MARCH 2023

DATA POLICY IMPACTS - AML AND REGTECH SOLUTIONS

CASE EXAMPLES

INSTITUTE OF INTERNATIONAL FINANCE

INSTITUTE OF INTERNATIONAL FINANCE

Foreword

National restrictions on the flow of data continue to proliferate around the globe. We are rapidly reaching an inflection point where data localization requirements and fragmented standards for data and privacy may begin to break the on-demand services and real-time systems that we have come to expect and rely on.

While recent years have revealed some serious problems with privacy, security, monetization and taxation in the digital economy, the policy responses have been rapid, fragmented, and poorly coordinated at the international level. Data localization measures, a lack of coordination of data governance requirements, hastily drafted privacy laws, digital identity efforts without interoperability standards, far-reaching artificial intelligence (**AI**) regulation, and an overall lack of coordination threaten to choke the future of the digital economy.

This is an increasing problem for broad-based sectors including dynamic startups, small and medium sized enterprises (**SMEs**) and other high-growth businesses which are driven by global digital infrastructure to support their activities. Restrictive data frameworks have real-world costs to businesses and consumers. The full impact of localization requirements and other restrictions are not always measured and frequently not part of the political debate.

This IIF staff paper is part of a series seeking to identify the broad impacts of restrictive data policies. The series began with Data Localization: Costs, Tradeoffs, and Impacts Across the Economy (December, 2020) which outlined the ways restrictive data policies had proliferated beyond clear data localization laws and how the costs and inefficiencies driven by these policies emanated broadly across the economy. It continued with Strategic Framework for Digital Economic Cooperation - State of Play (October, 2021) which highlighted the lack of clear international "rules of the road" for the digital economy, challenges to clear global standards, and the headwinds against initiatives such as the G20 "Data Free Flow With Trust". The next piece, Strategic Framework for Digital Economic Cooperation - A Path for Progress (April, 2022) outlined what is at stake for the financial services industry, where opportunities for improved data frameworks are possible, and suggested a modular approach for more international improvements, including trade agreements between like-minded economies, and industry-driven standards.

This year, the Japanese Presidency of the G7 has revived the Data Free Flow with Trust (DFFT) initiative and is proposing operationalizing it by establishing an institutional arrangement to promote interoperability across data regimes with solutions for cross-border data transfer through public-private cooperation. These discussions are in the digital ministers track rather than the finance ministers track but we highlight them as having significant implications for the financial services industry.

To help highlight the relevance of the DFFT policy debate for financial services, we are continuing our series of papers with the addition of three case examples sharing tangible impacts and real-world trade-offs in: fraud prevention; regulatory technology (**regtech**) and anti-money laundering (**AML**); and travel insurance. The first, Data Policy Impacts - Fraud Prevention (January 30, 2023) is now joined by this piece and we will publish the third in advance of G7 Digital and Tech Ministers' Meeting on April 29 & 30. We hope that exploring the impacts of data policy in these areas will trigger further reflection on the possible costs and potential for better solutions.

Table of Contents

I. Summary

Restrictive data policies and regulations can impair the efficiency and effectiveness of new AML and other regtech solutions by constraining or blocking the data needed to inform new models, reducing the predictive ability of new tools, and curtailing access to real time cloud-based technology. Data restrictions are proliferating and can take various forms including local data storage or copy and local processing requirements, data export prohibitions, and data standards fragmentation. These restrictions are rising at a time when financial institutions are facing a trilemma of pressures: compliance with ever-increasing regulatory and supervisory requirements; cost efficiency and operational improvement expectations; and customer demands for services at speed and with security. To make the impacts of data policy more tangible, this paper shares real world examples of new solutions to AML and compliance challenges and how they are effected by data policy. Policymakers are urged to consider these impacts—as well as costs to consumers, competition and financial inclusion—when they evaluate raising data barriers to achieve their policy objectives.

II. Background

Advanced compliance solutions, sometimes referred to as regtech,[1] enable new ways for financial institutions (**FIs**) to service customers and conduct business activities in a compliant manner, while achieving operational improvement and cost efficiency. They provide for new ways for FIs to address regulatory requirements and fulfil regulatory objectives.

Organizations are facing pressure to meet ever-increasing regulatory and compliance requirements; this will continue to be a challenge for most organizations in the post-pandemic world. A recent survey suggested that a third of FIs globally spend more than 5% of revenue on compliance,[2] while another study indicated that 62% of respondents said they expect the cost of time and resource devoted to conduct risk issues will continue to increase.[3]

Regtech solutions, like many digital systems implemented by FIs today, are increasingly reliant on new technologies, particularly cloud computing, artificial intelligence (**AI**) and advanced data analytics. By their nature such technologies are data-hungry, and their effectiveness can be impaired when high-quality, timely data is less available. AML solutions are particularly in need of these transformative technology solutions to improve efficiency and outcomes.

The case studies in this paper provide an overview of insightful short form use-cases that we have encountered where organisations have made use of advanced technology to meet regulatory requirements in new and interesting ways.

The case studies are intended to illustrate how AML and other regtech solutions are impacted by data policies, including data localization measures and other data barriers.

---

[1] See IIF (2017), Machine Learning: A Revolution in Risk Management and Compliance?, IIF (2017), Deploying Regtech Against Financial Crime and IIF (2016), Regtech in Financial Services: Solutions for Compliance and Reporting

[2] Kroll, Global Regulatory Outlook 2021. Results based on a survey of 250 senior executives working in financial services in U.S., the UK, Europe, India and China.

[3] Thomson Reuters, Cost of Compliance 2022

III. Data policies and their impacts

Data policies can, depending on their content, enhance or impair the ability of FIs to deploy advanced compliance solutions effectively. Data policies that encourage the free flow of data, with client consent and in a trusted and secure way, will be positive for such solutions, while data barriers will be negatives.

In general terms, **data barriers** can include local data storage or copy and local processing requirements, data export prohibitions, and data standards fragmentation.[4]

Because data barriers interfere with the efficient and effective deployment of cloud computing, AI and advanced data analytics, they tend to impair the efficiency and effectiveness of advanced compliance solutions, while increasing operational risk and reducing financial inclusion.

More specifically, data barriers can have the following negative impacts on advanced compliance and operations, especially for businesses and FIs that operate across borders:

- reducing or eliminating the scope for client or counterparty data aggregation, so reducing the predictive power of data models such as lending, pricing or actuarial engines, due to reductions in training data set sizes or in the timeliness or accuracy of training data;
- limiting the ability of financial groups active across borders to accurately model their risk positions, including counterparty credit risk, and large exposures to specific asset or counterparty types;
- increasing cyber risk by increasing the attack surface and entry points for cyber-attacks; and
- increasing the risk of incomplete or stale information leading to transaction fails or the breaking of straight-through processing (STP).

As well as reducing the effectiveness of compliance or operations, data barriers can also impose direct economic costs on FIs by limiting the economies of scale that would otherwise be reaped from cloud solutions. This can arise from duplication of infrastructure or operations due to requirements such as local storage or copy, or local processing. Compliance costs can also rise as companies must comply with different data regulations in each location where data is stored. Data barriers can also increase the complexity of data management and make it more difficult to transfer data between different regions, resulting in increased operational costs.

These additional costs will in many cases be passed on to consumers.

There are also financial inclusion costs to data localization. Data localization policies can make it harder for companies to access the data they need to make informed decisions, which can reduce financial inclusion by limiting access to financial services for certain populations. Data barriers can also limit the ability of companies to operate across borders, reducing competition and potentially leading to higher costs for consumers. They can also limit access to global marketplaces, making it harder for small and medium-sized businesses to reach new customers and expand their businesses.

[4] See IIF (January 14, 2022), Response to the FSB on Data Frameworks Affecting Cross-Border Payments, from which some of the following discussion is adapted.

IV. AML and other advanced compliance applications

In this section, we consider some recent examples of advanced compliance solutions that, in various ways, depend on the new technologies, particularly cloud computing, AI and advanced data analytics, that were discussed above as vulnerable to data barriers, both in terms of cost and effectiveness.

AML/CFT case studies

At a compliance function level, regtech applications are being used for compliance monitoring, regulatory reporting, financial crime (including AML, combating the financing of terrorism (**CFT**) and sanctions screening), as well as onboarding and know-your customer (**KYC**) obligations, and dealing with the impact of regulatory change.[5]

In the AML/CFT space in particular, advanced technologies are being deployed widely to reduce the false-positive reporting rates and allow compliance staff to focus on higher-value, more complex work. These technologies include digital identity and digital trust/verifiable credentials, and sanctions screening oracles and APIs in the crypto-asset space,[6] among a suite of tools used to increase hit rates and improve the granularity and accuracy of identity disambiguation and data matching.

AML/CFT alert decision engine

AML regulation requires that suspicious activities be reported to the regulator and investigated within defined time frames. In order to comply with regulatory requirements, one of Africa's largest diversified financial groups has invested in advanced monitoring technologies to detect potentially illicit behaviour.

The group embarked on a process to identity technology solutions that would alleviate the pressure on human resources from review of alerts and at the same time improve efficiency and response time. The objective was to use technology to improve efficiency without compromising the quality of the investigations.

An alert decision engine (**ADE**) was deployed as a "virtual" level 1 analyst to screen all alerts for false positives prior to a manual Level 2 analyst review for detailed investigation. The chosen technology provider's claimed outcomes included decision accuracy of 99%, and reduced decision times from 30 minutes to less than 3 seconds. The FI reported significantly reduced time spent in assessing alerts and re-invested this time in high value risk management activities, enabling the FI to add plug-ins based on data analytics, derived from behaviour, refining the system's ability to flag potential financial crime.

ADE decision making accuracy, seamless processing and human training of algorithms are all dependent on the availability of large quantities of high-quality training data, as well as on human expertise across the business.

A verifiable Legal Entity Identifier

Established by the G20 and the Financial Stability Board in June 2014, the Legal Entity Identifier (**LEI**) is a universal and standardized identification system for all legal entities, globally. An LEI is a single code representing a single organization so that anyone, anywhere

---

[5] Thomson Reuters, Cost of Compliance 2022, p. 10. Based on a survey of almost 500 practitioners worldwide, representing global systemically important banks, banks, insurers, asset and wealth managers, regulators, broker-dealers and payment services providers.
[6] E.g., Free Cryptocurrency Sanctions Screening Tools - Chainalysis

in the world, can trust an organization is who it claims to be. There are over two million active LEIs in use around the world.

A study by McKinsey & Co. and the Global LEI Foundation (**GLEIF**) estimated that on an annual basis, banks could potentially collectively save between $250 million to $500 million per annum if LEIs were used to identify international entities and to automate the tracing of their history for the issuance of letters of credit, including by reducing the incidence of false positives based on AML and other compliance lists.[7]

When today's businesses interact digitally, the absence of a single, open and universal protocol that allows the authenticity of information and data sources to be verified forces them to make unreliable decisions about who and what they can trust. Such a gap can make scams and fraud easier, including fundraising and other investor-directed scams such as fake prospectuses.[8]

In response, a verifiable LEI (**vLEI**) – a digital counterpart to an LEI – has been developed. This decentralized digital ID can establish computational cryptographic trust between legal entities worldwide and can be used by legal entities and their official representatives to automatically verify their authenticity.

The implementation of the vLEI is expected to provide legal entities, regulators, and other stakeholders with a globally secure mechanism for verifying organizational identity in all kinds of digital transactions and interactions. It will also allow the issuance of additional credentials to persons holding official or functional roles within an organization, enabling their authenticity to be automatically verified during interactions in which they represent the entity.

With regard to data barriers, the GLEIF has been involved in discussions with the FSB around possible proxy registers or global identifiers as envisaged by the G20 roadmap for enhancing cross-border payments.

Among the lessons learned, the GLEIF reports the importance of all stakeholders understanding the importance of ringfencing privacy issues to individuals and that privacy law concepts are not relevant to corporate identity. For example, the Global LEI System reference data is made available as open data under a Creative Commons license.

Cloud and regtech case studies

In previous publications, we have emphasised the role of cloud computing as a vital enabler of digital transformation for financial services, as well as a key source of resilience during the pandemic.[9] The following short case studies demonstrate the benefits that can be reaped through migrating compliance applications to public cloud environments from on-premises data centers, or building them as cloud-native to begin with.

One particular topic that has emerged as a major pain point for FIs seeking to adopt cloud solutions is data localization. The costs of data localization and other data barriers, as well as the public policy responses to the "data free flow with trust" agenda, outline a policy debate with significant implications for financial services and the broader economy.

---

[7] McKinsey & Co. and GLEIF (2017), The Legal Entity Identifier: The Value of the Unique Counterparty ID

[8] See, e.g., Australian Securities and Investments Commission, Alert: Fake IPO and pre-IPO investment scams

[9] See, e.g. IIF (2018), Cloud Computing in the Financial Sector Part 1: An Essential Enabler; IIF (2020), Cloud Computing: A Vital Enabler in Times of Disruption.

Fully compliant contactless payments

A Spanish global financial services group that operates in over 30 countries, with significant operations in Mexico, Turkey and South America, wanted to enable contactless (**NFC**) payments in its mobile banking app.

To develop a globally compliant NFC payment solution, the bank used a cloud-based hardware security module (**HSM**) that makes it simple for developers to generate and use their own encryption keys on AWS. The cloud based HSM solutions enabled compliance with NFC key management requirements without sacrificing high-quality service, whilst allowing scalability to meet demand.

The NFC payment solution is now live in several countries within the group's footprint. The group became the first FI to launch NFC payments in Peru, Argentina, and Colombia delivering valued services broadly in the economy.

Records retention

A U.S. registered investment advisor and broker-dealer uses technology solutions to fulfil financial advice and portfolio management services that have traditionally been offered through human interaction. The company was searching for a reliable records retention solution to replace an existing third-party solution, while helping it meet requirements under the Securities and Exchange Commission rules governing electronic record retention and resilient storage.

The company's third-party solution was built on a separate data storage and a web interface architecture, that was not compatible with its existing cloud architecture, and was not easy to scale to handle rapidly increasing volumes. Alternative third-party solutions were found to be expensive with similar integration limitations. The company migrated to a fully cloud-based solution in 8 weeks.

The key reported benefits included reduced cost of compliance, reduced complexity of the technology stack, reduced headcount supporting email archiving and third-party records management, enhanced storage search capabilities, and improved customer services.

Disaster recovery and redundancy

A global trade management software provider was using a time-consuming, manual Disaster Recovery (**DR**) process, requiring a team of engineers to manage two separate on-premises data centres. The DR process required a significant number of staff to travel to the secondary data centre to retrieve correct backup tapes if a DR event occurred.

The provider engaged a consultant to assist them with implementation of a cloud-based DR solution. A recovery site was setup in a virtual private cloud solution on AWS that met stringent security and compliance requirements. The recovery site was then used to replicate its full stack in a low-cost staging area, reducing the need to provision duplicate resources. Continuous replication means changes made in the production environment are updated in the disaster recovery site within seconds. Portal access to the DR site eliminated the need to physically travel to the secondary data centre to ensure DR processes are up to date and able to deal with service interruptions.

Technology risk management

A leading Singapore-based digital assets business was seeking a Digital Payment Token (DPT) provider licence under the Singapore Payment Services Act. This required adherence to the

applicable Technology Risk Management Guidelines, governing data protection, systems availability and redundancy, and change management controls.

The business chose a public cloud solution, which enabled the business to fortify its access controls with Identity and Access Management (IAM) and to automate encryption of data at rest and in transit. The business reported several benefits implementing an out-of-the-box cloud-based compliance solution, the most noteworthy of which were significant time savings relative to the months, if not years, it would have taken to develop the firm's own advanced security features; availability, resilience, and cost optimization; and accelerated compliance timeline for ISO 27001 certification. This cloud based solution helped improve the compliance and security of a new entrant to the financial services landscape.

Regional stock exchange market data

Regional stock exchanges operating hybrid architectures, with a mix of own servers and virtual machines running in a domestic cloud, may not be easily scalable, and international customers in particular may have concerns over the speed of accessing market data. Upgrading technology platforms to public cloud solutions may result in significant time savings relative to a bespoke inhouse solution, quicker security and compliance checks, increased agility in getting new products to market faster, enhanced data security, lower cybersecurity spending, and improved scalability and system performance.

V. Conclusion

Advanced regtech solutions offer new ways for FIs to service customers and conduct business activities in a compliant manner, while achieving operational improvement and cost efficiency. Organizations are facing pressure to meet ever-increasing regulatory and compliance requirements, a challenge for most organizations in the post-pandemic world. Data barriers, such as local data storage or copy, local processing requirements, data export prohibitions, and data standards fragmentation, can impair the efficiency and effectiveness of advanced compliance solutions, increasing operational risk and limiting financial inclusion. These barriers can also impose direct economic costs on FIs by limiting the economies of scale that would otherwise be reaped from cloud solutions, driving increased costs for consumers and limiting competition.

It is of course important for policymakers to consider the effects of barriers such as data localization policies on the effectiveness of advanced compliance solutions, as well as on cost to consumers, competition and financial inclusion. As a guiding principle, prior to imposing any data barriers, regulators and policymakers are encouraged to be clear on the regulatory objective, demonstrate that the rules imposed are the least restrictive means of achieving those objectives, and remain open to new alternative solutions.[10] FIs also need to be mindful of data barriers when planning and implementing regtech solutions.

In the face of increasing data barriers, the IIF has recently advocated for consideration to be given to setting out standardized gateways or exceptions, clarifying the circumstances under which authorities and FIs may make disclosures despite the presence of a data barrier. In this regard, the IIF has proposed that data barriers could be addressed by providing a "gateway" or exception to facilitate the sharing of information by a business about local citizens or businesses (data subjects) where the business reasonably considers it necessary or expedient:

[10] IIF (2022), Cloud in Latin America: Opportunities and Challenges for Financial Services

- to allow the business concerned to comply with its reporting or disclosure obligations in any jurisdiction;
- to allow the business concerned to share information with a corporate affiliate to enable that affiliate to comply with its reporting or disclosure obligations in any jurisdiction; or
- for the purposes of enabling the business concerned (or its affiliates) to make a fully informed decision about the risk of dealing with the data subject concerned or the risk of any transaction involving the data subject (including risks around fraud, AML and CFT).[11]

If better and more consistent data frameworks were in place, then fewer exceptions would be required and the benefits would extend across compliance solutions and the economy more broadly.

[11] IIF (January 14, 2022), Response to the FSB on Data Frameworks Affecting Cross-Border Payments. In this regard, it is notable that Commission Delegated Regulation (EU) 2019/758 under the Fourth Money Laundering Directive provides a framework for the financial entities being able to share information within their same group in order to comply with their AML obligations.

Appendix – References

1RS (2021), Counting the cost of Compliance vs. cost of non-compliance

Australian Securities and Investments Commission, Fake IPO and pre-IPO investment scams

Amazon Web Services (**AWS**), Betterment saves time and money using a flexible record retention solution

AWS (2021), BBVA uses AWS CloudHSM to enable fully compliant NFC Payments

AWS (2021), Thomson Reuters Implements Disaster Recovery for 300 Servers in Less than 10 Months on AWS

AWS (2021), Coinhako migrates to AWS for compliance and high availability

Bangkok Post (December 24, 2021), SET to launch digital asset exchange

GLEIF, Introducing the Verifiable LEI

GLEIF, The vLEI: Introducing Digital ID for Legal Entities Everywhere

Institute of International Finance (**IIF**) (2016), Regtech in Financial Services: Solutions for Compliance and Reporting

IIF (2017), Machine Learning: A Revolution in Risk Management and Compliance?

IIF (2017), Deploying Regtech Against Financial Crime

IIF (2018), Cloud Computing in the Financial Sector Part 1: An Essential Enabler

IIF (January 14, 2022), Response to the FSB on Data Frameworks Affecting Cross-Border Payments

IIF (2020), Cloud Computing: A Vital Enabler in Times of Disruption

IIF (2020), Data Localization: Costs, Tradeoffs, and Impacts Across the Economy

IIF (2021), Strategic Framework for Digital Economic Cooperation - State of Play

IIF (2022), Strategic Framework for Digital Economic Cooperation - A Path for Progress

IIF (2022), Cloud in Latin America: Opportunities and Challenges for Financial Services

IIF (2023), Data Policy Impacts - Fraud Prevention

Kroll, Global Regulatory Outlook 2021

McKinsey & Co. and GLEIF (2017), The Legal Entity Identifier: The Value of the Unique Counterparty ID

Merlynn, Digital Twins in Financial Crime Alert Management

PwC India, RegTech: A new disruption in the financial services space

Techcentral (2020), How Absa is using AI to fight financial crime

Thomson Reuters, Cost of Compliance 2022

Author

Laurence White
Consultant Senior Advisor, Digital Finance /Asia Pacific
lwhite-advisor@iif.com

Contributors

Conan French Director, Digital Finance
cfrench@iif.com

Jaco Grobler
Founder, New Paradigm Finance
jaco@newparadigmfinance.com