for Alternative Finance (CCAF) at Cambridge Judge Business School, and funded by the Gates Foundation. The programme examines how data protection authorities and financial-sector authorities in emerging markets and developing economies work together, why they often do not, and what would help.

Alongside this report, the programme has produced country case studies for each of the ten focus countries, a mapping of regional and global initiatives and a quantification framework, and has convened regulators and other stakeholders: a cross-regulatory workshop in Kigali in March 2026, a regulator-only roundtable in June 2026, an all-stakeholder virtual workshop in July 2026 and a public webinar in September 2026.

1.2 Audience

This report is written first for policymakers: data protection authorities and financial-sector authorities (central banks, conduct and prudential supervisors, payments regulators and financial intelligence units) in EMDEs, and the ministries that shape their mandates. It is also intended for the standard-setters, development partners and industry bodies that work with them, and for all those interested in better governance of digital financial services. Its aim is to help them decide where and how authorities should coordinate. The report's central argument is that, where two authorities govern the same data-intensive activity without a way of settling how their rules apply together, firms face uncertain and sometimes inconsistent expectations, and some risks fall between the two mandates. Uncertainty raises compliance costs, which weigh most on smaller and newer providers and can deter them from entering. Risks that fall between mandates reach consumers as harms without a clear route to redress and fall hardest on low-income consumers and marginalised groups with the fewest alternatives. Coordination that settles these questions earlier should therefore improve consumer protection, lower barriers to entry, support inclusion, and help integrity controls work without unnecessary data exposure. The research supports the links in this chain to different degrees, but broadly supports the argument as a whole.

1.3 Research approach

This report focuses on ten EMDEs: Brazil, Ethiopia, India, Indonesia, Kenya, Nigeria, Pakistan, the Philippines, South Africa and Uganda. These countries were selected to give a view across three dimensions. The first is geographical, with representation from western, eastern, and southern Africa, South and Southeast Asia, and Latin America. The second is the maturity of the data protection framework, ranging from jurisdictions with relatively established authorities and a developed body of practice to those whose statutes are recent, or that do not yet have an operational data protection regulator. This spread allows the report to examine coordination at different stages of institutional development. The third is relevance to the thematic areas set out in Section 2.4, so that each theme is live in more than one jurisdiction and comparison becomes possible. Size also mattered: the focus countries include five of the world's ten most populous countries and collectively represent about a third of the world's population.

The research also concentrates on the five thematic areas set out in Section 2.4. These five areas sit at the intersection of the two regulatory mandates; each is a question of significance in most of the focus countries; and together they span the customer lifecycle, different business processes and units, and different aspects of the regulatory process, allowing the analysis to examine coordination across multiple points where the two regimes meet. They also combine problems to be mitigated, such as fraud, with opportunities to be developed, such as open finance, where the aim is to improve competition and innovation.

Finally, the research takes in regional and global initiatives that aim, or could help, to improve DP–FS coordination more generally. In assessing these, the report pays particular attention to those that do or could involve some or all of the focus countries or thematic areas, while also considering broader initiatives that could strengthen DP–FS coordination.

Methodology

The evidence base for this report has four components.

The first is 27 semi-structured interviews with 27 individuals, held between late 2025 and April 2026: nine with data protection authorities or the bodies holding that remit, eight with financial-sector authorities, three with international and regional bodies, four with non-profit and civil-society organisations, and one each with industry, academia and an independent expert. They covered eight of the ten focus countries and two comparator jurisdictions. Interviews followed a common protocol, available on request, with follow-up questions tailored to each interviewee's institutional position and to the answers provided.

Interview transcripts were analysed thematically against the five thematic areas and the coordination framework set out in Section 2.3. AI tools were used to assist with transcription and summarisation; all AI-assisted outputs were reviewed and verified by the research team against the source material. The interview findings informed the country case studies, the identification of coordination mechanisms in Section 3 and the diagnosis in Section 7.

The second is a set of convenings: an in-person cross-regulatory workshop in Kigali in March 2026, bringing together data protection and financial authorities, industry and development partners; a virtual regulator-only roundtable in June 2026, with 22 participants from 13 organisations, including data protection and financial authorities from several focus countries; a virtual all-stakeholder workshop in July 2026; and a public webinar in September 2026. Box 12 summarises what was heard.

The third is a quantification exercise, modelling the costs of fragmentation and the gains from improved coordination across the five thematic areas, the method and results of which are set out in Annex C.

The fourth is desk research, covering legal and regulatory instruments, supervisory publications, and secondary literature, together with a mapping of regional and global initiatives presented in Annex B, and country case studies for each of the ten focus countries presented in Annex A. The examples of coordination in Section 3 were identified through the interviews and convenings and through a review of public sources: legislation, regulators' published instruments, guidance, annual reports and press releases, and secondary literature, covering the ten focus countries and selected comparators up to 30 September 2026, the report's cut-off date. That search was purposive; the examples illustrate coordination in each country.

All roundtable and workshop material is reported under the Chatham House Rule, and other evidence gathered from non-public sources is presented in a way that protects the privacy and anonymity of those sources.



1.4 Limitations

The findings should be read in light of four main limitations.

First, the research prioritises breadth over depth. It examines a broad and evolving regulatory question across ten jurisdictions and five thematic areas, and the strength and depth of the available evidence vary between countries and topics. The findings are therefore intended to surface recurring patterns, emerging themes, and illustrative examples across the focus countries, rather than to suggest that every finding applies equally across all EMDEs. Country-specific institutional and regulatory context remains relevant when interpreting the analysis and recommendations.

Second, much of the qualitative evidence rests on stakeholder accounts gathered through interviews, roundtables, and workshops. These perspectives offer valuable insight into how coordination works in practice, including aspects that may not be visible in legislation or public documents, though they may also reflect differing institutional experiences and interpretations. Where possible, stakeholder evidence has therefore been weighed alongside legislation, regulatory and supervisory publications, desk research, and evidence from other participants. The absence of publicly documented coordination should likewise not be taken to mean that informal cooperation does not occur; more generally, where the report notes an absence of evidence in the record, absence of evidence should not be read as evidence of absence.

Third, the report captures a regulatory landscape that is changing quickly. During the research period, several focus countries were establishing or strengthening data protection institutions, implementing new legislation, developing open finance frameworks, or weighing new approaches to AI, digital lending, and cross-border data governance. Some of the arrangements and initiatives described here may therefore continue to evolve beyond the research period. Where relevant, the analysis distinguishes between measures already in force and those that remained proposed, transitional, or under development. Unless otherwise indicated, it reflects information available at 30 September 2026, the report's cut-off date; later developments are noted only where they would materially change a finding. Limitations specific to the quantitative analysis, including those relating to data availability, assumptions, and the interpretation of modelled estimates, are discussed separately in Section 5.5 and Annex C.

Fourth, the field itself is new. DP–FS coordination has received little systematic study, especially in EMDEs: there are few prior datasets, no established measurement framework and little evaluation of what works. Many of the mechanisms described here are recent, and their effects cannot yet be observed. The report therefore distinguishes documented mechanisms from reported practice and missing evidence from proven absence, and treats its quantitative results as illustrative (Section 5.5).

1.5 Report structure

The report is organised as follows. Section 1 sets out the programme, the audience, the research approach and its limitations. Section 2 explains why joined-up regulation matters, defines what the report means by coordination, introduces the five thematic areas and describes the regulatory landscape. Section 3 maps where coordination is already happening, at the international, regional and national levels. Section 4 examines the gaps across the five thematic areas. Section 5 sets out a framework for measuring coordination, the Regulatory Coordination Index, and for sizing what is at stake, and illustrates both. Section 6 draws together the key findings. Section 7 diagnoses why coordination falls short, setting out five impediments and three patterns in how they play out across the focus countries. Section 8 makes seven recommendations, and Section 9 concludes.

The report also has four annexes and an appendix. Annex A consists of ten case studies analysing the state of DP–FS coordination in each of the ten focus countries. Annex B sets out the findings on regional and global initiatives in full. Annex C explains the methodology and results of the quantitative analysis in more detail. Annexes A to C are provided as separate documents. Annex D is a glossary of key terms and abbreviations used in the report and other annexes. The Appendix sets out the detailed country evidence tables summarised in Section 4.

The report examines five thematic areas, described in Section 2.4: (1) digital identity, KYC and AML/CFT, meaning digital identification (digital ID) and Know Your Customer (KYC) processes and the anti-money laundering and countering the financing of terrorism (AML/CFT) obligations they serve; (2) fraud; (3) open finance, including open banking (OBOF); (4) credit underwriting and the use of artificial intelligence (AI); and (5) cross-border data flows and localisation.

To help close the measurement gap described in Section 2.2, this report proposes a framework, the Regulatory Coordination Index (RCI), for measuring how much coordination exists and for sizing the costs and potential benefits associated with fragmentation that improved coordination might affect. By linking regulatory fragmentation to observable outcomes, the framework can help regulators identify where the most significant costs, harms, and missed opportunities arise; establish a baseline against which improvements in coordination can be assessed over time; support the prioritisation of interventions; and offer authorities and market participants a shared, evidence-based language for weighing trade-offs. The framework does not aim to capture every channel through which coordination may generate value, but to provide a method and an initial evidence base that can be applied and expanded as better data and additional outcome measures become available. Section 5 sets out the framework, and Annex C the full method.

The report is organised as follows. Section 1 sets out the programme, the audience, the research approach and its limitations. Section 2 explains why joined-up regulation matters, defines what the report means by coordination, introduces the five thematic areas and describes the regulatory landscape. Section 3 maps where coordination is already happening, at the international, regional and national levels. Section 4 examines the gaps across the five thematic areas. Section 5 sets out a framework for measuring coordination, the Regulatory Coordination Index, and for sizing what is at stake, and illustrates both. Section 6 draws together the key findings. Section 7 diagnoses why coordination falls short, setting out five impediments and three patterns in how they play out across the focus countries. Section 8 makes seven recommendations, and Section 9 concludes.

The report also has four annexes and an appendix. Annex A consists of ten case studies analysing the state of DP–FS coordination in each of the ten focus countries. Annex B sets out the findings on regional and global initiatives in full. Annex C explains the methodology and results of the quantitative analysis in more detail. Annexes A to C are provided as separate documents. Annex D is a glossary of key terms and abbreviations used in the report and other annexes. The Appendix sets out the detailed country evidence tables summarised in Section 4.

The report examines five thematic areas, described in Section 2.4: (1) digital identity, KYC and AML/CFT, meaning digital identification (digital ID) and Know Your Customer (KYC) processes and the anti-money laundering and countering the financing of terrorism (AML/CFT) obligations they serve; (2) fraud; (3) open finance, including open banking (OBOF); (4) credit underwriting and the use of artificial intelligence (AI); and (5) cross-border data flows and localisation.

To help close the measurement gap described in Section 2.2, this report proposes a framework, the Regulatory Coordination Index (RCI), for measuring how much coordination exists and for sizing the costs and potential benefits associated with fragmentation that improved coordination might affect. By linking regulatory fragmentation to observable outcomes, the framework can help regulators identify where the most significant costs, harms, and missed opportunities arise; establish a baseline against which improvements in coordination can be assessed over time; support the prioritisation of interventions; and offer authorities and market participants a shared, evidence-based language for weighing trade-offs. The framework does not aim to capture every channel through which coordination may generate value, but to provide a method and an initial evidence base that can be applied and expanded as better data and additional outcome measures become available. Section 5 sets out the framework, and Annex C the full method.



Chapter 2

Why joined-up regulation matters



2.1 Background and context

Finance has run on data for decades: credit bureaus, card networks, interbank messaging and core banking systems all predate the smartphone. Digital financial services nonetheless change more than the channel through which a product is marketed, delivered or serviced. Finance is now integrated far more deeply into daily life, so that paying, borrowing and saving now generate records of ordinary activity. The data are far more granular, extending from balances and repayments to device signals, location, contacts and behaviour. And the range of actors handling them has widened well beyond regulated institutions, to payment operators, identity providers, aggregators, telecoms companies, cloud services and analytics vendors. These changes, more than digitalisation as such, make the governance of personal data central to financial regulation. A payment initiated on a mobile device, a loan assessed remotely and an account opened through a digital identity system all depend on collecting, transmitting, retaining and using large volumes of data. Data are now central to the design, cost and delivery of nearly every financial product and service.

Data about identity, transactions, behaviour, devices and relationships are increasingly used to determine whether a person may enter the financial system, including which services are available and on what terms. New data sources such as mobile money transaction histories, device information, behavioural signals and social media data complement or substitute for the traditional collateral and credit histories required by legacy financial institutions, opening new credit channels and promising better terms to first-time borrowers and small enterprises. These developments expand access to finance for populations that were previously excluded from the formal system.



Box 1: Data and financial inclusion

Data have been central to the expansion of financial access in the focus countries, and so to the regulatory questions this report examines. Data from the World Bank's Global Findex Database show that, in the ten focus countries of this report, the percentage of the population that owns an account at either a financial institution or a mobile money provider rose from an average of 45.7% in 2014 (the first year for which the database records values for all ten countries) to 66.5% in 2024; five of the ten countries exceeded 80% penetration in 2024, compared to only two countries exceeding 50% in 2011.[7] National surveys in the focus countries support these figures. In Kenya, financial inclusion now reaches an estimated 84.8% of adults and mobile money usage approximately 82%, a transformation widely associated with the growth of mobile money services.[8] India has observed a similar boost through its digital public infrastructure, the Unified Payments Interface, the Aadhaar identity system and associated data-sharing tools, on which retail digital payments are projected to roughly double, to about USD 7 trillion, by fiscal year 2030.[9]

These gains are not only a matter of new channels. Much of the growth came through mobile money and digital onboarding, which became possible because identity could be verified, and creditworthiness assessed, from data rather than from paper documents and branch visits. The data that made these accounts possible are the same data that now need governing.

These services rest on digital technologies, both those in consumers' hands, such as mobile phones, and those firms use to build and run data-driven services. They also involve far more collection, retention, sharing and use of data by the providers of these services and other private and public entities in the digital ecosystem. The gains — and risks — from digital transformation fall on consumers, markets and, ultimately, whole societies.

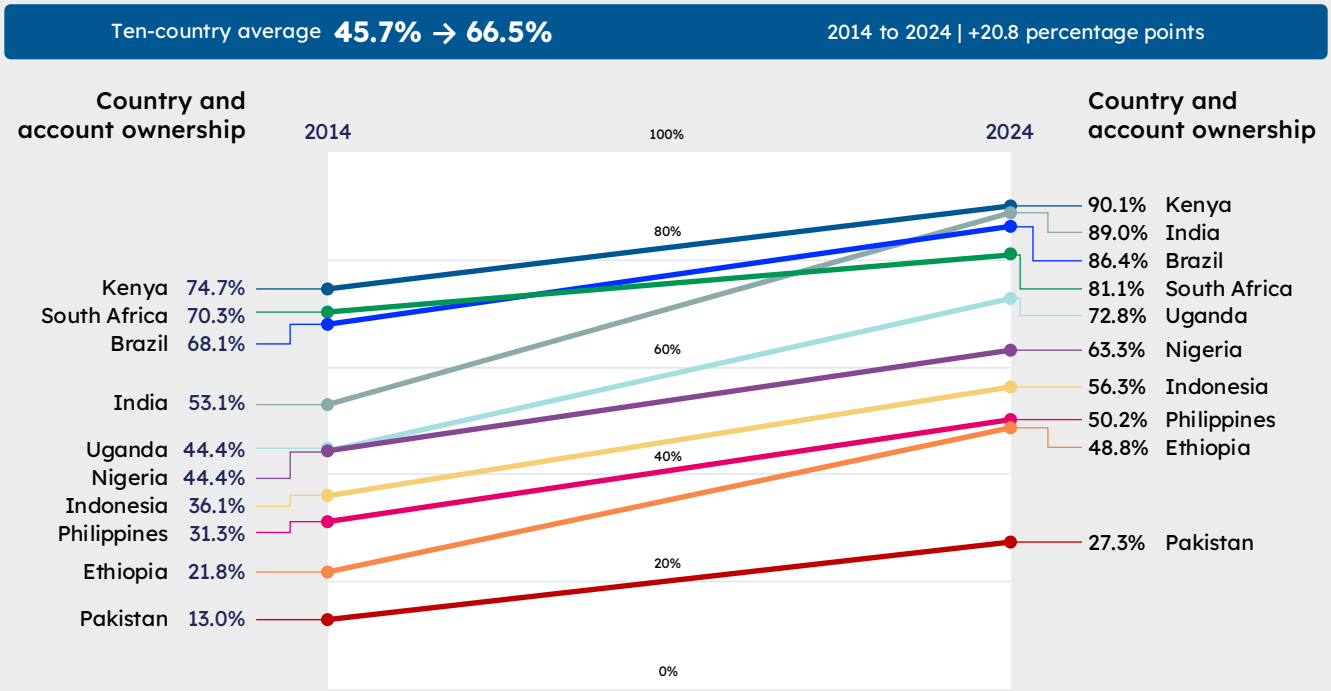
7. World Bank, Global Findex Database 2025, indicator FX.OWN.TOTL.ZS (account ownership at a financial institution or with a mobile-money-service provider, % of population ages 15+), https://data.worldbank.org/indicator/FX.OWN.TOTL.ZS. Averages are simple means across the ten focus countries; Ethiopia was not surveyed in 2011.

8. Central Bank of Kenya, Kenya National Bureau of Statistics, and FSD Kenya, 2024 FinAccess Household Survey (December 2024), https://www.knbs.or.ke/reports/2024-finacess-household-survey-report/, reporting formal financial access of 84.8% of adults and mobile money use of 82.3%. These survey measures differ from the Global Findex account-ownership indicator, which records 90.1% for Kenya in 2024 (World Bank, Global Findex Database 2025).

9. Kearney and Amazon Pay, "How Urban India Pays," July 2024, projecting retail digital payments to grow from USD 3.6 trillion in FY2024 to about USD 7 trillion by FY2030, https://www.kearney.com/industry/financial-services/article/how-urban-india-pays-a-sneak-peek-into-india-s-digital-payment-adoption-behaviors; reported in "India's Retail Digital Payments Set to Double to $7 Trn by 2030: Report," Business Standard, 14 July 2024, https://www.business-standard.com/finance/news/india-s-retail-digital-payments-set-to-double-to-7-billion-by-2030-report-124071400236_1.html. Growth rests on the "India Stack" comprising the Unified Payments Interface, Aadhaar (used for electronic know-your-customer verification) and DigiLocker.

Figure 2.1: Adult account ownership in the ten focus countries, 2014 vs 2024

Adults aged 15+ with an account at a financial institution or mobile money provider



Source: World Bank Global Findex Database, 2025
Average is the unweighted mean of the ten countries. Endpoint positions use unrounded values; labels show one decimal place.

But the data that enable inclusion also concentrate sensitive information in new places and exposes consumers to new categories of harm. Modern financial services are rarely delivered by a single institution. Fintechs, banks and other regulated firms increasingly rely on payment operators, identity providers, data aggregators, telecommunications companies, cloud services, and analytics vendors. As information moves through that wider chain, responsibility and accountability for its handling extend well beyond the perimeter within which financial supervision has traditionally been organised. The benefits of data-driven finance are therefore accompanied by new and greater risks of misuse, breach, inaccurate inference, unfairness, abuse, exclusion and unclear accountability.

Questions about the collection, use and governance of data, especially sensitive personal data, have become central to regulation of the financial sector. Decisions about which information is necessary and proper, who may access it, how it may be combined, how long it should be retained and how an affected person may challenge its use sit at the intersection of financial regulation and data protection, and engage both authorities at once. Their coordination — or lack of coordination — shapes the path of inclusion, competition and financial integrity; it also influences the scope and severity of risks including surveillance, loss of privacy and discrimination. Much of the data at issue are personal data, meaning information relating to an identifiable person, which most directly engages data protection law. The rest of this report uses the narrower term where the distinction matters.

2.2 The case for joined-up regulation

Joined-up regulation matters for reasons that go well beyond any single policy area. When two authorities govern the same data-intensive activity without an agreed way of settling how their rules apply together, costs fall on consumers, firms, markets and the authorities themselves.

For consumers, harms that engage both mandates can fall between them. A borrower harassed through a harvested contact list, or a customer wrongly flagged in a fraud database, may not know which authority to approach, and neither authority may treat the matter as its own (Box 2). For firms, overlapping obligations without an agreed interpretation mean duplicated reporting, divergent expectations and legal uncertainty. The cost of reconciling the two regimes falls on the regulated firm, and weighs most on smaller and newer providers.

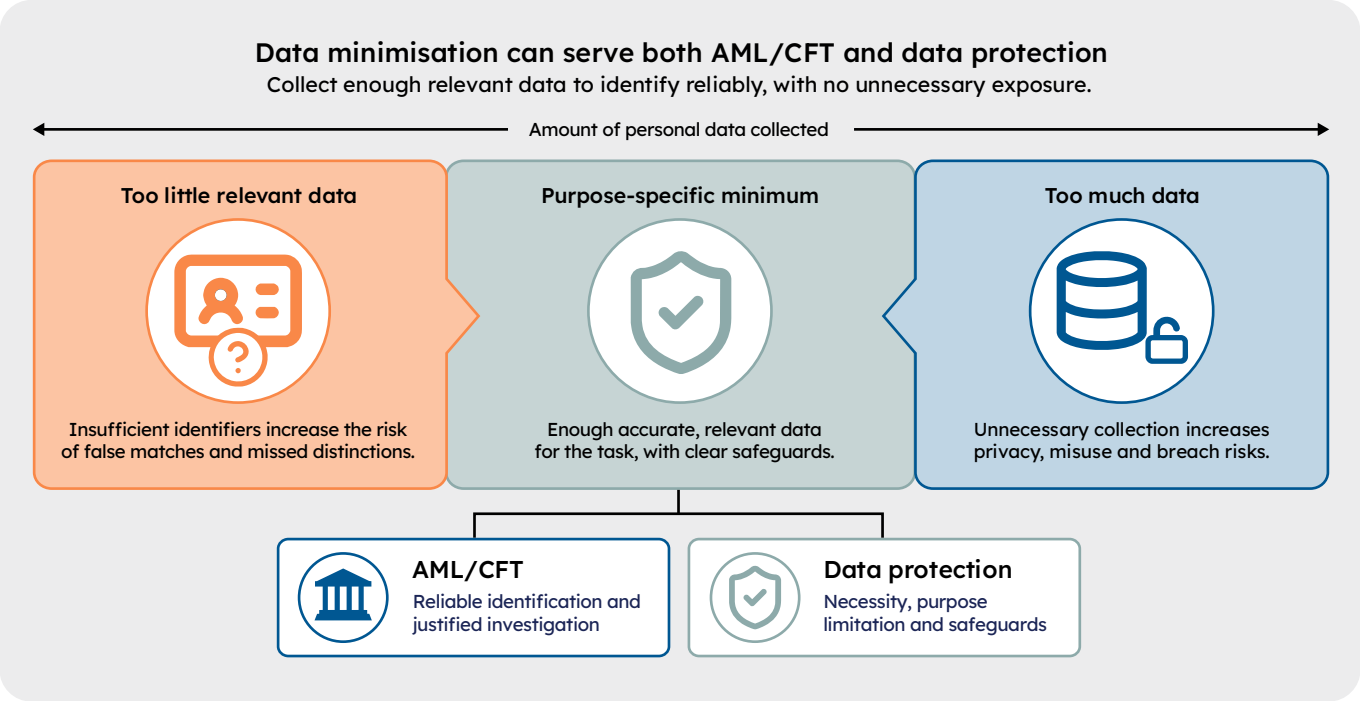
For markets, uncertainty about which rules apply, and whose interpretation prevails, deters entry and innovation. It can also be exploited: firms may structure products or data flows to fall where oversight is weakest, a form of regulatory arbitrage that coordination makes harder. For authorities, uncoordinated action duplicates supervisory effort, produces conflicting decisions and can expose a firm to two sanctions for one act (Box 7).

> "If you're a company that's subject to four different types of regulatory investigations, you may be asking … four very similar, but slightly different questionnaires from those regulators when that could be consolidated and streamlined."

Coordination addresses each of these. Consistent expectations lower compliance costs and reduce duplicated supervision; clear referral routes give consumers a single path to redress; and joint design lets integrity, inclusion and privacy objectives be met together rather than negotiated after the fact. These benefits are not automatic, and coordination carries costs and risks of its own (Section 5.1), but the evidence gathered for this report consistently points in this direction.

Ongoing developments make this case even stronger. AI-enabled services add risks that engage both mandates at once, such as opaque automated decisions, synthetic identities and automated fraud, and increase the need for clear supervisory responsibilities. Both data protection and financial regulation are also evolving quickly, so the interface between them is a continuing task rather than a one-time fix (Section 4.1). The remainder of this section illustrates the point through the case most often cited: AML/CFT.

Figure 2.2: Balancing data collection between AML/CFT and data protection



Conceptual illustration: the appropriate amount depends on purpose, data quality and risk.
Source: CCAF & Fii.

In some cases, data protection and financial regulation are perceived to be in tension. AML/CFT is the clearest example: they require financial institutions to collect, retain and disclose information for defined financial-integrity purposes, while data protection law calls for necessity, purpose limitation and appropriate safeguards with respect to the same information. Yet the overlap need not mean an inherent clash between the two regimes, or conflict between the authorities that implement them. In key respects, the schemes pursue compatible objectives, including consumer protection, data security and accuracy, accountability, fair treatment and trust in the financial system. Difficulty tends to arise when these principles have to be translated into operational requirements for the same activity: what information may be collected, how long it should be kept, when it may be shared, which safeguards apply, and which authority should step in when something goes wrong.

Two features of data protection law deserve particular attention. The first is minimisation, which requires information to be adequate, relevant and limited to what is necessary for a specified purpose. Adequacy is critical: too little information produces inaccurate decisions that harm individuals. Additional identifying attributes may be exactly what is needed to distinguish a customer from someone with the same name on a sanctions list or in a credit report, which serves financial-crime control and data protection at once. The Financial Action Task Force's (FATF) own draft guidance on Recommendation 16 (R.16) makes the same point about date of birth in payment messages.[10]

10. Financial Action Task Force (FATF), Guidance on Implementation of Recommendation 16, public consultation draft (June 2026).

Minimisation is easiest to achieve by design: building necessity, minimisation, access controls and deletion into a system or data-sharing arrangement when it is conceived, rather than adding safeguards once it operates. Privacy-enhancing technologies can help, but they complement a lawful basis and other safeguards rather than replace them.

The second is retention. Recordkeeping duties can, and often do, justify retention. The key questions are which records a duty covers, when the retention period starts, which purposes still apply, and when full or partial deletion or anonymisation is due. The justification for keeping a record is separate from the justification for each later use of it.

Some specific requirements can genuinely raise concerns about conflict. A clear current example is cross-border: under revised Recommendation 16, originator and beneficiary information must accompany cross-border payments, while some data protection laws restrict transfers to countries without adequate protection. The FATF's draft implementation guidance anticipates tensions of this kind: it encourages measures to ensure compatibility between AML/CFT and data protection rules, promotes safeguards and calls for coordination between the authorities concerned (discussed in Section 4.1), and describes financial regulation and data protection as 'mutually reinforcing', supporting the view that conflicts arise in implementation rather than in principle.

These operational challenges are compounded by uneven technical capacity and differences in institutional maturity and resources across data protection and financial-sector authorities. In many jurisdictions where coordination has not been institutionalised, cooperation remains informal, often depending on personal relationships between officials or arising in response to individual incidents.

Better coordination could help address this operational gap. More systematic coordination could enable regulators to convey more consistent expectations to regulated firms, reduce unnecessary duplication in supervision and compliance, create clearer referral and escalation routes, and allow faster information exchange and more coordinated investigations or supervisory responses. Over time, greater regulatory coherence of this kind could give firms more certainty when designing products and compliance systems, while strengthening consumer protection, trust, and the conditions for responsible innovation.



Box 2: One harm, two mandates

A borrower takes out a short-term digital loan. As a condition of disbursement, the lending application requires access to the borrower's mobile contact list. Consent is given because the loan will not otherwise proceed. On default, the lender messages the borrower's contacts, including family members, colleagues and employers, to pressure repayment. From a financial services perspective, the conduct concerns lending practice, consumer protection and the conduct of recovery and collections. From a data protection perspective, it raises the lawfulness of the original collection, purpose limitation and the proportionality of disclosure. It is a single harm that engages two mandates, and the remedy available to the consumer depends on whether a route between the two authorities exists and on whether either treats the matter as its own.

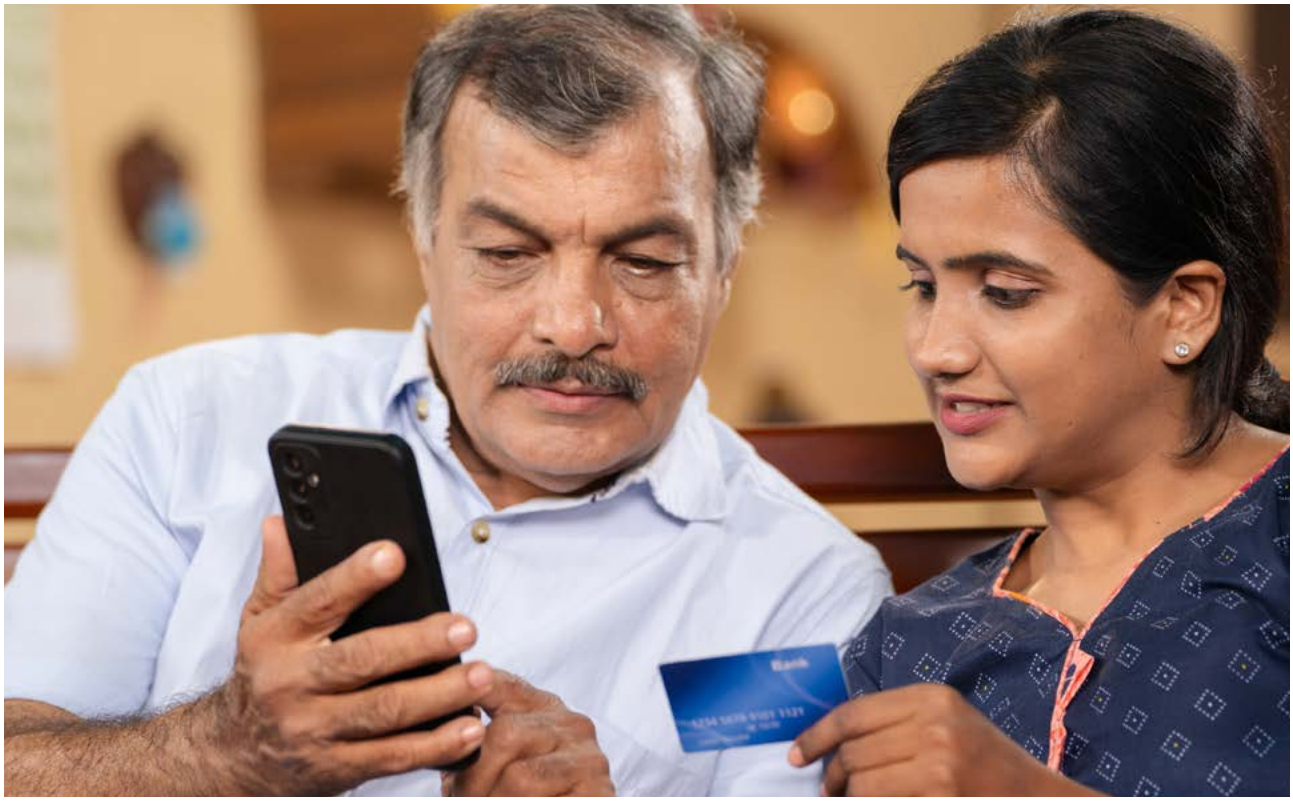
This pattern is documented in Kenya, and similar conduct has been reported in Nigeria (discussed in Section 4.4). In Kenya, the data protection authority was investigating 40 digital lenders[11] and had received 1,030 complaints by September 2022, of which 299 (54% of 555 admitted cases) related to digital lenders. In 2023, Mulla Pride Ltd was fined KES 2.975 million (about USD 20,000) for contacting borrowers' relatives and contacts.[12] By May 2024, the Data Commissioner reported that harassment of borrowers by digital lenders had fallen by around, 75%, crediting the Central Bank's regulation of digital lenders and her Office's engagement with them.[13]

The financial-supervision record is thinner. The Central Bank of Kenya has licensed digital credit providers since March 2022 under regulations that prohibit accessing a borrower's contact list or contacting their acquaintances in the course of debt collection.[14] By 30 September 2026, it had licensed 281 providers from more than 900 applications.[15] It does not publish complaint or enforcement data for these lenders, and we identified no public record of a provider's licence being suspended or revoked for collection conduct. The licence, however, is the one sanction the data protection authority cannot impose: the Data Commissioner can issue enforcement notices and fines of up to KES 5 million or 1% of annual turnover, whichever is lower, but has no power to revoke a lender's licence.[16]

11. "Data Protection Office Probing 40 Digital Lenders over Misuse of Personal Data," Capital FM, 5 October 2022, https://www.capitalfm.co.ke/business/2022/10/data-protection-office-probing-40-digital-lenders-over-misuse-of-personal-data/.
12. "Mulla Pride, Faircash Mobile Lending Apps Fined for Threatening Consumers," Nairobi News, 27 September 2023, https://nairobinews.nation.africa/mulla-pride-faircash-mobile-lending-apps-fined-sh2-9m-for-threatening-consumers/.
13. "Digital Lender Harassment Has Declined by 75%, Data Protection Commissioner Reveals," Citizen Digital, 15 May 2024, https://citizen.digital/article/digital-lender-harassment-has-declined-by-75-data-protection-commissioner-reveals-n342203.
14. Central Bank of Kenya (Digital Credit Providers) Regulations, 2022, Legal Notice No. 46 of 2022, https://new.kenyalaw.org/akn/ke/act/ln/2022/46/eng@2022-04-22.
15. Central Bank of Kenya (CBK), press release on the licensing of 29 additional digital credit providers, 30 September 2026, https://www.centralbank.go.ke/uploads/press_releases/366319113_Press%20Release%20-%20Licensing%20of%2029%20Additional%20Digital%20Credit%20Providers.pdf.
16. Data Protection Act, 2019 (Kenya), sec. 58 (enforcement notices) and secs. 62–63 (penalty notices of up to KES 5 million or, for an undertaking, 1% of annual turnover in the preceding financial year, whichever is lower), https://new.kenyalaw.org/akn/ke/act/2019/24/eng@2022-12-31; on continued debt-shaming, "Debt-Shaming Back as Digital Lenders Defy CBK," Business Daily, 25 June 2025, https://www.businessdailyafrica.com/bd/economy/debt-shaming-back-as-digital-lenders-defy-cbk-5094888.

In August 2025, her Office wrote to the Central Bank asking it to revoke the licences of two lenders whose breaches had continued despite earlier administrative action; there is no public record of the outcome.[17]

Artificial intelligence is likely to deepen this overlap. Kenya's data protection authority now treats AI credit scoring by digital lenders as high-risk processing, with a right to human review of an adverse automated decision,[18] while the lending decision itself remains a matter for the financial regulator. Complaint bodies elsewhere report few complaints so far about firms' own use of AI, but a clear rise in consumers using generative AI to draft complaints, which makes cases longer and harder to verify.[19] Digital lending is a fast-moving field: products, data sources, collection practices and the rules that govern them keep changing. The question of which authority answers a given harm is therefore not one the two authorities can settle once. They will need to keep revisiting it together.

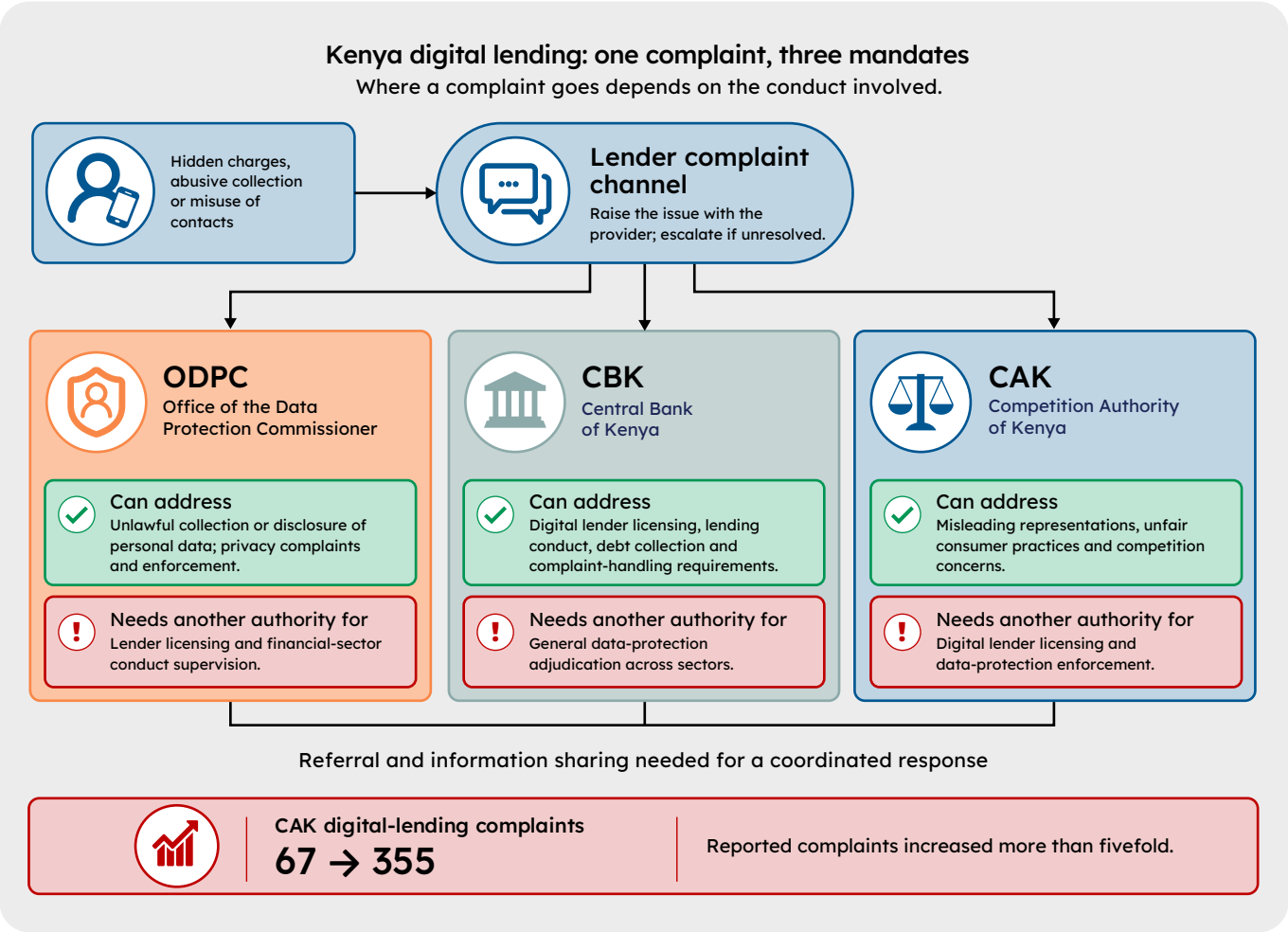


17. "Data Protection Office Asks CBK to Revoke Permits for Two Digital Lenders," Business Daily, 21 August 2025, https://www.businessdailyafrica.com/bd/economy/dpo-asks-cbk-to-revoke-permits-for-two-digital-lenders-5162924.

18. Office of the Data Protection Commissioner (ODPC) (Kenya), Guidance Note on Artificial Intelligence (July 2026), secs. 4.1, 6.6, and 9, https://www.odpc.go.ke/wp-content/uploads/2026/07/AI-Guidance-Note.July-2026.pdf.

19. Financial Ombudsman Service (UK), Financial Ombudsman Service Response to the Mills Review (February 2026), https://www.financial-ombudsman.org.uk/files/324744/Financial-Ombudsman-Service-response-to-Mills-Review.pdf; M. Harris, "Embracing AI's Transformational Impact on Consumer Complaints," Financial Ombudsman Service, 27 March 2026, https://www.financial-ombudsman.org.uk/businesses/resolving-complaint/our-insight/embracing-ais-transformational-impact-consumer-complaints.

Figure 2.3: Overlapping regulatory responsibility for digital lending in Kenya



Source: CCAF & Fii.

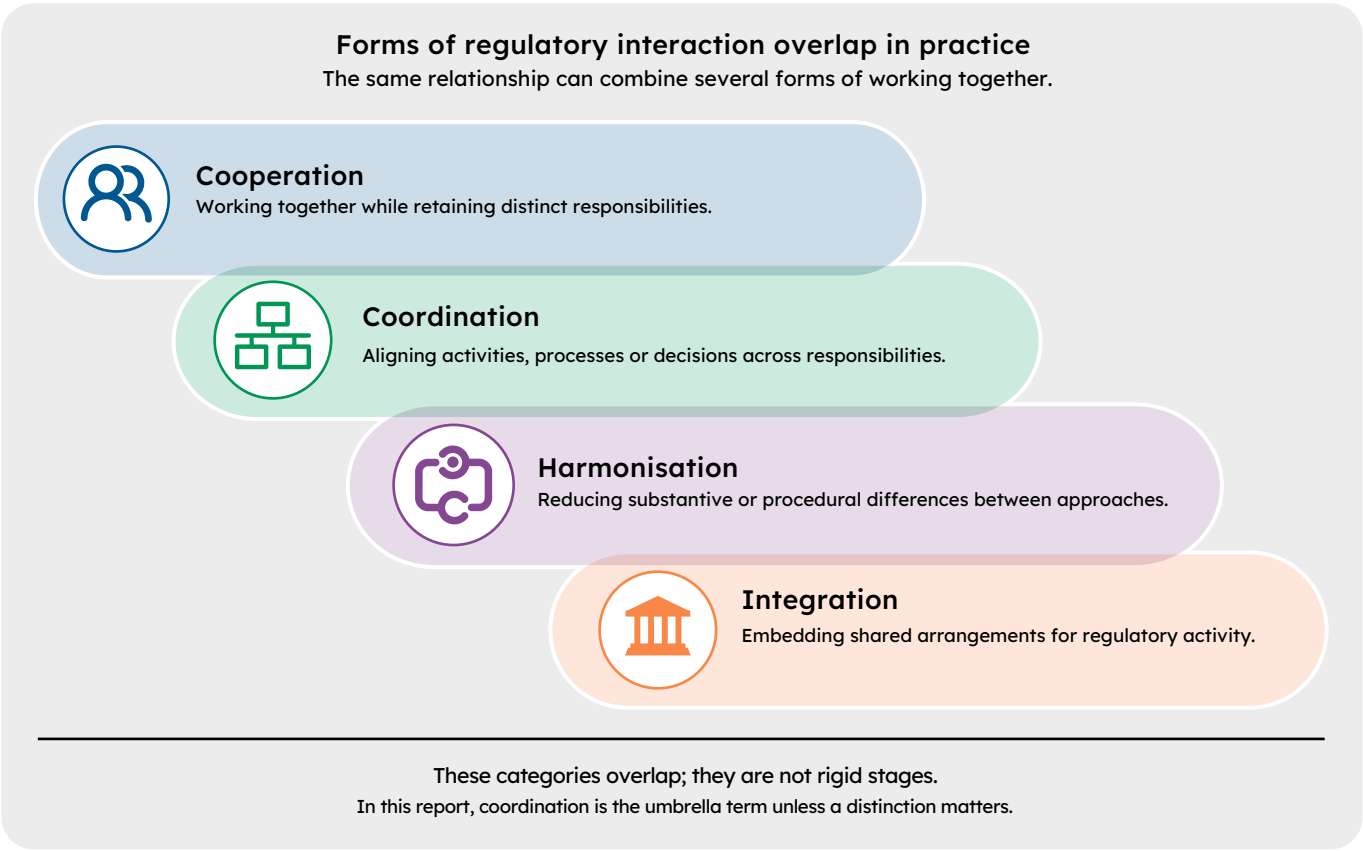
There is also a measurement gap. While regulatory fragmentation was widely recognised by stakeholders as creating additional costs, delays and uncertainty, this study did not identify a validated cross-country framework linking DP–FS coordination to attributable consumer and market outcomes, in a review of public and academic sources up to the cut-off date. Without such evidence, the case for coordination risks remaining largely qualitative, making it difficult for authorities to assess the scale of the problem, identify where intervention would have the greatest impact, or justify the allocation of scarce regulatory resources.

2.3 What we mean by coordination

This report uses 'coordination' as an umbrella term for the processes through which two or more authorities align or reconcile their activities and decisions while each retains its own powers. It covers four overlapping forms of working together, shown in Figure 2.4: cooperation (working together while retaining distinct responsibilities), coordination in the narrower sense (aligning activities, processes or decisions), harmonisation (reducing substantive or procedural differences) and integration (embedding shared arrangements). These categorisations, while helpful, are abstractions—a single relationship can combine several of them, and in practice often does.

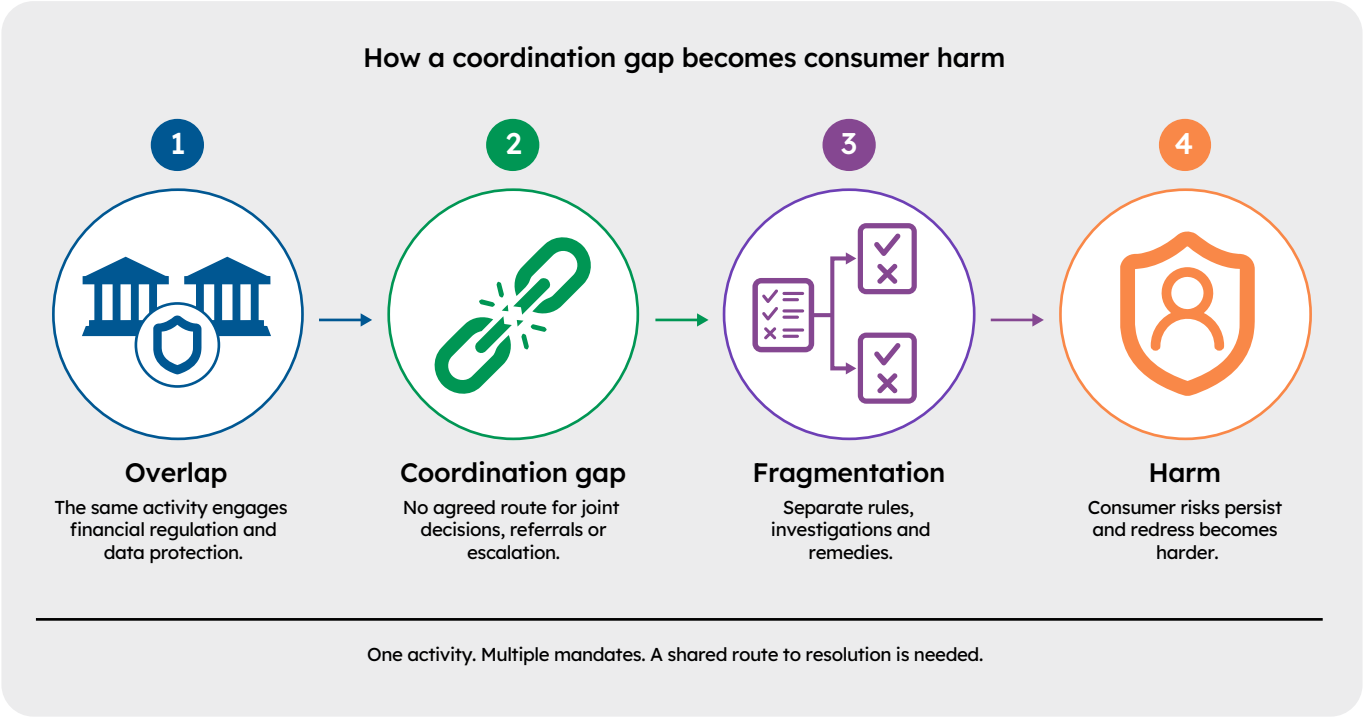
The report looks at coordination in three ways. Section 3 maps where it is already happening, through international and regional bodies and through national mechanisms such as contact points, joint guidance, sandboxes and information sharing. Section 4 examines where it is missing across the five thematic areas. Section 5 sets out how much coordination exists and what it might be worth, through the Regulatory Coordination Index, which scores a relationship from formal agreement through joint capacity-building, policymaking, supervision and enforcement to conflict resolution and review. The rest of this section explains the distinction on which all three rest: between overlap and the coordination gap.

Figure 2.4: Forms of regulatory interaction



Source: CCAF & Fii.

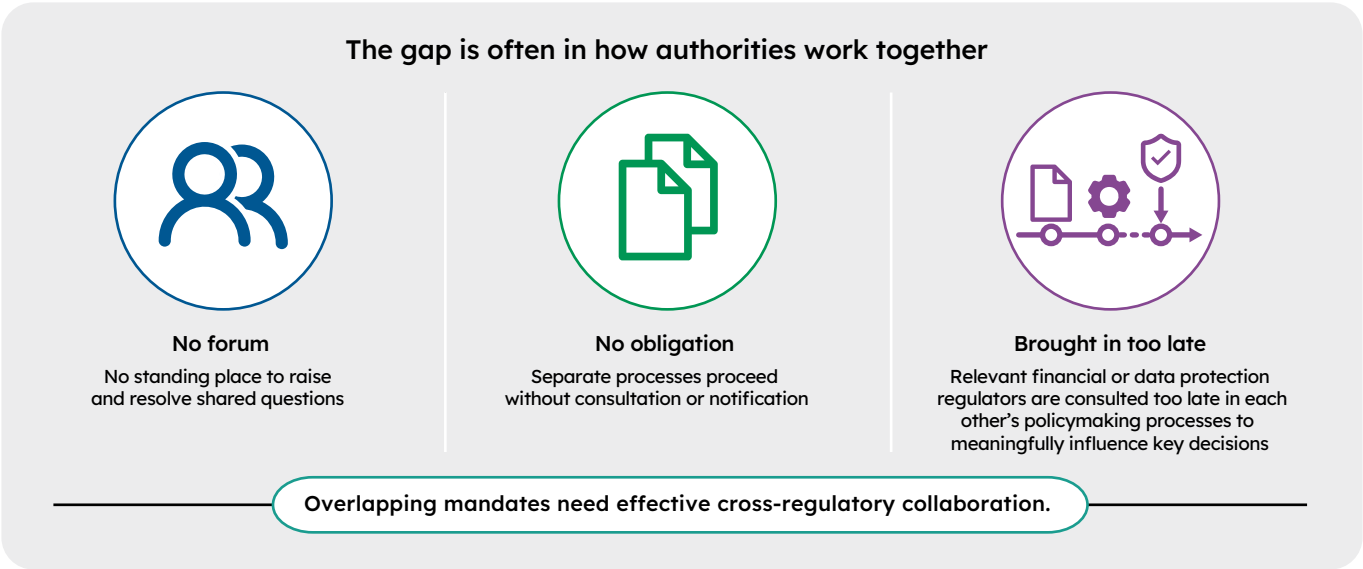
Figure 2.5: From coordination gap to consumer harm



Source: CCAF & Fii.

This report distinguishes two problems which are easily conflated. The first is that the two regulatory regimes overlap. As financial services have become data-intensive, financial regulation and data protection have come to bear on the same activities and frequently on the same records: the identity attributes collected at onboarding, the transaction histories used to detect fraud, the data used to underwrite credit, the payment messages that cross borders. Overlap of this kind is structural: the predictable consequence of one sector becoming a heavy processor of personal data while a regime of general jurisdiction over personal data matures around it. Overlap generates questions: for example, what may be collected for due diligence and for how long, whose consent architecture governs an open finance interface, which authority answers when an automated credit decision goes wrong. But overlap does not by itself determine whether those questions are answered well, badly, or at all.

Figure 2.6: Common barriers to collaboration between financial and data protection authorities



Source: CCAF & Fii.

The second problem is that, in practice, those questions largely go unanswered. It is this problem that the report calls the coordination gap. In focus countries, the legal tools to resolve the questions that overlap generates are generally already in place: authorities may consult one another, exchange information, issue guidance jointly and enter cooperative arrangements.[20] What is absent is the institutional machinery through which they would routinely do so. The main exception is jurisdictions that have yet to establish a data protection regulator (Section 4.3, Box 9).

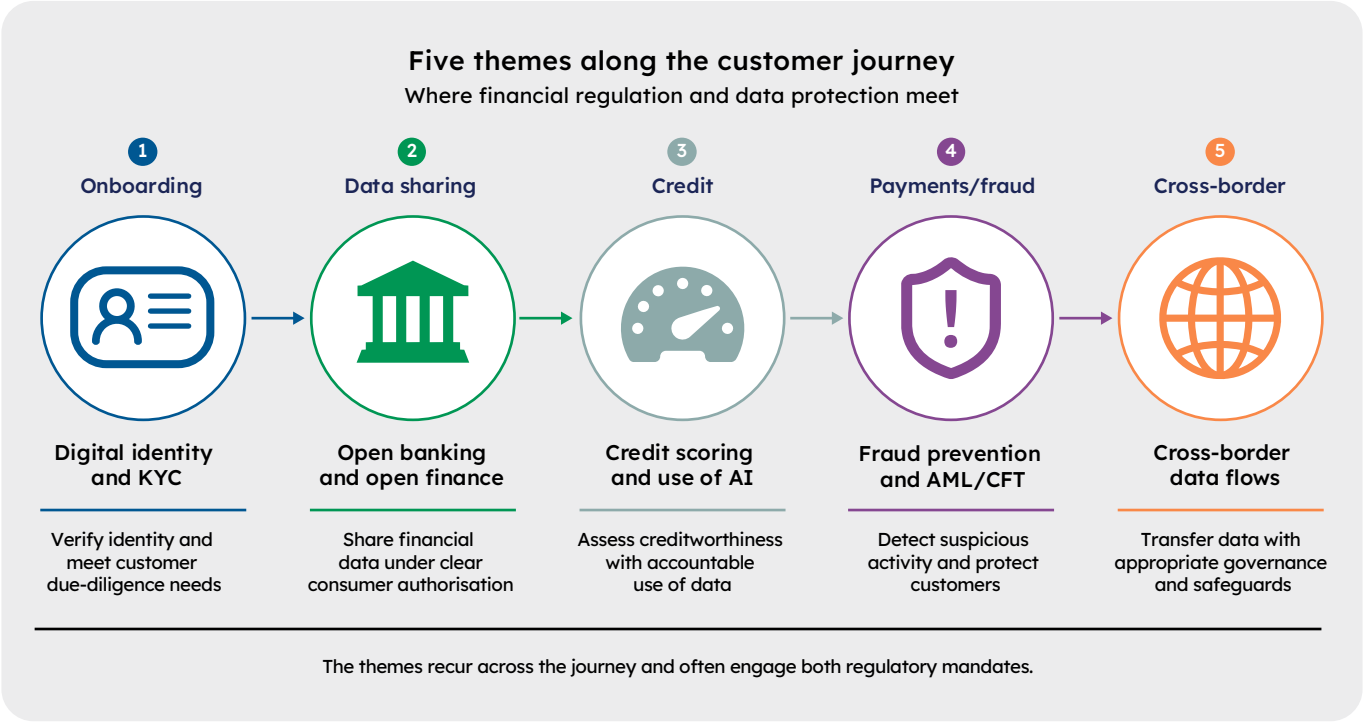
The distinction determines what would count as a remedy. If the two regimes imposed requirements that genuinely cannot both be satisfied, the answer would be substantive and largely legislative: rewriting rules, calibrating exemptions, allocating jurisdiction more cleanly. In some cases that may be warranted, but for most of the challenges this report identifies, the evidence points elsewhere. Where this research found actual or potential harm, it was rarely because a legal question was unanswerable. It was because no forum existed in which to ask it, no authority was obliged to ask it, or the authority that should have asked it was brought in after the answer had already been settled. Either authority can involve its counterpart too late. In the cases documented here it is usually the data protection authority that arrives after the main decisions, but the same risk applies in reverse, for example where data protection guidance on profiling or transfers is issued without financial-sector input. These coordination shortcomings in turn flow down into compliance burdens for firms and under-addressed risks to consumers.

20. The country-by-country basis for this finding is set out in Annex A. See also, for the general proposition that data protection and AML/CFT objectives are compatible rather than mutually exclusive, FATF, Guidance on Private Sector Information Sharing (November 2017), https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Private-Sector-Information-Sharing.pdf.

The report's analysis is anchored by a coordination framework. As set out in Annex C, the framework underpins the Regulatory Coordination Index (RCI), which measures coordination across the main activities through which regulators work together. It begins from some form of formal agreement, such as an MoU between regulators, and extends to joint capacity-building, policymaking, oversight (supervision and enforcement), conflict resolution, and inter-regulatory accountability. This framework shapes both the qualitative assessment that follows and the quantitative analysis in Section 5.

2.4 Five high-impact thematic areas

Figure 2.7: Areas of regulatory overlap across the customer journey



Source: CCAF & Fii.

The report examines five thematic areas of digital financial services where consumer impact is high and better coordination could do most good. Together they span problems to be reduced, such as fraud, and opportunities to be developed, such as open finance.

They capture key intersections between data protection and financial regulation across the customer journey. In each, both regimes apply to the same activity. Without coordination, firms are left uncertain about what is expected of them, risks go unaddressed and opportunities go unclaimed.

Digital identity, KYC and AML/CFT: the verification of customers' identity at onboarding, and the ongoing due diligence, monitoring, reporting and record-keeping that anti-money laundering rules require. The shared question is which identifying attributes are necessary to verify and screen a customer accurately, how long they must be kept and when they may be reused.

Fraud: the detection and prevention of fraud and scams, which increasingly depends on sharing transaction, identity and device data across institutions. The shared question is what may be shared across institutions, with whom and for how long.

Open finance, including open banking: arrangements that let customers authorise secure access to, and sharing of, their financial data with other providers, including beyond banking. The shared question is whether consent is meaningful and purpose-bound, and whether and how data stay protected once they leave the account provider.

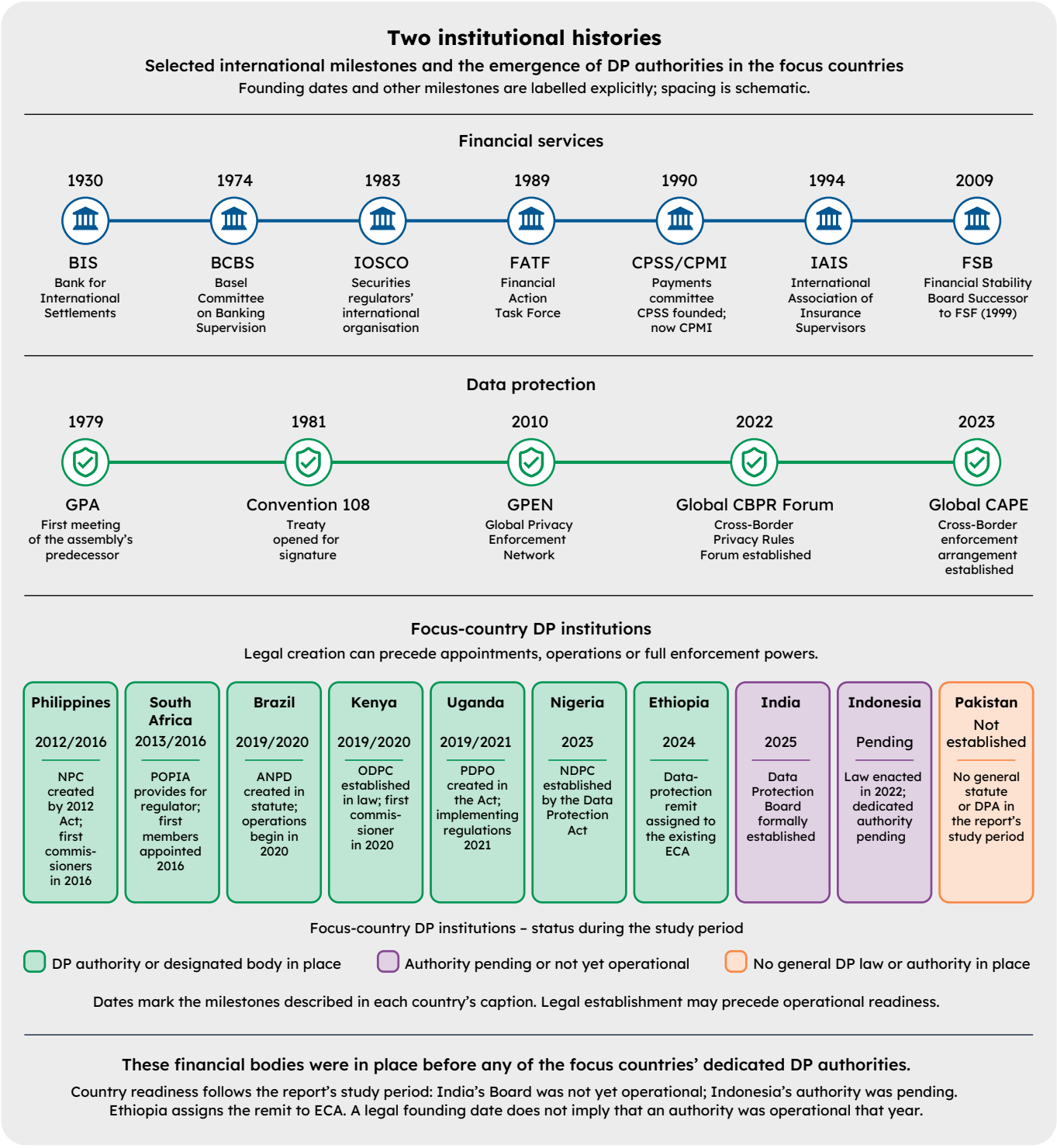
Credit underwriting and AI: the assessment of creditworthiness, increasingly using alternative data and automated or AI-enabled models. The shared question is which data sources are appropriate, and how fairness, transparency and the right to challenge apply to automated decisions.

Cross-border data flows and localisation: the movement of financial and personal data across borders, and requirements to keep data, or copies of them, in the country. The shared question is how transfer rules, local-storage requirements and supervisory access fit together.

In most cases both regimes can be satisfied at once; where both mandates are engaged, coordination may be needed to settle how.

2.5 Regulatory landscape

Figure 2.8: Timeline of international financial and data protection bodies, and focus-country data protection authorities



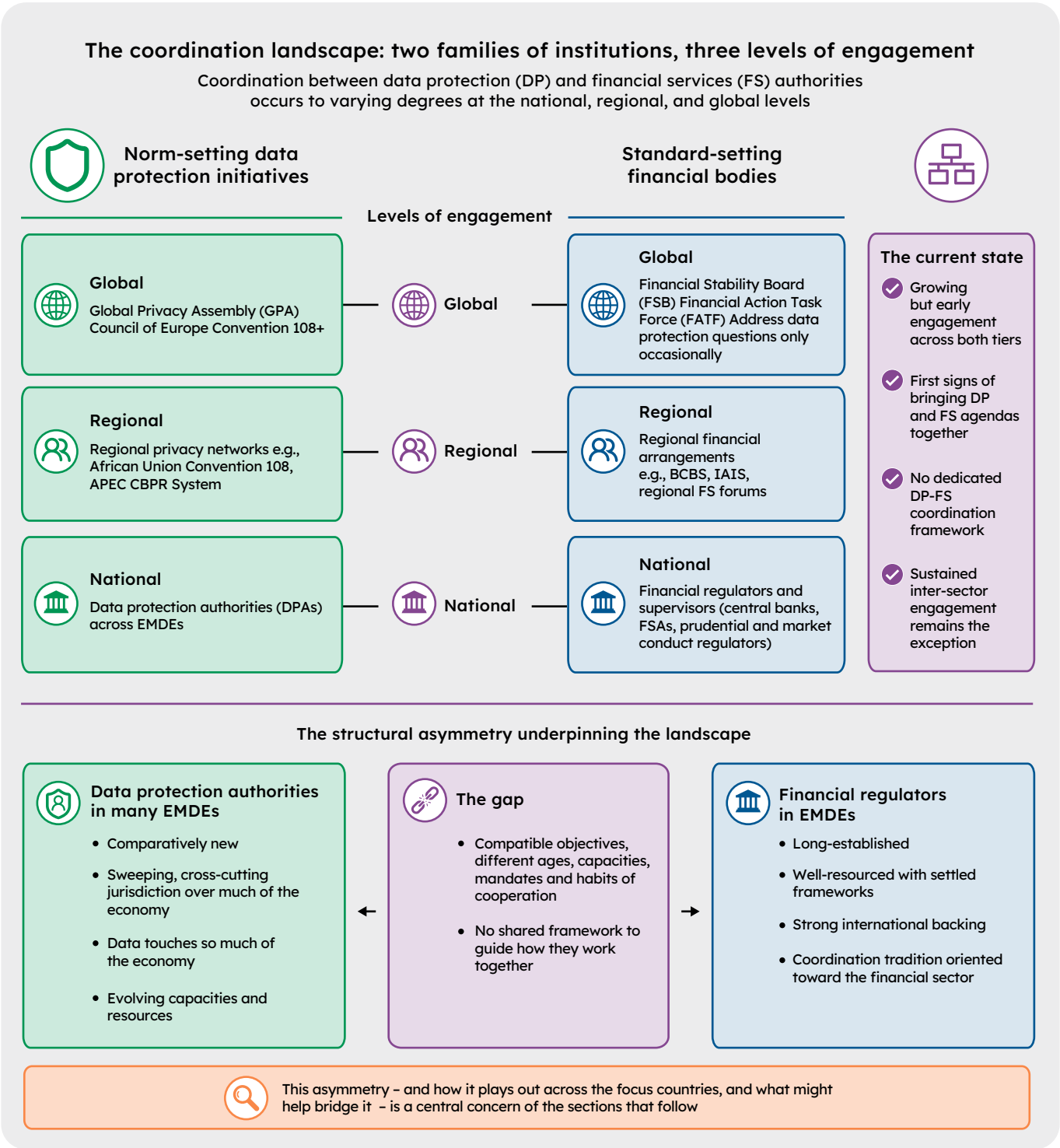
Source: CCAF & Fii.

Coordination between data protection and financial services authorities takes place at national, regional and global levels, and its character differs at each (Figure 2.8). Internationally, the two fields' infrastructures differ markedly in age and density. Financial regulation rests on a mature system of standard-setters whose standards are assessed through peer review and, in the FATF's case, through mutual evaluation with real consequences. Data protection's international architecture is younger and more loosely coupled: it convenes, deliberates, certifies and supports enforcement cooperation, and its most influential templates, the Organisation for Economic Co-operation and Development (OECD) Privacy Guidelines and Convention 108, have shaped national laws widely. But no data protection instrument carries an assessment with consequences comparable to FATF mutual evaluation. Section 3.1 describes both architectures.

A comparable mix operates at the regional level, where for several focus countries the arrangements are more consequential than the global tier. Across both tiers the picture is one of growing but still early engagement: a small number of genuine bridges between the two fields now exist, and Section 3.1 examines them, but a dedicated DP–FS coordination framework and sustained inter-sector engagement remain the exception. The same asymmetry often recurs at national level, shaping which authority convenes, which sets the agenda and which arrives after the substantive decisions have been taken, and it feeds the asymmetries in resources and capacity discussed in Section 7.



Figure 2.9: Overview of engagement between data protection and financial bodies at global, regional and national levels



Source: CCAF & Fii.

Chapter 3

Coordination today: Where it is happening



This section maps where DP–FS coordination is already happening: at the international and regional levels (Section 3.1) and nationally (Section 3.2), drawing where useful on examples from beyond the focus countries, including developed markets whose models may be relevant more widely. Section 4 then turns to the gaps.

One fact underlies much of what follows: data protection as a regulatory field is considerably newer than financial services regulation, and is correspondingly less institutionalised. This shows up internationally as much as nationally, and the discussion begins with the international picture.

3.1 International and regional architecture

Coordination at the international level matters because financial markets and data flows are global. Payments, remittances, cloud services and fraud cross borders daily, so national rules need to interoperate, and conflicting legal duties in different jurisdictions are costly for firms and can leave consumers unprotected. International bodies also shape national rules: financial standard-setters through standards, peer review and domestic implementation, and data protection bodies mainly through convening, model instruments and enforcement cooperation.

The international and regional bodies that support financial regulation and data protection differ in important ways. The financial side is served by a dense, layered and long-established set of bodies:

The Financial Stability Board (FSB) (established in 2009, succeeding the Financial Stability Forum of 1999) coordinates national authorities and international standard-setters and conducts peer reviews across its membership.

Sub-sectoral standard-setters—the Basel Committee on Banking Supervision (1974) for banks, IOSCO (which became an international body in 1983) for securities markets, the International Association of Insurance Supervisors (IAIS) (1994) for insurance, and the Committee on Payments and Market Infrastructures (CPMI) (founded in 1990 as the Committee on Payment and Settlement Systems) for payment systems—set standards for their own sectors.

- The Financial Action Task Force (1989) sets the global standards for anti-money laundering and counter-terrorist financing and, through mutual evaluation and the listing process, enforces them with a directness that has no counterpart in data protection.
- The Bank for International Settlements (BIS) (1930) hosts the secretariats of several of these bodies (the FSB, the Basel Committee, the CPMI and the IAIS, the last an independent association) and, through the Financial Stability Institute, supplies much of the comparative supervisory analysis on which they draw.
- Below the standard-setters sits a further layer of narrower bodies, including FinCoNet (2013) on market conduct, the International Association of Deposit Insurers (IADI) (2002), the International Organisation of Pension Supervisors (IOPS) (2004), and the Global Financial Innovation Network (2019), a voluntary network on regulatory innovation, whose membership includes authorities from several focus countries.

Most of the principal international financial regulatory bodies predate the spread of dedicated data protection authorities, and their membership and working methods reflect that. Much of their output is widely viewed as binding in effect, if not in law: FATF standards, for example, translate into domestic requirements through a peer-review mechanism with material consequences for a jurisdiction's standing in the international financial system. Core memberships centre on financial mandates, and participation by data protection authorities varies by body and mechanism, however directly the standards under discussion bear on personal data.

The data protection infrastructure is younger, thinner and differently constituted.

- The Global Privacy Assembly, (GPA), whose predecessor first met in 1979 and which took its current name in 2019, is its principal gathering: it accredits national supervisory authorities, adopts resolutions and runs working groups, but its instruments do not bind and it conducts no equivalent of mutual evaluation.
- Convention 108, opened for signature in 1981 and in force, remains the only binding international instrument in the field open to accession worldwide. Its 2018 amending protocol, commonly called Convention 108+, is not yet in force: on 15 May 2026 it had 34 of the 38 ratifications it needs.
- The African Union Convention on Cyber Security and Personal Data Protection (the Malabo Convention) has been in force since 8 June 2023 as a regional binding instrument. (No focus country is a party to Convention 108+ or the Malabo Convention).[21]
- Enforcement cooperation runs through the Global Privacy Enforcement Network (2010) and, for participating jurisdictions, the Global Cooperation Arrangement for Privacy Enforcement. Certification runs through the Global Cross-Border Privacy Rules (CBPR) Forum, which since 2022 has extended the Asia-Pacific Economic Cooperation (APEC) model beyond APEC membership.
- The OECD's Privacy Guidelines of 1980, revised in 2013, have served as a template for national data protection laws worldwide, including many in the APEC region,[22] and the G20/OECD High-Level Principles on Financial Consumer Protection, revised in 2022, include a principle on the protection of consumer data and privacy;[23] both are recommendations rather than assessed standards.
- The EU's General Data Protection Regulation has also exerted a strong pull on national laws, the so-called 'Brussels effect', including in several focus countries, although larger jurisdictions such as India have taken more distinct approaches.
- The OECD's Data Free Flow with Trust programme supplies analysis and convening rather than rules.

21. Council of Europe, "Republic of Moldova Becomes the 34th State to Ratify the Convention 108+," 21 May 2026, https://www.coe.int/en/web/data-protection/-/republic-of-moldova-becomes-the-34th-state-to-ratify-the-convention-108-.

22. OECD, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD/LEGAL/0188 (1980, revised 2013).

23. OECD, Recommendation of the Council on High-Level Principles on Financial Consumer Protection, OECD/LEGAL/0394 (endorsed by the G20 in 2011, adopted 2012, revised 2022).

Table 3.1: International architecture at a glance

Category	Financial services	Data protection
Standard-setting and assessment	FSB; Basel Committee and CPMI (committees hosted by the BIS); IOSCO; IAIS; FATF and FATF-style regional bodies. Standards are assessed through peer review and, for the FATF, mutual evaluation with real consequences.	No equivalent assessed standard-setter. The Global Privacy Assembly accredits authorities and adopts resolutions, but its instruments do not bind and it conducts no assessments.
Cooperation and learning networks	GFIN (voluntary; regulatory innovation); FinCoNet (market conduct); IADI; IOPS.	GPEN and the Global Cooperation Arrangement for Privacy Enforcement; regional networks such as the Network of African Data Protection Authorities, Asia Pacific Privacy Authorities and the Ibero-American Data Protection Network.
Binding legal instruments	No treaty; standards take effect through domestic implementation.	Convention 108 (in force); Convention 108+ (not yet in force); the African Union Malabo Convention (in force since 2023, regional); the EU GDPR, binding within the EU and influential beyond it.
Non-binding principles and certification	G20/OECD High-Level Principles on Financial Consumer Protection (revised 2022).	OECD Privacy Guidelines (1980, revised 2013); Global CBPR certification; OECD Data Free Flow with Trust.
Effect for national regulators	An external standard to anchor domestic requirements, plus a peer group and shared vocabulary.	Fewer external anchors with assessment behind them: instruments are mostly non-binding, and the binding ones have limited reach in the focus countries.

Source: CCAF & Fii.

None of these bodies, and no data protection instrument, sets a standard against which domestic authorities are assessed with consequences comparable to those of FATF mutual evaluation, and the difference matters in practice. Where a financial regulator can often cite an international standard as the basis for a domestic requirement, a data protection authority generally cannot, and the institutional asymmetry described throughout this report is reproduced internationally as well as nationally. Membership patterns deepen the effect, since both architectures set entry criteria that newer authorities may not yet meet. Representation in the Global Privacy Assembly varies widely across countries and levels of institutional maturity.[24]

24. Global Privacy Assembly, "List of Accredited Members," accessed 2 October 2026, https://globalprivacyassembly.com/participation-in-the-assembly/list-of-accredited-members/, classified using the IMF World Economic Outlook country groups (April 2026). Counting international bodies separately and subnational authorities with their country, 57 of 145 members are from EMDEs: 19 in Africa, 17 in Latin America and the Caribbean, 15 in emerging Europe and Central Asia, 5 in the Gulf and 1 in developing Asia. On the World Bank's income classification, the share from non-high-income economies is approximately a third (46 of 145).

Focus countries at an early stage of data protection maturity, including India, Pakistan, Indonesia and Ethiopia, are therefore often absent from the GPA, Convention 108+, GPEN, and the CBPR system, or present only as observers. Several interviewees described their jurisdictions as policy takers, shaping few of the standards against which they are later assessed. Section 8 returns to what might change this. The picture is not static, however, and a few early bridges between the two fields have begun to appear at the global level.

This could be attributed to the relative newness of the authorities concerned, which is part of the explanation. The more precise account, however, is structural. The membership rules of the global financial coordination bodies were written at a time when the counterpart institution did not exist in most jurisdictions. As a result, neither architecture was designed to include the other. This matters because lock-in of this kind is not resolved by the passage of time or by the maturing of individual authorities. It is resolved, if at all, by deliberately building the connecting mechanisms that the original designs omitted.

A further reason is conceptual. Financial regulation rests on broad agreement about what should be supervised (capital, liquidity, conduct and financial integrity), even where the calibration of particular measures is debated. Data protection regimes share core principles, and are becoming more formalised as laws and authorities multiply, but they differ in legal bases, enforcement design and public-sector exemptions. Some jurisdictions treat privacy as a fundamental right, in some cases in their constitutions; others treat it more pragmatically, balancing it against innovation, economic growth and other social priorities; and states differ widely in how far they allow their own agencies access to personal data. A single assessable standard is therefore harder to build, which is why interoperability rather than uniformity is the realistic aim (Recommendation 7). It also limits what coordination can do: machinery for joint working can settle operational questions, but not disagreements that are, at root, about values.

Box 3: Early DP–FS bridges at the global level

Four initiatives illustrate convergence between the two fields.

The Forum on Cross-Border Payments Data was established by the Financial Stability Board in March 2025, as an outcome of the FSB'sFinancial Stability Board´s (FSB) December 2024 recommendations on data frameworks for cross-border payments. It brings together experts from financial authorities, data protection authorities and the private sector, works with the FATF and the OECD, and has a mandate spanning both fields, with data protection authorities among its participants. Its establishment by a financial standard-setter is itself a signal that the data protection dimension of financial regulation is becoming recognised at the global level.[25]

25. Financial Stability Board (FSB), "FSB Announces Establishment of the Forum on Cross-Border Payments Data," 27 March 2025, https://www.fsb.org/2025/03/fsb-announces-establishment-of-the-forum-on-cross-border-payments-data/; FSB, "Forum on Cross-Border Payments Data Convenes for the First Time," May 2025, https://www.fsb.org/2025/05/forum-on-cross-border-payments-data-convenes-for-the-first-time/, recording participation by "data privacy and protection authorities."

The Consultative Committee of Convention 108 adopted, in 2023 and with input from the FATF and Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL), guidelines on the processing of personal data for anti-money laundering and counter-terrorist financing purposes. This is the clearest instance to date of a data protection body producing an instrument addressed directly to a financial-integrity question, and of financial standard-setters contributing to one.

The Global Privacy Assembly's Working Group on Data Sharing for Public Good has begun work at the intersection of AML/CFT and data protection, bringing a financial-integrity question into a data protection forum. So far this has taken the form of an open consultation in the second quarter of 2026, so the initiative is at an early stage.

The FATF's own work has begun to draw on data protection authorities. Its 2022 report on data protection and private-sector information sharing was developed in consultation with data protection and privacy bodies from six jurisdictions and with international bodies including the European Data Protection Board (EDPB,), the Council of Europe and the GPA's Data Sharing Working Group,[26] and its July 2026 report on information sharing to combat illicit finance recommends that countries establish common objectives and clear regulatory expectations through senior-level engagement and joint guidance between AML/CFT and data protection authorities.[27] The FATF's draft R.16 guidance, published weeks earlier and expected to be finalised in February 2027, encourages measures to ensure compatibility between AML/CFT and data protection rules, promotes safeguards and calls for coordination between the authorities concerned; expert stakeholders disagree on the degree to which that current draft guidance entails an imbalance or establishes precedence between the two regimes. Stakeholders indicate that engagement with data protection authorities is a priority in the FATF's 2026–2028 work programme.

Three observations follow. Engagement between the two fields has been episodic and project-based, and the FSB Forum is the most prominent mechanism with a continuing mandate. The traffic runs predominantly in one direction: the financial side convenes and the data protection side is invited. And the data protection authorities that have participated are drawn almost entirely from high-income jurisdictions — the six that contributed to the FATF's 2022 report were from Canada, Jersey, Luxembourg, Mexico, Norway and the United Kingdom.

26. FATF, Partnering in the Fight against Financial Crime: Data Protection, Technology and Private Sector Information Sharing (July 2022), https://www.fatf-gafi.org/en/publications/Digitaltransformation/Partnering-in-the-fight-against-financial-crime.html. Footnote 2 lists the national bodies consulted: Canada's Department of Innovation, Science and Economic Development, the Jersey Office of the Information Commissioner, the Luxembourg National Commission for Data Protection, Mexico's INAI, the Norwegian Data Protection Authority and the UK Information Commissioner's Office.

27. FATF, Information Sharing to Combat Illicit Finance: Global Overview of Public and Private Sector Partnerships and Data Protection Arrangements (July 2026), https://www.fatf-gafi.org/en/publications/Methodsandtrends/information-sharing-ppp-data-protection-arrangements.html.

At the regional level the picture is more varied and in places more advanced.

- Europe, outside the focus set, has the most developed regional architecture: national data protection authorities cooperate through the European Data Protection Board, which can adopt binding decisions to settle disputes between them, and the European Supervisory Authorities play a comparable role in financial supervision.
- The East African Community's Data Governance Policy Framework, validated in 2024 but not yet formally adopted, covers Kenya and Uganda and names payments and financial services among its use cases; it is the clearest regional connection between data governance and finance in the focus set (Annex B).
- The Network of African Data Protection Authorities, established in 2016, provides a continental convening function for the African focus countries and has run awareness work on personal data in fintech in partnership with the Council of Europe, though it has no standing arrangement with financial-sector bodies.
- The Association of Southeast Asian Nations (ASEAN) has developed model contractual clauses and a framework for cross-border data flows relevant to Indonesia and the Philippines.
- The Philippines also participates in the Global CBPR Forum, and its National Privacy Commission (NPC) in the Asia Pacific Privacy Authorities forum.
- Brazil's authority participates in the Ibero-American Data Protection Network.

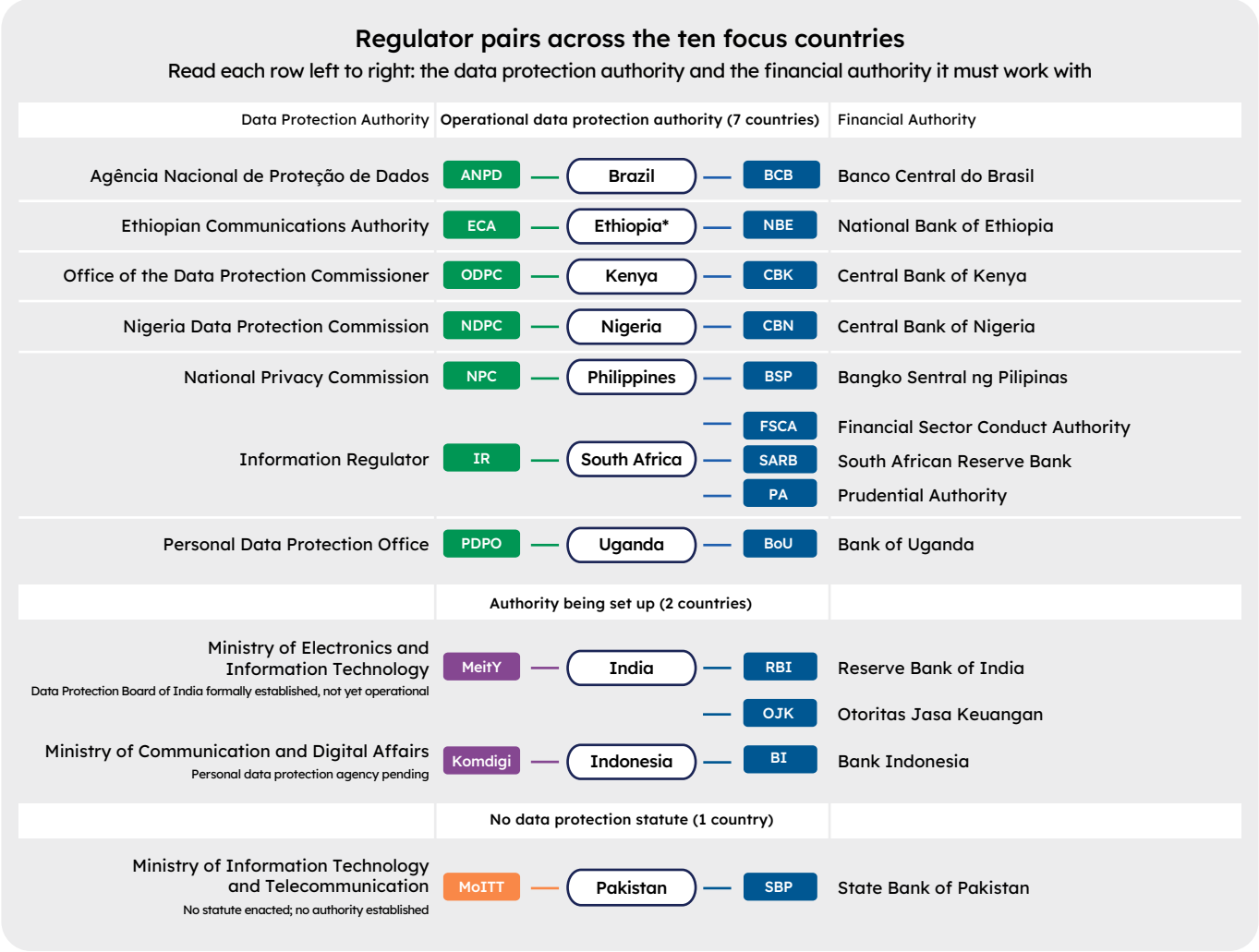
Harmonisation of this kind is attractive for smaller jurisdictions, since it lowers compliance costs and eases entry for firms operating across borders.

One pattern is worth noting before turning to the national picture. Where data protection and financial authorities meet internationally, they most often do so in forums convened by the financial side, on agendas set there. The regional data protection networks, which are the arenas in which the focus countries have most voice, are also the arenas with the least financial-sector engagement.



3.2 National architecture

Figure 3.1: Status of data protection authorities and financial regulators in the ten focus countries



Source: CCAF & Fii.
* Ethiopia assigns data protection functions to the Ethiopian Communications Authority (ECA). Status reflects the report's research period and is not a current-status update. Source: CCAF/Fii report, Table 2.

At the national level, coordination is growing but improvised. Public documents and interviews point to deepening collaboration between financial regulators and data protection authorities, drawn from a varied toolkit of binding and non-binding instruments that regulators match to the outcome they are seeking.

These instruments range widely in weight and purpose. MoUs offer a quick (albeit generally non-binding) route to closer cooperation, and tend to scale best where the financial-sector party holds a consumer-protection mandate, as the UK's FCA does, or speaks for a wider ecosystem of regulators, as the AMLC does in the Philippines.

Joint declarations set out a shared position on an ambiguous obligation for the benefit of the wider market. Working groups and inter-agency forums provide standing channels for communication, and in some cases a shared budget that lowers the cost of taking part. Unilateral guidance from a single authority can shape sectoral practice without any formal agreement at all. And where a data protection authority is still being established, as in Pakistan, or has only recently taken on the remit, as in Ethiopia, coordination often rests instead on cross-sectoral consultation during the drafting of the legislation itself.

Two patterns run across these instruments. The first is that regulators rarely rely on any one of them: countries at an intermediate level of regulatory maturity tend to layer several together. The second is structural. While most focus countries have a single data protection authority, their financial ecosystems often contain two or three regulators with consumer protection mandates, each of which may strike its own arrangements. That can leave coordination uneven within a jurisdiction, and it is part of why shared contact points and standing forums are proving useful. Where a country has several financial regulators, this report analyses the data protection authority's relationship with the regulator holding the principal mandate for the activity in question (for most thematic areas in most focus countries, the central bank), and brings in the others where they form part of the data chain, as with South Africa's conduct and prudential authorities or Kenya's Central Bank and its savings and credit cooperative regulator.

> "We are also looking to establish joint industry working groups. We have done that recently with the telecommunications sector … [we] would also benefit from something like that with the financial regulator, and one that would be a continuous one, so that would allow for ongoing dialogue."

The discussion that follows groups these instruments by the function they perform: single points of contact and joint desks; joint guidance and sectoral codes; shared and joint sandboxes; and information sharing between authorities.

Single points of contact and joint desks

At the national level, some regulators have set up single points of contact for external stakeholders and joint desks for areas of persistent overlap. As Section 4 discusses, these mechanisms remain under-implemented relative to their potential, but the existing instances are useful examples. Table 3.2 sets out the clearest examples across the focus countries.

Table 3.2: National contact points and joint desks

Jurisdiction	Mechanism	Purpose
Nigeria	Joint Enforcement Desk (NDPB–FCCPC), established 2022	Desk for enforcement where data protection and consumer protection overlap, including in digital lending, set up under the October 2022 FCCPC–NDPB MoU (the NDPB was the NDPC's predecessor); current activity not confirmed.
Nigeria	Single Regulatory Window	Proposed single window (at technical scoping stage) to coordinate licensing across agencies, set out in the CBN's February 2026 report Shaping the Future of Fintech in Nigeria: Innovation, Inclusion, and Integrity; the NDPC's role is not specified.[28]
Philippines	NPC as de facto reference point	Interviewees described financial regulators as relying on NPC advisory opinions, despite no legal obligation to consult; joint instruments include the NPC–Insurance Commission Joint Advisory 2025-001.
Brazil	Shared inter-agency channel	Interviewees reported an informal, real-time channel between the ANPD and the Central Bank; no formal cooperation agreement between the two was identified.
Nigeria; Philippines	MoU/MoA cooperation commitments	NDPC–NAICOM MoU (November 2024): training, compliance monitoring, enforcement and sector guidelines. NPC–Insurance Commission MoA (December 2024): joint work on privacy-enhancing technologies.

Source: CCAF & Fii. Drawn from public instruments and interviews; examples are illustrative, not exhaustive.

Two points draw these examples together. First, the arrangements range from the formally established, such as Nigeria's joint enforcement desk, to the informal, such as the reported reliance on the National Privacy Commission (NPC) in the Philippines even absent any obligation to consult it. Second, some go further than communication and allow direct supervision: the Nigeria Data Protection Act 2023, for instance, requires firms in data-intensive sectors such as financial services to register with the Nigeria Data Protection Commission (NDPC) and to file annual data protection audit returns. Nigeria's proposed Single Regulatory Window is not itself a DP–FS mechanism, but it shows a financial regulator planning a joint regulatory platform. Its design does not yet specify a role for the data protection authority.

28. Central Bank of Nigeria (CBN), Shaping the Future of Fintech in Nigeria: Innovation, Inclusion and Integrity, Policy Insight Series (released February 2026), as reported in "The CBN Has a Plan to Make Regulation Work for Fintechs. Here Is What It Looks Like," TechCabal, 26 February 2026, https://techcabal.com/2026/02/26/the-cbn-has-a-plan-to-make-regulation-work-for-fintechs-here-is-what-it-looks-like/.

Box 4: Developed-market models: standing cross-regulator platforms

Some jurisdictions run permanent platforms that keep financial and data protection authorities at the same table. The United Kingdom's Digital Regulation Cooperation Forum (DRCF) counts both the Financial Conduct Authority (FCA) and the Information Commissioner's Office (ICO) among its members,[29] and the Netherlands' Digital Regulation Cooperation Platform brings together the Dutch data protection authority and the Authority for the Financial Markets.[30] Both coordinate with comparable bodies elsewhere, though not all of those include financial regulators. Arrangements of this kind show how a standing forum can give the two sides a durable, shared venue rather than the ad hoc contacts more common across the focus countries.

The DRCF was established by the competition, data protection and communications regulators in July 2020 as new digital mandates approached, notably Ofcom's designation as online harms regulator, and built on joint work already under way, including a Competition and Markets Authority (CMA)-led taskforce on digital markets in which the FCA also took part; the FCA became a full member in April 2021.[31] The Samenwerkingsplatform Digitale Toezichthouders (Digital Regulation Cooperation Platform) (SDT) was launched in October 2021 by the consumer and competition, financial markets, data protection and media authorities, on the stated grounds that data protection, consumer protection and competition had become closely intertwined and that incoming EU rules would impose obligations engaging more than one authority.[32] In both cases the regulators acted ahead of the problem rather than after it.

Three features appear to sustain them. First, they sit on existing legal routes for sharing information. The Dutch competition and data protection authorities adopted a cooperation protocol, grounded in statutory information-sharing provisions, the year before the SDT launched, and the ICO and CMA updated their MoU alongside a 2021 joint statement on the interaction between competition and data protection.[33] The forums coordinate; the legal gateways make the exchange possible.

29. Digital Regulation Cooperation Forum (DRCF), "About the DRCF," accessed 21 October 2026, https://www.drcf.org.uk/about-us.

30. Authority for Consumers and Markets (ACM), "Dutch Regulators Strengthen Oversight of Digital Activities by Intensifying Cooperation," 13 October 2021, https://www.acm.nl/en/publications/dutch-regulators-strengthen-oversight-digital-activities-intensifying-cooperation.

31. DRCF, "Digital Regulation Cooperation Forum: Plan of Work for 2021 to 2022," GOV.UK, 10 March 2021, https://gov.uk/government/publications/digital-regulation-cooperation-forum-workplan-202122/digital-regulation-cooperation-forum-plan-of-work-for-2021-to-2022; "The Digital Regulation Cooperation Forum," GOV.UK, 10 March 2021, updated 28 March 2023, https://www.gov.uk/government/collections/the-digital-regulation-cooperation-forum; Ofcom, "The Digital Regulation Cooperation Forum: Working for Greater Cooperation in Regulating Online Platforms," 10 November 2021, updated 16 March 2023, https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/working-for-greater-cooperation-in-online-regulation.

32. ACM, "Nederlandse toezichthouders versterken toezicht op digitale activiteiten door meer samenwerking," 18 October 2021, https://www.acm.nl/nl/publicaties/nederlandse-toezichthouders-versterken-toezicht-op-digitale-activiteiten-door-meer-samenwerking.

33. "Samenwerkingsprotocol tussen Autoriteit Consument en Markt en Autoriteit Persoonsgegevens," Staatscourant 2020, 36741, https://zoek.officielebekendmakingen.nl/stcrt-2020-36741.html; "ICO and CMA Set Out Blueprint for Cooperation in Digital Markets," WiredGov, 19 May 2021, https://www.wired-gov.net/wg/news.nsf/articles/ICO+and+CMA+set+out+blueprint+for+cooperation+in+digital+markets+19052021142000?open=.

Second, they have dedicated capacity: the DRCF appointed a chief executive in November 2021.[34] Third, they are modular. The SDT has created topic-based chambers open to other authorities; its chamber on the Digital Services Act has twelve members, including the police and the public prosecutor. Its members now also hold a single joint meeting with each large platform rather than separate ones.[35]

Both remain voluntary, and the limits of that are debated. A House of Lords committee recommended in 2021 that the DRCF be placed on a statutory footing with an independent chair accountable to Parliament; the government declined.[36] The SDT's members have stated publicly that effective cooperation depends on political support and on adequate resources, instruments and powers.[37]

One difference limits how directly these models transfer. In both forums the financial member is the conduct regulator; the central bank and prudential supervisor (the Bank of England; De Nederlandsche Bank) sit outside. In most focus countries the principal financial supervisor is the central bank, with South Africa's twin-peaks structure and Indonesia's Otoritas Jasa Keuangan (Financial Services Authority) (OJK) as partial exceptions. A standing forum modelled on these examples would not by itself bring the data protection authority into the rooms where financial-sector coordination takes place; it would need to include the central bank from the outset.

Joint guidance and sectoral codes

Where the previous category concerns who stakeholders turn to, this category concerns what regulators tell the market. Joint instruments such as MoUs, MoAs and joint declarations are increasingly used not only to structure cooperation between authorities but also to issue guidance and codes for the financial sector. Guidance from a single authority can also function, in effect, as a sectoral code. Table 3.3 sets out the main examples.

34. G. Whitehead, "Bringing Together Regulatory Thinking in the Digital Space," Competition and Markets Authority (blog), 25 March 2022, https://competitionandmarkets.blog.gov.uk/2022/03/25/bringing-together-regulatory-thinking-in-the-digital-space/.

35. AFM, "SDT Members to Expand Their Collaboration regarding Digital Regulation," 24 March 2023, https://www.afm.nl/en/consumenten/actueel/2023/maart/uitbreiding-digitaal-toezicht-sdt; Tom Reijner, "Toezichthouders digitale sector slaan handen ineen," Binnenlands Bestuur, 24 April 2025, https://www.binnenlandsbestuur.nl/digitaal/toezichthouders-digitale-sector-slaan-handen-ineen; "Toezicht in tijden van digitale macht," ToeZine, 07 October 2025, https://www.toezine.nl/toezicht-in-tijden-van-digitale-macht/.

36. House of Lords Communications and Digital Committee, Digital Regulation: Joined-Up and Accountable (13 December 2021), https://committees.parliament.uk/publications/8186/documents/83794/default/.

37. SDT, "Effectief digitaal toezicht cruciaal voor verantwoorde digitalisering," Autoriteit Persoonsgegevens, accessed 21 October 2026, https://www.autoriteitpersoonsgegevens.nl/documenten/sdt-effectief-digitaal-toezicht-cruciaal-voor-verantwoorde-digitalisering.

Table 3.3: Guidance and sectoral codes across the focus countries

Jurisdiction	Instrument	Content and status
Philippines	NPC–Insurance Commission MoA (December 2024) and Joint Advisory 2025-001 (11 March 2025)	Joint, non-binding guidance on privacy-enhancing technologies for insurers and other Insurance Commission-supervised entities and their processors.
Philippines	NPC advisory opinions to the Bangko Sentral ng Pilipinas (Central Bank of the Philippines) (BSP)	Unilateral NPC opinions, usually requested by individual controllers; described by interviewees as relied on by BSP-supervised institutions as interpretive guidance.
Kenya	Office of the Data Protection Commissioner (ODPC) Guidance Note for Digital Credit Providers (December 2023)	Unilateral ODPC guidance that cross-references CBK rules; requires digital credit providers to register with the ODPC as controllers or processors even below the general size and turnover thresholds.
South Africa	Code of Conduct for the Credit Bureau Association (approved September 2022), alongside the Banking Association South Africa (BASA) code approved at the same time	Binding codes issued under POPIA's code mechanism; the credit bureau code governs processing in compliance with both POPIA and the National Credit Act.
Uganda	Uganda Microfinance Regulatory Authority (UMRA) digital money lending guidelines (2024); UMRA's functions are now exercised by the Ministry of Finance, Planning and Economic Development's Microfinance Regulation Department	Include data protection obligations in the licensing application requirements for Tier 4 lenders; how far this is enforced has not been assessed.
Nigeria	FCCPC Digital, Electronic, Online or Non-Traditional Consumer Lending (DEON) Regulations 2025	Require evidence of NDPA compliance (a compliance audit report and privacy impact assessment from a licensed Data Protection Compliance Organisation) as a condition of approval; enforcement resumed on 20 July 2026 after the Federal High Court dismissed a challenge to the Regulations.

Source: CCAF & Fii. Drawn from public instruments and interviews; examples are illustrative, not exhaustive.

The common thread is that an instrument nominally about inter-agency cooperation, or about a single authority's own remit, ends up setting compliance expectations for financial firms. Licensing is a recurring route: both Uganda and Nigeria fold data protection requirements into the conditions for operating in the financial sector. In Uganda the requirement applies at the licensing application stage; how far either is enforced has not been assessed.

Box 5: Developed-market comparators: bilateral guidance protocols

Outside the focus countries, bilateral instruments are often used to the same end. Under the UK's ICO–FCA MoU, the two authorities agree to support one another and to draw on their respective expertise in investigation and enforcement.

In the Netherlands, the data protection authority and De Nederlandsche Bank signed a revised cooperation protocol on 3 October 2022, extending their earlier payment-services cooperation across the full breadth of both supervisory mandates; under it, each passes to the other any reports and complaints that fall within the other's remit.[38] Arrangements of this kind give firms a clearer, jointly held view of what compliance requires.

Shared and joint sandboxes

Since the UK's FCA launched its regulatory sandbox in 2016, sandboxes have become a common way to test new technologies and regulatory approaches in a controlled setting with selected firms, particularly in financial services. Across the focus countries, sandboxes for financial services and data protection generally run separately, where a data protection sandbox exists at all. Table 3.4 summarises the position.



38. "Samenwerkingsprotocol tussen de Autoriteit Persoonsgegevens en De Nederlandsche Bank N.V.," Staatscourant 2022, 28259, art. 1, https://zoek.officielebekendmakingen.nl/stcrt-2022-28259.html; De Nederlandsche Bank, "Intensievere samenwerking DNB en de Autoriteit Persoonsgegevens," 1 November 2022, https://www.dnb.nl/nieuws-voor-de-sector/toezicht-2022/intensievere-samenwerking-dnb-en-de-autoriteit-persoonsgegevens/.

Table 3.4: Sandbox provision across the focus countries

Jurisdiction	Financial sandbox	Data protection sandbox	Joint or coordinated mechanism
Philippines	Yes (BSP)	Yes (NPC)	None; the two run separately
Brazil	Yes (BCB)	Yes (ANPD)	None; the two run separately
South Africa	Yes (multi-agency)	No	Multi-agency financial sandbox shows the capacity to onboard several agencies
Nigeria	Yes	No	None
Uganda	Yes	No	None
Indonesia	Yes	No	None
India	Yes	No	None
Pakistan	Yes	No	None

Source: CCAF & Fii. Drawn from public instruments and interviews; examples are illustrative, not exhaustive.

The pattern is one of parallel provision at best: even where both authorities run sandboxes, as in the Philippines and Brazil, they operate them independently. Yet the emerging, data-intensive models that most need joint testing, such as open banking, digital ID and AI governance, are those that span both mandates. South Africa's multi-agency financial sandbox already shows the technical capacity to bring several regulators onto a shared platform.

Box 6: Bringing the sandboxes together

Two models suggest how the two sides might share this space. In the UK, the FCA and the ICO run separate sandboxes, but through the DRCF's AI and Digital Hub, a one-year pilot launched in April 2024, they and two other regulators (the CMA and Ofcom) gave innovators joint informal advice on questions spanning their remits.[39]

Spain goes further: its financial authorities operate the sandbox, while the Spanish Data Protection Agency (AEPD) is a voting member of the sandbox's Coordination Commission.[40] Both point towards a workable middle ground between wholly separate sandboxes and a single merged one. The United Kingdom also shows how layered support can work.

Firms can draw on regulatory sandboxes for live testing, run by both the FCA and the ICO; on advice services for innovators (the FCA's Innovation Pathways and the ICO's Innovation Advice service); and on the FCA's Digital Sandbox, which gives firms synthetic data sets on which to test and develop products.[41]

Information sharing between authorities

The fourth category of coordination mechanism considered here is information sharing between authorities, which takes two forms that the law treats differently. In the first, authorities enable or require sharing between regulated firms, as with fraud intelligence or credit information, and must settle between them what may be shared, by whom and under what safeguards. In the second, authorities share information with one another about the firms they supervise, for supervision, intelligence, investigation and enforcement: for example, when a cyber breach at a bank engages both the financial supervisor and the data protection authority. The law does not always provide a clear legal basis for this second form, particularly where supervisory information is confidential or case-level personal data are involved. MoUs, MoAs and joint statements can set out how authorities will use the powers they have, but cannot supply a gateway the law does not provide. Where a firm legal basis exists, some authorities have gone further and built the exchange into shared systems, such as a common reporting platform or a secure channel with defined access rights, which makes the exchange more routine and easier to audit.

39. DRCF, "The DRCF Launches Informal Advice Service to Support Innovation and Enable Economic Growth," press release, 22 April 2024, https://www.drcf.org.uk/publications/press-releases/the-drcf-launches-informal-advice-service-to-support-innovation-and-enable-economic-growth.

40. Orden ETD/1305/2020, de 29 de diciembre (Spain), arts. 3, 4, and 6, BOE-A-2021-132, https://www.boe.es/buscar/act.php?id=BOE-A-2021-132.

41. Financial Conduct Authority (FCA), "FCA Innovation Hub," accessed 21 October 2026, https://www.fca.org.uk/firms/innovation; Information Commissioner's Office (ICO), "ICO Innovation Services," accessed 21 October 2026, https://ico.org.uk/about-the-ico/what-we-do/ico-innovation-services/.

The clearest common ground is anti-money laundering. All ten focus countries have AML/CFT laws that establish a financial intelligence unit (FIU) and allow it to share information with other competent authorities,[42] and international standards such as the FATF Recommendations set expectations for when and how agencies share data, and for how long they may be retained. As these systems become more automated, the underlying infrastructure is becoming more complex.

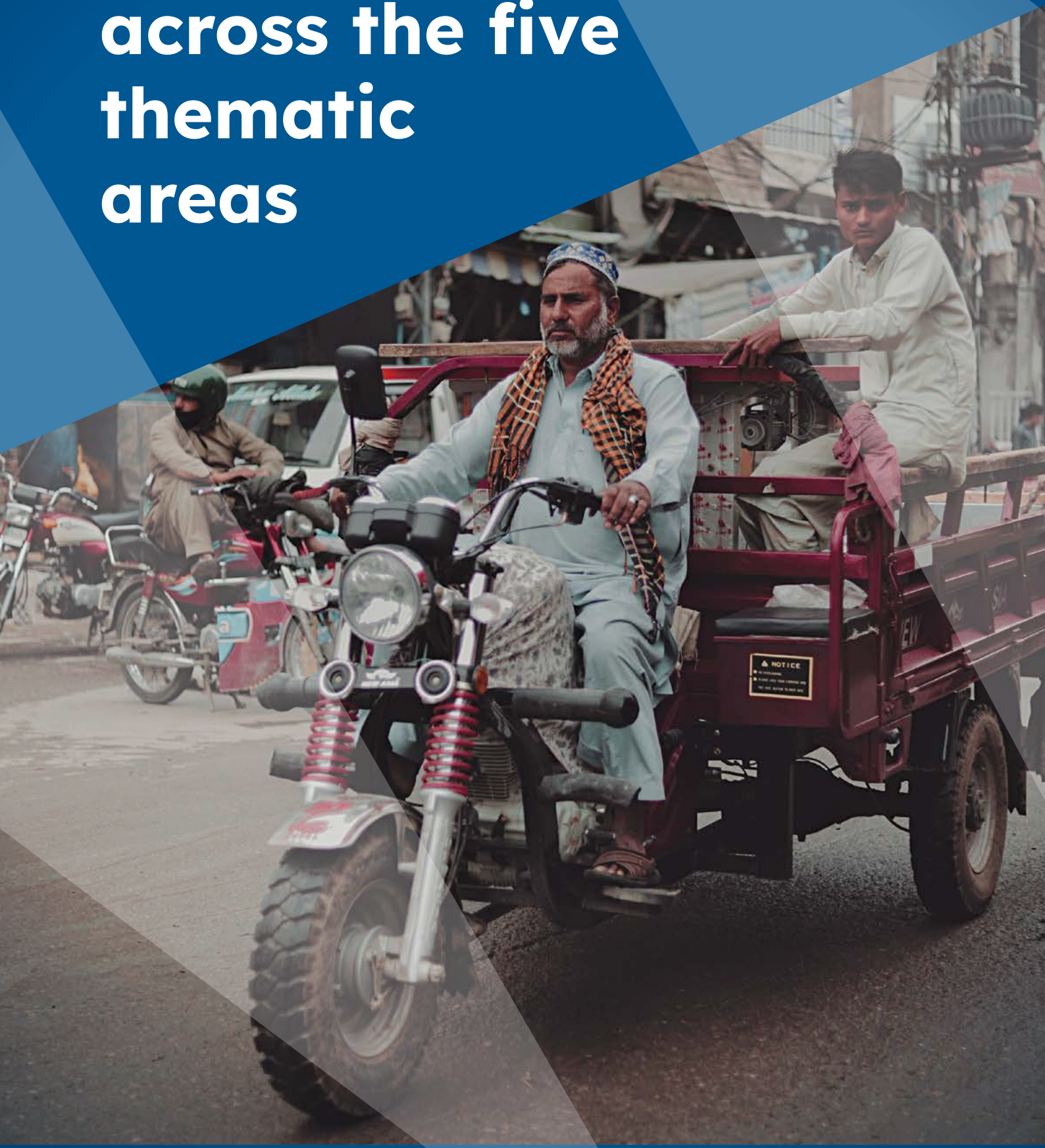
Open finance and digital identity wallets add to the first form rather than the second: they move customers' data between firms at the customer's direction (Section 4.3), not between authorities. Several focus countries are moving from physical identity documents towards digital IDs that let consumers hold personal data in a digital wallet and share them when required, which will make the rules for sharing between firms more important.



42. Brazil, Law No. 9,613 of 1998; Ethiopia, Proclamation No. 780/2013; India, Prevention of Money-Laundering Act, 2002; Indonesia, Law No. 8 of 2010; Kenya, Proceeds of Crime and Anti-Money Laundering Act, 2009; Nigeria, Nigerian Financial Intelligence Unit Act, 2018; Pakistan, Anti-Money Laundering Act, 2010; the Philippines, Anti-Money Laundering Act of 2001 (RA 9160); South Africa, Financial Intelligence Centre Act 38 of 2001; Uganda, Anti-Money Laundering Act, 2013. Each establishes or empowers a financial intelligence unit and provides for its dissemination of information to other competent authorities.

Chapter 4

Gaps in coordination across the five thematic areas

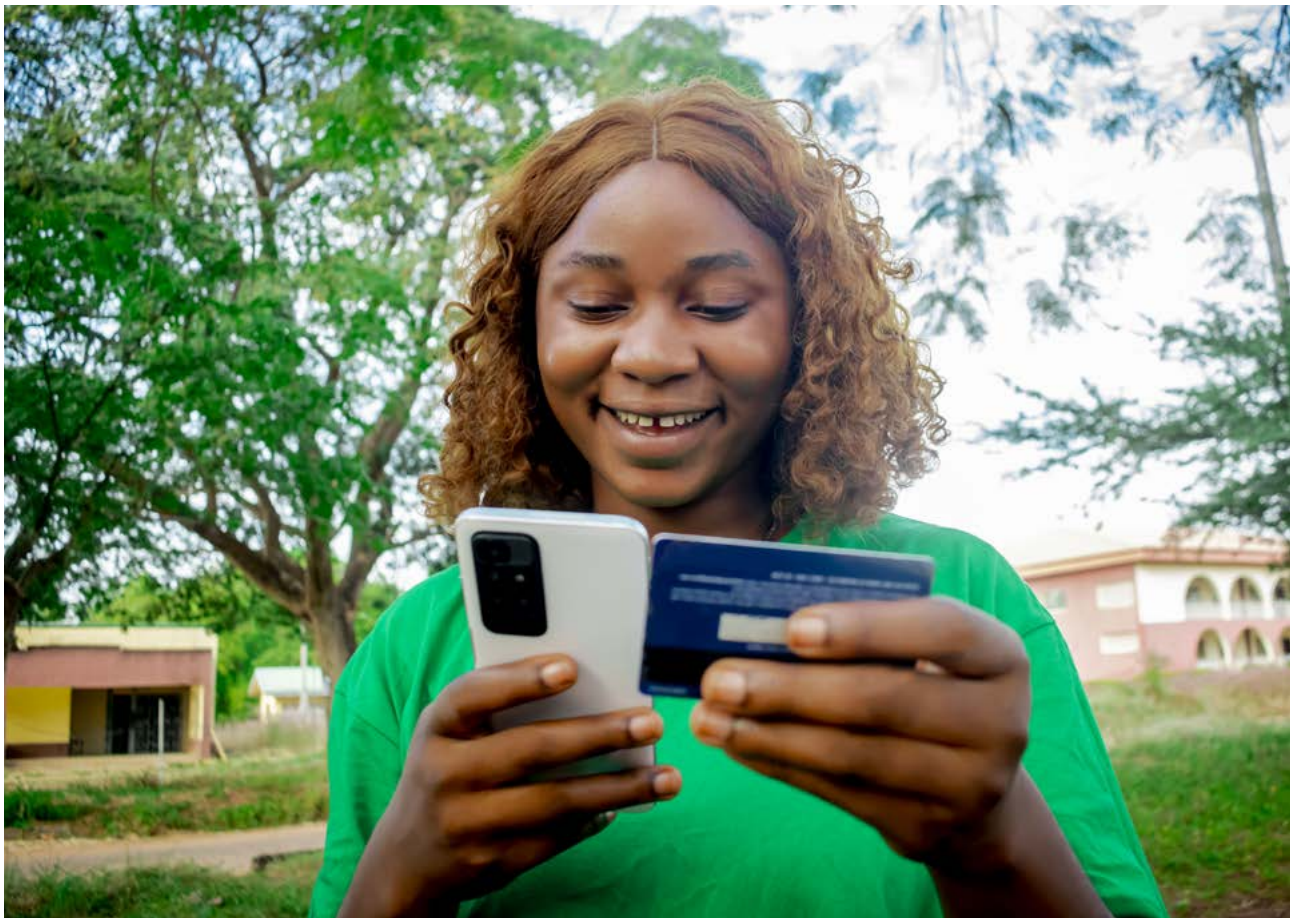


4. Gaps in coordination across the five thematic areas

Section 3 described the coordination mechanisms identified in this study. This section turns to the many areas where coordination is ad hoc, insufficient or absent, and identifies where gaps, fragmentation and under-institutionalisation appear. Section 5 then considers the costs and missed opportunities that flow from these shortcomings, and Section 7 examines their underlying causes.

Each of the five thematic areas below, taken in turn in Sections 4.1 to 4.5, documents two things: the overlap (the points at which the two regimes meet and the questions this raises) and the institutional failure to address it. Cutting across these themes are three structural and procedural patterns that recur throughout the focus countries: coordination that exists on paper but not in practice; unresolved overlaps and tensions between remits; and the absence of a permanent, dedicated data protection authority. These include examples of parallel, uncoordinated registration schemes; regulators publicly raising concerns regarding each other's regulations; and one regulator proceeding with action in an area of joint interest without consulting or coordinating with a counterpart, or proceeding even absent a counterpart to consult or coordinate with. The discussion draws them out in boxes at the points where each is most clearly illustrated.

These are not the only areas in which DP–FS coordination falls short. They are highlighted because they are the most significant, recur most consistently and best represent the shortcomings observed. The annex materials provide fuller detail, including further instances of gaps, fragmentation and under-institutionalisation.



4.1 Digital identity, KYC and AML/CFT

AML/CFT is perhaps the clearest case in which DP–FS coordination matters to the success of both frameworks. AML/CFT regimes require firms to collect, retain and, in some cases, disclose large volumes of sensitive information for defined financial-integrity purposes. Data protection law generally recognises processing required by law, but asks whether each requirement is necessary and proportionate to its purpose, how long records are kept and for what, and what safeguards apply when information is shared.

Settling those questions calls for coordination across several policy and operational areas, including:[43]

- Structuring the data collection, retention and sharing requirements of the underlying AML/CFT regime to meet both AML/CFT and data protection goals.
- Calibrating exceptions and carve-outs in data protection frameworks so that they clearly allow for AML/CFT compliance without undermining the broader framework.
- Promoting the adoption of privacy-enhancing technologies (PETs), such as encryption, pseudonymisation, and privacy-preserving analytics, that reduce the privacy risk of AML/CFT data processing while preserving the data utility compliance requires.
- Harmonising oversight, including supervision and enforcement, around dual compliance, so that firms receive consistent expectations from both authorities.
- Communicating the combined requirements of both frameworks to market participants in a way that supports efficient and effective dual compliance.

The interface is not confined to onboarding. AML/CFT obligations continue through the customer relationship: ongoing monitoring of transactions, suspicious transaction reporting to the financial intelligence unit, and record-keeping for at least five years after the relationship ends under FATF Recommendation 11, with longer periods in some national laws. Each engages data protection questions of purpose, retention and access, and each is shaped by financial-sector rules that the data protection authority rarely sees in draft.

There is no single right answer to any of these challenges.[44] Nor are they self-contained; a carve-out crafted for AML/CFT risks becoming a precedent for other public-interest claims on personal data, such as tax, security or broader law enforcement, and a broad exemption can hollow out the framework it sits in. This is one reason to draft exemptions narrowly and jointly, specifying the data, purpose and retention they cover.

43. FATF, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations (adopted 16 February 2012, last updated June 2026), Recommendations 10, 11, and 16, https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html. On the relationship between these requirements and data protection principles, see FATF, Guidance on Private Sector Information Sharing, which states that AML/CFT and data protection and privacy public policy goals are not mutually exclusive and should be balanced https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Private-Sector-Information-Sharing.pdf.

44. This report does not assess whether specific implementations of AML/CFT and fraud controls collect the right amount of data; that is a question for national authorities and international organisations, and one on which specialist views can differ (for example, as to which data fields are most effective and responsive to AML/CFT imperatives in different contexts). This report focuses on how these questions should be addressed, without weighing the merits of various potential answers to those questions.

Coordination is needed not to confirm the obvious but to work through difficult questions that involve balancing values shared across jurisdictions, among them privacy, dignity, financial integrity, financial inclusion, safety and lawfulness.[45]

This is also a challenge that tends to require cross-border cooperation, up to and including global standard-setting, which poses a particular difficulty for EMDEs. With limited access, capacity or standing to participate in key global initiatives, they can find themselves policy takers in the first instance, even as they still coordinate bilaterally, regionally, and globally to keep their AML/CFT and data protection regimes compatible with global standards.

Stakeholders generally agree on three points regarding DP–FS coordination on AML/CFT: that the goals above are achievable; that achieving them is nonetheless a substantial, ongoing undertaking involving many parties; and that the work has not yet been done. Stakeholders reported that, in many EMDEs, coordination shortcomings, and in some cases open disagreement between regulators, have tended towards the outcome they feared, in which regulatory uncertainty leads market participants to maximise data collection and retention at the expense of data protection principles, raising costs and risks for businesses and consumers alike.[46] Part of the explanation may be that sanctions for AML/CFT failures (including personal liability and criminal prosecution at the individual level, and FATF 'greylisting' or 'blacklisting' at the jurisdiction level) were described by stakeholders as weighing more heavily on firms than those for data protection breaches. The asymmetry matters for coordination: where data protection sanctions are markedly weaker, the data protection authority risks a diminished role in cases both authorities pursue or where requirements may be perceived to be in tension, and firms have less reason to weigh its requirements.

The clearest example comes from Nigeria, where, in the absence of any identified coordination mechanism between the Central Bank of Nigeria (CBN) and the Nigeria Data Protection Commission (NDPC), the two clashed publicly over the CBN's requirement, under its Customer Due Diligence Regulations, that financial institutions collect extensive personal data, including customers' social media handles (section 6(a)(iv) of the Regulations), to combat money laundering and other illicit finance.[47]

45. For example, purpose limitation does not in itself confine onboarding data to onboarding. Where AML/CFT law requires monitoring, investigation and reporting for the life of the customer relationship, and those purposes are specified when the data are collected, using verification data for them is not a new purpose. Three cases need distinguishing: use for the purpose specified at collection; use for one of several purposes specified at collection; and later use for a purpose not specified then, which needs its own justification. Marketing, credit scoring, commercial sharing with affiliates and disclosure beyond what a reporting duty requires usually fall in the third group. Lawful retention is also different from lawful reuse: a duty to keep records for five years justifies keeping them, not using them for something else. The line is not always obvious. A fraud flag derived from KYC data and shared with other institutions may fall on either side of it, and deciding which, in a given case, is a question the two authorities are better placed to settle together than any firm is alone.

46. Accumulated customer data are also a target. Identity documents, biometric templates and transaction histories retained for KYC and AML/CFT are valuable to fraudsters and exposed to insiders, including where organised crime infiltrates financial institutions or public agencies. The same is true of what is reported onward. Financial intelligence units receive reports at very large scale: Australia's AUSTRAC received about 398 million reports in 2023–24, almost all of them international funds transfer instructions (AUSTRAC, Annual Report 2023–24). FIU holdings have leaked, as the 2020 FinCEN Files showed (International Consortium of Investigative Journalists, FinCEN Files, 2020). Each addition to what is collected, kept and reported therefore adds security risk as well as compliance value. The FATF's draft R.16 guidance recognises this in asking for stronger safeguards for higher-risk data elements (FATF, Guidance on Implementation of Recommendation 16, sec. 9.4). Both authorities have a stake here: a breach of these stores is at once a data protection failure and a source of the fraud financial supervisors are trying to prevent.

47. Central Bank of Nigeria (Customer Due Diligence) Regulations, 2023, sec. 6(a)(iv), https://www.cbn.gov.ng/Out/2023/CCD/CBN%20Customer%20Due%20diligence%20Reg.%202023-combined.pdf, requiring financial institutions to obtain and verify customers' social media handles as part of customer identification. The Regulations complement the CBN's Anti-Money Laundering, Combating the Financing of Terrorism and Countering Proliferation Financing of Weapons of Mass Destruction in Financial Institutions Regulations, 2022. On the NDPC's position, see the statement of the National Commissioner reported in Blueprint, 30 June 2023, https://www.blueprint.ng/cbn-directive-on-bank-customers-social-media-handle-illegal-ndpc/.

The requirement was challenged in court by a private citizen on constitutional privacy grounds. The CBN's defence was not that AML/CFT objectives override data protection rights, but that social media handles are not sensitive information in the first place, comparable to an email address or phone number already collected for KYC, so no privacy interest was engaged. The court struck the suit out on the CBN's preliminary objection: it held that the Regulations are directed at financial institutions rather than private individuals such as the applicant, and that he had not shown that any bank had asked him for his handle. In passing, it described a social media handle as being 'of the same genre' as an email address or phone number. The requirement remains in place.[48] The key point is that the public record shows regulatory disagreement followed by private litigation, and no forum in which the two authorities settled the question: the only forum the dispute is known to have reached was a private citizen's constitutional lawsuit, which ended on procedural grounds without engaging the necessity and proportionality question the NDPC had raised.

A more fundamental version of the same problem is visible in India, where for years there was no institutional gap to bridge because there was no institution to coordinate with at all. In June 2017, the Prevention of Money-laundering (Maintenance of Records) Second Amendment Rules amended Rule 9 of the 2005 Rules to require banks to link customers' accounts to Aadhaar, a national identity number linked to centrally held biometric and demographic records, as part of strengthened customer due diligence. India had no independent data protection authority at the time, so an AML-driven mandate affecting a very large share of account holders proceeded with no data protection authority positioned to weigh in on its implications. The question was resolved, as in Nigeria, through private litigation: within the long-running constitutional litigation over Aadhaar, begun by a retired judge in 2012, the Supreme Court in 2018 struck down the mandatory bank-linkage requirement as disproportionate, building on its 2017 ruling that privacy is a fundamental right.[49] Parliament's response, the Aadhaar and Other Laws (Amendment) Act 2019, permitted voluntary Aadhaar authentication for KYC: again an AML-side legislative change made with no data protection authority in place. India's 2023 data protection legislation creates no express dedicated channel between its new Data Protection Board and AML regulators, and the Board, legally established in November 2025, had no appointed Chairperson or Members at 30 September 2026.

48. Chris Eke v. Central Bank of Nigeria, Suit No. FHC/L/CS/1281/2023, Federal High Court of Nigeria, Lagos Judicial Division (Dimgba J), ruling delivered 16 May 2024 (suit struck out on the CBN's preliminary objection; the court did not decide the merits, although some media reports characterised the ruling as upholding the Regulations). See "CBN Wants You to Link Your Social Media Handles to Your Bank Accounts. A Court Has Said It Is Okay," FIJ, 17 May 2024, https://fij.ng/article/cbn-wants-you-to-link-your-social-media-handles-to-your-bank-accounts-a-court-has-said-it-is-okay/; "Court Upholds CBN's Regulation on Collection of Customers' Social Media Handles," Channels Television, 16 May 2024, https://www.channelstv.com/2024/05/16/court-upholds-cbns-regulation-on-collection-of-customers-social-media-handles/; "Banks Can Demand Customers' Social Media Handles, Court Rules," The Cable, 16 May 2024, https://www.thecable.ng/banks-can-demand-customers-social-media-handles-court-rules/.

49. Prevention of Money-laundering (Maintenance of Records) Second Amendment Rules, 2017, G.S.R. 538(E) (1 June 2017), amending r. 9; Justice K.S. Puttaswamy (Retd) v. Union of India (2019) 1 SCC 1 (Aadhaar judgment of 26 September 2018), holding the mandatory linking of bank accounts to Aadhaar under the amended rule disproportionate.

Mature jurisdictions have not settled this either. In the European Union, the AML directives, the second Payment Services Directive (PSD2) and the General Data Protection Regulation (GDPR) govern overlapping uses of the same customer data, and their interaction has required successive clarification. The European Data Protection Board has issued guidance on the interplay between PSD2 and the GDPR.[50] The Transfer of Funds Regulation states expressly that processing under it is subject to the GDPR, and the European Data Protection Supervisor was consulted before its adoption.[51] Industry groups continue to call for closer alignment of AML/CFT and data protection priorities as the new Anti-Money Laundering Authority takes up its role.[52] The EU experience shows that coordination is a continuing task rather than a one-time fix, and it shows the value of settling the interface in the instrument itself.

Efforts at the global level are emerging, though they pull in more than one direction. In June 2026 the FATF published draft guidance on implementing revised Recommendation 16 for consultation.[53] Its chapter on data protection builds on the FATF's earlier work on data protection, notably its 2021 stocktake on data pooling, collaborative analytics and data protection and its 2022 report on private-sector information sharing.[54] It treats data protection as applying throughout the handling of payment information and sets out expectations on minimisation, proportionality, accuracy, retention and transparency. It also encourages measures to ensure compatibility between AML/CFT and data protection rules, promotes safeguards, and calls for close coordination between AML/CFT and data protection authorities, including to analyse gaps and resolve conflicts, and with counterparts abroad. However, some of the language in the draft has been interpreted more critically, as creating imbalance and even establishing precedence between the two regimes.[55] Expert stakeholders consulted for this research differed on both the current and the likely future state of AML/CFT requirements. That lack of consensus itself suggests that greater coordination is needed internationally, as well as regionally and nationally, to provide clarity and certainty and to ensure that compliance outcomes satisfy both financial and data protection mandates.

50. European Data Protection Board, Guidelines 06/2020 on the Interplay of the Second Payment Services Directive and the GDPR, version 2.0 (15 December 2020).

51. FATF, Guidance on Implementation of Recommendation 16, box 16.

52. Global Coalition to Fight Financial Crime, "Aligning EU's AML/CFT and GDPR Priorities to Ensure an Effective and Coherent Anti-Financial Crime Framework: Open Letter," 5 March 2026, https://www.gcffc.org/articles-and-publications/aligning-eus-aml-cft-and-gdpr-priorities-to-ensure-an-effective-and-coherent-anti--financial-crime-framework---open-letter.

53. FATF, "FATF Launches Public Consultation on Guidance to Increase Payment Transparency," 24 June 2026, https://www.fatf-gafi.org/en/publications/Fatfrecommendations/R16-Public-Consultation-June-2026.html. The consultation closed on 21 August 2026. The explanatory memorandum accompanying the draft Guidance states that it explains how AML/CFT and data protection and privacy objectives are mutually reinforcing, and provides actionable guidance to stakeholders in establishing relevant legal and operational frameworks: FATF, Public Consultation: Guidance on Implementation of Recommendation 16—Explanatory Memorandum (June 2026), https://www.fatf-gafi.org/content/dam/fatf-gafi/public-consultation/Public%20consultation%20explanatory%20memorandum.pdf.coredownload.inline.pdf. The revisions to Recommendation 16 were agreed in June 2025, with jurisdictions expected to be ready to implement by the end of 2030: FATF, "FATF Updates Standards on Recommendation 16 on Payment Transparency," 18 June 2025, https://www.fatf-gafi.org/en/publications/Fatfrecommendations/update-Recommendation-16-payment-transparency-june-2025.html. The FATF Plenary of June 2026 separately approved a Global Overview of Public and Private Sector Partnerships and Data Protection Arrangements, published in July 2026.

54. FATF, Stocktake on Data Pooling, Collaborative Analytics and Data Protection (July 2021), https://www.fatf-gafi.org/en/publications/Digitaltransformation/Data-pooling-collaborative-analytics-data-protection.html; FATF, Partnering in the Fight against Financial Crime https://www.fatf-gafi.org/en/publications/Digitaltransformation/Partnering-in-the-fight-against-financial-crime.html.

55. See, e.g., Ivo Jeník and Louis de Koker, "Is Integrity First, Data Protection Second a Wise Approach?" CGAP, 18 August 2026, https://www.cgap.org/blog/is-integrity-first-data-protection-second-wise-approach.

The GPA likewise launched a new international initiative in 2026 exploring the intersection between data protection and AML/CFT frameworks; its sub-working group on privacy and integrity in partnership will examine AML/CFT information-sharing in practice, with a view to improving clarity, trustworthiness, legal grounding, and the protection of individual rights while maintaining effective financial-crime enforcement.[56]

That global standard-setting bodies are themselves still working on this challenge suggests it is not a maturity gap unique to EMDEs but an unresolved design problem in financial regulation generally, of which the EMDE experience is a more visible and acute expression.[57] A pessimistic reading is that EMDEs, already facing the coordination deficits described in this report, must wait on an unfinished global reference point before addressing them. A more optimistic reading is that there is an opportunity now: because so many of the ten countries are at an early stage in establishing DP–FS coordination, there is a real chance to design FATF- and GPA-informed mechanisms from the outset, rather than retrofitting them onto mature institutions in the way the EU, the UK, and other developed economies are now having to do.[58]

Box 7: When mandates overlap: jurisdictional competition and double jeopardy

The overlap between financial and data protection regulation is structural; conflict between their requirements generally is not. The two mandates overlap by design, and in most focus countries no domestic rule allocates precedence between them (some read the FATF's draft R.16 guidance as proposing one; see Section 4.1), so the same conduct can engage several authorities at once with no agreed order for who acts first, who defers, or whose finding controls.

Even where privacy carries constitutional status, as in Kenya, precedence is not simply resolved in its favour but is established piecemeal, through litigation and targeted carve-outs, not by any general ex ante rule. A single incident (a mishandled onboarding, a compromised lending app or a poorly governed data-sharing arrangement) may at once raise unlawful-processing questions for a data protection authority, operational-risk questions for a financial regulator, and control-failure questions for a consumer protection or financial-intelligence body. The consumer experiences one harm; the system treats it as several separate matters.

56. FATF, Partnering in the Fight against Financial Crime https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf.

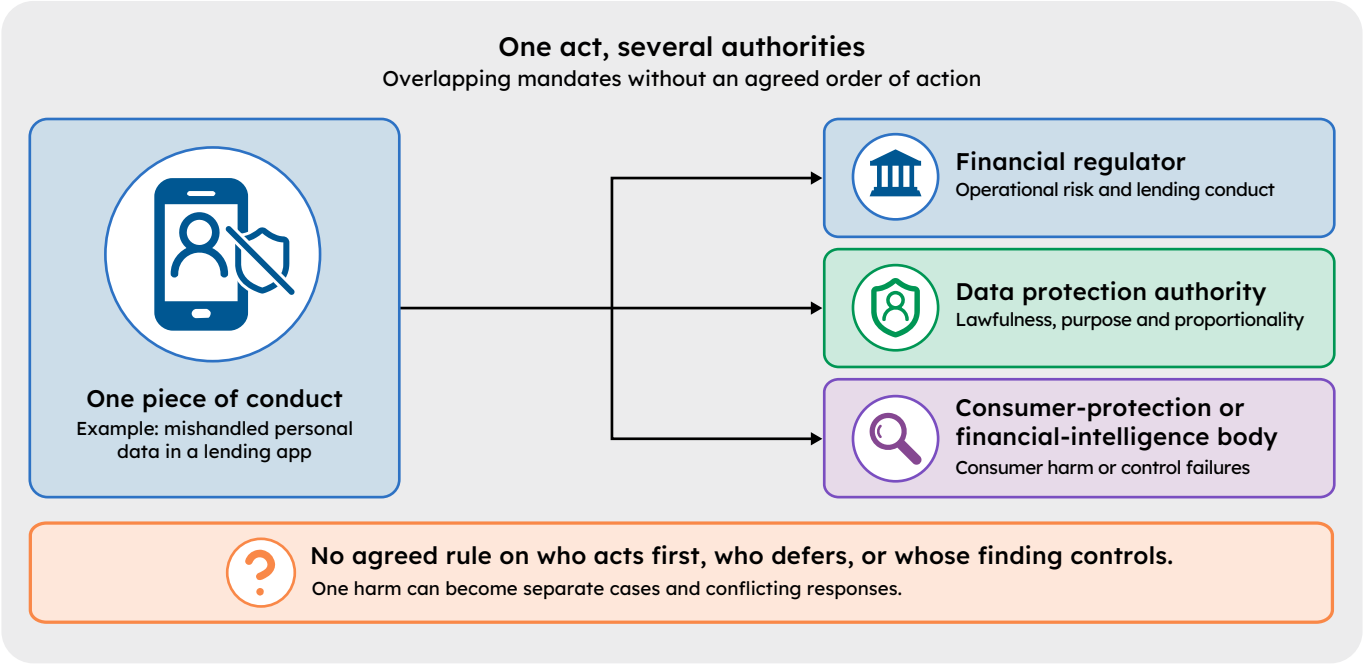
57. For one view on the legitimacy of public–private personal data sharing under the EU's anti-money-laundering framework, see Magdalena Brewczyńska, "Policing via Banks: The Question of Legitimacy of Personal Data Sharing" (PhD diss., Tilburg University, 2024), https://research.tilburguniversity.edu/en/publications/policing-via-banks-the-question-of-legitimacy-of-personal-data-sho/.

58. On the EU experience, see Global Coalition to Fight Financial Crime, "Aligning EU's AML/CFT and GDPR Priorities," written as the European Banking Authority's AML/CFT mandate passed to the new Anti-Money Laundering Authority at the end of 2025.

For firms, the main risk is double jeopardy: in some cases a firm can be sanctioned twice, by two authorities applying two different tests, for a single act. Kenya's Worldcoin episode shows a related problem, active competition for the same jurisdiction, with the data protection, communications, and capital-markets authorities each asserting jurisdiction over the same biometric-data operation.[59] The overlap recurs within the financial side too, as where Kenya's Central Bank and Communications Authority exercise parallel oversight of the same mobile money channel.[60]

Adjacent regulators add further layers: digital-identity authorities supply the enrolment and verification data that financial institutions consume, and telecommunications regulators often hold their own data protection powers over the mobile channels through which much of the market is served.

Figure 4.1: One act, several authorities



Source: CCAF & Fii.

59. ODPC (Kenya), enforcement action against Tools for Humanity Corporation concerning Worldcoin iris-biometric collection; see also the National Assembly Ad Hoc Committee inquiry into the activities of Worldcoin in Kenya (2023) and the subsequent High Court proceedings.

60. National Payment System Act, 2011 (No. 39 of 2011) and National Payment System Regulations, 2014 (CBK); Kenya Information and Communications Act (Cap. 411A) (Communications Authority of Kenya).

4.2 Fraud

Fraud merits separate treatment from AML/CFT even though the two are legally linked. Fraud is typically a predicate offence to money laundering. It also raises immediate consumer protection and business-loss concerns whether or not a laundering connection is ever established. A single account opened with a stolen identity harms the identity holder, exposes the institution and may facilitate laundering. The same identity, transaction and device data may inform each response. Yet establishing whether someone is the legitimate account holder is a different question from assessing whether funds are criminal proceeds.

This raises distinct data protection questions. Security matters because fraud often begins with compromised data; accuracy and correction matter because the person named in a fraud record may be the victim rather than the perpetrator. The coordination problem also differs: whereas AML/CFT information-sharing is substantially structured around statutory reporting to public authorities, effective fraud prevention increasingly depends on the rapid exchange of transactional information, identity attributes, behavioural indicators and risk intelligence. That exchange runs between regulators and law enforcement, between private institutions and across borders.

As digital payments, mobile money and instant-payment systems expand, fraud can move across banks, payment providers, telecommunications networks and identity systems faster than controls at any single institution can respond, and it crosses national borders almost as easily.[61] The central question is therefore not simply whether information can be disclosed to a public authority, but how it can move across the fraud-prevention chain quickly enough to prevent harm while remaining necessary, proportionate, secure, and purpose-bound.

Across the ten focus countries, financial-sector authorities, FIUs, cybersecurity bodies and law enforcement generally have more developed channels for coordinating on fraud with each other than any of them has with the data protection authority (DPA). The recurring gap concerns the position of the data protection authority within this architecture: it typically sets the general rules on lawful processing, security, proportionality, and individual rights, and may reappear when fraud produces a breach or complaint, but is less consistently involved in how transaction monitoring, fraud profiling and cross-institutional sharing are designed, or in setting the point at which suspicious indicators may be linked to identifiable individuals. The problem is therefore one of timing and integration rather than a complete absence of coordination.

61. On the cross-institutional character of contemporary payment fraud and the resulting information-sharing problem, see FATF, Partnering in the Fight against Financial Crime https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf.

Closing that gap does not necessarily mean placing the data protection authority inside live monitoring or individual investigations, which are reasonably seen as matters for financial-sector bodies and law enforcement and where speed matters most. Its contribution is likely greatest in framework design, in reviewing whether a sharing arrangement is necessary and proportionate, in audit and systemic supervision, and in complaints. The aim is involvement at defined triggers rather than routinely. Examples include the creation or material change of a sharing arrangement; a new data source or profiling technique; a change to the threshold at which indicators are linked to individuals; and recurring complaints from people wrongly flagged (see Recommendation 3). Table 4.1 summarises the position across the ten countries.

This matters because many fraud controls work by collecting, linking and sharing personal data, and some of the most effective use more of it than institutions would otherwise hold. Device and behavioural profiling, cross-institution mule-account databases, telecoms data on SIM swaps and payee-verification checks each improve detection. Each also raises questions of necessity, accuracy, retention and correction for the people they touch. The effect can also run the other way: once collected data leaks, or is accessed by insiders, it becomes raw material for further fraud, so the design of these controls, and of the digital identity systems that feed them, matters as much as their reach. The Consultative Group to Assist the Poor's (CGAP) review of fraud solutions identifies this trade-off directly.[62] It is a reason for authorities to design these controls with both authorities' questions in view, and on evidence of what works.[63] Privacy-enhancing technologies, such as tokenised or hashed identifiers for matching, pseudonymisation, federated analytics and secure multi-party computation, may enable institutions to detect shared fraud patterns without pooling raw customer data, although hashing or pseudonymisation is not automatically anonymisation or a lawful basis for sharing, and their benefits must be tested rather than assumed in each case.



62. CGAP, Solutions to Protect Consumers from Fraud in Digital Finance, working paper (May 2026), https://www.cgap.org/research/publication/solutions-to-protect-consumers-fraud-in-digital-finance.

63. The design stage is critical. Data protection by design means building necessity, minimisation, access control and deletion into a sharing arrangement from the start. Many stakeholders drew attention to privacy-enhancing technologies as one set of tools for doing so. They potentially allow institutions to detect shared fraud patterns without pooling raw customer data; examples include tokenised or hashed identifiers for matching, pseudonymisation, federated analytics and secure multi-party computation. They do not replace a lawful basis or the other safeguards, as the FATF's draft R.16 guidance notes (sec. 9.4). Further, their benefits should be tested rather than assumed: a pilot should state the problem it addresses and measure detection value, error rates, residual re-identification risk and cost. These techniques work best when chosen as a sharing arrangement is designed, not added once it is running. That design stage is where data protection input is most valuable and, as Table 4.1 shows, where it is least often present.

Table 4.1: Fraud coordination and the data protection authority: summary

Jurisdiction	Main fraud coordination actors	Data protection authority's position	Nature of the gap
Brazil	BCB (Pix rules, MED); COAF	ANPD has clear jurisdiction	Interface for blended incidents underdeveloped
Ethiopia	NBE; Financial Intelligence Service	ECA; no formal fraud-sharing arrangement	Coordination still forming
India	RBI; FIU-IND; I4C	Board established; no members at cut-off	Authority outside the architecture
Indonesia	OJK; Anti-Scam Centre; PPATK	Authority not yet established	Sequencing
Kenya	Financial Reporting Centre; CBK	ODPC role in FRC sharing untested	DP oversight of sharing not built in
Nigeria	CBN; NFIU; NIBSS	No formal NDPC role identified	Public–public gap
Pakistan	SBP; SECP; FMU	No authority	Sequencing
Philippines	BSP; CICC; AMLC	NPC lawyers assigned to Cybercrime Hub (2022 MoA)	Strongest integration; fragmented within FS
South Africa	FIC; FSCA; PA; SABRIC	Information Regulator an observer on one committee	DP expertise not embedded
Uganda	BoU; FIA; UCC	Case-based, including breach notification	Not institutionalised

Source: CCAF & Fii. The full table, with sources, is in Appendix Table 1.

Two features stand out across the table. The extent of DPA integration varies widely, from the Philippines, where formal cooperation and reciprocal training place data protection expertise inside cybercrime structures, to Pakistan and Ethiopia, where the interface is either sequencing-constrained or barely formed. And the public–public gap is clearest where fraud-intelligence systems pool identifiable data across the financial sector at scale without a defined role for the authority whose remit most directly engages accuracy, retention, proportionality and data-subject rights.

Taken together, the cases suggest the next coordination challenge is increasingly private–private as well as public–public. A scam may originate through a platform, compromise an identity credential, target an account at one institution, move funds through another, and disperse them through several more. No single institution necessarily holds enough information to see the whole pattern, yet allowing all participants to pool identifiable customer information indiscriminately would create its own risks. The appropriate question is therefore not whether fraud prevention needs 'more' or 'less' data-sharing in the abstract, but what degree of identification is necessary at each stage.

Minimisation is not confined to sharing: it governs what fraud controls collect in the first place, and how that information is linked, classified, retained and used. Where information must move between institutions, minimisation need not mean that less of it moves, but that what is exchanged takes the least identifying form capable of resolving the question being asked. One way to achieve this is a staged sequence: institutions first identify a pattern across transactions; then determine whether a particular indicator, account, device or credential is implicated; and only once a threshold is met connect that indicator to an identified individual. Such a pattern–indicator–identity sequence could allow cross-provider fraud to be identified without making identifiable customer information the default unit of exchange, though whether it suits a given arrangement depends on the type of fraud, how quickly a response is needed and who is party to the exchange. Tokenised credentials extend the same logic: a customer's verified attribute, such as a confirmed identity or a passed fraud check, can be shared as a token that confirms the fact without passing on the underlying data. Common governance conditions would help make such sharing sustainable: reciprocity as a signal of proportionality, so that arrangements are collective; purpose-binding and retention or sunset rules, so that fraud databases do not become indefinite repositories of allegations; and, where competitors share a platform, documented information barriers preventing repurposing for commercial coordination or unrelated profiling.

> "Voluntary codes must be bridges not an endpoint … they need a regulator 'safe harbour' signal … or firms will keep treating them as best-effort rather than as a governance basis they can rely on."

The cases also point to a more basic interoperability problem: institutions need a common language for the fraud they are trying to prevent. Account takeover, identity fraud, authorised push-payment scams, phishing, SIM-swap fraud, impersonation, and money-mule activity involve different actors and may justify different responses, and where institutions classify them differently, statistics become hard to compare and referrals less efficient. The absence of common fraud classifications is therefore not merely a measurement problem; it limits operational coordination and would benefit from greater domestic and, ultimately, international standardisation.[64] A 2026 survey of collaborative analytics platforms for tackling fraud found the same gap: there is no universal common taxonomy for fraud and scam attacks, and changing fraud methods make typologies hard to standardise.[65]

64. On the fraud focus of the revised Recommendation 16 and the accompanying guidance, see FATF, "FATF Launches Public Consultation on Guidance to Increase Payment https://www.fatf-gafi.org/en/publications/Fatfrecommendations/R16-Public-Consultation-June-2026.html Transparency."

65. Nick J. Maxwell and Olivier Kraft, A Survey of Collaborative Analytics Platforms to Tackle Fraud: Towards a Network of Networks, Future of Financial Intelligence Sharing research programme (RUSI, May 2026), 13, 38, https://www.future-fis.com/uploads/3/7/9/4/3794525/publication_version_-_ffis_survey_of_collaborative_analytics_platforms_to_tackle_fraud_2.pdf.

4. Gaps in coordination across the five thematic areas

The practical first step is modest: jurisdictions could develop a shared fraud typology and defined referral pathways linking financial regulators, data protection authorities, cybersecurity bodies, and law enforcement, with common principles governing private–private sharing. The objective is not to make data protection authorities responsible for fraud prevention, but to bring their expertise in at the points where fraud controls shape what happens to people's data: collection, the linking of records, the classification of an account or person as suspicious, the generation of indicators, and decisions based on them. Several of these happen inside a single institution, before any data are shared. One stakeholder observed that legal safe harbours for fraud-related data sharing often already exist, but that regulatory staff and firms' legal, risk and compliance functions do not know where they apply; joint guidance aimed at compliance departments could close part of the gap.

Box 8: Stop scams UK

Stop Scams UK is an industry-led collaboration of banks, telecoms and technology firms formed to stop scams at source.

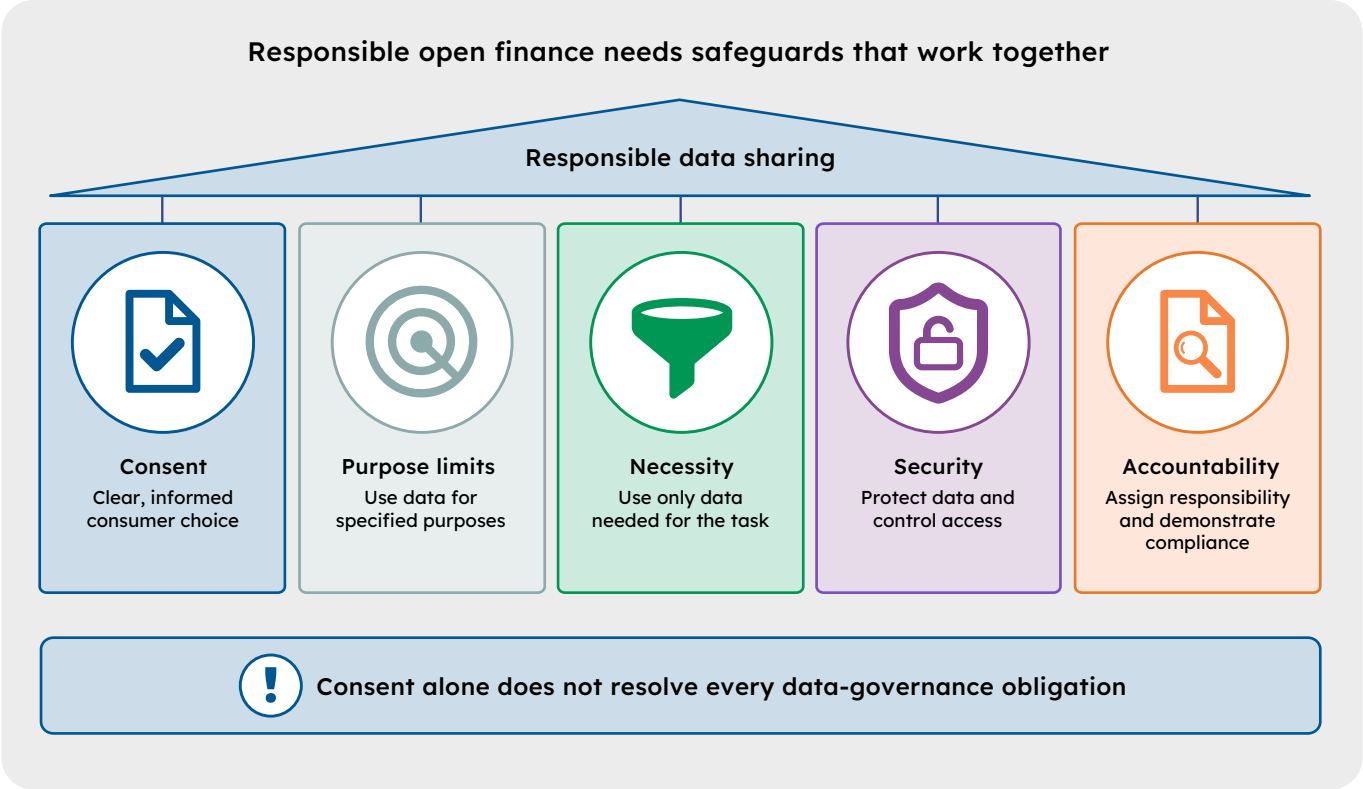
Its members are firms, but it has the support of sector regulators including Ofcom, the Financial Conduct Authority and the Information Commissioner's Office.[66] Its 159 service connects a customer who receives a suspicious call directly to their own bank. It illustrates one working model: the data protection authority supports an industry-led anti-fraud arrangement from outside, alongside the financial and communications regulators, rather than sitting inside it.



66. Stop Scams UK, "About," accessed 29 September 2026, https://stopscamsuk.org.uk/about/.

4.3 Open finance

Figure 4.2: Complementary safeguards underpinning responsible data sharing



Source: CCAF & Fii.

Open finance (arrangements that enable customers to authorise secure access to, and sharing of, their financial data across providers) is increasingly important in most of the focus countries, and credit underwriting is consistently cited as a major application. Schemes differ in whether they are mandated by regulation, voluntary or at pilot stage. Open finance sits at the intersection of financial regulation and data protection, and effective design needs the involvement of both DP and FS regulators.[67] Because most jurisdictions want open finance to support smaller providers and new entrants, coordination also matters for keeping these systems accessible to the responsible providers whose participation is central to their success.

67. For example, open finance compliance may require detailed guidance on how data protection principles apply in specific instances, or may feature additional rules about collection, use, and/or retention beyond those required generally by jurisdictions' data protection schemes.

4. Gaps in coordination across the five thematic areas

Across the ten focus countries, DP–FS coordination on open finance tends to lag the ambition of the underlying policy design, and three patterns recur. First, a sequencing problem: in several jurisdictions, India, Indonesia and Nigeria among them, the financial regulator designed its open banking or payment-API framework before the data protection authority existed in fully operational form, so early design choices were made without a data protection counterpart able to weigh in as an equal, and reconciliation has had to happen retroactively.

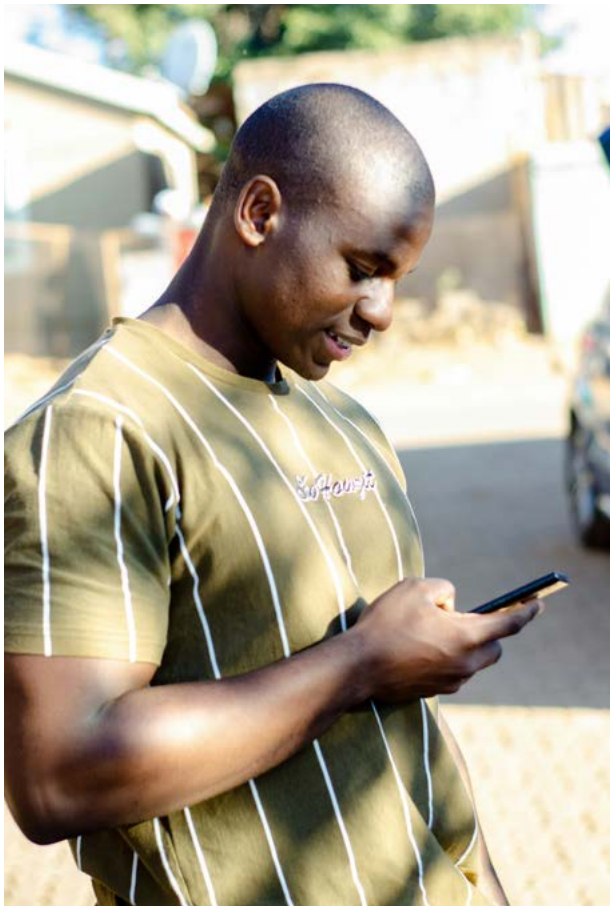
Second, formal coordination mechanisms, where they exist, are more often aspirational than operational: working groups, joint sandboxes and multi-agency councils are proposed, drafted into pending legislation, or described as future requirements, when what is needed is functioning bodies with a track record of resolving live disputes. Third, the simultaneous application of multiple sectoral and general data laws to the same activity tends to leave the burden of reconciliation on regulated entities. Table 4.2 sets out how these patterns present across the ten countries.

Table 4.2: Open finance frameworks and their data protection interface: summary

Jurisdiction	Status at 30 Sep 2026	Lead regulator and framework	Data protection counterpart	Coordination position
Brazil	Live	BCB/CMN open finance rules	ANPD	Statutory duty to coordinate (LGPD art. 55-J)
Ethiopia	No dedicated framework	NBE payments rules	ECA	No arrangement identified
India	Live (account aggregators)	RBI account aggregator directions	Data Protection Board (no members at cut-off)	Separate AA and consent-manager regimes
Indonesia	Live (payment APIs)	BI (SNAP); OJK	Authority not yet established; Komdigi interim	Alignment awaits the authority
Kenya	Proposed	CBK/Treasury draft NPS Policy and Bill (2026)	ODPC	ODPC named among relevant regulators
Nigeria	Framework adopted; rollout unverified	CBN framework (2021) and guidelines (2023)	NDPC	No joint guidance identified
Pakistan	Pilot (sandbox)	SBP sandbox	None	No counterpart yet
Philippines	Pilot	BSP Open Finance Framework (2021)	NPC	Bill proposes BSP-chaired council including NPC
South Africa	Proposed	FSCA-led policy work	Information Regulator	Regulator contributed to policy work
Uganda	No dedicated framework	BoU authorisation	PDPO	Separate processes; no joint body

Source: CCAF & Fii. The full table, with sources, is Appendix Table 2.

The range runs from Brazil, whose data protection law already requires the authority to coordinate with sector regulators, and the Philippines, where a pending bill would create a BSP-chaired Philippine Open Finance Council that includes the NPC, to Pakistan and Ethiopia at the least-institutionalised end, where a data protection counterpart either does not yet exist or has only recently taken on the role. The common thread is that where the financial regulator moved first and the data protection authority arrived later, reconciliation is still being negotiated after the fact. South Africa shows the reverse sequence is possible: the Information Regulator contributed recommendations to the Financial Sector Conduct Authority's (FSCA) open finance work before any framework was adopted.[68]



Consent carries much of the weight in open finance, more than it can bear alone. It is one possible legal basis, not a substitute for purpose limits, necessity, security and accountability. Consent bundled into access to a service, or given by a customer with no real alternative, offers little choice; withdrawing it needs to stop onward flows, not only future collection; and some data must be retained by law whatever the customer decides. Rights of access, correction and deletion also need a route that follows the data from the bank to a third party outside the financial perimeter, including across borders, subject to lawful exceptions. Who answers for each step of that chain is a question the two authorities need to settle together before a framework launches, not after. Several further questions sit between the two regimes: when consent, rather than another lawful basis, is required; how long it remains valid; whether it supports onward sharing along a chain of recipients, for example from a data aggregator to several lenders; and how liability is allocated between the parties. Each calls for a joint position rather than parallel ones.

> "Consent is a legal basis, not a control."

68. The possibility for the reverse is valid, but not yet observed in this context.

Box 9: When data leave the financial perimeter

A financial regulator can protect customer data only within its licensing perimeter. Beyond it, protection depends on an operating data protection authority and on an agreed handover between the two. Open finance often tests this directly, because it may entail customer data to firms outside that perimeter.

Where there is no authority, the perimeter is all the protection there is. At the 30 September 2026 cut-off, India and Indonesia were still establishing their authorities and Pakistan had none; Ethiopia had assigned the function to its communications regulator, so a counterpart exists, though with a young mandate.[69] With no data protection authority in place, one financial regulator described protecting customer data by allowing it to move only between licensed firms, so any other firm seeking access must come under its supervision. Protection then ends where the perimeter does, and open finance narrows to fit it, excluding the unlicensed innovators it was meant to bring in. Interim arrangements do not close the gap. In India, the ministry responsible for the Act makes rules and runs appointments but does not supervise or enforce.[70] In Indonesia, key parts of the new implementing regulation, including its cross-border transfer mechanisms and the authority's input on financial-sector exemptions, cannot work until the authority exists.[71]

The same gap appears where an authority does exist. When a customer directs a bank to share data with a firm outside the perimeter, such as an unlicensed fintech, an analytics provider or a merchant, the financial regulator's oversight stops at the bank, and the data protection authority's general jurisdiction is the only protection for what happens next. Unless the two authorities have agreed how that handover works, neither may be watching the recipient.

The handover is cheapest to design before an authority is operating. One financial regulator in a jurisdiction without an authority proposed that the future authority set the principles and sectoral regulators translate them into operational rules, so that firms answer to one set of principles rather than two. This research found little evidence that India or Indonesia is using the transition to build such arrangements into the new authority's founding design. The point extends beyond open finance: in these countries, AML/CFT, fraud and credit rules are also being written without an operating data protection counterpart.

69. Personal Data Protection Proclamation No. 1321/2024 (Ethiopia), designating the Ethiopian Communications Authority as the authority responsible for data protection regulation and enforcement.

70. Digital Personal Data Protection Act, 2023 (No. 22 of 2023), secs. 18–27, establishing the Data Protection Board of India. The Ministry of Electronics and Information Technology makes rules under the Act and runs appointments to the Board; the Act gives it no supervisory or enforcement role.

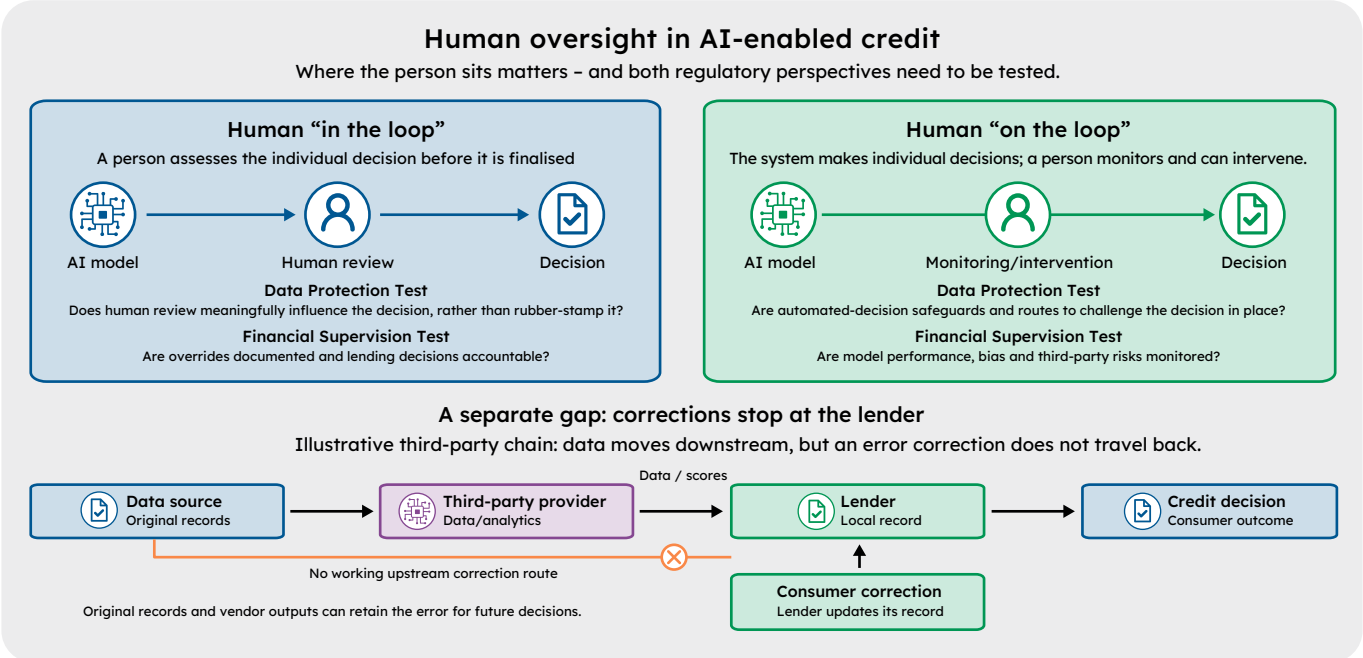
71. Government Regulation 33 of 2026 (Indonesia), arts. 148(1)(d) and (3), 149(1)(d) and (3), and 153 (exemptions for financial-sector supervision and the authority's input); art. 223 (pending the authority's regulations, processing continues so long as it does not conflict with the regulation); on transfers, arts. 165 (sequence), 167–170 (equivalence and standard contractual clauses), and 173 (consent: non-repetitive, limited numbers, notified to the authority); official certified copy, https://static.banyumaskab.go.id/website/file/peraturan_pemerintah_no._33_tahun_2026_100926115902.pdf.

4.4 Credit underwriting and AI

Credit provides one of the clearest examples of the growing interdependence between data protection and financial services regulation. Credit assessment has always depended on the collection and interpretation of personal and financial information, but digital lending and increasingly sophisticated machine-learning and AI techniques are expanding both the quantity and variety of data used in underwriting.[72] These developments create opportunities to improve risk assessment and extend access to consumers poorly served by conventional scoring, but they also amplify longstanding questions of data quality, fairness, privacy, transparency, and accountability.

Here the coordination challenge runs the other way. In several focus countries, general data protection rules already apply to profiling and automated decision-making, while financial-sector rules addressing AI specifically remain less developed. Rather than data-protection regulation following an established financial framework, data protection obligations may already be in force while financial regulators are still working out how AI-specific risks fit into sectoral supervision. The need is therefore not necessarily for new legal principles, but for existing ones to be translated into workable financial-sector expectations.

Figure 4.3: Human oversight models and data correction gaps in AI-based credit decisions



Source: CCAF & Fii.
Tests are illustrative oversight questions; specific duties depend on the applicable framework. Chain shown is a failure scenario

72. Juan Carlos Crisanto, Adrien Currat, Johannes Ehrentraud, and Wenguang Wu, "In Data We Trust? Emerging Policy and Supervisory Approaches to AI Data Use in Financial Services," FSI Insights on Policy Implementation No. 73 (Bank for International Settlements, 26 March 2026), https://www.bis.org/fsi/publ/insights73.htm.

Underwriting data and automated decisions

Stakeholders consistently identified AI-enabled credit underwriting as an area where stronger coordination could be particularly valuable. The upside is significant: new data sources and better analytics may improve lenders' ability to assess consumers with limited conventional histories.[73] So is the downside: AI-enabled underwriting draws on large, heterogeneous datasets, generates complex inferences, and involves external providers, so data-quality problems, excessive collection, discriminatory outcomes, and insufficient transparency can translate directly into consumer harm. Stakeholders raised uncertainty about the standards applicable to AI-driven underwriting, the transparency consumers should receive, and how they should be able to challenge significant decisions, concerns consistent with the wider supervisory picture, in which authorities lean on existing data-management and model-risk frameworks while AI-specific expectations remain uneven.[74]

The problem is often framed as 'alternative' versus 'traditional', but that distinction does not track the risk and is not how practitioners describe their inputs. Two other questions matter more. The first is how far a data source sits from the borrower's financial conduct and from the purpose for which the information was provided. Social media information, device data and phone contents may be technically available without being appropriate for underwriting. The further data travel from their original context, the harder the questions of necessity, proportionality and reasonable expectation become. The second is what kind of statement an input makes about the borrower (see 'Third-Party Data and Vendors' below).

Neither question can be resolved from one regulatory perspective alone. Both connect credit to the AML/CFT questions in Section 4.1, since in each case regulators must decide when personal information is justified by a financial objective. Where these workstreams develop independently, similar data may face different expectations depending on whether they are being considered for credit, due diligence or fraud. Different purposes can legitimately warrant different treatment; the concern is differences that are unexplained or contradictory.

Country experience shows the asymmetry from both sides. India's Reserve Bank Digital Lending Directions, 2025 require data collection through lending apps to be need-based and consented, with an audit trail, and prohibit access to phone resources such as contact lists, call logs, and files, permitting only limited one-time access to a camera, microphone, or location for onboarding or KYC.[75] These are financial-sector rules that are, in substance, also data protection policy. India's broader AI framework, by contrast, remains a set of recommendations rather than a binding rulebook, so highly specific protections coexist with an evolving supervisory architecture.[76]

73. World Bank, The Use of Alternative Data in Credit Risk Assessment: Opportunities, Risks, and Challenges (18 March 2025), https://openknowledge.worldbank.org/entities/publication/7738aa96-6c1b-4fa3-86cb-be30f69d5a30.

74. Crisanto et al., "In Data We Trust?" https://www.bis.org/fsi/publ/insights73.htm

75. Reserve Bank of India (Digital Lending) Directions, 2025, issued 8 May 2025, consolidating and repealing the Guidelines on Digital Lending (2 September 2022) and related circulars. The Directions require data collection to be purpose-specific, consent-based and minimal, with an audit trail; prohibit digital lending apps from accessing borrowers' phone resources including media and files, contact lists, call logs and telephony functions, save for one-time access to the camera, microphone or location for KYC purposes with the borrower's consent; and require all borrower data to be stored in India, with any data processed overseas repatriated and deleted from foreign servers within 24 hours.

76. Reserve Bank of India (RBI), Framework for Responsible and Ethical Enablement of Artificial Intelligence (FREE-AI) Committee Report (2025).

South Africa illustrates the other side: its data protection framework already contains automated-decision safeguards, and the Information Regulator's approved banking Code requires participating banks to notify data subjects, explain the information and reasoning used, and allow representations, translating general principles into credit-relevant terms even without a standalone financial AI regime.[77] That Code also does something distinctive under POPIA, exempting member banks from prior-authorisation requirements while addressing credit-reporting processing, a combination of statutory safeguards, sectoral expertise and regulator-approved industry rules that fits none of the usual categories. Nigeria, similarly, reaches automated decision-making through the data protection side ahead of a sector-specific AI framework, via the right not to be subject to automated decision-making under the NDPA 2023 and mandatory impact assessments for high-risk profiling under its 2025 Directive, though these do not answer every operational question a lender or supervisor faces.[78]

Human oversight is often cited as the safeguard for automated credit decisions, but it takes two forms that offer different assurance: in the first, a human in the loop reviews each decision before it takes effect; in the second, a human on the loop monitors the system and can intervene, while individual decisions proceed without review. High-volume digital lending is likely to run mostly on the second model. The distinction matters to both regulators, for different reasons. Data protection rights concerning decisions based solely on automated processing, such as those under POPIA and the NDPA, may turn on whether a human meaningfully reviews the individual decision. A financial supervisor will ask instead whether oversight can detect drift, bias or error across the portfolio. A lender can satisfy one test without the other, which makes this a natural subject for joint guidance.

Who should lead on what follows from mandates rather than technology. Generally, DPAs' mandates make them best placed to judge the lawfulness of data sources and to enforce rights in relation to automated decisions; financial supervisors, to supervise model risk and monitor fairness across a lender's portfolio; and, where applicable, consumer protection bodies, to address unfair conduct towards borrowers. Explanation and routes of challenge engage all of them and are best settled jointly.

> "Let's come together, whatever we come up with regarding AI — let it be joint, let everybody have input into it."

77. Protection of Personal Information Act 4 of 2013 (South Africa), sec. 71, governing automated decision-making; Information Regulator (South Africa), Code of Conduct for the Banking Sector, developed by the Banking Association South Africa and approved under sec. 60 of the Protection of Personal Information Act 4 of 2013.

78. Nigeria Data Protection Act, 2023, sec. 37, conferring the right not to be subject to a decision based solely on automated processing; and Nigeria Data Protection Commission (NDPC), General Application and Implementation Directive 2025 (GAID), issued 20 March 2025 and effective 19 September 2025, which prescribes the circumstances in which a Data Privacy Impact Assessment is mandatory, including evaluation or scoring activities such as profiling and automated decision-making producing legal or similarly significant effects. The GAID replaced the Nigeria Data Protection Regulation 2019 and its Implementation Framework 2020.

Four supervisory expectations would turn fairness and explainability from principles into something supervisors can check: documented provenance for each data source used in a model; reasons given to an applicant for an adverse decision, in terms the applicant can act on; defined triggers for human review; and periodic bias testing, with results available to both authorities. The allocation may shift as data protection authorities take on wider roles in AI governance. In Brazil, the AI bill, approved by the Senate in December 2024, would make the data protection authority the coordinator of a national AI regulation and governance system that includes sector regulators. At the 30 September 2026 cut-off the bill remained before the Chamber of Deputies, where a government bill proposing a different governance structure has been attached to it, so that role is not yet settled.[79]

Third-party data and vendors

Much of the data that reach a lender's model have already been shaped by someone else. Institutions buy databases from third-party vendors and search the open web. By the time they do, the provider has already made consequential judgments: which sources to use, how to match records to individuals, how to categorise them and what to infer. Those judgments are made outside the institution and, in most jurisdictions, outside either regulator's direct view.

The resulting inputs are not all of one kind. An external risk indicator may be a verified fact, an allegation, an inferred association or a vendor-generated score, yet these are often treated identically once they reach a decision. A lender needs to know whether the information concerns the right person, whether it is current and adequately contextualised, and whether it supports the specific decision being made. Where it does not, errors propagate. A mismatched record or a stale allegation can carry through into credit decisions, fraud flags and AML screening. A consumer who corrects it with one institution may find it persists elsewhere, because correction at one point does not always follow data back to source.[80]

This problem applies equally to rules-based systems and to human judgment, and a technically sound model cannot compensate for unsuitable or misleading inputs. It also bears on minimisation, which cuts both ways here: removing context can make information misleading, while adding information without a demonstrated purpose creates unnecessary exposure. Institutions may remain responsible for lending decisions even where data sourcing, model design or analytics are supplied externally. The vendor layer therefore engages data protection, consumer protection, outsourcing, operational resilience and prudential supervision at once, and sits between the two regulators without clearly belonging to either.

79. Projeto de Lei No. 2,338/2023 (Brazil), approved by the Federal Senate on 10 December 2024 and sent to the Chamber of Deputies. At 30 September 2026, it remained before a special committee of the Chamber awaiting the rapporteur's report, https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2487262. A government bill, PL 6,237/2025, attached to it in March 2026, would give coordination to a new Brazilian AI Council, with the ANPD as lead regulator for sectors without specific AI rules.

80. For more on these types of risks and how they relate to a focus country, see, for example, CBK, draft Risk Management Guidelines (September 2026), https://www.centralbank.go.ke/wp-content/uploads/2026/09/Draft-Central-Bank-of-Kenya-Risk-Management-Guidelines.pdf.

Abusive collection and credit shaming

Fragmented oversight is most visible where data gathered for lending are later used to coerce repayment. In Nigeria, the Federal Competition and Consumer Protection Commission (FCCPC) has reported online lenders using public shaming, defamation, and intimidation, and has since regulated digital lending, including data-privacy and ethical-recovery requirements.[81] A single harm thus engages both lending conduct and the lawfulness, purpose, and proportionality of the underlying data handling, so one act may give rise to both a financial-services claim and a data protection claim. Where there is no referral route or shared understanding, the consumer suffers one harm while the system treats it as several. Concrete responses are possible: India's prohibition on lending apps accessing contact lists removes one route through which contact data could be repurposed for abusive collection.[82] The comparison should not be overstated, since markets and frameworks differ, but it shows that specific safeguards can be embedded directly in financial-sector regulation, and the wider challenge is ensuring such lessons travel across domains.

The evidence does not support portraying advanced AI underwriting as equally prevalent across all ten countries; adoption and maturity are uneven, while the direction of travel makes coordination increasingly important. The case for joined-up regulation does not depend on every market having reached the same stage, but on the opportunity to set common expectations before fragmented approaches entrench. In the near term, jointly developed guidance could clarify how existing data protection principles apply to data drawn from outside the borrower's financial relationship, vendor-supplied inputs, automated decisions and AI-enabled underwriting, while setting financial-sector expectations on model governance, transparency, data provenance and error correction, and consumer challenge, without waiting for comprehensive AI legislation. Over the medium term, that could grow into shared supervisory expectations, structured information-sharing, and joint testing for AI-enabled credit products, so that regulators examine the same use case together. Credit thus reinforces a broader finding: the central gap is often not the absence of applicable law, but the absence of mechanisms through which existing mandates are operationalised together, and building that in early is easier than reconciling divergent approaches after markets have scaled.

81. Federal Competition and Consumer Protection Commission (Nigeria), Digital, Electronic, Online, or Non-Traditional Consumer Lending Regulations, 2025, https://fccpc.gov.ng/wp-content/uploads/2025/11/DEON-Consumer-Lending-Guidelines-2025.pdf, which replaced the Limited Interim Regulatory/Registration Framework and Guidelines for Digital Lending, 2022.

82. Reserve Bank of India (Digital Lending) Directions, 2025 (8 May 2025).

Box 10: Coordination on paper, not in practice

A recurring finding is that coordination often exists on paper while remaining dormant, uncertain, or unimplemented. Cooperation between financial and data protection authorities frequently stops at a documented agreement, such as an MoU, without translating into practical cooperation. Regulatory staff sometimes could not say whether a given MoU remained in effect, or how their offices fit within it, and in some cases neither authority could confirm that an instrument existed at all. Paper coordination is best understood as a friction: an instrument can be cited as evidence that coordination has been addressed, while producing no notification duty, no joint decision-making, and no institutional consequence.

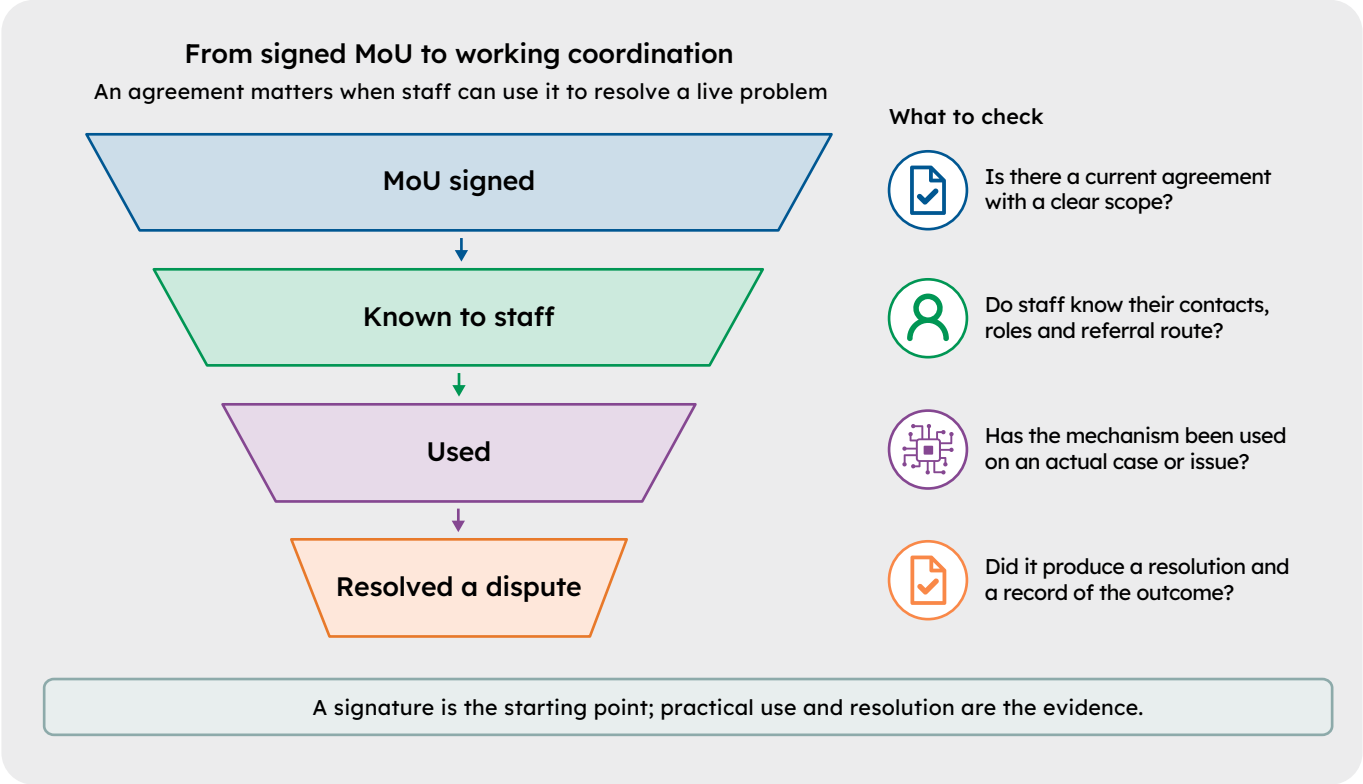
Kenya offers the clearest statutory illustration. Digital credit providers, for example, must both register with the ODPC and be licensed by the Central Bank of Kenya, yet neither process requires the other authority to be consulted or notified.[83] Two statutory mechanisms run in parallel over the same firms without a formal point of contact. Coordination that does occur tends to be event-driven, surfacing only once a public controversy or enforcement failure forces two regulators into the same room, and dissolving again once the episode passes. This is not to dismiss documented instruments altogether: the Philippines' bilateral enforcement MoUs show that a narrowly drawn instrument can carry live, case-level cooperation (Section 4.5).[84]

The lesson is that an instrument is an enabling framework, not an end in itself: its effectiveness depends on legal gateways, assigned staff, procedures and demonstrated use, and it needs to be built on. That is why Section 8 proposes an audit of whether such mechanisms exist and function, and sets out the conditions under which paper coordination becomes practical coordination.

83. Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021 (Kenya); Central Bank of Kenya (Digital Credit Providers) Regulations, 2022; Microfinance Act, 2006; and the Central Bank of Kenya Act (Cap. 491) in respect of foreign exchange bureaux.

84. National Privacy Commission (Philippines), memoranda of understanding with the Office of the Privacy Commissioner for Personal Data, Hong Kong (2023); the Office of the Privacy Commissioner of Canada (2023); and the Office of the Privacy Commissioner, Bermuda (2025).

Figure 4.4: Assessing the practical effectiveness of coordination structures



Source: CCAF & Fii.
Qualitative stages only. Funnel widths are schematic and do not represent measured attrition.

4.5 Cross-border data flows and localisation

A key finding is that data protection law generally sets the safeguards for cross-border transfers, supervised by the data protection authority where one exists, while hard localisation requirements typically originate from financial regulators, cybersecurity agencies, payment-system operators, or sector-specific authorities rather than from data-protection laws themselves. There are exceptions: Ethiopia's data protection law requires locally collected personal data to be stored in Ethiopia; Kenya's data protection regulations require strategic-interest data to be processed, or copied, in Kenya; and India's DPDP Rules give the government a power, from May 2027, to bar transfers of specified data held by significant data fiduciaries. This matters because localisation debates are often framed as a data protection issue when, in practice, most of the restrictive requirements affecting financial institutions arise from prudential supervision, operational resilience, national security, payments governance, and regulatory access.

Sovereignty and AI make the theme increasingly important. Governments are weighing where financial and personal data should be held and processed as cloud and AI services concentrate in a few providers and jurisdictions. Offshore cloud or AI processing of financial data can engage, at the same time, data protection safeguards on transfer, financial-sector rules on outsourcing and operational resilience, and supervisory access, and each authority sees only part of that picture.

This distinction can be taken further. Four obligations, commonly grouped under 'cross-border data', must be distinguished; different authorities impose them, for different reasons, with different remedies. The first is transfer permission: whether personal data may lawfully leave the country, and by what mechanism (adequacy, contractual safeguards, consent or a prohibition list). It is usually set by the data protection law and supervised by the DPA. The second is local storage/copy: whether data, or a copy of them, must be held domestically regardless of whether a transfer is otherwise permitted. These requirements usually come from payments, prudential, cyber or critical-infrastructure rules. The third is supervisory access and outsourcing control: whether a financial regulator can obtain data from, and audit, an offshore or cloud provider. This does not require data to stay in the country, only that they remain reachable. The fourth is information that must accompany payments or AML/CFT reports, such as originator and beneficiary information under FATF Recommendation 16. This obliges data to move rather than restricting where they go. These obligations are independent of one another: for example, a transfer permissible under a data protection statute may still breach a local-copy rule. Joint guidance can explain how the four interact in a given jurisdiction, but it cannot produce a single test for all four.

India illustrates the architecture clearly. Transfers are currently governed by the 2011 SPDI Rules, which permit them where the recipient ensures equivalent protection and the transfer is necessary for a lawful contract or consented to. From May 2027, section 16 of the Digital Personal Data Protection Act will take a relatively permissive, prohibition-list approach, allowing personal data to move abroad except to countries the government restricts, and it imposes no broad localisation itself; separately, Rule 13(4) of the DPDP Rules will let the government bar the transfer of specified data held by significant data fiduciaries, although none has yet been specified.[85] Yet multiple sectoral regulators mandate local storage for specific datasets, and the review found no coordination mechanism between data protection and financial-sector regulators on transfers; section 16(2) will preserve stricter sectoral safeguards, so financial-sector localisation will remain enforceable despite the flexible statute.[86] Pakistan mirrors this even without an enacted law, with cross-border financial-data governance driven by State Bank of Pakistan (SBP) rules (Securities and Exchange Commission of Pakistan's (SECP) cloud guidelines remain a draft) while a draft bill contemplates transfer restrictions expected to sit alongside, not displace, sectoral obligations.[87] Together they suggest an emerging design pattern: the data protection law sets a baseline, and financial regulators retain authority to go further. Table 4.3 summarises transfer and localisation approaches across the focus countries.

85. For a practitioner summary, see King Stubb & Kasiva, "India's New Cross-Border Data Transfer Framework," 2025, https://ksandk.com/data-protection-and-data-privacy/indias-new-cross-border-data-transfer-framework/.

86. Digital Personal Data Protection Act, 2023 (No. 22 of 2023), sec. 16(1) (transfers permitted except to territories notified by the Central Government) and sec. 16(2) (the section does not restrict the application of any other law providing a higher degree of protection for or restriction on transfer of personal data outside India), https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf.

87. Ministry of Information Technology and Telecommunication (MoITT) (Pakistan), Personal Data Protection Bill (draft, May 2023), https://moitt.gov.pk/SiteImage/Misc/files/Final%20Draft%20Personal%20Data%20Protection%20Bill%20May%202023.pdf; the official legislation register labels the instrument "Draft."

Table 4.3: Cross-border transfer regimes and localisation requirements: summary

Jurisdiction	Transfer rule (DP law)	Local storage or copy	Supervisory access and outsourcing
Brazil	Adequacy, clauses, consent; EU adequacy (2026)	No general mandate	BCB access to offshore services
Ethiopia	PDPP grounds; ECA approval for sensitive data	PDPP art. 22; NBE banking data	NBE approval for covered transfers
India	SPDI Rules now; DPDP s.16 from May 2027; Rule 13(4) power	Sectoral (RBI payments, SEBI, insurance)	SEBI and IRDAI access; CERT-In logs
Indonesia	PDP Law hierarchy; some routes await the authority	Bank data centres in Indonesia	OJK approval and access
Kenya	Safeguards, adequacy, consent	Strategic-interest data (reg. 26)	CBK outsourcing approval and access
Nigeria	NDPA safeguards and derogations	Payment-transaction data (CBN, from 2027)	CBN shared-services approval
Pakistan	No enacted law (draft bill)	No blanket mandate (SBP prefers onshore)	SBP approval and audit rights
Philippines	Accountability-based (DPA 2012)	No general mandate	BSP outsourcing and access rules
South Africa	Adequacy or consent; authorisation for special data	No general mandate	PA directives; joint standard planned
Uganda	Equivalence or consent; PDPO no-objection in practice	E-money issuers' primary data centre	BoU inspection and information powers

Source: CCAF & Fii. The full table, with sources, is Appendix Table 3.

These regimes increasingly intersect with financial obligations. Kenya is the clearest case: the Data Protection Act requires safeguards and, for sensitive personal data, consent (the Act's definition includes 'property details', and whether routine payment data fall within it has not been settled),[88] yet financial institutions participate in regional payment and remittance systems that depend on frictionless exchange, so where payment data are treated as sensitive, obtaining and evidencing consent for routine transfers can delay or constrain flows for regional banking groups and remittance operators. The fourth obligation runs in the opposite direction from the others. Revised Recommendation 16 requires customer-identifying information to travel with cross-border payments, so institutions must send data abroad as a condition of the transaction.

88. Data Protection Act, 2019 (Kenya), secs. 2 (definition of "sensitive personal data") and 49(1); ODPC, Guidance Notes for Cross-Border Data Transfers (September 2026), https://www.odpc.go.ke/wp-content/uploads/2026/09/ODPC-%E2%80%93-Guidance-Notes-for-Cross-border-Data-Transfers.pdf.

Whether data protection law permits this is itself unsettled in some jurisdictions: the FATF's draft implementation guidance acknowledges that destination-country rules can create uncertainty and asks countries to state expressly that these transfers are in the public interest (draft guidance, section 3.2.1). Beyond that lie questions of what, and how much, information must travel, how long intermediaries may retain it, and which authority assesses whether what is sent satisfies all applicable obligations.[89] Kenya, Ethiopia, Indonesia, Brazil, Nigeria, and Uganda all show a version of this, most acutely for payment corridors, remittances, digital-asset services, and regional arrangements such as PAPSS.[90]

The March cross-regulatory workshop in Kigali highlighted an important link between the two domains: decisions taken within data protection frameworks have downstream consequences for financial supervision. Adequacy determinations, transfer restrictions, and localisation obligations shape cloud outsourcing, operational resilience, and third-party risk management. A cloud arrangement lawful from a data protection view may still concern a financial regulator responsible for cyber resilience or supervisory access, while a localisation requirement from a payments regulator may effectively determine whether a permitted transfer mechanism can realistically be used. Decisions in one domain constrain the options available in the other. The economic stakes are substantial, since cross-border flows underpin payments, remittances, trade finance, fraud monitoring, cloud computing, onboarding, reporting, and, increasingly, the development and training of AI models; meanwhile the costs of localisation (duplicated infrastructure, higher compliance costs and less flexibility in sourcing) fall disproportionately on smaller firms, with significant consequences for competition and, ultimately, the welfare of lower-income and financially excluded consumers.

Regional harmonisation is increasingly viewed as a partial answer. Kenya's adequacy dialogue with the EU, the Philippines' participation in the Global CBPR system, GPEN, the GPA, and ASEAN, and initiatives such as PAPSS all show growing cooperative effort.[91]

89. FATF, Recommendation 16 and its Interpretive Note, as revised in June 2025, requiring originator and beneficiary information to accompany cross-border payments; countries are expected to be ready to implement the revised Standard by the end of 2030. See FATF, "FATF Updates Standards on Recommendation 16 on Payment Transparency https://www.fatf-gafi.org/en/publications/Fatfrecommendations/update-Recommendation-16-payment-transparency-june-2025.html

90. African Export-Import Bank, "Afreximbank and AfCFTA Announce the Operational Roll-Out of the Pan-African Payment and Settlement System (PAPSS)," 28 September 2021, https://www.afreximbank.com/afreximbank-and-afcfta-announce-the-operational-roll-out-of-the-pan-african-payment-and-settlement-system-papss/; PAPSS, "How It Works," accessed 19 August 2026, https://papss.com/how-it-works/.

91. Global Cross-Border Privacy Rules Forum membership; Global Privacy Enforcement Network membership; Global Privacy Assembly accredited membership; ASEAN Model Contractual Clauses for Cross Border Data Flows (2021) and the ASEAN Framework on Digital Data Governance; Collaboration on International ICT Policy for East and Southern Africa, "Advancing Sustainable Cross-Border Data Transfer Policies and Practices in Africa," 30 April 2024, https://cipesa.org/2024/04/advancing-sustainable-cross-border-data-transfer-policies-and-practices-in-africa/.

The Philippines has also used bilateral instruments for case-level enforcement, signing MoUs with Hong Kong's Office of the Privacy Commissioner for Personal Data (2023), Canada's Privacy Commissioner (2023), and Bermuda's PrivCom (2025), each built to move investigative material between two named authorities, the kind of confidential sharing a large multilateral forum rarely accommodates.[92] Regional convergence may nonetheless coexist with fragmentation between regions, which reinforces the value of interoperability and mutual-recognition arrangements. Across most focus countries, though, there is limited evidence that coordination on transfers, adherence to FATF recommendations, localisation, and outsourcing occurs systematically at the design, implementation, or supervision stage, and institutions frequently report navigating these overlapping obligations largely on their own, which shows the value of stronger and more formalised coordination between the two domains.

92. National Privacy Commission (Philippines), memoranda of understanding with the Office of the Privacy Commissioner for Personal Data, Hong Kong (2023); the Office of the Privacy Commissioner of Canada (2023); and the Office of the Privacy Commissioner, Bermuda (2025).

Chapter 5

Measuring coordination and what it is worth



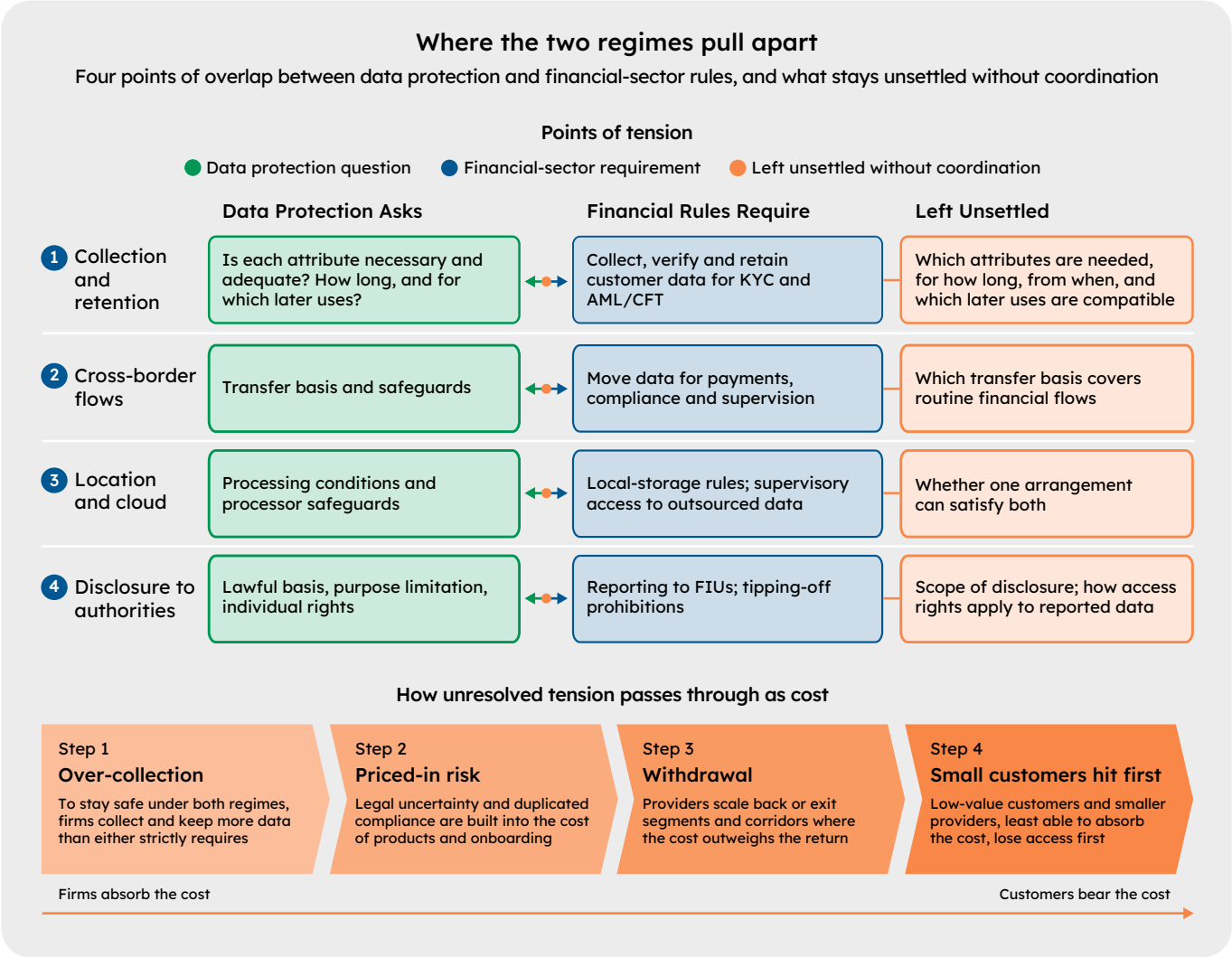
This section proposes how coordination, and what is at stake when it is missing, could be measured. Section 5.1 explains why measurement matters. Section 5.2 sets out the Regulatory Coordination Index (RCI), which scores each relationship between a data protection authority and a financial-sector authority on how far coordination is in place across the regulatory cycle. Section 5.3 applies it to the ten focus countries on an illustrative basis, and Section 5.4 shows how the outcomes coordination could affect might be sized. Section 5.5 sets out the framework's limitations and how it could be developed; the full methodology is in Annex C. The country scores in this section are consistent with this research's findings but are not yet evidence-coded index values, and should be read as illustrations of how the framework works.

5.1 Why measurement matters

As discussed above, coordination gaps can impose additional costs on firms, consumers and markets. Where two authorities' obligations overlap and no mechanism exists to settle how they apply together, the cost of reconciliation falls on the regulated firm. Firms subject to both regimes may face duplicated reporting, divergent interpretations of overlapping obligations, and legal uncertainty where mandates intersect. Uncertainty is greatest where KYC and AML/CFT duties to collect and retain customer information meet data protection questions of necessity, retention and onward use, but it is not confined there. Firms may pass part of that cost on. Where compliance is uncertain, providers may collect more data than they need, price in regulatory risk, or withdraw from products and customer segments that are costly to serve. Customers with small accounts and loans are likely among the first affected. These dynamics can depress competition and innovation, ultimately harming low-income and financially excluded consumers and to the economic growth and development of EMDEs.



Table 5.1: Where data protection and financial-sector obligations pull in different directions



Source: CCAF & Fii.

These frictions are difficult to address for several reasons. Individually, none may be attributable to a single regulatory failure, and their full extent may not be visible to either authority acting on its own. Cumulatively, however, they can raise compliance costs and pose barriers to market development, effective consumer protection and financial inclusion. The burden is also unevenly distributed: divergent data protection regimes, and differing standards for cross-border data transfers in particular, can weigh disproportionately on firms in emerging economies, especially newer and smaller ones, which are least able to absorb the cost of navigating them.[93]

93. See, e.g., UNCTAD, Data Protection Regulations and International Data Flows: Implications for Trade and Development (2016), https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf.

For consumers, the effect shows up in access and redress. Customers who cannot readily supply documents, or who transact in small amounts, are most exposed to defensive over-collection and de-risking. When harm occurs, they are also least able to work out which authority to approach, or to pursue a complaint through two. This can raise barriers to entry, slow consumer-friendly innovation and entrench incumbent players and business models, which in turn can perpetuate financial exclusion and slow economic development.

These frictions also show where coordination would add most value. Coordination is not free: consultation takes time, joint arrangements need governance, and duties to consult can slow decisions. Its value lies where these costs are smaller than the frictions they remove, which is why Section 8 begins with lightweight measures. Where DPAs and FSAs align their interpretations, sequence their requirements, and settle uncertainties and differences of interpretation before they reach regulated firms, lower compliance costs and greater regulatory certainty can reinforce each other to the benefit of all stakeholders. Clearer and more predictable rules lower the barrier to entry for smaller firms, support responsible data-driven innovation, and allow each authority to pursue its own mandate without undercutting the other. This is the central argument of the report: closer coordination between DPAs and FSAs is an important lever for building a more inclusive and responsible digital financial ecosystem, and for the broader economic activity that depends on it.

Coordination can also go too far, or in the wrong direction. Reviewers and stakeholders cautioned that joint working between authorities of unequal standing carries a risk of capture: a long-established, better-resourced financial regulator can set the joint agenda, frame data protection questions in its own terms and, over time, draw a newer data protection authority into its priorities. Where either authority lacks independence, closer coordination can also give the executive more influence over outcomes. Joint arrangements can blur accountability, making it harder to see which authority answers for a decision, and can duplicate investigations and sanctions. These are reasons to design coordination proportionately rather than to avoid it: to preserve each authority's statutory decision rights, to set joint agendas mutually, to record disagreements rather than smooth them over, and to judge each mechanism by what it achieves (Section 8).

The methodology developed in this section aims to measure how much coordination actually exists, and where it is missing. Drawing on selected levels of Metcalfe's nine-level scale of policy coordination,[94] it builds a Regulatory Coordination Index (RCI): an illustrative diagnostic of the documented relationship between a data protection authority and a financial-sector authority. The RCI does four things. It records which pre-conditions for coordination are in place (a legal basis, a route to resolve conflicts and review of the relationship); it scores how far coordination is practised across information sharing, capacity building, policy design, supervision and enforcement (Section 5.2); it maps those scores onto the stages of the regulatory and supervisory cycles, showing where coordination is concentrated or missing; and, paired with outcome data, it supports scenario sizing of what is at stake (Section 5.4). With the right inputs, it would produce the evidence base that regulators and policymakers need to prioritise institutional reform.

94. Les Metcalfe, "International Policy Co-ordination and Public Management Reform," International Review of Administrative Sciences 60, no. 2 (1994): 271–90.

Box 11: How coordination gaps reach underserved consumers

The case that coordination matters for inclusion rests on four pathways.

First, when a harm engages both mandates, fragmented complaint handling prolongs it: the consumer must work out which authority to approach and may be passed between them. Second, errors in identity and risk data exclude legitimate customers. A mismatched record or a stale allegation can cost someone an account or a loan, and correction routes rarely follow the data (Section 4.4). Third, where credit is conditional on extensive data collection, as with access to a borrower's phone contacts in digital lending, consent offers little real choice to people with few alternatives. Fourth, compliance uncertainty weighs most on smaller providers, which are often the ones serving low-income, rural and informal-sector customers (Section 4.5).

Each pathway is likely to bear hardest on women, low-income consumers, rural users and small firms, who have fewer alternatives, fewer documents and less capacity to pursue redress through two authorities. Earlier Kenyan survey research found a gender gap in the use of formal digital credit.[95] Proxy variables in credit-scoring models may reproduce disadvantage, including for women, and require bias testing.[96] International frameworks such as the G20 High-Level Principles for Digital Financial Inclusion treat proportionate, coordinated data and consumer-protection rules as a condition for reaching excluded groups.[97]

5.2 The regulatory coordination index

The RCI has two elements: a scale that captures how deeply coordination runs, and a set of components that identify where in the regulatory system to look for it. Each component is scored on the scale, and together they provide a comparable institutional baseline across the ten focus countries.

The index draws on selected levels of Metcalfe's nine-level scale of policy coordination (Figure 5.1).[98] The scale runs from independent decision-making at Level 1; through information exchange and consultation at Levels 2 and 3; divergence avoidance and consensus-seeking at Levels 4 and 5; and arbitration of differences at Level 6; to centrally set parameters, priorities and a unified strategy at Levels 7 to 9. The RCI is an adaptation: it uses the scale heuristically, to describe how deep each kind of coordination runs, and maps each component to the level it represents when fully in place (Table 5.2).

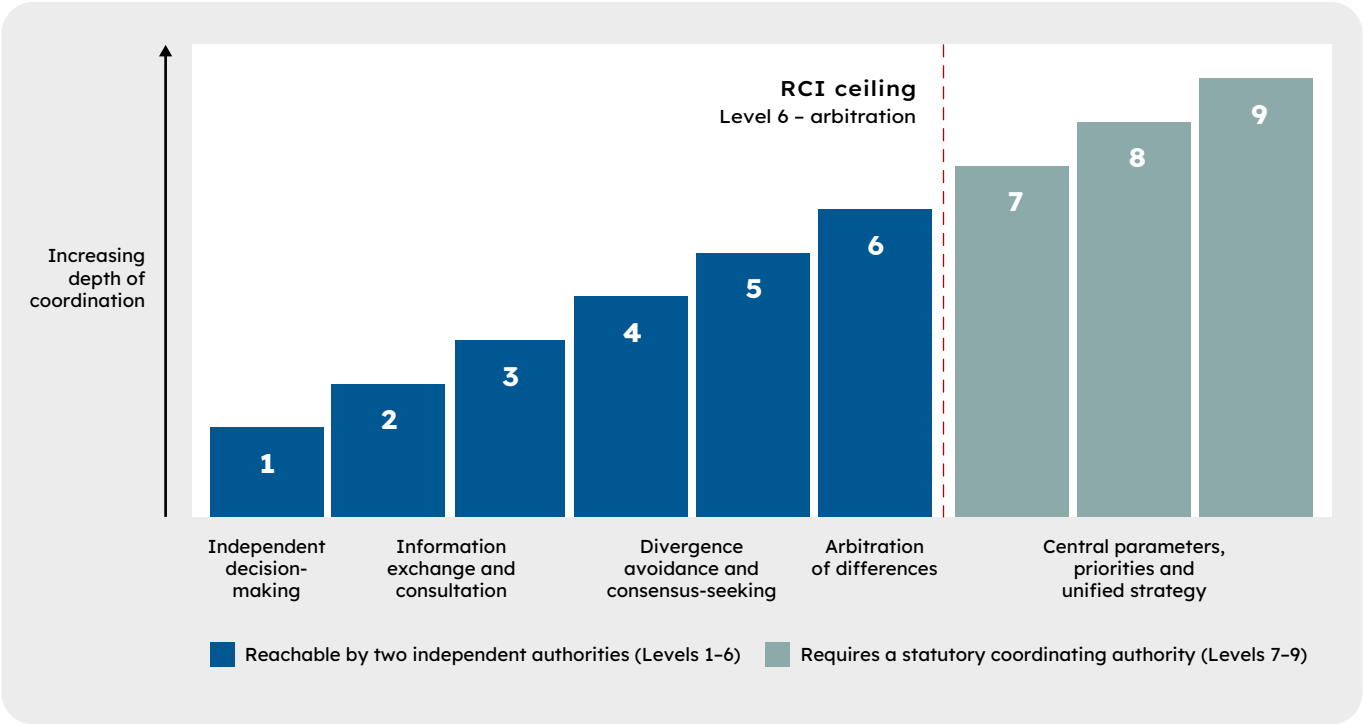
95. Constantin Johnen and Oliver Mußhoff, "Digital Credit and the Gender Gap in Financial Inclusion: Empirical Evidence from Kenya," Journal of International Development 35, no. 2 (2023): 272–95, https://doi.org/10.1002/jid.3687.

96. S. S. Dzreke and S. E. Dzreke, "Double Discrimination: Algorithmic Amplification of Gender Bias in African Fintech Credit Scoring—A 10-Algorithm Audit Reveals 37% Underfunding Penalty against Women-Led SMEs," Advanced Research Journal 8, no. 1 (2025): 58–81, https://doi.org/10.71350/3062192576.

97. Global Partnership for Financial Inclusion, G20 High-Level Principles for Digital Financial Inclusion (2016).

98. Metcalfe, "International Policy Co-ordination."

Figure 5.1: Mapping the depth of coordination in the regulatory coordination index (RCI)



Source: CCAF & Fii.

The RCI is capped at Level 6. This is a modelling choice: without a superior body, two independent authorities cannot be required to follow a unified strategy, so the index treats arbitration of differences (Level 6) as the highest form of coordination the DPA–FSA relationship can reach on its own. Levels 7 to 9 require something above the two authorities: a coordinating authority or mandate created by statute, or a national strategy or voluntarily agreed priorities within which both work. Those arrangements are outside the scope of this version of the index, though a later version could recognise them.

Eight components are scored against that scale, spanning the regulatory and supervisory lifecycles. They fall into two tiers.

- Three are pre-conditions, closer to binary than the others but not wholly so: a legal gateway for cooperation either exists or it does not; a route to resolve a binding conflict either exists or disputes go unresolved; a mechanism to review the relationship either exists or the relationship goes unmonitored. Even these vary: a legal gateway may exist for some activities and not others, and conflict-resolution and review mechanisms differ in strength, so they are scored on the same three-point scale as the other components.
- Five are coordination components proper, and each can be graded: the routineness of information exchange, the frequency of joint training, the use of a consultation channel, whether a joint sandbox operates day to day, whether enforcement cases are actually referred and jointly progressed.

Two further features matter for coordination but are not scored: joint policy signalling, such as joint public statements of priorities, is treated as part of policy design consultation where it occurs; technological systems that enable coordination, such as secure channels and shared registers, are treated as context. These elements should be considered alongside the index when assessing the level and effectiveness of regulatory coordination.

The components were selected to cover each stage of the regulatory and supervisory cycles at which the two authorities' mandates meet, drawing on the coordination literature, the mechanisms identified in Section 3 and expert review. Components that could not be observed consistently across the ten countries were excluded. Annex C sets out the selection and the mapping of each component to the Metcalfe scale.

Table 5.2: The eight RCI components

Tier	Component	What it Measures	Metcalfe Level
Pre-condition	Formal Mandate	Legal and institutional basis for DPA–FSA cooperation.	2
Pre-condition	Conflict Resolution	Mechanisms for managing binding regulatory conflicts while preserving mandates.	6
Pre-condition	Accountability and Review	Review, reporting and monitoring of the coordination relationship.	6
Coordination	Information Sharing	Gateways, shared registers, common definitions and taxonomies, joint horizon scanning.	2
Coordination	Capacity Building	Joint training, secondments, attachments, shared learning.	2–3
Coordination	Policy Design Consultation	Structured involvement of each authority in the other's relevant rulemaking.	3–4
Coordination	Joint Supervisory Structure	Joint reviews, lawful data-sharing gateways, shared sandboxes or equivalent.	5
Coordination	Joint Enforcement Structure	Joint or cross-referred enforcement, lawful evidence sharing, cross-regime admissibility.	5–6

Source: CCAF & Fii. Component weightings and the derivation of the two tiers are set out in Annex C

Each component is scored 0, 0.5 or 1. Table 5.2 gives the Metcalfe level that a component represents when it is fully in place. A score of 1 means the mechanism exists and is used routinely at that level; 0.5 means it exists but is used only occasionally, operates on paper, or covers some activities only; and 0 means it is absent. The nine Metcalfe levels therefore describe how deep each kind of coordination runs, while the three-point score records how far it is in place. Component-specific definitions and worked examples are in Annex C (Section C.2.5).

Where a country has more than one relevant financial regulator, each relationship between the data protection authority and a financial regulator is scored separately. The country profile reports the relationship with the regulator holding the principal mandate for the activity concerned (Section 3.2), with the others shown alongside it rather than averaged in, since an average would hide the weakest relationship.

Separating the tiers changes how the index should be read. A low score on the coordination components alongside a high score on the pre-conditions indicates unused institutional capacity: the scaffolding exists but is not being activated. A jurisdiction can score well on Formal Mandate on the strength of an MoU never operationalised. A low score on the pre-conditions is a different and more binding constraint, because no amount of goodwill between officials substitutes for the absence of a legal gateway. That constraint is concentrated where the data protection authority is not yet operating, and in specific activities where a particular gateway is missing. Elsewhere, as the summary notes, the statutory framework is rarely the obstacle. As Section 8 discusses, reform should address the pre-conditions before the gradable components.

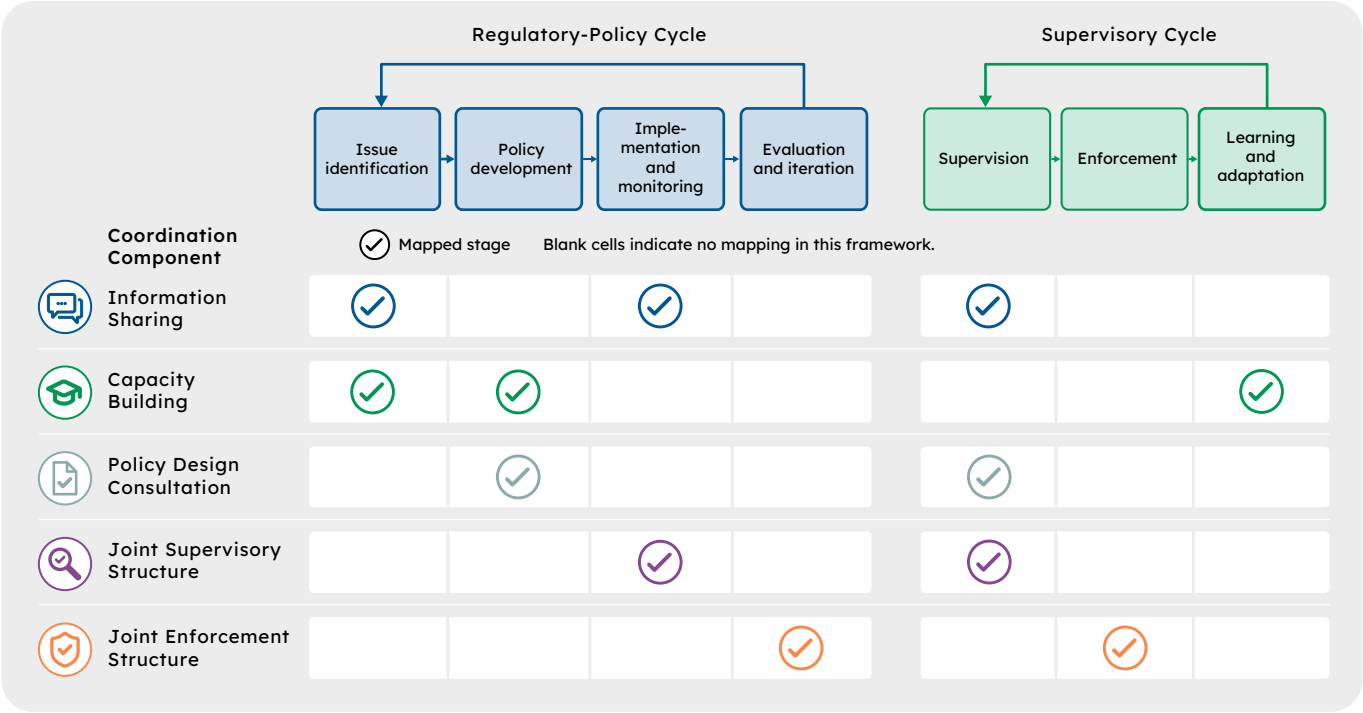
Because the index adds the two tiers together, a strong coordination score can partly offset a missing pre-condition in the composite. Section 5.3 therefore reports the pre-condition and coordination sub-scores alongside each country's band, and the absence of a dedicated data protection authority should not be read as meaning that no cooperation is possible.

5.3 What the index shows

With the right evidentiary base, the index provides a quantified and comparable profile of regulatory coordination in a jurisdiction. Consistent with the report's evidence, the scores here provide a provisional, illustrative profile of each focus country's DPA–FSA relationship. Because each component is mapped to specific stages of the regulatory-policy and supervisory cycles, the pattern of component scores also shows where in those cycles coordination is concentrated or absent, which a single composite figure would conceal.

On the regulatory-policy side, the stages are issue identification, policy development, implementation and monitoring, and evaluation and iteration. On the supervisory side, they are supervision, enforcement, and learning and adaptation. Each of the five coordination components maps to a stage of both cycles (Annex C, Table C.1): Information Sharing to issue identification, implementation and monitoring, and supervision; Capacity Building to issue identification, policy development, and learning and adaptation; Policy Design Consultation to policy development and supervision; Joint Supervisory Structure to implementation and monitoring, and supervision; and Joint Enforcement Structure to evaluation and iteration, and enforcement. This dual mapping reflects that DPAs and FSAs interact as regulators and as supervisors at the same time. The three pre-conditions underpin every stage.

Figure 5.3: Where coordination mechanisms apply across the regulatory lifecycle



Source: CCAF & Fii.

The index can therefore be used to identify the stages of the regulatory cycle that need policy attention. A country scoring well at the front of the cycle because of routine information exchange and active joint training but poorly at the back, owing to a lack of joint enforcement referrals or a formal review mechanism, shows a coordination relationship that functions informally but has not been institutionalised into supervision or enforcement. This is a materially different problem, and a different reform priority, from a relationship that scores evenly low throughout. The index is therefore designed to support stage-specific diagnosis as well as cross-country comparison: it can show whether a country's binding constraint sits at the pre-condition level (Section 5.2) or at a particular stage of an otherwise-functioning cycle.

The component weights represent a design choice; the 30:70 split between pre-conditions and coordination components is theory-informed rather than statistically estimated, and country orderings drawn from them should be considered provisional until checked against reasonable alternative weightings. On the illustrative scores, two alternatives (equal weights of 12.5% for each component, and an even 50:50 split between the tiers) leave the bands below unchanged and the broad ordering similar, although Kenya and South Africa become nearly tied under the 50:50 split. Once scores are coded against evidence, any ordering that does not hold across such alternatives should be reported as such rather than presenting a single weighting as definitive.

This is central to interpreting the index: the tier split and lifecycle profile matter more than any single composite ranking, since they hold regardless of the exact weights chosen, while fine-grained country-to-country ranking differences of one or two places should be treated with more caution.

The country scores in Tables 5.3 and 5.5 should be read with that in mind. They were assigned by the research team on the three-point scale, drawing on what the country studies, interviews, convenings and desk research revealed about each relationship, and are consistent with those findings. They are nonetheless provisional, and provided mainly for illustration. They should not be treated as equivalent to index values derived from the kind of evidence base this report encourages jurisdictions to develop (Recommendation 6). Their purpose is to show how the index works on real cases and what kind of picture it produces: a real-country illustrative calibration, in which the institutional facts are verified but the numerical judgements are provisional. Small differences in score should not be interpreted as meaningful differences in performance without stronger evidence and uncertainty analysis, which is why this section reports bands rather than a ranking (Section 5.5).

Three focus countries did not have an operating data protection authority at the cut-off: India and Indonesia, where an authority is provided for in law but not yet operational, and Pakistan, which has no comprehensive data protection law. Scoring these relationships on the same basis as the others would mechanically depress their index values, since several components presuppose an authority to coordinate with. This section therefore places them in a separate readiness tier: their component coding is shown for completeness, but they are not banded. Ethiopia, where an existing regulator holds the data protection remit, is scored.

Table 5.3: Illustrative coordination bands

Band	Countries	Basis
Upper (composite 0.60 and above)	Kenya, Nigeria, Philippines, South Africa	Pre-conditions largely in place; no zero on the heavily weighted components
Middle (0.50–0.59)	Brazil, Uganda	Pre-conditions partly in place; partial coordination across all components
Lower (below 0.50)	Ethiopia	Joint supervision and enforcement absent; young mandate
Readiness tier (not banded)	India, Indonesia, Pakistan	No operating data protection authority at the cut-off

Source: CCAF & Fii.

The illustrative bands are consistent with the qualitative typology of three patterns in Section 7.3, which draws on overlapping evidence: the four emergent jurisdictions fall in the lower band or the readiness tier. The index does not, however, distinguish co-active from uneven relationships, which differ in kind rather than in degree. The bands should therefore be read alongside the institutional characteristics of each country rather than as a standalone measure of regulatory effectiveness.

Table 5.4: RCI component weights

Band	Component	Weight	What it captures
Coordination	Information Sharing	5%	Routine exchange/use of information between data and financial regulators.
Coordination	Capacity Building	10%	Joint training, knowledge transfer, secondments, attachments or shared learning.
Coordination	Policy Design Consultation	15%	Substantive involvement of both authorities in relevant policy/rulemaking.
Coordination	Joint Supervisory Structure	20%	Coordinated or joint supervisory activity, reviews, gateways or equivalent mechanisms.
Coordination	Joint Enforcement Structure	20%	Coordinated/cross-referred enforcement, investigations or lawful evidence sharing.
Pre-condition	Formal Mandate	10%	Formal legal or institutional basis enabling cooperation.
Pre-condition	Conflict Resolution	10%	Mechanism for resolving disagreements or overlapping regulatory responsibilities.
Pre-condition	Accountability and Review	10%	Monitoring, reporting, evaluation and review of the coordination relationship.

Source: CCAF & Fii.



Table 5.5: Illustrative country coding

Scores of 0, 0.5 and 1 are illustrative coding values. They show how the weighted RCI is generated, and they also enter the indicative calibration in Section 5.4, which is therefore illustrative too.

Band	Info	Capacity	Policy	Supervision	Enforcement	Mandate	Conflict	Review	Pre-conditions (of 0.30)	Coordination (of 0.70)	Band
Kenya	0.5	1	1	0.5	0.5	1	0.5	0.5	0.20	0.48	Upper
Nigeria	1	1	0.5	0.5	0.5	1	0.5	1	0.25	0.43	Upper
Philippines	1	1	1	0.5	0.5	1	0.5	1	0.25	0.50	Upper
South Africa	0.5	0.5	0.5	0.5	0.5	1	0.5	1	0.25	0.35	Upper
Brazil	0.5	0.5	0.5	0.5	0.5	1	0.5	0.5	0.20	0.35	Middle
Uganda	0.5	0.5	0.5	0.5	0.5	1	0.5	0.5	0.20	0.35	Middle
Ethiopia	0.5	0.5	0.5	0	0	0.5	0	0.5	0.10	0.15	Lower
India	0.5	0.5	0.5	0	0	0.5	0.5	0.5	0.15	0.15	Readiness tier
Indonesia	0.5	0.5	0.5	0	0	0.5	0	0.5	0.10	0.15	Readiness tier
Pakistan	0.5	0	0	0	0	0	0	0.5	0.05	0.03	Readiness tier

How to read this table: Each score is multiplied by its component weight in Table 5.4, and the products are summed within each tier. Kenya, for example, is coded 0.5 on Information Sharing, 1 on Capacity Building, 1 on Policy Design Consultation, 0.5 on Joint Supervision, 0.5 on Joint Enforcement, 1 on Formal Mandate, 0.5 on Conflict Resolution and 0.5 on Accountability and Review, which gives 0.20 on the pre-conditions and 0.475 on coordination, a composite of 0.675.

Source: CCAF & Fii.

Nigeria and Kenya show why the profile matters more than the composite. Both have a composite of about 0.68 and fall in the upper band, but on different foundations. Nigeria's score rests more on its pre-conditions (0.25 of a possible 0.30) and on routine information exchange; Kenya's rests more on consultation in policy design, with weaker review of the relationship (0.20 on the pre-conditions). The same composite therefore points to different next steps: in Nigeria, using an established relationship in policy design; in Kenya, putting the relationship on a firmer and reviewable footing. Subject to the caveats above, this illustrative result shows the diagnostic potential of the index.

The gap between the middle band and the lower band and readiness tier is larger than the gaps within bands. With so few observations, coded so coarsely, this should not be read as a structural break: it mainly reflects the weight the index gives to joint supervision and joint enforcement. The upper and middle bands are distinguished from the lower band less by full scores across the board than by avoiding zero on the heavily weighted components (Joint Supervision, Joint Enforcement and Policy Design Consultation), even where their other scores remain partial. What lifts the upper band above the middle is full scores on one or more lighter components or on review of the relationship. By construction, the index rewards formal joint mechanisms of oversight and design more than communication or capacity-building, so the banding partly reflects the weights chosen (Table 5.4). Whether the bands differ in kind rather than degree is a question for coding against evidence, which these illustrative scores cannot settle.

5.4 What coordination is worth

A measurement of coordination must be matched to a measurement of impact. The index is therefore paired with the outcomes coordination is expected to influence across the report's five thematic areas. The framework is deliberately modest about the strength of that link: it does not claim the index causes movement in any indicator, only that observable channels exist through which coordination could plausibly influence outcomes. Variables were selected against three criteria: a clear theoretical mechanism linking the variable to coordination, relevance to both mandates, and credible measurement. The mechanisms, variables and sources are set out in Annex C.

Where outcomes can be monetised,[99] the framework applies a calibration rather than an estimate. For each country and use case it takes the monetary size of the outcome at stake (Q), multiplies it by the country's coordination gap (G = 1 – RCI, the share of the coordination the index can register that is not yet in place), and multiplies the result by an explicit attribution parameter (a): the share of the outcome that improved coordination could plausibly influence. 'a' is an illustrative scenario parameter common to all countries, not estimated for any of them, and is reported at three values: 2%, 5% and 10%. The country-specific differentiation comes from Q and G.

The calculation, for each country c and use case u, is:

$$\text{Coordination opportunity}(c,u) = Q(c,u) \times (1 - RCI(c)) \times a$$

On the strongest available monetary evidence, country-level figures for reported fraud in all ten focus countries, the combined indicative coordination opportunity is of the order of USD 53.9 million at the low sensitivity, USD 134.6 million at the central scenario and USD 269.3 million at the high (Table 5.6). It is the sum of the country-level values (Q × G × a) across the ten countries. These are scenario figures, not estimated savings.

99. Much of what coordination affects cannot sensibly be converted into money, and that evidence is presented in its observed form (Annex C, Section C.4.6). It is, in several respects, the more robust of the two bodies of evidence. India's Account Aggregator ecosystem had linked 119.6 million accounts and fulfilled 143.6 million consent requests by December 2024; Brazil's open finance framework recorded more than 800 participating institutions and over 60 million active consents in 2024. India's reported eKYC cost fell from around USD 12 to USD 0.06 per verification, with manual verification compressed from five to seven days to seconds. Indonesia's OJK sandbox processed 108 providers, of which 36 received recommended status, with OJK and Bank Indonesia exploring a coordinated sandbox. In Nigeria, 83.3% of surveyed respondents considered eKYC faster and more convenient than traditional KYC.

Table 5.6: Indicative coordination opportunity, fraud and consumer harm: ten focus countries combined

Scenario	Attribution share	Aggregated coordination opportunity
Low	2%	~USD 53.9 million
Central	5%	~USD 134.6 million
High	10%	~USD 269.3 million

Source: CCAF & Fii. Figures are aggregated calibrations, not estimates of savings realised. They rest on the illustrative RCI scores in Table 5.5. Country-level evidence and the full calculation are in Annex C (Table C.9)

The figure above covers fraud and consumer harm alone, not all five thematic areas, because fraud is the only use case with a monetary figure for every focus country that can be combined consistently with the RCI. The other four have evidence of scale, such as payment values, market size and unit costs, but not yet a defensible monetary measure of the outcome coordination would affect (Annex C, Section C.4.6). The total is also concentrated: India accounts for about four-fifths of it and Brazil for most of the rest. India's figure records the amount involved in frauds reported by banks, the majority of it being loan fraud, rather than realised consumer losses, while other countries report losses on different definitions. Because the country measures are not commensurate, the direction of any bias in the total is unknown.

These country figures differ in reporting period and measurement scope, and no annualisation has been applied. They are calibration inputs, not directly comparable estimates of annual losses, and the aggregate should not be described as an annual figure or as realised savings. For the readiness-tier countries, the coordination gap partly reflects the absence of an operating data protection authority (Section 5.3).

5.5 Limitations and future of the framework

The framework's strength is that it makes every assumption explicit. Unlike a regression-based point estimate, nothing material is buried in specification choices invisible to the reader. In small-n cross-country settings, where potential confounders are numerous relative to observations, explicit calibration is often more defensible than a regression whose parameter choices are embedded out of sight. It can also be applied where outcome data are unavailable for enough jurisdictions and years, or where the outcome is qualitative.

Its principal limitation is the subjectivity of the attribution parameter. Even with disclosure and sensitivity analysis, that parameter represents an analytical judgement about what share of an observed gap is attributable to coordination failure versus macroeconomic conditions, infrastructure quality, political stability or population characteristics. That judgement cannot be fully disciplined by data within a calibration framework, and different but equally defensible values produce figures differing by a factor of two or more. Calibration exercises are particularly vulnerable to motivated reasoning in the choice of central parameters, even where ranges are presented. The framework mitigates this by disclosing the parameter and reporting results across a range of values rather than as a point estimate. The current values (2%, 5% and 10%) are scenario assumptions and are not yet anchored in published benchmarks. The limitation cannot be eliminated.

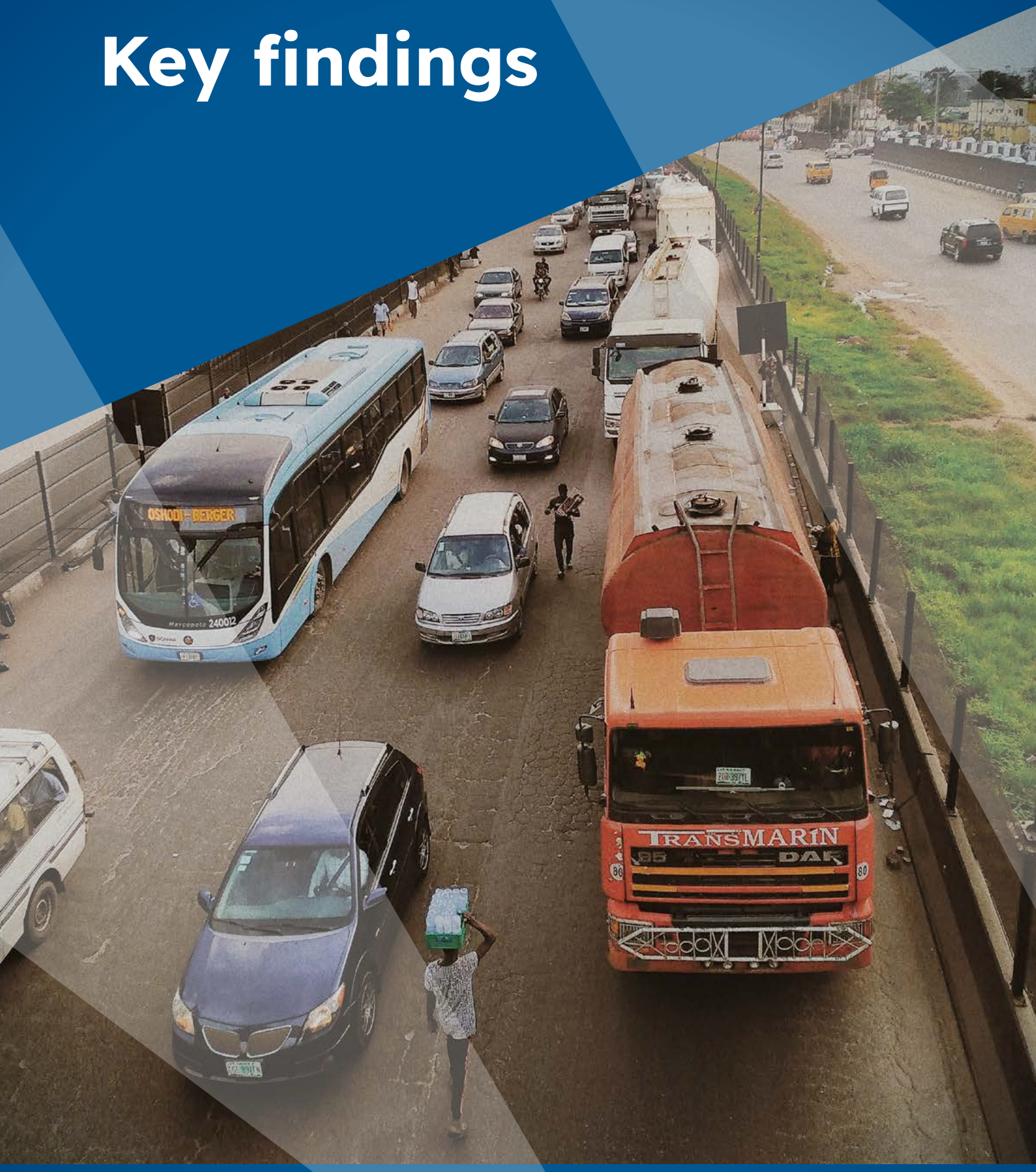
A second limitation is that the framework is static. It sizes the coordination-sensitive opportunity at a point in time. It does not model the path by which that opportunity would be realised, the pace at which improvements in coordination would translate into outcome changes, or the adjustment costs of institutional reform. Static opportunity estimates in regulatory impact assessment systematically overstate near-term benefits by omitting transition costs and adjustment lags. The figures here should be read as indicating the direction and order of magnitude of coordination effects, not as forecasts of achievable gains within a defined period.

The evidence base itself remains heterogeneous. Some observations are case-study or institutional; for the four use cases not yet monetised, regional averages and comparable-country proxies stand in for country evidence and should be replaced by direct evidence as it becomes available. The monetary figures also inherit the provisional status of the illustrative RCI scores. Priorities for future work are comparable country-level outcome measures, transaction volumes, unit costs, time-series data, and attribution parameters estimated empirically.

The framework is designed to improve with use. The next steps are to code scores against documented evidence; to build comparable outcome panels across countries and over time; to estimate attribution parameters empirically rather than assume them; to add uncertainty and sensitivity analysis to every reported figure; to account for the implementation costs and time lags of reform; and to update the index periodically. Authorities could also adopt it as a self-assessment tool, as Recommendation 6 proposes.

Chapter 6

Key findings



Seven findings run through the evidence in Sections 2 to 5 and the country case studies in Annex A. They are summarised here before Sections 7 and 8 turn to the causes and the response.

1. **Overlap is structural; the coordination gap is institutional**. As financial services have become data-intensive, financial regulation and data protection have come to govern the same activities, and often the same records, in every focus country (Section 2.3). Where a data protection authority is operating, the legal tools to settle the questions this raises are generally in place, although particular activities, such as exchanging case-level personal data, may need a specific legal gateway. What is missing is the institutional machinery to use those tools routinely, and the working knowledge each authority needs of the other's domain. The result is uncertainty over which rules apply and who should act, which raises costs for firms and weakens protection for consumers. Authorities on both sides consistently expressed willingness to coordinate more.
2. **Coordination is growing, but it is improvised, and it takes hold around concrete shared problems**. Contact points, joint guidance, sandboxes and information-sharing arrangements exist in several focus countries, but most are bilateral, event-driven or dependent on individuals, and some exist on paper only (Section 3.2; Box 10). Where coordination has taken hold, it has done so around a specific problem that both authorities regard as urgent. Fraud prevention was the problem regulators and stakeholders named most consistently, with open finance and AI-driven credit scoring also recurring (Section 4.2; Box 12).
3. **The data protection authority is often involved late, and the time to design coordination in is now**. In open finance, fraud prevention and AML/CFT, financial-sector frameworks were typically designed before the data protection authority was involved, so reconciliation happens after launch, when it is costlier and less effective (Sections 4.1 to 4.3 and 7.1). (The reverse dynamic is also observed, albeit less frequently.) Coordination is most effective, and least costly, when it is built in before frameworks and institutions are settled, and several focus countries are at that point now: India's Data Protection Board takes on its first functions from November 2026, Indonesia's implementing regulation takes effect in January 2027, and Kenya has consulted on a payments policy and bill that anticipate open finance (Section 9).
4. **Capacity is unequal, and the asymmetry shapes the relationship**. Data protection authorities are generally newer, smaller and responsible for every sector of the economy; financial regulators are generally older, better resourced and embedded in international standard-setting. Without deliberate design, joint work drifts towards the stronger authority's priorities (Sections 3.1, 5.1 and 7.1).
5. **The international architecture reproduces the gap**. Financial standard-setters set standards and assess their implementation; data protection bodies mainly convene. Early bridges exist, such as the FSB's Forum on Cross-Border Payments Data and the FATF's July 2026 recommendation of joint guidance, but they are recent and mostly convened from the financial side, and regional links between data governance and payments remain thin (Section 3.1). International bodies increasingly accept that the overlap needs joint handling; the open question is how.

6. **Protection stops at the financial regulator's perimeter unless the two authorities agree the handover**. Where no data protection authority is operating, financial regulators protect customer data through their own licensing perimeter, so protection ends where the perimeter does and data-driven services such as open finance narrow to licensed firms. Where an authority does exist, data that a customer directs to a firm outside the perimeter pass from one authority's oversight to the other's, and unless the two have agreed how that handover works, neither may be watching the recipient. The period before an authority is established is the cheapest time to design that handover in (Box 9; Section 7.3).

7. **The costs of the gap fall hardest on those with fewest alternatives**. Compliance uncertainty weighs most on smaller and newer providers, and harms that fall between mandates weigh most on low-income consumers, women and rural users, who have fewer alternatives and less capacity to pursue redress. These costs can in principle be measured, but robust measurement awaits evidence-coded scores and comparable outcome data (Section 5).

Taken together, the findings point less to new law than to a working regulatory bridge between the two authorities: designated counterparts, an agreed route for shared problems, and the habit of consulting before acting. Sections 7 and 8 set out what stands in the way of building it and how to do so.



Box 12: Messages from the programme's convenings

The programme held four convenings in 2026: an in-person cross-regulatory workshop in Kigali in March, a regulator-only roundtable in June, an all-stakeholder virtual workshop in July and a public webinar in September. Workshop and roundtable discussions were held under the Chatham House Rule. Five messages recurred.

No single authority can regulate digital financial services alone. Participants from several jurisdictions confirmed that products and markets routinely engage both mandates. In cases such as online lending fraud, no single regulator holds the full picture: the financial regulator may see unusual transactions, the data protection authority consent or processing irregularities, and law enforcement organised crime, but these signals are rarely combined.

An MoU is a first step, not the destination. Participants stressed that agreements need practical mechanisms behind them, such as named contacts, joint enforcement, shared investigations and working groups, and that cooperation should not depend on who occupies a post. Several suggested that a clearly positioned anchor institution, often the central bank, helps; others stressed that the data protection authority must be an equal partner.

Targeted, procedure-led cooperation works best. Regulators favoured goal-defined cooperation with tightly defined procedures and specific shared objectives. Fraud prevention, open finance and AI-driven credit scoring were repeatedly named as the most immediate candidates.

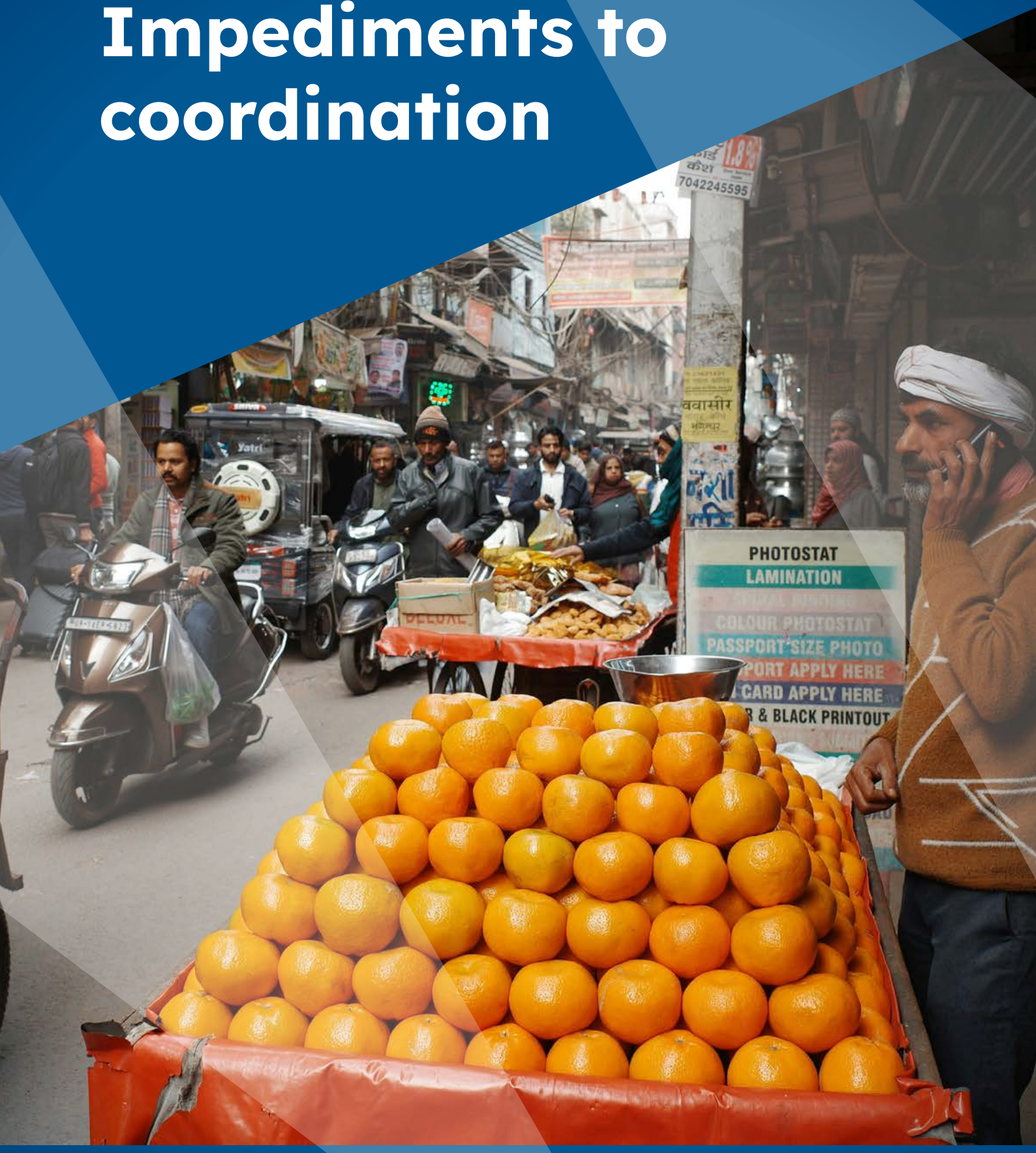
Shared language comes before joint action. Differences in professional background create communication barriers between institutions. Participants called for a shared diagnostic and common terminology before joint interventions, and for financial and data literacy work aimed at consumers.

Compliance should not be a choice between regimes. Industry participants argued that firms should never be forced to choose between complying with one regime or the other, and that clear joint guidance would unlock responsible data sharing that firms currently avoid.

Source: CCAF & Fii's convening notes (Kigali, March 2026; regulator roundtable, June 2026; all-stakeholder workshop, July 2026; public webinar, September 2026).

Chapter 7

Impediments to coordination



Sections 2 and 4 established that overlap between the two regimes is pervasive and structural: across all five thematic areas, financial regulation and data protection bear on the same activities and often on the same records. In jurisdictions with an operational data protection authority, the questions this generates are mostly legally answerable. The powers to consult, to issue joint guidance and to enter cooperative arrangements are already in place, although the power to disclose particular information is narrower and some activities need a specific legal gateway. They also established that those questions largely go unanswered. This section asks why, and what would change it.

The answer is largely institutional. Where a data protection authority is operational, coordination does not generally fall short because the law forbids it or because regulators oppose it; across the research, authorities on both sides were consistently willing and frequently enthusiastic. It falls short mainly because little in the way either authority is mandated, resourced, measured or organised causes coordination to happen, and a good deal makes it difficult. This section sets out five factors that produce this result (Section 7.1), the dynamic through which they reinforce one another (Section 7.2), and three patterns in how they play out across the focus countries (Section 7.3). Section 8 sets out seven recommendations.

If the constraint were the overlap itself, the remedy would be legislative and largely outside the reach of the authorities concerned. Because the constraint is institutional, the remedy is mostly within their reach. That is a more hopeful diagnosis than the one usually offered. It is also more demanding, since it locates responsibility with the institutions themselves rather than with legislatures.

Five factors impede DP–FS coordination across the focus countries: (1) capacity constraints and the asymmetries between authorities; (2) under-prioritisation in goal-setting; (3) under-prioritisation in workstreams, which means that coordination arrives late; (4) silos and institutional culture; and (5) the absence of shared frameworks through which joint work could be done. Each affects how fast coordination develops, how well the efforts that do occur work, and whether they become systematic.

One factor is largely absent from that list: the state of the law. In the focus countries with an operational data protection authority, statutory frameworks generally neither obstruct coordination nor deny regulators the powers to establish it, although specific gateways may be missing for particular activities. In three of them the statute goes further and directs the authority to coordinate or collaborate with other regulators, most specifically in Brazil, where the authority and sector regulators must coordinate their activities; in two others it makes explicit provision for delegation or for sectoral codes.[100]

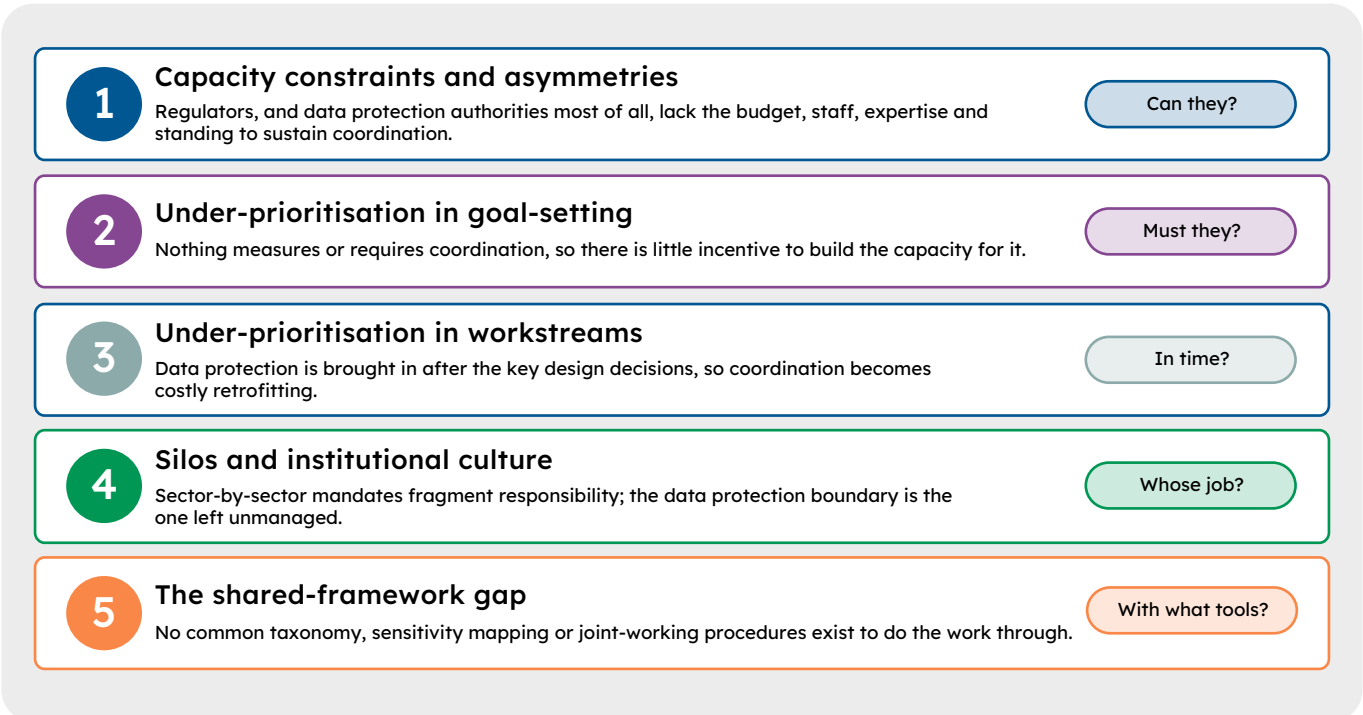
100. Lei Geral de Proteção de Dados Pessoais (Law No. 13,709/2018), art. 55-J(XXIII) and secs. 3–4 (the ANPD and sector regulators must coordinate their activities, and the ANPD must maintain a permanent forum with them); Nigeria Data Protection Act, 2023, sec. 5(h) (the Commission "shall… collaborate with any relevant ministry, department, agency…"); Data Privacy Act of 2012 (Philippines), sec. 7(f) (among the Commission's functions, to "coordinate with other government agencies…"); Data Protection Act, 2019 (Kenya), sec. 10 (delegation of powers to a regulator established by an Act of Parliament); Protection of Personal Information Act 4 of 2013 (South Africa), ch. 7 (secs. 60–68). For country detail, see Annex A. Indonesia's Law 27 of 2022 contains no duty to coordinate with sectoral regulators. Its implementing regulation, Government Regulation 33 of 2026 (in force from 16 January 2027), requires a ministry or agency that designates additional categories of specific personal data to coordinate with the data protection authority (art. 6(3)). This is an issue-specific link at regulation level rather than a general coordination duty and is not counted here. Uganda's Data Protection and Privacy Act, Cap. 97, contains no express coordination duty, although regulation 44 of the 2021 Regulations lets the PDPO seek the assistance of any person or authority in an investigation. The Data Protection and Privacy Regulations 2021 require the Personal Data Protection Office to cooperate with government ministries, departments and agencies, and require them to assist it (reg. 6). Separately, the National Payment Systems Act 2020 requires the Bank of Uganda to "cooperate with Government agencies whose functions are relevant to payment systems" (sec. 71(1)).

The main exception is where no authority is yet operating, as in India, Indonesia and Pakistan. Coordination with whichever body holds the data protection remit in the interim is possible and creates an opportunity to build coordination into the foundations, but coordination with a permanent, operational data protection authority cannot yet exist. The recommendations in Section 8 therefore distinguish three situations: work that existing powers already permit; work that needs a specific legal gateway or clarification first; and jurisdictions where the data protection authority is not yet operational.

Each of the five impediments can largely be addressed without primary legislation, although particular activities and structural reforms need separate legal assessment. The factors do, however, compound. Each makes the others harder to overcome, producing a cycle in which coordination attempted without adequate preparation disappoints, and disappointment teaches both authorities to invest less next time (Section 7.2). The cycle can be made to run the other way, provided an intervention is substantial enough to produce a visible result.

7.1 The five impediments

Figure 7.1: Identified barriers to effective cross-regulatory coordination



Source: CCAF & Fii.

Capacity constraints and asymmetries

Capacity was the factor stakeholders cited most often, and frequently the primary one. Regulators in the focus countries face constraints that limit their ability to establish and maintain institutionalised collaboration with one another, even where stakeholders expect it to deliver benefits to consumers and markets that exceed its cost. Capacity here means more than budget and staff. Stakeholders also counted expertise, institutional knowledge, organisational effectiveness and institutional standing.

These constraints are compounded by asymmetry. Data protection authorities generally face more severe constraints than their financial-sector counterparts on most dimensions: budget and staffing, institutionalisation and standing. Financial regulators' resourcing in EMDEs is itself uneven, however, and the gap is narrower in some jurisdictions than in others. Many data protection authorities are new enough that they are still settling the scope of their own remit, which makes it harder to be assertive where that remit overlaps with a long-established counterpart's.

The asymmetry is widened by the breadth of the data protection mandate, in which financial services is one sector among many.[101] A data protection authority therefore has limited resources to direct at financial markets, in contrast to the concentrated presence a financial regulator maintains in its own domain. Yet each authority needs enough understanding of the other's domain to discharge its own mandate. A financial supervisor cannot judge whether a fraud-monitoring or credit-scoring system is sound without understanding the data it depends on; a data protection authority cannot assess whether financial processing is necessary and proportionate without understanding the product it powers. Shared domain expertise is therefore a supervisory capability for both authorities, and coordination builds capacity a data protection authority needs rather than only competing for its bandwidth.

Under-prioritisation in goal-setting

The second factor concerns whether coordination is on either authority's agenda at all.

Across the focus countries, DP–FS coordination is almost never an objective against which either authority is measured. It appears in few statutory mandates or strategic plans as a duty, target or indicator, and in none as a standalone measure of success. Financial authorities are measured on prudential soundness, market conduct, financial integrity, payment-system stability and, increasingly, inclusion; data protection authorities on registrations, complaints handled, breaches notified and awareness raised. A global review of data protection authorities' strategies suggests that they have generally found it hard to set strategic, outcome-based measures of their own performance. Until recently, few employed economists, although some more mature authorities have begun to do so.[102] Where an activity carries no institutional consequence, no one has reason to fill the capacity gap that makes it hard. Prioritisation is what gives regulators a reason to build the capacity coordination requires.

101. The effect is greater where data protection is one function of a broader, pre-existing regulator, whether permanently or in the interim; see Section 4.3, Box 9.

102. PrivacyX, "Data Authority Strategies: A Global Review of Current Practice," April 2024, https://privacyx.substack.com/p/data-authority-strategies-a-global; and comments by Steve Wood on a draft of this report.

The clearest evidence lies in how supervisory instruments are built. One financial regulator reported that it had no means of detecting unlawful use of customer data by the institutions it supervises, and that data protection did not feature in its supervision framework. It described its posture as reactive: able to respond to complaints and incidents, but not to examine data-handling risk in advance. The authority had not decided against treating data protection as its concern; its review framework simply never asked the question, so it generated no finding to share, and the occasion for coordination never arose.

Practitioners cautioned, however, that mandating coordination tends to produce slow and rigid structures, and that statutory duties to consult can cause delay. Section 8 therefore distinguishes improving existing arrangements, where lighter measures come first, from designing new institutions, where coordination is cheapest to write in at the start.

Under-prioritisation in workstreams

The third factor concerns when, within a given piece of work, coordination arrives. An authority that wants coordination at the strategic level may still reach its counterpart late in each practical instance. The pattern recurs across the focus countries. In Nigeria, the Central Bank's baseline standards for automated anti-money-laundering solutions drew on FATF standards, but no public evidence of data protection input was identified, although such systems collect, retain, match and transmit personal data at scale; the same is true of the five workstreams established to develop Nigeria's open banking framework. In India, the Reserve Bank's account aggregator framework was designed in 2016, seven years before the data protection law that now governs the same consent-based sharing. In Kenya, the design of open finance is being led by the central bank through the draft National Payment System Policy and Bill, with the data protection authority named among relevant regulators but no documented co-design process (Section 4.3). Open banking is a data-governance design exercise conducted through financial-sector machinery: consent architecture, permitted data categories, retention periods and participant obligations.

The corroborating evidence from other focus countries comes from the financial side. A central bank representative described its data protection authority as having been brought into the open finance programme after the principal design decisions had been taken, and added, unprompted, that it understood the same to have happened in a second jurisdiction. Accounts of late involvement are easy to discount when they come from the authority that was brought in late. They are far harder to discount when the authority that did the involving describes the sequence in the same terms.

The consequence is that coordination, when it comes, is retrofitting, which is both more expensive and less effective than designing in. A data protection authority brought in once a framework is settled has less room to shape its fundamentals, although later coordination can still improve supervision and enforcement. Late involvement also helps explain the paper-only mechanisms examined in Section 4.4, Box 10: a memorandum signed after the principal design decisions have been taken governs less of what matters. This research found one counter-example. The Philippine national identity system's statutory policy council includes the data protection authority and the central bank from the outset, with a mandate to develop implementation policy.[103] The arrangement rests on the instrument that established the system, not on an agreement negotiated between the two authorities afterwards. Designing in coordination is possible.

103. Philippine Identification System Act (Republic Act No. 11055), sec. 16, https://www.lawphil.net/statutes/repacts/ra2018/ra_11055_2018.html; PhilSys, "Composition," accessed 21 October 2026, https://philsys.gov.ph/composition/.

Silos and institutional culture

Regulatory mandates are drawn sector by sector: a banking supervisor for banks, a securities regulator for capital markets, a telecommunications regulator for networks, a payments authority for payment systems. Personal data respect none of those lines. The same identity attribute or transaction record passes through institutions answerable to several supervisors, and the boundaries that make each mandate workable become barriers at the data layer.

Because each authority is accountable only for what falls within its mandate, no authority is responsible for what happens across the line. One data protection regulator described the posture it met from financial-sector counterparts as a 'big brother' relationship: "We already know what we are doing, you are hindering us, and you do not understand the sector." One stakeholder described relations between agencies in the digital sector of their jurisdiction in terms approaching cannibalism, and the arrival of the data protection authority as prompting the question of who this new player was and what it was entitled to decide. These are individual perceptions reported as such, but they illustrate how fragmentation in the digital sector can hamper coordination.

Institutional incentives and professional formation reinforce the silos. Each authority's budget, performance measures and accountability run to its own mandate, so time spent on the other's questions is rarely rewarded. Participants at the programme's Kigali workshop also pointed to differences in professional background, legal and technical, as a source of communication barriers between institutions: the same issue can look like a question of rights to one authority and a question of risk to the other.

> "There is definitely a disconnect between the two where … the regulators work in silos and so they're not able to properly appreciate some of the nuances in the two environments."

Silos within the financial sector are, by contrast, actively managed. The Philippines maintains a standing forum for its financial-sector authorities, and Pakistan's central bank and securities commission operate a joint committee. Managing boundaries between regulators is therefore possible. The boundary with data protection is simply the one most likely to go unmanaged: it is the newest, the most cross-cutting in subject matter, and one of the few at which the counterpart sits outside the financial sector (competition authorities being another notable example).

This is not a case against sectoral mandates, which establish who answers for what, allow deep specialist expertise to accumulate, and give firms certainty about whose rules apply. The point is that fragmentation across mandates creates a coordination gap that, in most focus countries, no institution has been assigned to close. What this points to is a shared work programme across the authorities that touch the data layer, one that leaves each mandate intact but assigns responsibility for the questions that fall between them. The ways the gap materialises are set out in Section 4.1, Box 7, and Section 4.3, Box 9: double-penalty exposure for firms, competing assertions of jurisdiction, and the ministry-as-proxy problem.

The shared-framework gap

The fifth factor is the most operational and the most tractable. Suppose the first four were resolved: two authorities want to work together, have the capacity, have prioritised it in their plans, have sequenced it correctly into their workstreams and face no cultural obstacle. They would still be obstructed, because there is no shared framework through which to do the work: no common taxonomy, no agreed mapping of sensitivity, and no settled procedure for the mechanics of joint working.

Taxonomy shows why. Financial-sector classifications are organised around function and supervisory risk: customer due diligence data, transaction data, credit information, payment data. Data protection classifications are organised around the data subject and the risk to that person: personal data, sensitive or special-category data, biometric data, children's data. The same dataset is described in two vocabularies, and what is sensitive in one may be unremarkable in the other. Transaction-level records may be routine supervisory material to a financial regulator and, to a data protection authority, a granular record of a person's life; conversely, a field treated as ordinary personal data may be the element that enables account takeover. Each authority classifies correctly by its own framework, with no mechanism for reconciling the two, so disagreements that are really about classification present themselves as disagreements about principle.

Demand for shared frameworks has been voiced from several directions. A central bank in one focus country stated a preference for cross-cutting guidance to be written jointly before release, rather than issued separately and reconciled afterwards, and an international expert observed that joint guidelines that regulated entities could apply directly would be of real value. Unlike capacity, which needs sustained funding, or institutional culture, which needs time and repeated contact, this gap can be narrowed substantially by producing artefacts that other authorities can adapt, although each needs local adaptation and maintenance (Recommendation 4).

7.2 The coordination 'anti-flywheel'

The five factors would impede coordination even in isolation; in combination they reinforce one another. To reverse the common metaphor, they form an 'anti-flywheel': efforts to improve coordination that do not produce visible, measurable improvement become part of the problem, feeding further under-prioritisation, redirected capacity and an institutional lesson about what not to try.

Inertia strengthens the loop. Stakeholders acknowledged that some market participants benefit from the status quo: not only bad actors, but also firms whose investment in navigating a low-coordination environment gives them an edge over newer competitors. Regulators may likewise see the risks of closer integration with a counterpart, such as ceding ground or losing relevance, more clearly than its benefits.

The result is under-institutionalisation. Regulators lack tested procedures for cooperation: which information they can exchange and how, which counterparts to work with on what and when, protocols for joint policymaking or oversight, and agreed ways of measuring cooperation and its effects. Cooperation therefore starts at a disadvantage, and if it does not bear fruit quickly, the lesson learned is to invest less.

Loops can also be reversed. Stakeholders were clear that the right investment, in the right initiatives at the right time, could break the cycle. The measure of an early initiative is not only whether it solves a problem but whether it changes what each authority expects the next attempt to achieve. Early measures must be seen to succeed, not merely succeed. That principle orders the recommendations in Section 8.

7.3 How the impediments play out: three patterns

The five impediments play out differently across the focus countries, depending largely on the posture and capacity of the two authorities. Three patterns recur (Table 7.1); these qualitative working profiles, drawn from the country studies and interviews, should be distinguished from the classifications derived from the index in Section 5. These profiles are broad, their boundaries are porous, and they are time-bound: countries can show features of more than one, and their position shifts as institutions and relationships mature.

Co-active. In Brazil, Nigeria, the Philippines and South Africa, both authorities are relatively mature and active in data-intensive financial services. The challenge is not a lack of engagement but the parallel development of sector-specific financial safeguards and horizontal data protection requirements, which can surface as public disagreement. Nigeria's dispute over the collection of customers' social media handles is the clearest example.[104] The priority is alignment and de-confliction: joint work on high-impact themes, consultation before either authority issues rules with significant implications for the other, and a standing working group with defined responsibilities.

Uneven. In Kenya and Uganda, policy development in areas of overlapping mandate is led predominantly by the financial regulator, and data protection participation in that work is uneven. In Uganda, coordination is case-by-case rather than codified: the data protection authority receives breach notifications, handles referred complaints, may seek the assistance of other authorities in investigations, and gives no-objections to individual institutions' cross-border transfers, but no standing instrument governs its relationship with the Bank of Uganda. This is not a question of the data protection authority's capability or activity, generally or specifically with respect to the financial sector. Kenya's data protection authority enforces actively against financial-sector firms, including digital lenders,[105] and received four awards at the 2025 Global Privacy Assembly, which it will host in 2027;[106] yet the design of open finance is being led by the central bank without a clearly documented co-regulatory process. The priority is to make data protection participation in financial policy design and supervision systematic rather than occasional.

104. See Section 4.1. Central Bank of Nigeria (Customer Due Diligence) Regulations, 2023, sec. 6(a)(iv) https://www.cbn.gov.ng/Out/2023/CCD/CBN Customer Due diligence Reg. 2023-combined.pdf; Chris Eke v. Central Bank of Nigeria (suit struck out on the CBN's preliminary objection).

105. Data Protection Office Asks CBK to Revoke Permits"; on the ODPC's investigation of 40 digital lenders, "Data Protection Office Probing 40 Digital https://www.capitalfm.co.ke/business/2022/10/data-protection-office-probing-40-digital-lenders-over-misuse-of-personal-data/Lenders."

106. "Kenya's Data Protection Office Shines with Global Awards, to Host 2027 Privacy Assembly," The Star, 19 September 2025, https://www.the-star.co.ke/news/2025-09-19-odpc-scoops-four-honors-at-global-privacy-assembly.

Emergent. In Ethiopia, India, Indonesia and Pakistan, the data protection architecture is nascent or still evolving, but in three different ways that matter for what can be done now. In Ethiopia, an existing regulator has been given a new remit: the communications regulator has begun providing a registration interface for controllers and processors,[107] so the financial regulator's counterpart is an operating authority with a young mandate. In India and Indonesia, the law provides for a dedicated authority that is not yet fully operational. Indonesia's law has been in force since October 2022, with its transition period ending in October 2024, and its implementing regulation, Government Regulation 33 of 2026, takes effect in January 2027. The authority the law provides for has not yet been established: a draft Presidential Regulation was submitted to the President in May 2026, and the Ministry of Communication and Digital Affairs, through its Directorate General of Digital Space Supervision, oversees personal data protection in the interim. Petitions before the Constitutional Court have sought a deadline for establishing the authority; the government has told the Court that the absence of a deadline should not be read as a legal void;[108] India's Data Protection Board was established in law in November 2025 but, at 30 September 2026, had no appointed Chairperson or Members.[109] In Indonesia, coordination runs through the interim body; in both, it should run into the design of the new authority. Pakistan has not yet enacted a comprehensive data protection law; the immediate counterpart is the ministry leading the legislation, and the opportunity is to write coordination into the law itself. In all three, roles and relationships are still being formed, which creates uncertainty but also the chance to build coordination in before silos set.



107. Communications Service Proclamation No. 1148/2019 (Ethiopia), establishing the Ethiopian Communications Authority; the mandate was extended to data protection by Personal Data Protection Proclamation No. 1321/2024 (Ethiopia) (adopted 4 April 2024; in force 24 July 2024), https://justice.gov.et/en/law/personal-data-protection-proclamation/.

108. Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi, https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022. On the authority's status: Constitutional Court, hearing in case 236/PUU-XXIV/2026 (government testimony that the draft Presidential Regulation was submitted to the President on 20 May 2026), https://www.mkri.id/berita/pembentukan-lembaga-pdp-sedang-dibahas-25476; Constitutional Court, case 153/PUU-XXIV/2026, https://www.mkri.id/berita/kekosongan-lembaga-independen-pelindungan-data-pribadi-25005; on PP 33/2026, https://meridianhukum.com/peraturan/pp-no-33-tahun-2026.

109. Raghvendra Kumar Chaudhary, "India's Data Protection Board: Established in Law, Absent in Fact," LiveLaw, 1 August 2026, https://www.livelaw.in/articles/india-data-protection-board-established-law-543751. The Board provisions came into force with the Digital Personal Data Protection Rules, 2025, notified on 13 November 2025. The Ministry of Electronics and Information Technology invited applications for the posts of Chairperson and four Members on 6 May 2026,

Table 7.1: Three patterns of DP–FS coordination in the focus countries

Pattern	Countries	Principal Coordination Problem	Initial Priority
Co-active: two active and engaged—but not necessarily coordinated—regulators	Brazil, Nigeria, Philippines, South Africa	Active regulators address overlapping issues through separate or issue-specific channels.	Align and de-conflict mandates.
Uneven: policy development led by the one regulator, with uneven participation from the other; coordination often case-by-case	Kenya, Uganda	Data protection input to financial policy design and supervision is occasional rather than systematic.	Make data protection participation in policy design and supervision systematic.
Emergent (i): existing regulator with a new data protection remit	Ethiopia	A young mandate within a broader authority; working relationships still forming.	Establish the working relationship and build capacity.
Emergent (ii): dedicated authority provided for but not yet fully operational	India, Indonesia	Permanent authority still being set up; functions held by an interim body in Indonesia, and by no body in India.	Coordinate with the body holding the remit, where there is one; design coordination into the new authority.
Emergent (iii): no comprehensive data protection law	Pakistan	No dedicated authority; requirements dispersed across laws.	Write coordination into the legislation.

Source: CCAF & Fii.

Chapter 8

Recommendations



This section sets out seven recommendations. Each responds to one or more of the factors in Section 7.1, and each sets out what it involves, where it applies, what it needs, the safeguards it requires and how progress would be judged. Table 8.1 sets out the timing of all seven. In some jurisdictions existing powers already permit the work; in some, a specific legal gateway or clarification is needed before it can proceed; and in others the data protection authority is not yet operational, so that coordination can be built into its foundations. Many practical improvements can begin under existing powers; particular activities (such as exchanging case-level personal data) and structural reforms need separate legal assessment in each jurisdiction. The test throughout is whether a mechanism operates, not whether it exists (Section 4.4, Box 10).

The recommendations are parallel workstreams with dependencies, not a sequence to be completed one after another. A small set of foundations should be put in place together at the start: a senior sponsor and a responsible manager in each authority, allocated staff time, named contacts, the choice of an anchor problem and a baseline (Recommendations 1, 2 and 6). Joint instruments (Recommendation 4) will often be the anchor's first deliverable rather than a later stage. Beyond the foundations, two tracks run at different speeds. Improving existing arrangements is gradual: lighter measures first, and firmer commitments where they have shown their value. Designing new institutions and frameworks follows the timetable of the framework itself: where an open finance regime, a digital identity system or a new data protection authority is being established now, the data protection role should be secured now, in the establishing instrument. Table 8.1 sets out both tracks.

Coordination has costs and risks of its own. Joint working takes staff time and adds governance overhead, and duties to consult can delay decisions. It can blur accountability, making it less clear which authority answers for an outcome, and a joint position can be harder to challenge than a single authority's decision. Where capacity is unequal, joint work can drift towards the stronger authority's priorities, which for a newer data protection authority can shade into erosion of its independence. Sharing information between authorities widens access to personal and confidential data and creates cybersecurity exposure. And the authorities' objectives overlap without being the same: safety and soundness, financial integrity, consumer protection and individual rights can pull apart in a given case.

These are reasons to design coordination carefully, not to avoid it, and the measures below were developed with these costs and risks in mind. Consultation will often be enough; targeted referral suits matters that engage both mandates; and on some questions each authority should act independently and in parallel. In every case each keeps its own statutory decisions, and those decisions remain open to challenge in the courts. Starting with lightweight, reversible measures, framed around processing rather than individual cases (Recommendation 2), keeps these costs low.

Recommendation 1: **Start with one shared problem and make the result visible**

The 'anti-flywheel' (Section 7.2) means that the first thing coordination must do is work, and work visibly. Authorities should begin with one or two anchor problems which intersect mandates, addressed with time-bound joint workstreams leading to defined outputs, rather than general commitments to cooperate.

Of the five thematic areas above, three emerged from the research as the most promising.[110] Fraud prevention depends on timely data sharing across institutions, yet the legal basis, safeguards and operational conditions for that sharing are often unclear; authorities in focus countries repeatedly named it as a priority. Credit underwriting, including AI, sits between the financial authority's oversight of lenders and the data protection authority's mandate over personal data, and practices such as intrusive data collection, opaque automated decisions and debt shaming call for consistent standards. Open finance is a strong anchor wherever its design choices (consent standards, the scope of portable data, third-party eligibility) are still open; where a framework is already operating, joint work turns to supervision and redress.

Where the problem warrants it and capacity allows, the anchor can grow into a joint pilot, including tests of privacy-enhancing technologies, with published findings; a well-run bilateral workstream may be enough on its own.

This applies in all three patterns. Where a legal gateway is missing, the first deliverable should be one that does not depend on it; where the data protection authority is not yet operational, the work should proceed with the body that holds the remit in the interim. Agreeing the anchor, a joint lead in each authority and the first deliverable should take no more than a quarter, and the deliverable itself should follow within a year: for example, a joint statement on lawful fraud-data sharing (Recommendation 4) or a referral protocol for digital-lending complaints (Recommendation 2). The work needs a responsible manager and protected part-time commitment from a small number of officials in each authority, access to legal advice on data sharing and, where the data protection authority is the smaller partner, support for its participation, such as drafting capacity, technical input or a funded secondment. A joint statement or referral protocol can generally proceed under existing powers. A fraud-data-sharing deliverable needs a legal assessment first of whether each authority may disclose the data, to whom, on what basis and under what conditions; where no gateway exists, the deliverable becomes an analysis of the legal change required.

Each authority keeps its own statutory decisions, and disagreements that remain are recorded rather than smoothed over. Where practitioners and industry contribute expertise, their interests are declared and the assessment of evidence stays with the authorities; some resistance, particularly from those who benefit from the status quo (Section 7.2), will not yield to dialogue and should not be expected to. Progress is judged in three steps: whether the first deliverable is adopted on time; whether officials and firms apply it and matters are handled under it; and whether indicators tied to the anchor, such as referral delays or unresolved complaints, improve. Those indicators need careful reading, because better reporting and better access to redress can raise recorded fraud and complaint volumes. The twelve-month review therefore asks whether the mechanism operates and shows credible progress, not whether aggregate fraud losses have fallen, and decides whether to continue, widen or stop.

110. While AML/CFT is a pressing area requiring additional coordination, stakeholders generally viewed this as a challenge that invariably entails the international layer, making it less promising as a candidate for immediate national-level coordinated action.

Recommendation 2: **Designate counterparts and referral routes**

Silos (Section 7.1) show up first as uncertainty about who owns an issue. Each pair of authorities should name cross-regulatory contact points with escalation rules, and adopt a referral protocol that sets out which authority or department handles each category of matter: AML/CFT investigations involving personal data, fraud intelligence, cross-border transfers and cloud outsourcing, open finance, AI and digital lending, and data breaches at regulated firms, where the protocol should say who is notified and who leads.

A pair of authorities is the starting point, not the limit. An arrangement should widen to a third authority when the data chain or the remedy runs through it: the telecommunications regulator for SIM-swap fraud, the identity authority for digital ID enrolment and verification, the consumer protection or competition authority for debt shaming and other abusive collection, and the financial intelligence unit for suspicious-transaction data. Where several financial regulators share a mandate, each should be party to the protocol for the matters it supervises. On the firm side, data protection officers are a natural point of contact for matters routed under the protocol.

Before creating anything new, they should audit what already exists. The audit will typically find instruments that are live and operating, instruments that are live on paper only, and instruments that are dormant or that neither authority can locate. Operating instruments should be given the procedural detail that makes them self-executing: notification duties, named counterparts, escalation routes and review dates. Dormant ones should be revived with a work programme or formally retired, and paper-only ones pushed into one or the other.

Where a formal agreement is unnecessary, an administrative arrangement, joint statement or standing contact desk may serve. If the volume and complexity of matters warrant it, the channel can develop into a working group with a defined mandate, published procedures and time-bound outputs. In many cases a functioning bilateral referral arrangement is the right durable solution, and some authorities prefer bilateral arrangements where sensitive supervisory material is involved. Joint scenario exercises, on a fraud investigation or a cloud-outsourcing incident for example, test the protocol before a live matter does.

> “When you have a designated point of contact, it makes collaboration a lot easier. It builds [institutional] memory and also the relationship.”

This can proceed under existing powers, and in emergent jurisdictions with the body that holds the remit in the interim. Named contacts should be in place within one quarter, alongside the other foundations; the audit within two quarters; and a referral protocol within a year. The work needs a contact point in each authority with protected time, a manager accountable for the protocol and staff time for the audit. Naming contacts and referring matters can generally proceed under existing powers; exchanging personal data about specific cases needs a legal assessment in each jurisdiction and may need a gateway, and framing referrals around types of processing rather than individual cases avoids much of this.

The protocol should state which authority owns a consumer's complaint, when and how the consumer receives an answer, and the time limits that apply; any information exchanged should have a stated purpose, a defined access list, a retention period and a route for correction. Progress is judged by whether contacts are named, the audit completed and the protocol adopted; whether matters are referred under it and every instrument on a joint register is classified as operating or retired; and, as outcomes, by time to resolution for referred matters and the share of in-scope complaints (those engaging both mandates, as the protocol defines them) that have an identified owning authority, tracked through a shared log.

Recommendation 3: **Bring the data protection authority in at the design stage**

Late involvement (Section 7.1) turns coordination into costly retrofitting. Authorities should build consultation triggers, with clear materiality thresholds, into processes they already run: registration, licensing, accreditation, outsourcing and cloud approvals, and supervisory reviews. Thresholds can turn on the scale of processing, the number of customers affected, the degree of automation, cross-border transfers, or the potential effect on consumer rights and financial stability. Each authority should also consult the other before issuing rules, guidance, and similar documents with significant implications for the other's mandate — ideally early in the process.

Sandboxes are a natural place to start. A fully joint sandbox requires both authorities to run testing infrastructure; giving the data protection authority a defined role at the admission, review and exit stages of an existing financial-sector sandbox requires only one, and is the more widely achievable route. For frameworks now being designed, such as open finance, digital identity and wider digital public infrastructure, the data protection authority should sit in the design body from the outset. Kenya's Draft National Payment System Policy and Bill, published for consultation in September 2026, is a live example of such a framework.[111] Indonesia offers another. Law 4 of 2026, amending the financial-sector development law, requires the Government to form a task force covering unlicensed financial activity and licensed firms showing indications of collection violations, data misuse or consumer protection breaches. Its membership, to be fixed by a Presidential Regulation that is still pending, will show whether the data protection function has a seat.[112]

111. National Treasury and CBK, Draft National Payment System Policy and National Payment System Bill, 2026 (comments due 9 October 2026), https://www.centralbank.go.ke/2026/09/21/draft-national-payment-system-policy-and-national-payment-system-bill-2026/.

112. Law 4 of 2026 (Indonesia), art. 247(1) (17 June 2026), https://pasal.id/peraturan/uu/uu-no-4-tahun-2026/pasal-247 (unofficial text); Robertus Andrianto, "DPR & Pemerintah Sepakati Bentuk Satgas Pindar & Judol di RUU P2SK," CNBC Indonesia, 3 June 2026, https://www.cnbcindonesia.com/market/20260603180818-17-739875/dpr-pemerintah-sepakati-bentuk-satgas-pindar-judol-di-ruu-p2sk.

This applies wherever existing powers permit and, above all, wherever a framework or institution is being designed now. A standing statutory role requires legal change, which is easiest to secure in the instrument that establishes the framework, following the Philippine route (Section 7.1). Authorities should identify the frameworks in design at the start, secure the data protection role in each on the framework's own timetable, and agree triggers and a pre-consultation protocol within twelve months. The main resource constraint is staff time in the data protection authority to respond within consultation windows, together with a coordinator in the financial authority to operate the triggers. Consultation between authorities can generally proceed under existing powers, although some statutes prescribe consultation procedures.

Consultation windows should be time-limited, so that consultation does not become delay, and consultation does not transfer the decision. Progress is judged by whether triggers and a protocol are adopted and a data protection role is secured in frameworks under design; by the share of in-scope rules and licensing decisions that receive data protection input before they are finalised; and by the changes made as a result, set against the time consultation adds.

Recommendation 5: **Build each authority's understanding of the other's domain**

Capacity and associated asymmetries (Section 7.1) are addressed most directly by building each authority's working knowledge of the other's field: for data protection authorities, prudential supervision, AML/CFT obligations and payments architecture; for financial regulators, lawful basis, profiling, automated decision-making and transfer mechanics. Options range from two-way attachments and joint scenario exercises, through longer secondments carrying responsibility for live matters and communities of practice at technical and senior levels, to joint training built into induction and continuing professional development. Choices should follow problems and capacity.

Two further measures support this. Secondments and joint work should count towards progression in the home institution; otherwise, the officials most valuable at the interface bear potential career costs, which falls hardest on the smaller authority. And where regional arrangements exist, skills that single authorities struggle to sustain, such as model auditing, assessment of privacy-enhancing technologies and forensic data analysis, can be pooled and drawn on by members, which matters most to data protection authorities.

This applies in all three situations, and most urgently where the data protection authority is new. A first step is one attachment in each direction and one joint scenario exercise on the anchor problem within twelve months. The resources are the placement itself, cover for the seconded officer's role and training time; for a smaller authority, funded placements may be the only practical route. Confidentiality of supervisory information may limit what a secondee can see, and secondment agreements should settle this in advance.

The joint agenda should be set mutually, so that joint work does not drift towards the larger authority's priorities. Progress is judged by whether attachments and exercises are completed; whether officials with cross-domain experience work on live matters and are retained after they return; and whether joint matters proceed without stalling for lack of expertise, and communities of practice survive the departure of their convenor and the end of external funding.

Recommendation 6: **Measure and report on coordination**

Under-prioritisation in goal-setting (Section 7.1) persists because little in how either authority is measured counts coordination as work done. Engagement is needed at two levels. Coordination that reaches only working level tends to depend on individuals and to lapse when they move; leadership commitment without working-level engagement produces agreements that are never put into operation. Each authority should therefore name a senior sponsor, include coordination objectives in departmental work plans, allocate staff time, and report on coordination to leadership, anchored to a small number of shared indicators, such as time to resolution of referred matters or the share of complaints with an identified owning authority. Where governments fund regulatory priorities centrally, earmarked funding that authorities bid for jointly can reward coordination without the rigidity of a mandate. For existing institutions, coordination can later be written into mandates, strategies, budgets and performance frameworks once mechanisms have produced results worth protecting: encourage first, embed later, and never preserve any arrangement for its own sake. For institutions being created now, the sequence reverses: coordination duties and a role for the counterpart are cheapest to write in at inception (Recommendation 3).

Measurement should run throughout. Working groups that publish outputs, sandboxes that publish findings and instruments registered together generate an evidence base at little cost; reconstructing it later is expensive and usually incomplete. Indicators should count resolution rather than activity: matters referred and resolved, time to resolution, adoption of joint outputs, and complaint volumes in areas both authorities own. Peer review, on models already familiar to financial authorities, should be developmental rather than tied to ratings, with findings usable by the reviewed authority before anyone else. The Regulatory Coordination Index illustrated in Section 5 could become a self-administered tool of this kind, once validated with the authorities against coded evidence, and built on live and workable outcome (not activity) indicators.

This can proceed under existing powers; for a new authority, it belongs in the founding strategy and, where possible, the establishing instrument. At the start, alongside Recommendations 1 and 2, each authority should name a senior sponsor and a responsible manager, include one coordination objective in its next annual plan and record baseline indicators. It needs senior time for sponsorship, staff time to keep a shared log and report, and a funded convenor if peer review is pursued. Plans and reporting need no legal change; embedding coordination in the mandates of existing authorities requires legislation and separate legal assessment.

Indicators should reward resolved matters rather than meetings, and peer review should be developmental rather than punitive. Progress is judged by whether objectives are in plans and baselines recorded; whether coordination is reported on at leadership level; and whether resolution-based indicators improve, read with attention to changes in reporting, with claims about attribution framed with appropriate caution.

Recommendation 7: **Connect national coordination to regional and international standard-setting**

National coordination is harder where the international architecture leaves one side out. The membership of the global bodies that set financial standards was settled before data protection authorities existed in most of the focus countries. Whatever the reasons participation remains limited today, widening it is a long-horizon project.

Three routes are realistic. The first is data protection participation in international mechanisms as they are created or renewed; the Financial Stability Board's Forum on Cross-Border Payments Data, which involves data protection authorities, is a precedent.[113] The second is a channel between the global data protection bodies and financial standard-setters for joint guidance where both regimes bear on the same obligation, a direction the FATF itself endorsed in July 2026 when it recommended joint guidance between AML/CFT and data protection authorities.[114] The third, where the focus countries have most leverage, is regional: linking regional data protection and financial working groups, and working towards mutual recognition of specific artefacts such as transfer assessments, sandbox outcomes and supervisory findings.

The aim is generally interoperability between regimes, not uniformity within them; stakeholders repeatedly stressed the need for national contexts to shape national-level policies and implementations.

This applies in all three situations. A first step is a coordinated national position in the next relevant international consultation, together with identification of the regional bodies through which to pursue mutual recognition. It needs staff time to coordinate national positions, and participation in international fora carries real preparation and travel costs, which weigh most on data protection authorities. Sharing supervisory findings across borders requires gateways and separate legal assessment.

The aim is interoperability rather than uniformity, so that national authorities keep their discretion. Progress is judged by whether coordinated national positions are submitted; whether data protection authorities participate in the relevant international and regional fora; and whether at least one artefact is recognised across jurisdictions.

113. FSB, "FSB Announces Establishment of the Forum on Cross-Border Payments Data https://www.fsb.org/2025/03/fsb-announces-establishment-of-the-forum-on-cross-border-payments-data/"; FSB, "Forum on Cross-Border Payments Data Convenes for the First https://www.fsb.org/2025/05/forum-on-cross-border-payments-data-convenes-for-the-first-time/Time."

114. FATF, Information Sharing to Combat Illicit Finance https://www.fatf-gafi.org/en/publications/Methodsandtrends/information-sharing-ppp-data-protection-arrangements.html.

Table 8.1: Parallel workstreams: foundations, improvement of existing arrangements, and design of new frameworks

Workstream	Months 0–3: Start together	Months 3–12	Years 1–3 (options, where warranted)	New frameworks and institutions (on their own timetable)
1. Anchor problem	Choose the anchor; name joint leads.	First deliverable by month 9–12; twelve-month review.	A second anchor or a joint pilot.	Make the anchor part of the framework's design work.
2. Counterpart and Routing	Named contacts.	Audit by month 6; referral protocol.	Working group if volume warrants; revive or retire instruments.	Referral routes built into the framework.
3. Design stage	Identify frameworks in design.	Triggers; pre-consultation protocol.	Data protection role in sandbox admission, review and exit.	Data protection role in the design body and establishing instrument, now.
4. Joint instruments		Joint guidance as first deliverable, where suited.	Cross-domain taxonomy; model instruments, adapted locally.	Shared definitions adopted in the framework.
5. Capacity		One attachment each way; scenario exercise.	Secondments; communities of practice; regional pooling where available.	Joint induction for staff of a new authority.
6. Make it count	Senior sponsors; manager; staff time; baselines.	Objective in annual plan; shared log.	Resolution-based reporting; developmental peer review; validate an index.	Coordination duties in the establishing instrument.
7. Regional and international		Coordinated national positions.	Regional links; mutual recognition of artefacts.	

Source: CCAF & Fii.

Chapter 9

Conclusion



This report examined coordination between data protection and financial-sector authorities across ten emerging markets. Where a data protection authority is operational, most of the statutory tools that coordination needs already exist: authorities can consult one another, issue guidance jointly and enter cooperative arrangements, and in three focus countries the law directs the data protection authority to coordinate or collaborate with other regulators. The power to disclose particular information is narrower, and some activities will need a specific legal gateway; an MoU can implement existing powers but cannot create them. Where the authority is not yet operational, as in India, Indonesia and Pakistan, the task is to build coordination into its foundations. What is most often missing is the institutional machinery to use these tools routinely. Coordination today is mostly ad hoc, event-driven and dependent on individual relationships.

Five factors generally explain why: capacity constraints and asymmetries; under-prioritisation in goal-setting; late entry into workstreams; silos; and the absence of shared frameworks. They reinforce one another, but the cycle can be reversed by interventions substantial enough to produce visible results.

The stakes are practical. For consumers, coordination means that a single harm meets a single coherent response and a route to redress. For responsible firms, it means building products on a settled legal basis with a lighter compliance burden (one set of reconciled expectations instead of overlapping reports, interpretations and investigations), a benefit that matters most to smaller and newer providers. For regulators, it means scarce expertise pooled and supervision that keeps pace with increasingly data-intensive markets. Together, these support competition, innovation and inclusion, to the benefit of consumers, markets and economic development in EMDEs.

Timing matters too. The rules for AI in credit, digital identity, open finance and the data that accompany cross-border payments are being set now, and coordination designed in is generally cheaper and more effective than coordination retrofitted. Delay risks entrenching inconsistent regulatory expectations and institutional practices, making coordination harder and more costly to establish later.

The next twelve months offer specific openings. India's Data Protection Board takes on its first functions from November 2026, with most obligations following in May 2027; Indonesia's implementing regulation takes effect in January 2027, while its authority is still to be formed; Kenya is finalising a payment-system law with open finance provisions; Pakistan's data protection bill has yet to be enacted; and the FATF expects to finalise its Recommendation 16 guidance in February 2027. In each case, the data protection role can be written in now, at little cost, or retrofitted later, at much greater cost.

In summary, data protection and financial authorities should together choose one shared problem and produce a result within a year, using powers they already hold. They should route matters to a named counterpart, under a protocol that says which authority answers the consumer. And they should bring each other into designs of frameworks now being built, before the principal decisions are taken. These initial efforts should be supported by targeted capacity building and assessment of results, with successful approaches embedded in standing protocols and shared workplans.

The theme that recurred most persistently across this research was trust: consumers trust that their information will be treated fairly and that the system will respond when it is not; firms trust that the rules are coherent; and regulators trust in one another to consult before rather than after, and to accept that a mandate exercised jointly is not a mandate diminished. Data protection and financial integrity are non-negotiable conditions of the trust on which data-driven finance depends. The first step is deciding that coordination is worth the work.

Appendix

Detailed country evidence tables

This appendix sets out the full country evidence tables summarised in Section 4 (Tables 4.1 to 4.3), with their sources. Status is at 30 September 2026 unless otherwise stated. Reported fraud figures for all ten countries, with their sources and periods, are in Annex C, Table C.9; they are not directly comparable across countries and are not repeated here.

Appendix table 1: Fraud coordination and the position of the data protection authority

Jurisdiction	Financial crime/ fraud coordination	Data protection authority's role	Nature of the gap
Nigeria	CBN, NFIU, NIBSS; the Person of Interest Portal, developed by NIBSS with the CBN and security agencies, lists more than 13,000 individuals linked to suspected fraud[115]	No formal NDPC role identified in the fraud-intelligence mechanisms reviewed.	Public–public: identifiable intelligence pooled without the authority whose remit it most engages.
India	RBI, FIU-IND, SFIO, Enforcement Directorate, I4C; I4C's Citizen Financial Cyber Fraud Reporting and Management System links banks and police[116]	Data Protection Board legally established (November 2025) but no Chairperson or Members appointed at 30 September 2026; MeitY represented on the FSDC by its Secretary (a ministry, not the regulator).	DPA outside the architecture; over-broad controls risk de-risking and exclusion.
Philippines	BSP, CICC, NBI, SEC, AMLC (FIU); BSP investigative and account-hold powers under the Anti-Financial Account Scamming Act (2024)	NPC–CICC MoA (June 2021) on reciprocal training; a December 2022 MoA provides for assignment of NPC privacy lawyers to the National Cybercrime Hub.[117]	Strongest DP integration, but fragmented within FS (separate BSP/IC/SEC ties).

115. On fraud trends and the portal: NIBSS, 2023 Annual Fraud Landscape (2024), https://nibss-plc.com.ng/wp-content/uploads/2024/04/2023-Annual-Fraud-Landscape.pdf (₦11.61bn in 2020; ₦17.67bn in 2023); NIBSS, "Digital Payment Fraud Drops 51% to N25.85b, Lagos Accounts for 63%," 22 January 2026, https://nibss-plc.com.ng/digital-payment-fraud-drops-51-to-n25-85b-lagos-accounts-for-63/ (₦52.26bn in 2024, "largely driven by a single fraud incident of N31.1 billion involving one entity"; ₦25.85bn in 2025); on the portal, "CBN, NIBSS Name 13,417 Fraud Suspects on New Portal as Crackdown Tightens," Legit.ng, 26 January 2026, https://www.legit.ng/business-economy/economy/1694100-cbn-nibss-13417-fraud-suspects-portal-crackdown-tightens/.

116. Prevention of Money-Laundering Act, 2002, sec. 12, and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, requiring reporting entities to furnish suspicious transaction reports to the Financial Intelligence Unit — India. The Indian Cyber Crime Coordination Centre (I4C) operates under the Ministry of Home Affairs.

117. Memorandum of Agreement between the National Privacy Commission and the Cybercrime Investigation and Coordinating Center (Philippines).

Jurisdiction	Financial crime/ fraud coordination	Data protection authority's role	Nature of the gap
Kenya	FRC with CBK, DCI and ARA[118]	Whether the ODPC counts as a 'competent authority' for FRC information sharing under the AML regulations is untested; its own powers derive from the Data Protection Act.	Established statutory sharing among financial-crime bodies; DP oversight of that sharing not yet built in.
South Africa	Twin Peaks; FIC, FSCA, PA, police; SABRIC (industry); SAMLIT, Fusion Centre, inter-agency groups[119]	Information Regulator not a member of the principal forums; observer on the AML/CFT/CFP Interdepartmental Committee.	Mature coordination capacity, DP expertise not embedded.
Uganda	BoU, FIA, UCC, police, industry	No standing mechanism integrating the PDPO; coordination is case-based, including breach notification to the PDPO under section 23 of the Data Protection and Privacy Act, in parallel with reporting to the Bank of Uganda.	Practical collaboration without institutionalised DP governance.
Ethiopia	NBE and the Financial Intelligence Service; largely sector-by-sector; Fayda digital ID emerging	ECA (under PDPP 1321/2024) sets general principles; no formal fraud-sharing arrangement identified.	Cross-sector fraud risks (for example, SIM-swap) are likely to outpace coordination.
Pakistan	SBP, SECP, FMU; SBP-SECP Coordination Committee	No enacted comprehensive data protection law or authority; privacy protections through the Prevention of Electronic Crimes Act 2016 (as amended), with cybercrime enforcement now by the NCCIA.	Sequencing: data-intensive FS controls ahead of any DP counterpart.
Brazil	BCB rules for Pix participants and fraud controls, including the Special Return Mechanism (MED); COAF (FIU)	ANPD jurisdiction over unlawful processing, safeguards, and breaches.	Clear individual mandates; interface for blended incidents underdeveloped. (interview evidence)
Indonesia	OJK Regulation 12/2024 on anti-fraud strategy; PPATK (FIU); Indonesia Anti-Scam Centre; Police, Komdigi[120]	PDP Law in force since 2022; dedicated authority not established at 30 September 2026 (Komdigi acting in the interim).	Sequencing: a dedicated cross-sector anti-scam platform operates ahead of the data protection authority.

Source: CCAF & Fii.

118. On banking-sector fraud trends: CBK, Financial Sector Stability Report 2024, reporting that direct fraud losses in the Kenyan banking sector rose to approximately KSh 1.6 billion in 2024 from KSh 412 million in 2023, with reported cases rising to 353 from 173 and total exposure climbing to approximately KSh 1.96 billion. Mobile banking accounted for the largest share of losses at approximately KSh 810 million. See also "Kenya's Sh1.6 Billion Fraud Losses Expose Rising Mobile Banking Risks," Kenya Banking Insights, 10 September 2025, https://kenyabankinginsights.co.ke/kenyas-sh1-6-billion-fraud-losses-expose-rising-mobile-banking-risks/. The figures used here are from the report's fraud table; the report's narrative gives 153 cases and KSh 596.4 million in losses for 2023, so the 2023 baseline differs between parts of the same report.

119. South African Anti-Money Laundering Integrated Task Force (SAMLIT), established by the Financial Intelligence Centre in 2019 as a public–private partnership; and the Fusion Centre, convened under the Anti-Corruption Task Team. Financial Sector Regulation Act 9 of 2017 establishes the Twin Peaks architecture comprising the Prudential Authority and the Financial Sector Conduct Authority.

120. Otoritas Jasa Keuangan (OJK), Peraturan OJK No. 12 Tahun 2024 tentang Penerapan Strategi Anti Fraud bagi Lembaga Jasa Keuangan (2024), https://ojk.go.id/id/regulasi/Pages/Penerapan-Strategi-Anti-Fraud-Bagi-Lembaga-Jasa-Keuangan.aspx.

Appendix table 2: Open finance frameworks and their data protection interface

Jurisdiction	Imple-mentation status	Open finance framework and lead regulator	Data protection counterpart	Coordination position and remaining gaps
Brazil[121]	Live	Central Bank of Brazil (BCB) and National Monetary Council (CMN): Joint Resolution 1 of 4 May 2020, as amended, and BCB implementing rules. Open finance is operational; the LGPD supplies the general privacy layer.	ANPD administers the LGPD. Special autonomous authority status dates to 2022. Its subsequent conversion into a regulatory agency began in September 2025 and was confirmed by Law 15,352 of 25 February 2026 (published 26 February).	LGPD Articles 55-J and 55-K expressly require coordination with sector regulators and assign ANPD central responsibility for interpreting the LGPD. Separate sector and privacy requirements remain.
India[122]	Live	Reserve Bank of India (RBI): NBFC Account Aggregator Directions, 2016, as amended. Account Aggregators (AAs) support operational, consent-based financial information sharing.	Digital Personal Data Protection Act 2023 and final DPDP Rules 2025. The Data Protection Board was legally established in November 2025 but had no Chairperson or Members at 30 September 2026; commencement is phased. Consent Manager provisions start in November 2026 and most substantive obligations and enforcement provisions in May 2027.	AA licensing and DPDP Consent Manager registration are distinct regimes. The final rules do not themselves grant automatic Consent Manager status to licensed AAs.
Pakistan[123]	Pilot (sandbox)	State Bank of Pakistan (SBP): open banking was a theme of the first regulatory sandbox cohort. Three open banking participants tested from January to June 2026; SBP announced cohort completion on 15 September 2026, noting that completion does not imply regulatory approval. This establishes a pilot stage, not a national operational framework.	Comprehensive data protection legislation remains a bill, with no authority yet established under it. Sectoral banking, technology and cybercrime requirements continue to apply.	No data protection counterpart yet exists, so data protection questions in the open banking pilot rest with SBP rules alone. A comprehensive law, when enacted, would be the moment to settle the authority's role in open finance.

121. ANPD's special autonomous status dates to 2022; its later conversion into a regulatory agency is a separate event. Central Bank of Brazil (BCB) and National Monetary Council (CMN), Joint Resolution No. 1 of 4 May 2020, as amended, https://normativos.bcb.gov.br/Lists/Normativos/Attachments/51028/Res_Conj_0001_v3_P.pdf; BCB, "Open Finance comemora 5 anos de regulamentação em evento no próximo dia 28 de Agosto," 27 August 2025, https://www.bcb.gov.br/detalhenoticia/20813/noticia; ANPD, "Base jurídica da estrutura organizacional e das competências," accessed 21 October 2026 (legal basis and institutional history, including Laws 14,460/2022 and 15,352/2026), https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/base-juridica; LGPD, arts. 55-J(XXIII), 55-J secs. 3–4, and 55-K, https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

122. Legal establishment of the Board and commencement of enforcement powers are different milestones. Final Rule 4 and the First Schedule create a separate Consent Manager registration pathway; they do not provide for automatic recognition of licensed AAs. Sahamati's March 2025 paper is an industry submission about then-draft rules, not a binding reconciliation instrument. RBI, Account Aggregator Directions, 2016, as amended, including Review of Financial Information Provider (FIP) under Account Aggregator Framework, RBI/2023-24/76, 26 October 2023, https://www.rbi.org.in/scripts/FS_Notification.aspx?Id=12557&Mode=0&fn=14; Ministry of Electronics and Information Technology (MeitY), G.S.R. 844(E), 13 November 2025 (Board establishment), https://www.meity.gov.in/static/uploads/2025/11/cc217843dc3bcb37b2b05bcc3b4e031f.pdf; MeitY, G.S.R. 843(E) (phased commencement), paras. (a)–(c), https://www.meity.gov.in/static/uploads/2025/11/c56ceae6c383460ca69577428d36828b.pdf; MeitY, Digital Personal Data Protection Rules, 2025, rr. 1 and 4 and First Schedule, https://www.meity.gov.in/static/uploads/2025/11/53450e6e5dc0bfa85ebd78686cadad39.pdf; Rutvik Paikine, "Reconciling the Account Aggregator and Consent Manager Frameworks," Sahamati, 18 March 2025, https://sahamati.org.in/reconciling-the-account-aggregator-and-consent-manager-frameworks/.

123. "Pilot" includes a completed pilot awaiting a wider regime. The January SBP notice specifies controlled live testing for up to six months; its September media listing confirms cohort completion. A May 2026 parliamentary answer refers to the initiative as an "Act" but describes a finalised bill; it has not been enacted. State Bank of Pakistan (SBP), "SBP Announces the Shortlisted Applicants for the First Cohort of Its Regulatory Sandbox," press release, 6 January 2026, https://archive.sbp.org.pk/press/2026/Pr-06-Jan-2026.pdf; SBP, "SBP Concludes First Cohort of its Regulatory Sandbox," 15 September 2026, https://www.sbp.org.pk/assets/documents/press-release/PR-15-Sep-2026.pdf; National Assembly of Pakistan, Debates, 14 May 2026, 34 (Personal Data Protection Legislation), https://na.gov.pk/uploads/documents/6a1d62bdce349_708.pdf; Ministry of Law and Justice (Pakistan), published legislation and draft bill listing, accessed 21 October 2026, https://molaw.gov.pk/.

Jurisdiction	Imple-mentation status	Open finance framework and lead regulator	Data protection counterpart	Coordination position and remaining gaps
Nigeria[124]	Framework adopted; no official go-live announced at 30 September 2026	Central Bank of Nigeria (CBN): Regulatory Framework for Open Banking, 2021, and Operational Guidelines, 2023.	Nigeria Data Protection Act 2023 established the Nigeria Data Protection Commission (NDPC). Its General Application and Implementation Directive (GAID) followed in 2025.	CBN rules already address retention and consent withdrawal, including a seven-year minimum retention provision. How these rules apply alongside NDPA requirements needs clarifying. No published joint CBN–NDPC open banking guidance was identified in the record reviewed; the CBN's February 2026 fintech report commits to guidance on data portability, a natural opportunity for joint guidance.
Kenya[125]	Proposed	Central Bank of Kenya (CBK) and National Treasury published draft National Payment System Policy and Bill, 2026, for consultation on 21 September 2026 (consultation open at the cut-off; it closed on 9 October 2026). The package includes open finance provisions. It goes beyond the earlier payments strategy and feasibility work.	Office of the Data Protection Commissioner (ODPC), under the Data Protection Act 2019. General data protection obligations apply independently of the proposed payments reforms.	The draft policy includes ODPC among relevant regulators. Final allocation of responsibilities and implementation rules remains to be settled. The Open Finance Initiative is an industry/development partnership of FSD Kenya, KBA and AFIK; it does not itself enact or administer a statutory regime.
South Africa[126]	Proposed	Financial Sector Conduct Authority (FSCA), working with other authorities: 2023 draft position paper was followed by Open Finance Policy Recommendations in March 2024. A tailored mandatory framework is proposed; existing commercial data-sharing activity is not equivalent to its adoption.	Information Regulator under the Protection of Personal Information Act 4 of 2013 (POPIA). It is not listed as a member of the Intergovernmental Fintech Working Group (IFWG), but contributed substantive recommendations to FSCA's open-finance work.	Coordination is already occurring: FSCA's policy work describes the Information Regulator as a key partner and records its recommendations on consent, impact assessments, security and complaints. Further institutional arrangements and standards remain part of the programme of work.

124. Nigeria. No official national go-live has been announced. Open Banking Nigeria's page, labelled updated July 2026, still describes launch preparations, but also retains older forward-looking dates; it does not give a reliable launch timetable. CBN's 2026 sandbox invitation permits open-banking applications without establishing that a national pilot or production regime has begun. CBN's Shared Information Framework, sections 4.1–4.2 (pages 58–59), addresses retention and withdrawal. Withdrawal of consent is not necessarily immediate erasure where retention is legally required. CBN, Operational Guidelines for Open Banking in Nigeria, March 2023, including Shared Information Framework, https://www.cbn.gov.ng/Out/2023/CCD/Operational%20Guidelines%20for%20Open%20Banking%20in%20Nigeria.pdf; CBN, Shaping the Future of Fintech in Nigeria: Innovation, Inclusion and Integrity, Policy Insight Series (released February 2026) (implementation priorities), https://www.cbn.gov.ng/Out/2026/CCD/CBN_FINTECH_REPORT_.pdf; CBN, "CBN Regulatory Sandbox: Cohort 2 Applications Open," accessed 21 October 2026 (scope and admission limitations), https://sandbox.cbn.gov.ng/; Open Banking Nigeria, "Open Banking in Nigeria," last updated July 2026, https://openbanking.ng/open-banking-in-nigeria/; NDPC, Annual Report 2025 (2026) (NDPA and GAID implementation), https://ndpc.gov.ng/wp-content/uploads/2026/02/Print_NDPC-Annual-Report-2025-1.pdf.

125. Kenya. The consultation opened on 21 September 2026. The draft policy identifies open finance as an area requiring modernisation and includes ODPC in implementation arrangements. The accompanying draft bill lists clause 29 on open finance. These proposals are not adopted law. CBK, "Public Notice: Draft National Payment System Policy and National Payment System Bill, 2026," 21 September 2026, https://www.centralbank.go.ke/press/; National Treasury and CBK, Draft National Payment System Policy (August 2026), secs. 1.3 and 4.1 and implementation matrix, https://www.centralbank.go.ke/wp-content/uploads/2026/09/Draft-National-Payment-System-Policy-2026.pdf; CBK, draft National Payment System Bill, 2026, cl. 29, indexed official text, https://www.centralbank.go.ke/wp-content/uploads/2026/09/National-Payment-System-Bill-2026.pdf; FSD Kenya, "Navigating Open Finance Webinar: Key Insights and Opportunities for Kenya's Financial Sector," 5 November 2024 (Open Finance Initiative partners and purpose), https://www.fsdkenya.org/news/navigating-open-finance-key-insights-and-opportunities-for-kenyas-financial-sector/; ODPC, determination in Complaint No. 1837 of 2023 (legal mandate and bank supervision context), https://www.odpc.go.ke/wp-content/uploads/2024/02/ODPC-COMPLAINT-NO.1837-OF-2023-DETERMINATION.pdf.

126. South Africa. The March 2024 recommendations build on the 2023 draft position paper. They remain recommendations rather than an enacted dedicated regime. Pages 14–15 record the Information Regulator's input; page 20 addresses further institutional arrangements. Financial Sector Conduct Authority (FSCA), Open Finance Policy Recommendations (March 2024), 3–5, 14–15, 17–20, and 24, https://www2.fsca.co.za/Regulatory%20Frameworks/FinTechDocuments/2024%20Open%20Finance_FSCA%20Position%20Paper.pdf; FSCA, Regulatory Strategy 2025–2028, https://www.fsca.co.za/Documents/FSCA%20Regulatory%20Strategy%202025-2028.pdf; Intergovernmental Fintech Working Group (IFWG), "About Us," accessed 21 October 2026 (published member list), https://www.ifwg.co.za/Pages/About-Us.aspx.

Jurisdiction	Imple-mentation status	Open finance framework and lead regulator	Data protection counterpart	Coordination position and remaining gaps
Indonesia[127]	Live (payment APIs)	Bank Indonesia (BI): National Open API Payment Standard (SNAP), established in 2021 and operational for payment APIs. OJK Regulation 21/2023 governs commercial-bank digital services. 'Live' here refers to the payments/API scope, not a comprehensive cross-sector open-finance regime.	Personal Data Protection Law 27/2022; implementing regulation, Government Regulation 33/2026, promulgated July 2026 and in force from 16 January 2027. The dedicated authority has not yet been established (a draft Presidential Regulation was submitted to the President in May 2026; reports in September 2026 that it had been signed were unconfirmed at the cut-off); Komdigi oversees personal data protection in the interim. Existing BI and OJK oversight continues.	SNAP already includes data protection and consumer protection governance; OJK also imposes safeguards. Alignment with the general PDP regime and the future authority remains. Government Regulation 33/2026 adds a right to data portability and interoperability where processing is automated and based on explicit consent or a contract; API standards, accreditation and liability allocation stay with BI and OJK, and SNAP remains the technical standard for payment APIs.
Philippines[128]	Pilot	Bangko Sentral ng Pilipinas (BSP): Circular 1122 of 2021 established the Open Finance Framework. Open Finance PH pilot launched in 2023; OFxPERA went live in July 2025. BSP still describes the relevant use case as a limited pilot.	National Privacy Commission (NPC), under the Data Privacy Act 2012. Privacy obligations and the NPC's existing powers apply to open finance activity now, independently of proposed new legislation.	BSP says broader cooperative oversight and a formal governance body are still being developed. House Bill 9149 (Twentieth Congress), filed May 2026, proposes a BSP-chaired Philippine Open Finance Council that includes the NPC; this is not an enacted council.
Uganda[129]	No dedicated framework	No dedicated national open-banking/open-finance regulatory framework was identified. Bank of Uganda (BoU) banking/payment authorisation, PDPO registration and applicable NITA-U certification are separate general requirements, not an open-finance framework.	Personal Data Protection Office (PDPO), an office within the National Information Technology Authority Uganda (NITA-U) with functional independence under section 5(3) of the Act, administers the Data Protection and Privacy Act, Cap. 97 (formerly Act 9 of 2019) and the 2021 Regulations.	Multiple compliance processes may apply according to the activity. BoU's 2025 Payment Systems Oversight Framework expressly provides for inter-agency cooperation. No dedicated BoU–PDPO open finance body was identified.

127. SNAP is a national payment API standard with data protection governance, not a comprehensive entitlement to share all financial-sector data. BI reports operational SNAP transactions. On the data protection authority: a draft Presidential Regulation was submitted to the President on 20 May 2026 (government testimony in Constitutional Court case 236/PUU-XXIV/2026); reports in September 2026 that it had been signed were unconfirmed at the 30 September 2026 cut-off. On PP 33/2026, see https://meridianhukum.com/peraturan/pp-no-33-tahun-2026. Bank Indonesia (BI), "Standar Nasional Open API Pembayaran (SNAP)," accessed 21 October 2026 (legal basis, governance and transfer of standard management to ASPI in September 2023), https://www.bi.go.id/id/layanan/Standar/SNAP/default.aspx; BI, "BI-Rate Lowered by 25 bps to 5.25%: Maintaining Stability, Strengthening Economic Growth," news release No. 27/153/DKom, 16 July 2025 (operational SNAP transaction growth), https://www.bi.go.id/en/publikasi/ruang-media/news-release/Pages/sp_2715325.aspx; OJK, "OJK Issues Regulation and Guideline to Support Banking Sector Digital Transformation," press release SP 197/GKPB/OJK/XII/2023, 29 December 2023 (POJK 21/2023), https://ojk.go.id/en/berita-dan-kegiatan/siaran-pers/Pages/OJK-Issues-Regulation-And-Guideline-To-Support-Banking-Sector-Digital-Transformation.aspx; Ministry of Communication and Digital Affairs (Komdigi), "Wamen Nezar Patria: Indonesia siapkan otoritas pelindungan data pribadi yang independen," 22 July 2026, https://portal.komdigi.go.id/kanal-publik/berita-kini/10412.

128. Philippines. BSP's current programme page distinguishes its live limited pilot from account-information and transaction use cases still under design. It also dates the end of the transition group's mandate. House Bill 9149 of the Twentieth Congress, filed 6 May 2026, section 7, proposes a council with NPC representation; it has not been enacted. Bangko Sentral ng Pilipinas (BSP), Open Finance PH, regulatory and legal frameworks, governance, milestones and priority use cases, https://www.bsp.gov.ph/SitePages/FinancialStability/Open-Finance-OFPH.aspx; House of Representatives (Philippines), House Bill No. 9149, An Act Establishing the Philippine Open Finance Framework, Ensuring Consumer Financial Data Portability, Enhancing Competition and Innovation in the Financial Sector, Strengthening Data Privacy and Security, and for Other Purposes, Twentieth Congress, 6 May 2026, sec. 7, https://docs.congress.hrep.online/legisdocs/basic_20/HB09149.pdf.

129. Uganda. General licensing and registration requirements apply; there is no dedicated open finance framework. NITA-U's services concern IT certification and security assessment; applicability depends on the business. PDPO sits within NITA-U. BoU's 2025. Bank of Uganda (BoU), National Payment Systems Oversight Framework 2025, secs. 2.3–2.5, https://bou.or.ug/uploads/Revised_BOU_National_Payment_Systems_Oversight_Framework_2025_698b3e9745.pdf; Personal Data Protection Office (PDPO), "About Us," accessed 21 October 2026 (institutional position and legal mandate), https://www.pdpo.go.ug/about-us; PDPO, press release on the requirement to register with the PDPO (operationalisation in August 2021), https://pdpo.go.ug/media/2022/11/Press-Release-Requirement-to-register-with-PDPO.pdf; National Information Technology Authority – Uganda (NITA-U), "IT Certification: Service Providers," accessed 21 October 2026, https://nita.go.ug/services/legal-and-regulatory/it-certification-service-providers; NITA-U, "Security Assessment: FINTECH (E-Service Providers)," accessed 21 October 2026, https://nita.go.ug/services/legal-and-regulatory/security-assessment-fintech-e-service-providers.

Jurisdiction	Imple-mentation Status	Open finance framework and lead regulator	Data protection counterpart	Coordination position and remaining gaps
Uganda	No dedicated framework	No dedicated national open-banking/ open-finance regulatory framework was identified. Bank of Uganda (BoU) banking/payment authorisation, PDPO registration and applicable NITA-U certification are separate general requirements, not an open-finance framework.	Personal Data Protection Office (PDPO), an office within the National Information Technology Authority Uganda (NITA-U) with functional independence under section 5(3) of the Act, administers the Data Protection and Privacy Act, Cap. 97 (formerly Act 9 of 2019) and the 2021 Regulations.	Multiple compliance processes may apply according to the activity. BoU's 2025 Payment Systems Oversight Framework expressly provides for inter-agency cooperation. No dedicated BoU–PDPO open finance body was identified.
Ethiopia[130]	No dedicated framework	No dedicated national open-finance regulatory framework was identified. National Bank of Ethiopia (NBE) payments directives and digital-payments strategies provide adjacent infrastructure and regulation, rather than a general customer-directed financial-data-sharing regime.	Personal Data Protection Proclamation 1321/2024 assigns data-protection oversight to the Ethiopian Communications Authority (ECA).	A dedicated NBE–ECA open finance coordination arrangement was not identified. Defining consent, liability and supervision remains a prospective design task.

Source: CCAF & Fii.

130. ECA is the named data-protection authority, so an institutional counterpart exists; no dedicated open-finance arrangement was identified. NBE's earlier strategy identifies Payment Instrument Issuer Directive ONPS/01/2020 and Agents Directive FIS/02/2020, which predate the 2024 Proclamation. FSD Ethiopia's July 2026 first-party readiness assessment supports the absence of a dedicated framework. ECA, "About," accessed 21 October 2026 (current personal data protection mandate under Proclamation 1321/2024), https://www.eca.et/about/; Personal Data Protection Proclamation No. 1321/2024 (Ethiopia), Ministry of Justice copy, https://justice.gov.et/en/law/personal-data-protection-proclamation/; National Bank of Ethiopia (NBE), National Digital Payment Strategy 2021–2024, references to 2020 directives, https://nbe.gov.et/wp-content/uploads/2023/04/National-Digital-Payment-Strategy.pdf; NBE, draft National Digital Payment Strategy 2026–2030, publication page, accessed 21 October 2026, https://nbe.gov.et/ndps/; FSD Ethiopia, "Ethiopia's Open Finance Future Is Closer Than It Looks," 20 July 2026 (first-party readiness assessment), https://fsdethiopia.org/2026/07/20/ethiopias-open-finance-future-is-closer-than-it-looks/.

Appendix table 3: Cross-border transfer regimes and localisation requirements

Jurisdiction	Transfer permission (data protection law)	Local storage or local copy	Supervisory access and outsourcing
India	No operating DPA. Current: SPDI Rules 2011, Rule 7 permits transfers with equivalent protection where necessary for a lawful contract or with consent.[131] DPDP Act 2023, section 16's restriction-list regime is not yet operative; commencement is scheduled for May 2027.[132] DP-law power: DPDP Rules, Rule 13(4) (from May 2027) allows the government to bar transfer of specified data held by significant data fiduciaries; nothing yet specified.	Binding sector duties: RBI payment-system data in India (foreign-leg exception);[133] SEBI cloud data/logs in India, with a qualified foreign-investor exception;[134] insurance policy/claim records in Indian data centres.[135]	SEBI's cloud framework preserves regulator access.[136] IRDAI requires access for inspections/investigations.[137] CERT-In requires 180-day logs and production on request; FAQ 35 permits storage abroad also, subject to timely production; FAQ 36 and Direction (iv) retain Indian-jurisdiction language.[138]
Pakistan	No DPA. The Personal Data Protection Bill 2023 remains identified by MoITT as a draft. Its proposed transfer restrictions are not an operative DP-law permission regime.[139] Sector rules apply independently. No comprehensive data protection law had been enacted at 30 September 2026.	The draft bill is not a binding localisation source.[140] SBP's cloud framework prefers onshore providers but permits offshore workloads subject to its conditions; this is not a blanket local-storage or local-copy mandate.[141] The federal Cloud First Policy (2022) applies to public-sector data only.	SBP requires approval for material offshore cloud workloads of specified institutions, and contractual audit, on-site and information-access rights for SBP and auditors, including subcontractors.[142] SECP's cited 2021 Cloud Adoption Guidelines were issued as a draft and are not treated here as binding.[143]

131. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (India), r. 7, https://www.wipo.int/wipolex/en/text/494931.

132. MeitY, G.S.R. 843(E), 13 November 2025 (DPDP Act commencement notification), cl. (c), https://www.meity.gov.in/static/uploads/2025/11/c56ceae6c383460ca69577428d36828b.pdf; sec. 16 commences 18 months after publication.

133. RBI, Storage of Payment System Data, 6 April 2018, para. 2(i), https://rbi.org.in/Scripts/NotificationUser.aspx?Id=11244.

134. Securities and Exchange Board of India (SEBI), Framework for Adoption of Cloud Services, 6 March 2023, Principle 3, reproduced in the Master Circular for Stock Brokers (June 2025), 333–34, https://www.sebi.gov.in/sebi_data/attachdocs/jun-2025/1750158789381.pdf.

135. Insurance Regulatory and Development Authority of India (IRDAI), Maintenance of Information by the Regulated Entities and Sharing of Information by the Authority Regulations, 2025, regs. 9, 12–15, and 18 (repeal of earlier rules), esp. reg. 9(iii), https://financialservices.gov.in/sites/default/files/Act-Policies/2026-01/1-IRDAI-Maintenance-of-Information-by-the-Regulated-Entities-and-Sharing.pdf.

136. SEBI, Framework for Adoption of Cloud Services, Principle 3(i), https://www.sebi.gov.in/sebi_data/attachdocs/jun-2025/1750158789381.pdf.

137. IRDAI, Maintenance of Information Regulations, 2025, reg. 9(iii), https://financialservices.gov.in/sites/default/files/Act-Policies/2026-01/1-IRDAI-Maintenance-of-Information-by-the-Regulated-Entities-and-Sharing.pdf.

138. Indian Computer Emergency Response Team (CERT-In), Directions under section 70B, 28 April 2022, direction (iv), read with FAQs of 18 May 2022, question 35. Both instruments are linked on the official page.

139. MoITT (Pakistan), Personal Data Protection Bill (draft, May 2023); the official legislation register, https://www.moitt.gov.pk/Legislations, labels the instrument "Draft."

140. MoITT (Pakistan), Personal Data Protection Bill (draft, May 2023), https://www.moitt.gov.pk/Legislations.

141. SBP, Framework on Outsourcing to Cloud Service Providers, BPRD Circular 01/2023, secs. E and J, esp. sec. E.2, https://archive.sbp.org.pk/bprd/2023/C1-Annix-A.pdf.

142. SBP, Framework on Outsourcing to Cloud Service Providers, secs. E.2 and J, https://archive.sbp.org.pk/bprd/2023/C1-Annix-A.pdf.

143. Securities and Exchange Commission of Pakistan (SECP), draft Cloud Adoption Guidelines for Incorporated Companies (2021), official publication explicitly designated draft, https://www.secp.gov.pk/document/draft-cloud-adoption-guidelines-for-incorporated-companies/.

Jurisdiction	Transfer permission (data protection law)	Local storage or local copy	Supervisory access and outsourcing
Kenya	Data Protection Act 2019, sections 48–49 and General Regulations, Part VII permit transfers through safeguards, adequacy, necessity or consent routes. Sensitive personal data require consent plus confirmation of appropriate safeguards.[144]	Binding, targeted: General Regulations 2021, Regulation 26 requires processing in Kenya or at least one serving copy in Kenya for strategic-interest data. Categories include civil registration, elections, state public finance, designated protected computer systems, and specified education/health data.[145]	CBK requires prior approval for material outsourcing. Offshore arrangements must not impede CBK supervision or unfettered access by CBK and auditors.[146] This coexists with the Regulation 26 local-copy duty for strategic-interest data.
Nigeria	NDPA 2023, sections 41–43: adequate protection through law, binding corporate rules, contractual clauses, codes or certification; alternatively specified derogations, including informed consent. Record the transfer basis and adequacy assessment. GAID 2025, Article 45 and Schedule 5 guide evaluation.[147]	CBN's 15 June 2026 Circular (PSS/DIR/PUB/CIR/001/004), paragraph 2, as reported, requires Nigerian payment-transaction data to be stored and managed in Nigeria, with full compliance effective 1 January 2027.[148] Earlier domestic-switching requirements concern processing, not by themselves a local-copy duty.[149]	CBN's Shared Services Guidelines require approval for covered parent-company arrangements, including ICT; board governance, independent annual review and regulatory reporting also apply.[150] These are outsourcing controls, not a general storage mandate.
Indonesia	PDP Law 27/2022, Article 56 establishes a hierarchy: destination protection equal to or higher than Indonesian protection; failing that, adequate binding safeguards; failing both, data-subject consent. Government Regulation 33/2026 (in force from 16 January 2027) keeps this sequence and limits consent to one-off transfers involving few data subjects; on the authors' reading of Articles 167–170, the equivalence and standard-contractual-clause routes depend on the authority and cannot be used until it is constituted.[151]	Commercial banks must locate data centres and disaster-recovery centres in Indonesia. OJK may approve specified offshore arrangements; integrated AML systems are one qualifying case, not a general exemption.[152] Insurers and payment processing are subject to separate rules (OJK; Bank Indonesia's national payment gateway framework, PBI 19/8/PBI/2017).	Offshore bank IT arrangements require OJK approval and must preserve effective supervision, information access and inspection rights; the relevant foreign supervisor must not object to inspection. Offshore transaction processing is separately controlled.[153]

144. Data Protection Act, 2019 (Kenya), secs. 48–50, https://www.odpc.go.ke/wp-content/uploads/2024/02/TheDataProtectionAct__No24of2019.pdf; Data Protection (General) Regulations, 2021 (Kenya), reg. 26 and pt. VII (cross-border transfers), https://www.odpc.go.ke/wp-content/uploads/2024/03/THE-DATA-PROTECTION-GENERAL-REGULATIONS-2021-1.pdf; ODPC, Guidance Notes for Cross-Border Data Transfers, secs. 10 and 12, clarifying strategic-interest data and sensitive-data transfers, https://www.odpc.go.ke/wp-content/uploads/2026/04/Guidance-Note-on-Cross-border-Data-Transfers.pdf.

145. Data Protection (General) Regulations, 2021 (Kenya), reg. 26 and pt. VII (cross-border transfers), esp. reg. 26, https://www.odpc.go.ke/wp-content/uploads/2024/03/THE-DATA-PROTECTION-GENERAL-REGULATIONS-2021-1.pdf; ODPC, Guidance Notes for Cross-Border Data Transfers, secs. 10 and 12, esp. sec. 10, clarifying strategic-interest data and sensitive-data transfers, https://www.odpc.go.ke/wp-content/uploads/2026/04/Guidance-Note-on-Cross-border-Data-Transfers.pdf.

146. CBK, Prudential Guidelines, 2013, Guideline on Outsourcing (CBK/PG/16), secs. 4.6 and 4.7, including 4.7.5, https://www.centralbank.go.ke/wp-content/uploads/2016/08/PRUDENTIAL-GUIDELINES.pdf.

147. Nigeria Data Protection Act, 2023, pt. VIII, secs. 41–43, official NDPC publication, https://ndpc.gov.ng/download/nigeria-data-protection-act-2023; NDPC, General Application and Implementation Directive 2025, art. 45 and sch. 5, https://ndpc.gov.ng/wp-content/uploads/2025/03/NDP-ACT-GAID-2025-MARCH-20TH.pdf. The Act prevails over conflicting GAID provisions (art. 3(2)).

148. CBN, Circular PSS/DIR/PUB/CIR/001/004, 15 June 2026, para. 2. Primary circular reproduced at https://www.scribd.com/document/1060014541/CIRCULAR-ON-INTRODUCTION-OF-MARKET-STRUCTURE-REQUIREMENTS-DATA-LOCALISATION-ULTIMATE-BENEFICIAL-OWNERSHIP-DISCLOSURE-AND-SYSTEMIC-OVERSIGHT-MEASURE; localisation compliance date is 1 January 2027.

149. CBN, Guidelines on Point of Sale Card Acceptance Services, August 2011, sec. 4.4.8 (domestic transactions and switching), https://www.cbn.gov.ng/cashless/POS_GUIDELINES_August2011_FINAL_FINAL%20%282%29.pdf.

150. CBN, Guidelines for Shared Services Arrangements, 26 May 2021, secs. 4–6 and 8. Primary instrument transcribed at https://regalert.today/document/guidelines-for-shared-services-arrangements-b7006068-38c7-4ecc-bfab-02dbfcfb5962; also indexed in CBN, Rule Book, vol. 4, 677.

151. Law No. 27 of 2022 on Personal Data Protection (Indonesia), art. 56, official Ministry of Communication and Digital Affairs text, https://jdih.komdigi.go.id/produk_hukum/view/id/832/t/undangundang%2Bnomor%2B27%2Btahun%2B.

152. OJK, Regulation 11/POJK.03/2022 on IT Implementation by Commercial Banks, official English summary, points 61–77, esp. points 61–63, https://ojk.go.id/en/regulasi/Documents/Pages/Implementation-of-Information-Technology-by-Commercial-Banks/OJK%20Regulation%2011%202022%20concerning%20Implementation%20of%20Information%20Technology%20by%20Commercial%20Banks.pdf. These are summary point numbers, not article numbers.

153. OJK, Regulation 11/POJK.03/2022, official English summary, points 64–77, https://ojk.go.id/en/regulasi/Documents/Pages/Implementation-of-Information-Technology-by-Commercial-Banks/OJK%20Regulation%2011%202022%20concerning%20Implementation%20of%20Information%20Technology%20by%20Commercial%20Banks.pdf.

Jurisdiction	Transfer permission (data protection law)	Local storage or local copy	Supervisory access and outsourcing
Uganda	DPPA (Cap. 97), section 19 requires an equivalent level of protection in the destination or data-subject consent for overseas processing/storage. The 2021 Regulations, Regulation 30 implements this rule; a contract is not a standalone statutory transfer.[154] In practice, banks seek PDPO no-objection for specific transfers, and the PDPO has issued conditional no-objections.	Binding and specific: an electronic-money issuer must establish and maintain its primary data centre for payment-system services in Uganda. This is a specific primary-data-centre duty rather than a general local-copy requirement.[155]	Bank of Uganda may inspect payment-service providers and system operators and demand relevant information within a specified reasonable time; it may also appoint an external auditor.[156] These access powers supplement the section 68 (original numbering) data-centre duty.
South Africa	POPIA section 72 permits adequate protection through recipient law, binding corporate rules or agreement, or specified consent/necessity grounds. Special personal information or children's data sent to a non-adequate country require prior authorisation under section 57(1)(d).[157]	No general local-storage/local-copy mandate in POPIA. Banks may use offshore/cloud arrangements subject to the separate prudential conditions.[158] Sector-specific recordkeeping rules may still apply.	PA Directive 3/2018 requires bank cloud/offshoring arrangements not to obstruct supervisory access; Guidance Note 5/2018 supplements it.[159] Joint Communication 2/2025 confirms these bank instruments and describes broader best-practice expectations, not a new binding localisation rule.[160] The FSCA and PA are developing a binding Joint Standard on cloud computing and data offshoring.
Brazil	LGPD Articles 33–36 permit adequacy, approved contractual/corporate safeguards, specific informed consent and other statutory routes. ANPD Resolution 19/2024 implements transfer mechanisms, including standard contractual clauses.[161] ANPD Resolution 32/2026 recognised the EU as adequate, the first LGPD adequacy decision.	No general local-storage/local-copy mandate in LGPD. CMN Resolution 4,893/2021 permits covered institutions to contract data/cloud services abroad subject to conditions; it does not impose a blanket domestic-storage rule.[162]	Covered financial institutions must ensure foreign law does not impede access and retain BCB access to contracts, service information, stored data, backups and access credentials. Offshore conditions include supervisory cooperation, or BCB authorisation where the required agreement is absent.[163]

154. Data Protection and Privacy Act, 2019 (Uganda), sec. 19, consolidated statutory text, https://ulii.org/en/akn/ug/act/2019/9/eng%402023-12-31; Data Protection and Privacy Regulations, 2021 (Uganda), reg. 30, official PDPO publication, https://pdpo.go.ug/media/2022/03/Data_Protection_and_Privacy_Regulations-2021.pdf.

155. National Payment Systems Act, 2020 (Uganda), sec. 68, https://wakilii.org/laws/act/national-payment-systems-act.

156. National Payment Systems Act, 2020 (Uganda), secs. 21–22 and 68, esp. secs. 21–22; statutory text reproduced at https://wakilii.org/laws/act/national-payment-systems-act.

157. Protection of Personal Information Act 4 of 2013 (POPIA) (South Africa), secs. 57–58 and 72, https://www.justice.gov.za/legislation/acts/2013-004.pdf.

158. POPIA, secs. 57–58 and 72, https://www.justice.gov.za/legislation/acts/2013-004.pdf; Prudential Authority, Directive 3/2018, Cloud Computing and the Offshoring of Data, para. 2.2.9, https://www.resbank.co.za/en/home/publications/publication-detail-pages/prudential-authority/pa-deposit-takers/banks-directives/2018/8749.

159. Prudential Authority, Directive 3/2018, Cloud Computing and the Offshoring of Data, para. 2.2.9, https://www.resbank.co.za/en/home/publications/publication-detail-pages/prudential-authority/pa-deposit-takers/banks-directives/2018/8749; Prudential Authority, Guidance Note 5/2018, Cloud Computing and the Offshoring of Data, para. 4.9 (supervisory access), https://www.resbank.co.za/en/home/publications/publication-detail-pages/prudential-authority/pa-deposit-takers/banks-guidance-notes/2018/8747.

160. FSCA and Prudential Authority, Joint Communication 2 of 2025, paras. 3.3–3.5 and 4 (existing bank instruments and recommended best practice), https://www.resbank.co.za/content/dam/sarb/publications/prudential-authority/pa-public-awareness/covid-19-response/2025/Joint%20Communication%202%20of%202025%20-%20Cloud%20computing%20and%20offshoring%20of%20data.pdf.

161. Law No. 13,709/2018 (LGPD) (Brazil), arts. 33–36, official legislative text as amended, https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm; ANPD, Resolution CD/ANPD 19 of 23 August 2024 (International Data Transfer Regulation and standard contractual clauses), https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no-19-de-23-de-agosto-de-2024.

162. Law No. 13,709/2018 (LGPD) (Brazil), arts. 33–36, official legislative text as amended, https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm; CMN, Resolution 4,893 of 26 February 2021, arts. 16–17, esp. arts. 16 and 17(VII), https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?numero=4893&tipo=Resolu%C3%A7%C3%A3o+CMN; applies to institutions within its scope.

163. CMN, Resolution 4,893 of 26 February 2021, arts. 16–17, esp. art. 17(VII), https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?numero=4893&tipo=Resolu%C3%A7%C3%A3o+CMN; applies to institutions within its scope.

Jurisdiction	Transfer permission (data protection law)	Local storage or local copy	Supervisory access and outsourcing
Ethiopia	PDPP 1321/2024, Articles 18–21 require appropriate destination protection and provides specified transfer grounds, including informed explicit consent and necessity, subject to ECA oversight. Under Article 22(3), sensitive personal-data exports require prior ECA approval.[164]	Binding: PDPP Article 22(1) requires Ethiopian storage of locally collected/obtained personal data; Article 22(2) provides for designated critical data to be processed only locally.[165] NBE Directive SBB/94/2025, Article 9.1 separately localises specified core banking/customer data and primary/backup storage.[166]	NBE Article 9.2 requires prior written approval and security, audit and data-access arrangements for covered cross-border transfers. Article 9.3 provides a limited approved route for customer-related data without personally identifiable details.[167] DP-law approval and local-storage duties remain separate.[168]
Philippines	RA 10173 (Data Privacy Act), sections 12–13 and 21 allow lawful processing/transfers while retaining controller accountability for domestic and international third-party processing. Contracts or other reasonable means must provide comparable protection.[169]	No general domestic-storage/local-copy duty in the Data Privacy Act.[170] BSP permits offshore and cloud outsourcing subject to regulatory conditions; the regime does not make domestic hosting the general rule.[171]	BSP Circular 1137/2022, MORB section 112 and Appendix 78 impose outsourcing/IT risk controls and supervisory access. Approval depends on the arrangement and supervisory/materiality conditions. BSP's FAQ confirms cloud outsourcing, including core operations, remains subject to these rules.[172]

Source: CCAF & Fii.

164. Federal Democratic Republic of Ethiopia, Personal Data Protection Proclamation No. 1321/2024, Federal Negarit Gazette, 30th year, no. 35 (July 24, 2024), art. 22, https://justice.gov.et/wp-content/uploads/2025/04/seasiisia-seusiNse%C2%A1-1321-2016.pdf.

165. Personal Data Protection Proclamation No. 1321/2024 (Ethiopia), arts. 18–22 and 70; official Gazette published 24 July 2024, Ministry of Justice copy, https://justice.gov.et/wp-content/uploads/2025/04/seasiisia-seusiNse%C2%A1-1321-2016.pdf.

166. NBE, Requirements for Licensing and Renewal of Banking Business and Representative Office Directive SBB/94/2025, art. 9 (localisation and cross-border data transfers), https://nbe.gov.et/wp-content/uploads/2025/06/REQUIREMENTS-FOR-LICENSING-AND-RENEWAL-OF-BANKING-BUSINESS-AND-REPRESENTATIVE-OFFICE-DIRECTIVE-NO.-SBB942025-1.pdf.

167. NBE, Requirements for Licensing and Renewal of Banking Business and Representative Office Directive SBB/94/2025, art. 9 (localisation and cross-border data transfers), https://nbe.gov.et/wp-content/uploads/2025/06/REQUIREMENTS-FOR-LICENSING-AND-RENEWAL-OF-BANKING-BUSINESS-AND-REPRESENTATIVE-OFFICE-DIRECTIVE-NO.-SBB942025-1.pdf.

168. Personal Data Protection Proclamation No. 1321/2024 (Ethiopia), arts. 18–22 and 70, https://justice.gov.et/wp-content/uploads/2025/04/seasiisia-seusiNse%C2%A1-1321-2016.pdf; NBE, Requirements for Licensing and Renewal of Banking Business and Representative Office Directive SBB/94/2025, art. 9 (localisation and cross-border data transfers), https://nbe.gov.et/wp-content/uploads/2025/06/REQUIREMENTS-FOR-LICENSING-AND-RENEWAL-OF-BANKING-BUSINESS-AND-REPRESENTATIVE-OFFICE-DIRECTIVE-NO.-SBB942025-1.pdf.

169. Data Privacy Act of 2012 (Republic Act No. 10173) (Philippines), secs. 12–13 and 21, official NPC text, https://privacy.gov.ph/data-privacy-act/; National Privacy Commission, Implementing Rules and Regulations of the Data Privacy Act of 2012, esp. the accountability requirements for transfers, https://privacy.gov.ph/implementing-rules-regulations-data-privacy-act-2012/.

170. Data Privacy Act of 2012 (Republic Act No. 10173) (Philippines), secs. 12–13 and 21, official NPC text, https://privacy.gov.ph/data-privacy-act/.

171. BSP, Manual of Regulations for Banks 2022, sec. 112 and app. 78, incorporating Circular 1137 of 18 February 2022, https://www.bsp.gov.ph/Regulations/MORB/2022MORB.pdf; BSP, Memorandum M-2022-046, 27 October 2022, FAQs on Circular 1137, secs. B–C (offshore/intragroup and cloud outsourcing), https://www.bsp.gov.ph/Regulations/Issuances/2022/M-2022-046.pdf.

172. BSP, Manual of Regulations for Banks 2022, sec. 112 and app. 78, incorporating Circular 1137 of 18 February 2022, https://www.bsp.gov.ph/Regulations/MORB/2022MORB.pdf; BSP, Memorandum M-2022-046, 27 October 2022, FAQs on Circular 1137, secs. B–C (offshore/intragroup and cloud outsourcing), https://www.bsp.gov.ph/Regulations/Issuances/2022/M-2022-046.pdf.



Financial Innovation for Impact

Cambridge Centre for Alternative Finance

UNIVERSITY OF CAMBRIDGE Judge Business School

With the support of

Gates Foundation