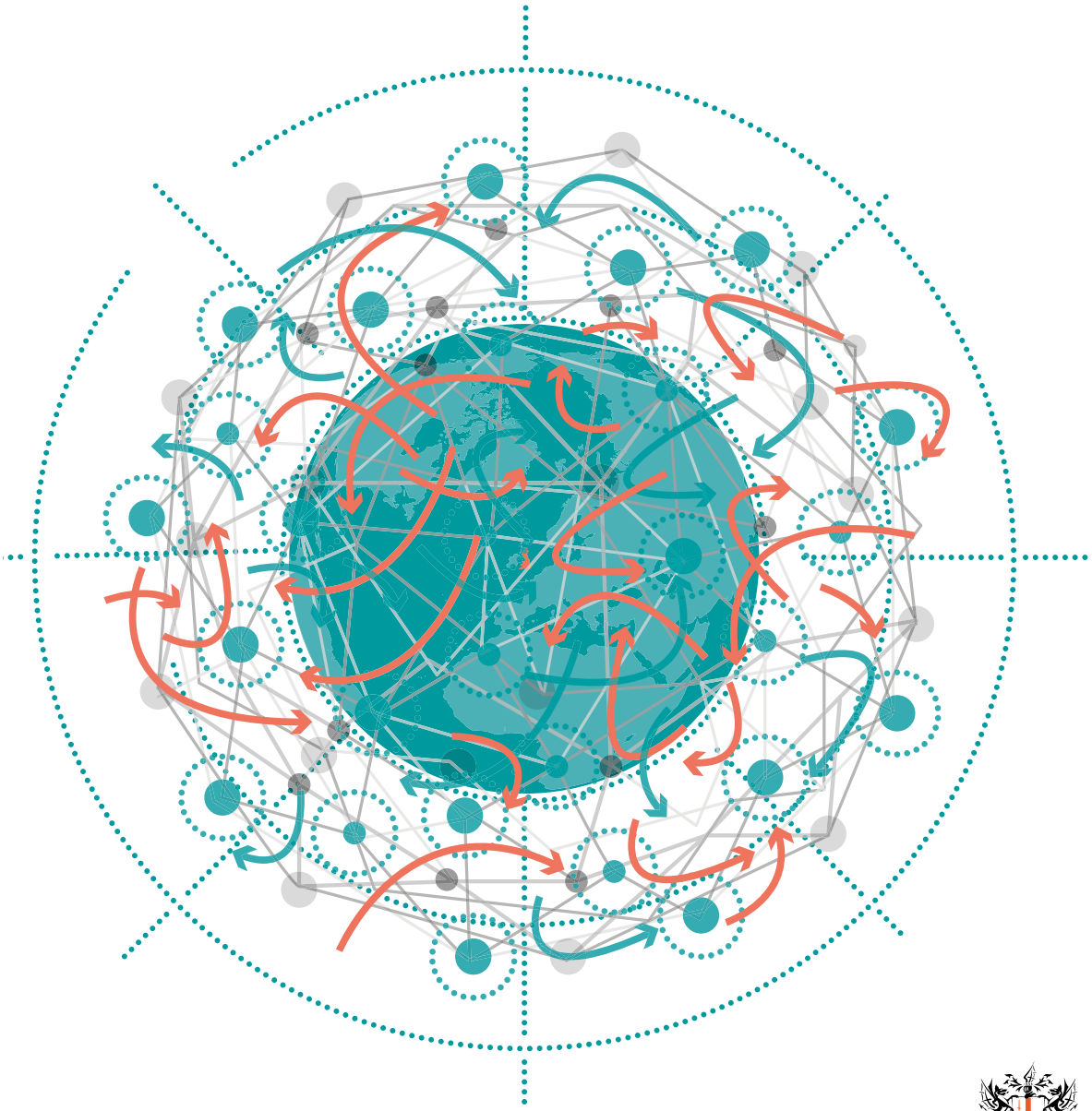
IRSG
INTERNATIONAL
REGULATORY
STRATEGY GROUP

KPMG
Law

The future of international data transfers

A discussion paper by the International Regulatory Strategy Group
in association with KPMG Law



April 2022

CITY OF LONDON

TheCityUK

About the IRSG

The International Regulatory Strategy Group (IRSG) is a practitioner-led group comprising senior leaders from across the UK-based financial and related professional services industry. It is one of the leading cross-sectoral groups in Europe for the industry to discuss and act upon regulatory developments.

With an overall goal of promoting sustainable economic growth, the IRSG seeks to identify opportunities for engagement with governments, regulators and European and international institutions to advocate for an international framework that will facilitate open and competitive capital markets globally. Its role includes identifying strategic level issues where a cross-sectoral position can add value to existing views.

About KPMG

KPMG is a Limited Liability Partnership, providing professional services for over 150 years, relating to audit, tax and legal, deal advisory and consulting. Working hand in hand with industry, KPMG supports clients to design and implement practical, customer-friendly and legally compliant systems and controls.

KPMG Law in the UK, is regulated by the Solicitors Regulation Authority (SRA) (SRA ID: 615423) and has the breadth of capability and insight to understand both big picture issues and focused detail. We provide complete solutions by combining legal expertise with access to insight and expertise from across the KPMG network of firms. We can provide global solutions at scale and seamlessly with more than 2,700 legal professionals in 80 countries. Focusing on what matters to our clients, we enhance existing ways of doing things and collaborate creatively to deliver the best outcomes.

Recent events have changed how we live and work, creating immense challenges for businesses and governments around the globe. Digitisation of everyday life has accelerated. KPMG operates at the forefront of global digitisation and technological improvements – anticipating shifting business needs and priorities, in line with national and international strategies and events.

TheCityUK and the City of London Corporation co-sponsor the IRSG.

CITY OF LONDON

TheCityUK

KPMG Law

CONTENTS

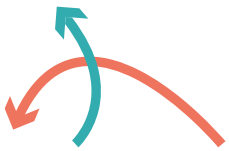
FOREWORD

Vivienne Artz OBE
Chair of the IRSG
Data Committee

Data, whether personal or non-personal, and in all its forms (whether digital, audio, video, meta, structured, unstructured) is increasingly powering our technology, our societies and our economies, and never more so than as we emerge from the global pandemic. The move to digital, particularly in financial services, has exponentially increased during the pandemic, together with the awareness of the reality of our interconnected digital world, and the recognition of the fundamental importance of ready access to and the free flow of data to enable our education, research, government, business and society to operate.

This pace of change challenges our existing legislative and policy responses to regulating data, and the mechanisms that have developed to support trusted access to and sharing of data across jurisdictional boundaries. Today 60% of the global population access the internet, and the vast majority do so via mobile devices. The move from the industrial based economy to the digital economy is upon us. Our traditional industrial based economies and bi-lateral flows of goods, services and data has of necessity become digital and global, from digital payments, to banking, to services, to news.

We live in a world where our digital and physical spaces have become inseparably linked. As part of this digital transformation, we are also seeing more data regulation, with over two thirds of countries globally having implemented or are implementing privacy and data protection laws. A developing trend associated with increased data laws is also an increase in measures to restrict data flows.



"We live in a world where our digital and physical spaces have become inseparably linked. As part of this digital transformation, we are also seeing more data regulation, with over two thirds of countries globally having implemented or are implementing privacy and data protection laws."

In a world where data has evolved in an accessible internet, relatively free of geographical restrictions and boundaries, the imposition of jurisdictional data flow restrictions creates new tensions and challenges for the digital reality in which we live and operate. It is also putting unprecedented pressure on the ability for financial firms to provide seamless services to their customers, and for customers to access the full range of innovative services and products from financial firms.

In this report we explore what is the current trajectory of current data transfer restrictions, and the impact that this could have on financial services firms and their customers. We also propose a number of recommendations as to actions and measures that can be taken to better achieve a consistent level of protection to allow data flows today and in the digital world of the future.

It is imperative that as we seek to address the increase in data sharing and digitisation of our economies and our lives, this is achieved across governments and industries, and does not reflect a protectionist or self-interested approach.

FOREWORD...

It is essential that the digital realities of our lives and economies result in the building of bridges to help facilitate responsible data sharing and support data protection standards which build a consistent global framework to foster responsible and accountable innovation and use of data.

To be successful, we must ensure that we are not seeking to leverage approaches which are more suited to the industrial based economy, as these will not provide the answers needed to provide future proof solutions for the digital world into which we are moving. IRSG stands ready to engage with DCMS, DRCF, the ICO and other international fora to further discuss the findings and recommendations in this report to collaborate on a constructive way forward to support international data flows.

Our digital world needs modern, flexible, accountable and multi-lateral policy and regulatory approaches to safeguard responsible data flows, to enable the future we expect, with data at its heart.

"Our digital world needs modern, flexible, accountable and multi-lateral policy and regulatory approaches to safeguard responsible data flows, to enable the future we expect, with data at its heart."

EXECUTIVE SUMMARY

As the pace of technological innovation accelerates and the sharing of data across borders is more prevalent, the collection, creation, use, transfer, and protection of data is increasingly subject to legal, regulatory, political and societal scrutiny.

The power of data is an issue which is regularly visited in terms of its regulation, so much so that it is almost pre-determined as 'problematic'. Despite this, the true power of data when lawfully and ethically harnessed in a global sphere, is its power to transform developed and emerging economies where data can flow with certainty so that potential can be unearthed. The value of data cannot be measured in units or distilled into algorithms- it is in its ability to change people's lives for the better and there is no numerical figure that can be attached to opportunity, health and prosperity.

Financial services in particular has undergone a process of dematerialisation of financial assets and processes over the past fifty years, transforming financial products and information into digital data and digitising the processes (e.g. open outcry to electronic trading). This makes financial services one of the most digitalised, globalised, and regulated sectors of the global economy. Data is no longer just the linchpin of financial services; finance is data, and the sector is reliant on the transnational movement of data due to the reality that financial transactions are transfers of data; financial infrastructures, such as stock exchanges and payment systems, are data networks; and financial institutions, like banks and other intermediaries, are data processors – gathering, analysing, and trading the data generated by their customers[1].

The IRSG membership wishes to bring its knowledge and experience to bear on what is one of the most important issues of our generation which is the humble and earnest ambition of this paper. We explore how the time is upon us to create workable data solutions that see regulatory mechanisms as a way to create opportunity for future generations both at home and in countries where the internet is still not ubiquitous. We ask you to join us in taking action to promote a world where a robust geo-sensitive common course of conduct can be created and indeed welcomed – thereby unlocking this extraordinary opportunity, rather than stifle innovation or deprive emerging markets of opportunity. It is our fervent hope that through the sharing of data we can enable knowledge transfer, education, trade deals, cross border collaboration, increased job opportunities and access to digital products will lead to increased prosperity for all sovereign nations.

The term 'data' is often perceived to be synonymous with 'personal data' as defined under data protection laws. Personal data has been an increasing area of focus for organisations due to the proliferation of differing legislation, regulation, and guidance across multiple jurisdictions concerning how it may be collected, processed, stored, shared, erased and even in how it is defined. Unfortunately, whilst the majority of countries now have data protection laws, in the development of those laws, the majority have not considered that the destinies of law and technology are intertwined and regulation must be responsive to be future proof. For example in financial services, the concept of data portability does not take into account reciprocal data sharing in the context of open banking.

Outside of personal data, other data such as confidential commercial data, also has inherent value, and its handling is increasingly subject to legal and regulatory obligations, and transfer restrictions. For example, in China the concepts of personal data, personal financial data, financial regulatory records and important data are each separately regulated but must be handled holistically as the types of data tend to be intertwined – it is rare that data can be separated to enable a single set of rules or regulatory regime to be applied to its use. Scrutinising both personal and non-personal data allows for the identification of new opportunities, insights and improvements to products and services. Data analysis helps financial services institutions better innovate to meet customer needs, improve risk management, detect and prevent financial crime, help customers gain greater choice, and enhances customers' experience of doing business with such institutions and

1 Financial Data Governance: The rise of open banking and the end of the data centralization paradigm. Douglas W.Arner, Guilano G Castellano, Eriks K SElga

consumers expect more tailored, personalised service offerings, derived from data analytics (provided they have consented to them). Given the inter-connectedness of personal and non-personal data, for the purposes of this paper, references to "data" includes both.

Within this paper we:

A Provide an overview of the importance of international data transfers to the financial services sector and the economy and society at large.

B Set out where the current approach to regulation may lead for the future of international data transfers; and

C Open up a discussion regarding options for a simpler and potentially more rationalised, aligned and beneficial arrangement for international transfers of data, which would make the UK more competitive and ensure that the UK continues to be a leading country from which to launch digital businesses to global customers, and to support societal and business objectives.

We recommend an improved approach

Societal and governmental acceptance of data-based innovation is dependent on an outcome focussed and consistent global framework. Unlocking the power of data in modern economies via data free flow with trust – a major international initiative first launched by heads of governments under Japan's G20 leadership in 2019 and supported by the Ministerial Declaration of the G7 Digital and Technology Ministers' meeting (28 April 2021) – will be key to enabling countries in their recovery from the COVID19 pandemic and in achieving their environmental, societal and governmental ambitions. During the process of writing this paper we went out to industry with a survey to determine key challenges for financial services firms. The results of our survey clearly show the adverse impact on the ability to innovate is a primary concern for market participants. Encouraging consistency in technological change necessitates a collaborative approach on the part of stakeholders (including regulators), data experts and technical specialists. Sharing knowledge, perspectives and experience, and allowing regulatory and legislative ideas to be tested against real-world scenarios, will ensure that discoveries and new advances occur within the boundaries of responsible data processing.

International cooperation to construct a strong culture of data protection across jurisdictions will ensure that societies can innovate and thrive. Many countries outside of the EU, are open in their desire to maintain global data flows, and the perception outside of the EU is often that it is the EU that is driving increased localisation, whereas the perception in the EU is that it is being driven outside. An improved approach needs to be underpinned by consistency for it to have strong foundations. Without societal buy-in, any framework will be easily swept away, circumvented or ignored as technologies, political leanings and society changes. Consistency may be achieved with a sustainable, outcome focussed framework, designed by reference to sound principles and arranged to achieve clear, agreed outcomes, which will allow stakeholders to leverage technology and harness digital economy opportunities while protecting data rights and individual freedoms. A framework which transcends a line-by-line comparison of data laws.

Regulation needs to be thoughtful and introduced in a business and consumer centric-friendly way, recognising that consumer attitudes to data differ depending on cultures and generations. Regulation must be responsive to the realities and needs of data flows, rather than the theory. Clear expectations as to outcomes should combine with flexibility as to how those outcomes can be achieved. Complicated webs of precise, overlapping rules and expectations, subject to varying interpretation, must be avoided. Instead, rules should be implemented that are able to evolve with the framework, enabling the testing of new ideas and sharing of the knowledge gained. The engagement of politicians, international organisations and

trade bodies with a deep understanding of the issues will be vital if we are to draw the current, disparate strands of data protection together into a coherent whole.

The Current Trajectory

In our global economy, a complex web of international data flows (ranging from the provision of visual access to data for one or many overseas parties, through to the transfers of full datasets) exists which is achieved in many different and evolving ways. Movement of data is governed by a patchwork of regulatory regimes, differing between countries and cultures which increases barriers to trade and prevents companies and economies being able to use it at pace. The patchwork approach impedes the provision of high-quality products and services to customers and is a significant barrier to trade more generally,
forcing organisations to put in place extensive and complex legal frameworks to enable the transfers, of which there are a limited number. These legal frameworks include binary adequacy arrangements, an increasing range of bilateral contractual agreements, codes of conduct, certifications, binding corporate rules and schemes such as the Asia-Pacific Economic Cooperation ("APEC") Cross-Border Privacy Rules System ("CBPR") which is a government-backed certification scheme for organisations in approved APEC jurisdictions and which is similar to binding corporate rules, but broader as it applies to intra-group transfers, for transfers between unaffiliated companies and for transfers to non CBPR companies.

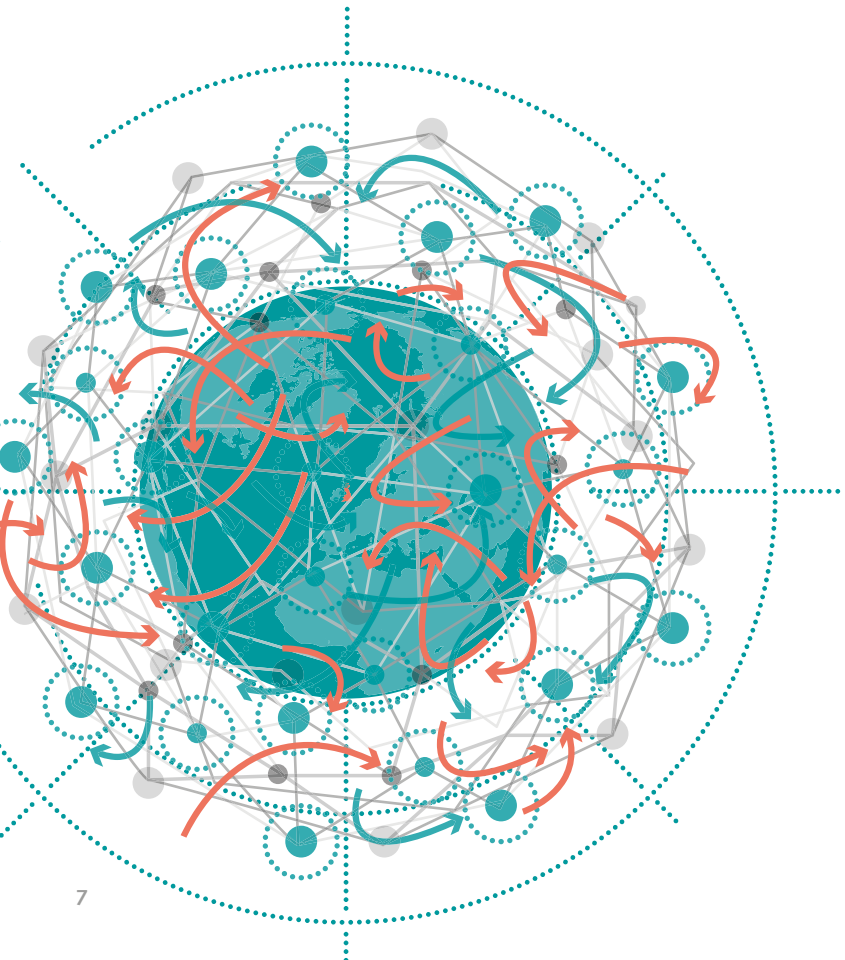
Due to the many compliance silos this creates, the current approach is a drain on resource, with consequent impacts on the broader privacy compliance framework and availability of high-quality customer service and interactions. The breadth of legal, sectoral and other specialist knowledge (including banking secrecy, data ethics, copyright, data classification, information security and privacy considerations) required to assess risk and maintain compliance for international data transfers cannot feasibly be maintained by one or two individuals within an organisation – forcing organisations to grow their compliance teams and back-office structures, resulting in increased bureaucracy and the risk of disjointed decision making. Sector participants have expressed to us their worries over the need for duplication of data and extensive resources, including increased compliance costs and increases in information security risks, if the current trajectory continues.

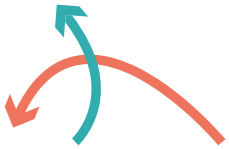
Struggling to meet the time, cost, inconsistent and sometimes conflicting privacy obligations and other demands of mature compliance, there is a risk that smaller and less developed firms either cannot compete – to the detriment of customers – or seek security
in developing paperwork that gives the impression of compliance rather than embedding the underlying outcomes that data regulation is intended to deliver as organisations struggle to follow it in a
coherent manner.

Forward-looking firms are well-aware of the opportunities and risks presented by data collaboration and digitization with many larger organisations having digital transformation as a board level issue. Those with the resources to invest have carried out horizon-scanning initiatives resulting in those firms upscaling and upskilling their strategic, regulatory, and policy-focused colleagues to meet future regulatory challenges and to continue to augment the customer experience. However, multi-disciplinary teams are required to adequately identify and comply with the myriad of data transfer issues – for both internal audiences and customers. The current approach of detailed, prescriptive regulation supported by very specific guidance – as opposed to taking an outcomes-based approach – drives companies to compliance with the letter of the law rather than its spirit, and means companies are not focused on the key objective of best serving and protecting their customers, but on box-ticking. Efforts to achieve compliance with burdensome expectations on paperwork and pre-determined processes, inhibit innovative or alternative (but equally effective) approaches.

Without action, the future for the regulation of international data transfers is increasingly unattractive. As set out in our report of December 2020: *How the trend towards data localisation is impacting the financial services sector,* the industry is seeing growing protectionist behaviours on a global scale in the form of 'data localisation' in the broadest sense. Requirements imposed by national governments and regulators, whether driven by concerns about control or oversight of the Internet – "Internet sovereignty" – and online activities, overt protectionism, or as an unintended consequence of efforts to resolve a wide range of potential data concerns such as outsourcing and third party risk management requirements, both of which have been visible in recent years, are being interpreted as requiring data originating within a jurisdiction to remain in that jurisdiction. It is notable that any future era of protectionism is likely to be more affected by digital protectionism, rather than through tariffs, reflecting a fundamental shift to a digital versus the traditional industrial approach to the world's economies.

States are rightly concerned with protecting their citizens and may implement restrictions on data transfers as a response to fears that inaction will result in harm, and as a reaction to high profile data incidents. That implementation may not take into account that technology helps drive compliance, and there have been seismic leaps in technology including architecture and security, that have addressed many of the arguments about data sovereignty and security. Some restrictions are implemented in reaction to rapid technological advances, where governments are unable to adapt sufficiently quickly to change, and instead elect to create barriers to implementation of those technologies. This creates compliance and competition issues by reducing the choice of where organisations may store and send data.





"It is notable that any future era of protectionism is likely to be more affected by digital protectionism, rather than through tariffs, reflecting a fundamental shift to a digital versus the traditional industrial approach to the world's economies.

SECTION 1
THE FUTURE OF INTERNATIONAL DATA TRANSFERS

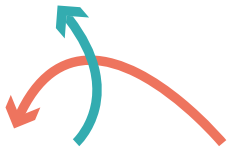
1.1 An alternative future

A world in which each jurisdiction is taking a differing approach to, and implementing inconsistent and conflicting rules for the governance of data will not provide the best outcome for individuals, customers or the companies that serve them. In addition, the current bilateral, contractual approach (in the absence of a relevant adequacy decision between the affected countries) does not map well onto the multilateral, multijurisdictional data sharing initiatives of today and the future.

The current approaches to data transfers mandates a complex framework of tracking data flows from point to point, documenting and assessing risk, and entering into multiple contracts. This approach is not flexible enough to embrace the realities of the many different models of data sharing, and the benefits which can be accessed through the use of privacy enhancing technologies. It also requires continuous updating.

Solutions need to streamline the international data transfer process in a way that can flex and scale to meet the reality of the multiple ways that data is shared together with sector and consumer demands for data sharing, opening the door for new entrants, while retaining appropriate protections for the data in question. Data regulation should focus on achieving an environment that facilitates competition, in which resources are directed based on risk, where businesses can create and access opportunity, and processes are modernised. Updating and transforming ways of working will expand customer choice and better meet customer needs.

As set out previously, the current patchwork approach is leading the sector towards data localisation, an inefficient, manual, data duplicative and legalistic approach to compliance, and inconsistency of obligations, which is struggling to keep up with the reality of data sharing, as it continues to focus on point-to-point data flows. However, work can be done to improve the situation and create an environment where data can flow openly by creating solutions that are fit for the current and future realities of data and the digital economy.



Solutions need to streamline the international data transfer process in a way that can flex and scale to meet the reality of the multiple ways that data is shared together with sector and consumer demands for data sharing.

Ultimately, the rules need to address challenges from a wide-ranging set of perspectives – considering the practical realities of data sharing and evolving technologies, the legal position, individual rights, whether mandated responses to threats function cost effectively, and whether measures achieve the desired outcome. All stakeholders – customers, governments, regulators and businesses – need to be involved in such discussions.

The benefits to customers from a streamlined and forward-looking approach are numerous. By pooling data drawn from across the globe, financial services firms have the ability to reduce and potentially eliminate siloed approaches involving unnecessary and wasteful duplication. Structured oversight, against the backdrop of appropriate systems and controls for data governance obligations and legal compliance, will improve data insights, accuracy, and effective risk control. Increased speed, better consistency, and lower risk all result in improved services for and reduced cost to customers.

Following our investigation, we consider there to be three main recommendations, each of which should be pursued in the long, medium and short term:

1. **Unilateral decisions by jurisdictions with strong data protection cultures to recognise and accept the legitimacy of differing cultural and societal approaches to data handling;**

2. **Overarching/global/interoperable codes of conduct and certifications; and**

3. **A global set of principles.**

RECOMMENDATION 1

Accelerate legitimacy assessments for third countries with similar outcomes for privacy legislation

The most obvious measure, which would be effective as a first interim solution while the other solutions are in development, would be the publication of unilateral decisions by jurisdictions with strong data protection cultures to recognise and accept the legitimacy of differing cultural and societal approaches to data handling in other jurisdictions, which could open up routes for data sharing and collaboration. The EU GDPR has succeeded in creating an EU community for data sharing, enlarged by the 13 countries within the Adequacy Decisions, making it the largest current data sharing community. The Cross Border Privacy Rules systems (CBPR) in Asia is an alternative multi-country and multi-entity model, encompassing nine economies including the USA, Mexico, Japan, Canada, Singapore, the Republic of Korea, Australia, Chinese Taipei

and the Philippines. Yet the approach to similar communities of data sharing continues to be very slow, although it is notable that multiple jurisdictions around the globe have independently moved towards a position in which data subjects are considered to have rights in relation to their data and the ability to control (where appropriate) how it is used.

The UK may have the beginnings of a way forward in this context with the current exploration of adequacy with countries outside of the EU including with Australia, Brazil, Colombia, the Dubai International Financial Centre, India, Indonesia, Kenya, the Republic of Korea, Singapore and the US. This broader approach to recognising the legitimacy of other privacy regimes potentially offers certainty to all business models and sectors as well as data sharing with government entities. However, from experience of the EU adequacy decisions, the discussions take considerable time and, while helpful in promoting high data protection standards and supporting business and economic development, due to the time delay, they do not keep up with the pace of innovation and the needs of businesses in what is already a global digital economy. To achieve adequacy/legitimacy at scale, given that over two-thirds of countries globally now have privacy laws, will require many such decisions.

It is also important that these adequacy/legitimacy decisions are mutual, to give businesses and citizens certainty in data flows, and to build a community where the essential role of data flows for the operation of financial services and the digital economy is recognised.

RECOMMENDATION 2:

Overarching Codes of Conduct and Certifications

The secondary, intermediate term solution would be to shift away from using bilateral agreements for specific projects and transfers, to move to developing multilateral agreements supported by the use of wider-ranging codes of conduct and certifications, developed cross-jurisdictionally by industries in conjunction with and approved by relevant regulators, and underpinned by a strong governance framework. The current bilateral agreements cover a myriad of issues but are for the most part invisible to third parties (including customers) and are only enforceable by the parties – who usually have little incentive or desire to commence any form of proceedings.

Overarching codes of conduct and certifications – enforceable by regulators, but administered by approved third parties – would create certainty and reduce the strain on firms and regulators. In particular, smaller market players who do not have the resources or expertise to easily handle the current compliance burden would be able to engage and comply with them, ensuring competition and innovation are not stifled.

Codes of conduct and certifications are also more accessible to and better understood by customers and other individuals, where they provide clear and comprehensive expectations, focussed on the outcomes to be achieved. Customers have little interest in the detail of legal contracts between companies but would be much more engaged with published codes of conduct or certifications which were visible and visibly enforced.

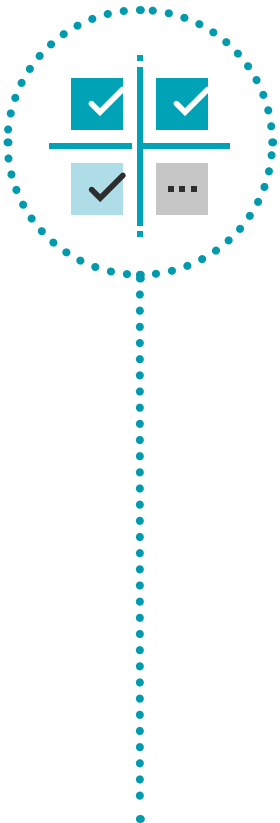
Codes of conduct or certifications designed to achieve principle-based outcomes also have the potential to resolve the issues many in the sector face when seeking to share data with regulators or governmental organisations. At present, data sharing is often conducted on an ad hoc basis, requiring deep analysis of the various legal provisions to identify a (potentially ill-fitting) justification for the desired data transfer. One of the most significant challenges is that the data transfers in question may be multiple and continuous, and are not one-off, making the case-by-case assessment of individual transfers impractical and highly complex. No piece of legislation can cover all eventualities, which is why we consider that a more flexible and multilateral approach is needed.

RECOMMENDATION 3:

A global set of principles

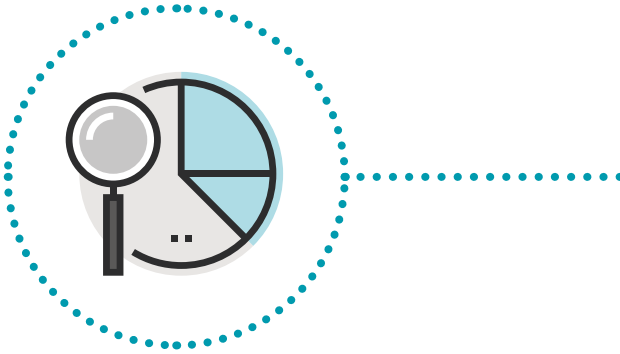
The third, and preferred long-term solution would be the development of an international scheme based on mutually acceptable principles of Free Flow of Data with Trust that multiple countries feel happy to implement and promote.

In terms of future growth of these current models, the divide between European data protection principles and many other countries – including some of the world's largest economies and those with significant economic and political power – may be too wide to bridge. The EU GDPR's development was driven in no small part by the unique cultures and history within Europe and may not fit the approach or attitudes found elsewhere in the world. Imposition of a set of rules developed in one cultural context is a tidy solution in theory, but the reality is that such rules would be unlikely to survive contact with other laws, philosophies and values.

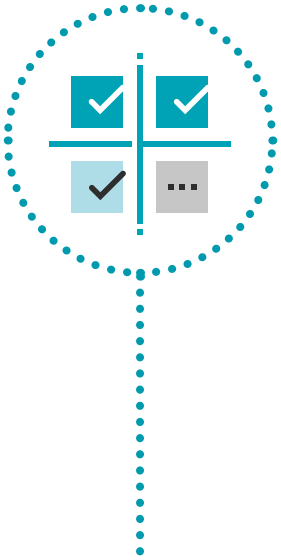


Reflecting the increasingly urgent need to find an alternative to the current contractual and bilateral approaches which are resource intensive, challenging to implement, siloed, and have demonstrated a lack of scalability, there is already some movement at the international level towards consistent and mutually agreed overarching rules for digital trade. At the Eleventh WTO Ministerial Conference (MC11) in late 2017, a large number of WTO members agreed to a Joint Statement under which negotiations would be launched with the aim of establishing an agreed framework for e-commerce (being WTO terminology for digital trade). The negotiations are taking place under the combined chairmanship of

three co-convenors (Australia, Japan, and Singapore). It had been hoped that an agreement might be presented for endorsement by the Twelfth WTO Ministerial Conference (MC12) taking place in late 2021 but following delays a joint statement was released setting out progress made and that they would "intensify…efforts to steer the initiative and forge convergence on major issues by end-2022"2. Negotiations among the 86 participants have gone well, in terms of identifying organising subject matter for discussion and pursuing the objective of an agreement on rules for digital trade. Six articles have been accepted by the participants in plenary without objection, covering e-authentication (e-signatures), spam (unsolicited messages), online consumer protection, transparency and open government data. Work continues on the remaining principles, covering open internet access, paperless trading, e-invoicing, cyber security and competition. However, other critical articles (notably on data movement and data localisation) remain subject to widely divergent views.



Development of a global set of principles or building upon those already in existence will create a stronger foundation for the development within each jurisdiction of technological and practical norms which protect data. Those principles must focus not on process and rigid procedures or on sectors, but on the outcomes sought. Whether an outcome is achieved should be assessed by reference to the principles as operated and applied in practice. Outcomes can be achieved in multiple ways and should be assessed in the round. There should be no requirement for a country to merely accept rules and approaches determined by another state as this creates friction as each country is their own sovereign nation. To achieve this, legislators should move away from mapping one specific legal approach. International consensus of a de minimum standard rather than a legalistic review is required and may be achieved by leveraging already held agreed standards of protection of data. This approach is incredibly useful because it does not discriminate but is all encompassing, and it will require governance, enforceability and measurements, and to be adhered to on a government-by-government basis. The international consensus on intellectual property rights as set out by WIPO is an example of an effective working model in this regard. This approach may also leverage the UK-Japan CEPA approach of the free-flow of data with trust, although it would need to look at the caveats and consider when it is justifiable to prevent free flow of data, and what mechanisms can be put in place to enable discussion and challenge, and what procedures should be created to resolve disputes. Regulators may also leverage the OECD Privacy Principles and Guidelines on the Protection of Privacy and Transborder Flows of Personal Data- but look to expand these to address sharing of all data rather than just personal data. They may also take the form of recommendations similar to the Financial Action Task Force (FATF) Recommendations which are the basis upon which all countries should meet the shared objective of tackling financial crime. In addition to the FATF Recommendations, FATF currently grades



2 World Trade Organisation Joint Statement on E-Commerce 14 December 2021

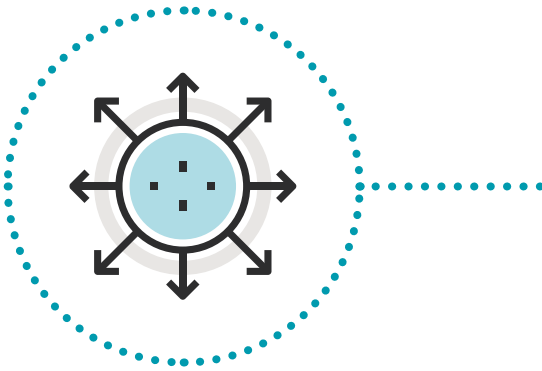
countries and maintains a black and grey list of countries which are assessed as uncooperative in the fight against financial crime. The ICC Digital Standards Initiative is another example of a multi-lateral consensual approach to finding solutions for the digital age based on outcomes and establishing agreed norms, developed to "solve… the key barriers hindering trade digitisation"[3] by digitising the global trade system.

Any approach should be implemented and used within an overarching intention to promote stronger data protection across jurisdictions, including those which are less advanced in relation to data protection. Knowledge, as relates to best practices and new solutions needs to be shared regularly and in an organised manner.

1.2 What the future looks like on the current trajectory

The current framework

Across the world, each country is developing its own approach to data governance and protection. There are many similarities, but also stark differences. Data rules and protections can develop organically from local cultural, business and societal approaches to privacy, individual rights and ethical concerns. Others are on their face transpositions of a current 'leading' data governance regime – often that of the European Union as set out in the GDPR, but, in reality, how these principles are interpreted, applied and enforced are starkly different in practice. Each approach is, and will continue to be, enforced by a variety of data regulators with variable views and resources, including whether or not they view privacy as a fundamental human right, which many do not. This varied approach is not necessarily a problem unless data laws are being used to build walls rather than bridges between people, sectors and countries. The result is that the splinternet is becoming an increasing reality for data as technology, politics, national networks and policies are dividing rather than uniting nations and preventing the flow and use of data for the common good and innovation.



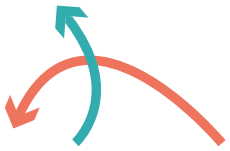
Adequacy decisions, such as those granted by the EU, remain rare. They do not cover important jurisdictions offering significant and wide-ranging digital services such as the United States and India. In relation to the United States – a clear leader in digitisation, data analytics and technological advancement – prospects for an adequacy decision seem bleak. The CJEU July 2020 decision in Data Protection Commission v. Facebook Ireland (usually referred to as "Schrems II), effectively removed the possibility of an adequacy decision in the absence of significant changes to the US approach to judicial oversight of data regulation.

In the absence of adequacy recognition, organisations must look at the current alternatives. Binding Corporate Rules (BCRs) are legally

3 About the ICC Digital Standards Initiative (iccwbo.org)

binding and enforceable rules that companies can adopt to regulate internal data transfers within the same corporate group. This limitation, coupled with the fact that BCRs have not been adopted by sufficient numbers of organisations means that BCRs do not have a material impact on the international data transfer landscape, and we do not expect that position to change significantly. In addition, BCRs will need to be updated to address the challenges identified in the Schrems II decision, notably where group companies are in the US or certain other third countries. Finally, BCR implementation is a lengthy process and costs significant amounts in funds and resources, meaning their availability is of limited benefit to, or even an option for, smaller and less mature groups.

The most useful legal framework and alternative to adequacy, which is most widely utilised, is for parties to enter into available, approved bilateral contracts, such as the European Commission's Standard Contractual Clauses (SCCs). Published on a jurisdiction-focused basis, use of such clauses enable the transfer of personal data to parties beyond the territorial reach of local legislation. Ostensibly, use of SCCs extends the expected protections for the transferred personal data, on a bilateral contractual basis, to parties whose data processing under their local legislation would not ordinarily cover.



The most useful legal framework and alternative to adequacy, which is most widely utilised, is for parties to enter into available, approved bilateral contracts, such as the European Commission's Standard Contractual Clauses (SCCs)

Bilateral contracts, while useful for simple bilateral commercial arrangements, are not suitable for private/public sector data sharing, and can become unwieldy where multiple parties, jurisdictions and/or data flows/projects are involved. Save where draftsmen actively take into account the data regimes of potential data partners' jurisdictions, there is a high risk of cultural and legislative incompatibility between the available terms.

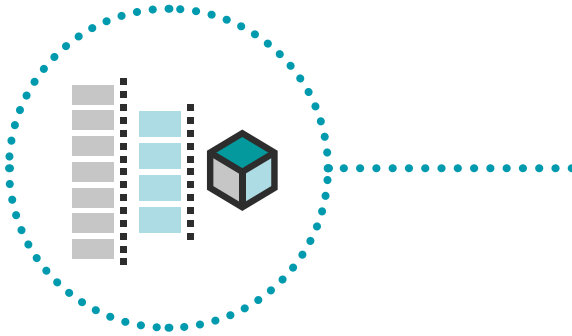
There has been a proliferation of bilateral contracts both within and across multiple jurisdictions, with further examples under consultation and yet more proposed for the future. They are intended to deal with specific relationships and circumstances, and are generally legalistic rather than practical, and are not generally effective when addressing data "sharing" as opposed to "transfer", particularly when multiple parties are involved.

In globalised supply and processing arrangements, incompatibility can cause significant delays and commercial risk. Multiple sets of bilateral contracts are likely to be needed to ensure that all transfers of data packets along the supply chain are covered. The current trajectory will lead to increasingly lengthy and complex contracts, involving numerous compliance challenges, in which multiple sets of bilateral contracts are annexed as companies attempt to cover all possible eventualities.

In the EU, for personal data international transfers alone, the compliance burden has increased significantly over the last 12 months. Companies need to complete data transfer impact assessments and implement multiple data processing agreements, execute SCCs to cover multiple relationship scenarios, develop additional country specific clauses (the latter untested by the courts and developed in the absence of detailed guidance). These documents are additional to the

legitimate interest assessments, data processing impact assessments, record of processing updates and other day to day aspects of data protection governance. Resourcing decisions will need to be made, with potential impact on innovation, trade, competition, customer access to services and individual protections for data.

Contributing to this lack of certainty is the EDPB investigation launched into cloud services, the results of which are due at the end of 2022, and create uncertainty for the growing number of companies using cloud solutions, particularly SME's.



In addition to the resourcing issues for companies, the complexity of relying on multiple data transfer mechanisms which require their own assessments is likely to create complexity and confusion for individuals and make it more challenging for them to understand how their data is being used and protected. It is already extremely difficult for consumers to understand the data transfer provisions included in privacy notices and contractual terms and conditions. Customers do not have the time nor desire to investigate these aspects of modern financial services in detail – instead they simply want assurance that their data will be safe wherever it is being processed.

On a macroeconomic level, if data protectionism continues to rise, the impact on global growth, and especially on growth in the developing world, could be severe. An ECIPE study in 2014 considered the losses that might result from data localisation requirements and related data privacy and security measures. Measures that discriminate against foreign suppliers of data were calculated to reduce GDP and cut domestic investment. A reduction in exports flowed from a resulting loss of competitiveness. On the domestic side, welfare losses were predicted to be substantial due to higher prices and displaced domestic demand that could not be met by available supply.[4] These outcomes are supported by the survey results we conducted, showing that firms are willing to pull out of jurisdictions, limit investment and expansion, and curtail customer offerings in the face of increasing data protectionism.

The economic consequences of data protectionism can be expected to become more severe as the global economy continues to digitalise; data protectionism could well be the 21st century counterpart to the proliferation of tariffs on goods trade in the 1930s. The political consequences of data protectionism should not be overlooked either. As more and more people come to understand the world around them via digital channels, it is important that people have access to common information and services. If data protectionism creates a "splinternet" in which different jurisdictions develop their own digital ecosystems, then people in different countries will not be able to access common global data, and international dialogue and cultural exchange will be threatened. For all of these reasons – economic, cultural and political – the trend towards data protectionism should be resisted.

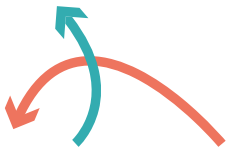
4 Matthias Bauer et al., "The Costs of Data Localisation: Friendly Fire on Economic Recovery", European Centre For International Political Economy, May 2014, https://ecipe.org/wp-content/uploads/2014/12/OCC32014__1.pdf

Sector concerns

As would be expected, the financial and professional services sectors have their own concerns about data protectionism. The cost of doing business within jurisdictions that promote localisation is increasing, in part due to the proliferation of local processing and staffing to meet data requirements. Where previously work would have been handled in centralised or specialist environments, where security, efficiency and limited duplication of data can be achieved, it is now dealt with by an additional local workforce due to the implicit or explicit need to localise data to ensure regulatory or legal compliance. The impact of the measures increase costs and reduce speed and resilience due to data and resource duplication and the reduced ability to use the resources and technology of global, market-leading third parties,the eventual impact of which is ultimately borne by customers.

In addition, our survey respondents expressed fear that additional measures for data transfers may be excessive when considered against the outcomes the rules are seeking to achieve. Compliance efforts may divert resources from threats where harm to individuals is more likely to occur, such as investment in data and cyber security.

Where international data transfers remain necessary, organisations within the sector are facing a need to take immediate steps to ensure compliance, as well as implementing significant ongoing monitoring. Supplier contracts, projects and processes involving international data transfers need to be identified, risk assessed and prioritised for remediation, but the compliance options available come with complexity, and the challenges articulated. Given the current diversity of international approaches, and the limited levels of adequacy recognition for data protection in third countries, institutions face the reality that they will not be able to proceed with certain transfers – leading to a need to implement data localisation alternatives or withdrawal from the market altogether. As previously discussed, there are implications for customers as well as financial and other business implications for such a move.



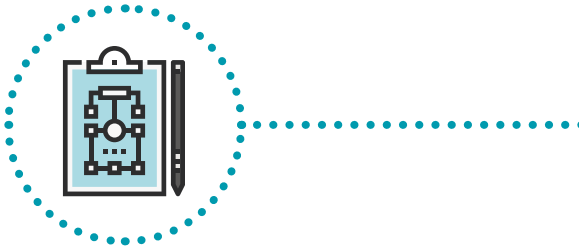
Where international data transfers remain necessary, organisations within the sector are facing a need to take immediate steps to ensure compliance, as well as implementing significant ongoing monitoring.

Repatriation of data assets and a continuing shift to data localisation is viewed as detrimental for business and for its customers in the UK and many countries, but there are others where it is viewed as an opportunity to drive inward investment, albeit a flawed approach. While our survey respondents had few concerns that data localisation would cause their own firms to experience competitive disadvantage or loss of customers, the majority of survey respondents did not think that the current rules on international data transfers will foster economic growth for the countries in which they operate. Over half of respondents thought that the ease of doing business overall would reduce, with a quarter of respondents having a high level of concern regarding the impact on business growth.

The current obligations on data transfers do require organisations to have a detailed understanding of the customer data journey However, these outcomes could equally be achieved without the attendant friction and negative consequences of data localisation by a better regulatory approach or more mature accountability frameworks where

expectations as to outcomes are aligned but organisations are provided with greater flexibility as to how they can be achieved. Although organisations comply with transparency requirements regarding international data transfers, the reality is that customers do not engage with the legal minutiae. Instead, customers and regulators are focussed on outcomes – they are not generally opposed to the secure transfer of personal data for legitimate reasons, but instead want to be able to both access the service that requires the transfers to access the data to which they are entitled, and to enforce their rights in the event that something goes wrong.

Consequences of data balkanisation/data localisation



As set out in our report of December 2020: *'How the trend towards data localisation is impacting the financial services sector'*, the financial services industry is seeing increasingly restrictive behaviours on a global scale via 'data localisation' in the broadest sense, which inhibits the flow of data, both personal and non-personal, between jurisdictions, disrupts regional and global outsourcing models and impacts on regulators and supervisors being able to execute their mandates, particularly prudential regulators focused on financial stability. Requirements imposed by national governments and regulators mean that data originating within a jurisdiction must remain in that jurisdiction. We note the challenge that data localisation poses to global companies. These include creating single customer views across a global enterprise; supporting anti money laundering operations; deploying global technology operating models; complying with regulatory reporting; delivering effective risk management and providing a consistent, seamless customer journey for customers no matter with which part of a global organization they engage.

We agree with the aim of national governments and international organisations that all data is held securely and subject to appropriate protections and controls. However, we consider that data localisation obligations are likely to lead to, rather than away from, the outcomes that many governments profess to seek to avoid, which is why financial services in particular face increasing barriers. An increasing divergence of expectations between jurisdictions is undermining and, in some cases, entirely blocking the benefits offered by increased digitisation. It is also limiting the choices of the individuals whose data they are seeking to protect, many of whom increasingly see themselves as global citizens. Rules need to align with positive outcomes for citizens, the economy, and wider society.

One example is the Security and Exchange Board of India (SEBI) in India, which was intended to create better resilience for the Indian financial services sector. Restrictions on the transfer of payments data has impacted both payments systems and banks and has created blockages in what were previously smooth processes. While the intention behind the legislation was to protect the sector, the net result has been that certain services and protections cannot be offered to Indian consumers.

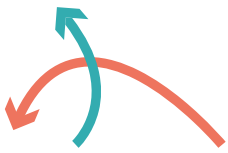
Another aspect of data localisation that can result in increased fragmentation is the requirement for physical infrastructure in some jurisdictions. As localisation requirements become widespread, the previously open and interoperable architecture and governance structures of digitally connected organisations will require significant redesign. Global service providers will need to rent or build physical infrastructure in each jurisdiction in which they operate. The result will be that data is held in and services are provided from a series of fragmented networks, each with their own idiosyncrasies, quirks, complications and broader operational resilience issues.

To support such a complex system, financial institutions have already made massive investments in compliance and architecture. This will only increase in scale, with localised compliance teams for each jurisdiction (or series of compatible jurisdictions). Those teams will have to cooperate with one another from a distance. Where methods of sharing data cannot be identified, firms engaging in research will have to run multiple, duplicative analyses around the world.

The impact of such a compliance setup is already significant, diverting resources from other areas of the business and is a problem that will only increase. Decreased efficiency leads to higher prices for consumers. Innovation requiring new or unusual data processing will be restricted, leading to competitive disadvantages both at the organisational and state level. The knock-on impact on economic growth will be felt via a failure to grow GDP to the degree that would otherwise be possible, which itself may trigger social and governance problems. It will also inhibit innovation and the development of improved customer experience, services and products.

These wide ranging and complex compliance requirements also inhibit new and smaller entrants from the market, thereby solidifying the presence of current incumbents. With a lack of new challenger organisations, the usual outcomes are slower innovation, higher price and less customer choice – all of which are adverse impacts for individuals and markets

Fragmented data storage often leads to local providers competing only against each other. This poses risks to overall operational resilience, limiting reducing innovation and data security. Security is best maintained via the competitive development of state-of-the-art software and practices, which is supported through access to the full breadth of the market with multiple participants from across the globe. A lack of cohesion in data handling and practices and conflicts between applicable rules will also increase the risk of errors. Risk management will need to focus on reducing the scope for liabilities, though it is unlikely to be possible to eliminate them.

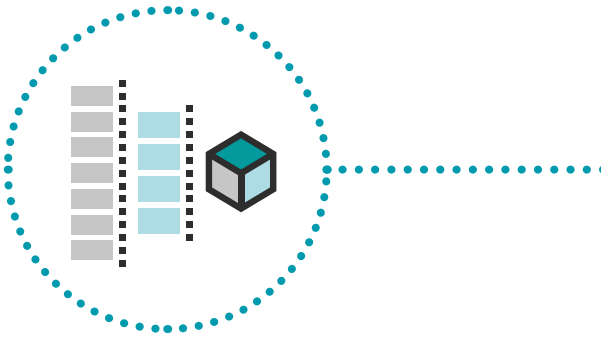


A lack of cohesion in data handling and practices and conflicts between applicable rules will also increase the risk of errors. Risk management will need to focus on reducing the scope for liabilities, though it is unlikely to be possible to eliminate them.

SECTION 2
WHY DO WE NEED TO CHANGE THE TRAJECTORY?

Economic growth is increasingly propelled by the application and use of data. Over 67% of UK services exports are digitally delivered – even though digital trade restrictions doubled in the decade up to 2019. Digital offerings are embedded in the modern economy and the data underpinning prosperity needs to be adequately protected without unduly restricting growth and opportunities. At the macro level, regulators, trade bodies, national governments and international bodies develop, implement, and refine their digital strategies continuously, with a view to creating the right environment for growth and innovation while protecting individual and societal rights and freedoms. Economies including the UK, EU, China, India and others are developing cross-sectoral Digital Economic strategies, and other economies are following. While the US has traditionally led the way via Silicon Valley, it has been imperative for all economies to embrace technology and digital industry in order to attract inward investment, allow local businesses to access and grow in other markets, and to meet consumer needs.

On an individual level, the pursuit of efficiencies, product improvements, consumer appeal, choice and a desire for expansion all serve to motivate exploration and innovation amongst market participants. Data is the fuel which is enabling the exploration and opening of new market opportunities, and companies that are able to realise the potential of their data are moving ahead.

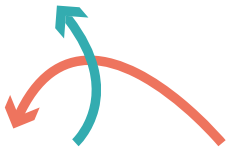


Meeting customer needs

So how do international data transfers improve the customer journey? Customers often have bank accounts in more than one country and engage in cross border payments and purchase/ supply cross border services. To be able to deliver the best customer experience and offerings, firms need to understand who their customers are, the nature of those customers' interactions with the firm, and their views and opinions about the services they receive. Interrogation of the vast quantities of data held by financial institutions to provide their services to customers has the potential to reveal preferences and trends on both an individual and cohort level, which can inform product design and anticipation of

customer needs, as well as help customers better manage their risks and choices.

Cross-border transfers of data are necessary to enable businesses to access insurance markets that can offer the required capacity to mitigate their risks, some of which may span operations across multiple jurisdictions, and at competitive rates. Further, as goods and services move across geographical boundaries, so must the attendant data. The risks covered by such products and services cover a wide range of sectors, from construction and infrastructure projects to aviation and shipping. These, as well as consumer products, such as travel insurance, rely on international transfers of data in a timely way, particularly in the context of claims.



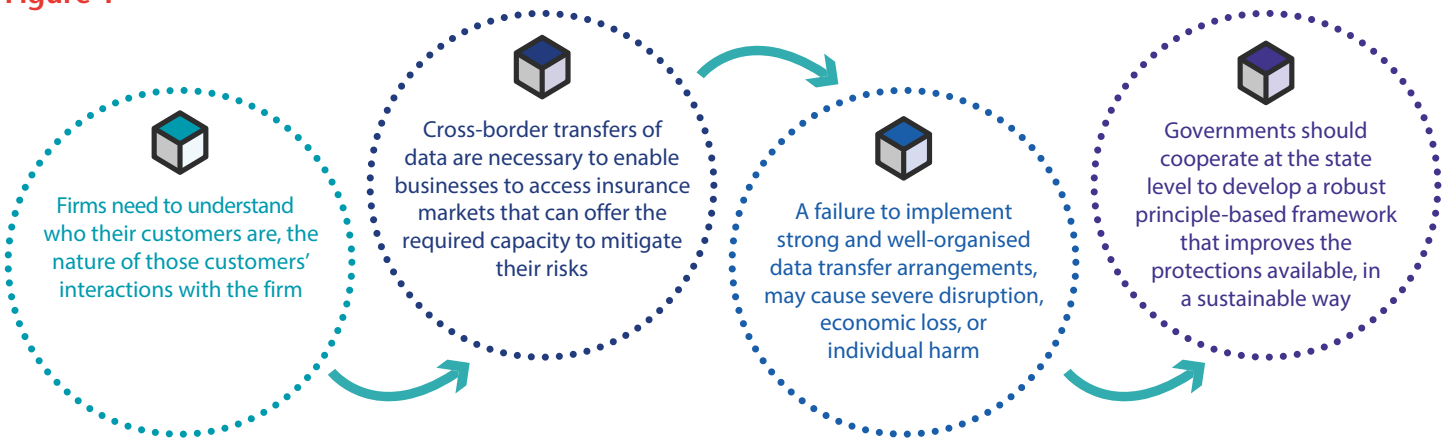
Cross-border transfers of data are necessary to enable businesses to access insurance markets that can offer the required capacity to mitigate their risks, some of which may span operations across multiple jurisdictions, and at competitive rates.

A failure to implement well-organised international data transfer arrangements may, at best, inconvenience customers and, at worst, cause severe disruption, economic loss, or individual harm. Prohibitions or restrictions on the transfer of personal data following personal accidents while travelling may delay treatments and cause unnecessary suffering.

Payments' data is a prime example of information that needs to move between jurisdictions regularly and swiftly. Data localisation which includes transfer restrictions can result in the inability to retain copies of transaction data outside the jurisdiction in which they occur and inhibits the provision of anti-fraud and identity theft facilities, reducing customer access to services and their benefits.

It is our view that countries and their governments should cooperate at the state level to develop a robust principle-based framework that facilitates cross-border data transfers and improves the protections available, in a sustainable way, on a global level. The availability of multiple transfer mechanisms, along with the recognition of the equivalence of similar (though not identical) legal and practical protections for data, is needed to ensure that the service and efficiency provided by financial institutions are not inconsistent from state to state. Uniformity in the service as offered across jurisdictions matters to the insurance, banking, and other industries, and is expected by customers.[5]

Figure 1



5 Cited in A blueprint for UK Digital Trade' (TechUK, 2021)

Advancing growth for the financial services sector will deliver customer benefits

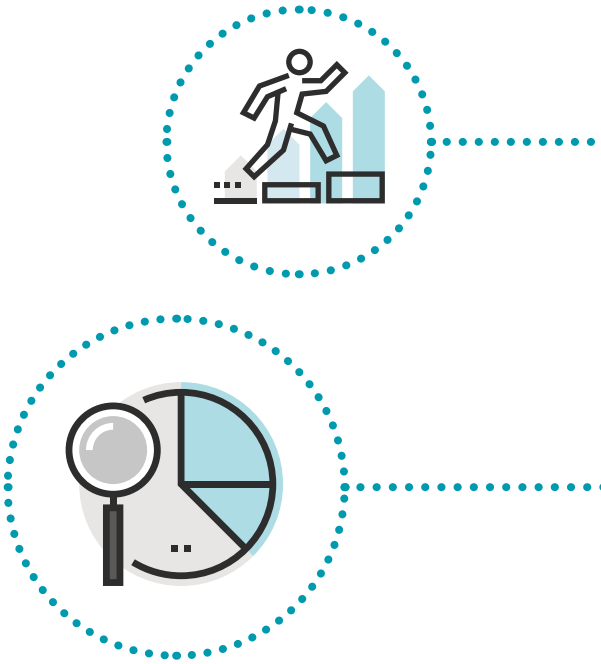
The Covid-19 pandemic has propelled economies to embrace a hybrid approach to work and to societal change at increased speed. Citizens can increasingly access essential government services remotely through digital portals, and governments are progressing on the digital identity path. The UK recently published an updated 'digital identity & attributes trust framework'[6] with the ultimate aim of making it quicker and easier for people to verify themselves using modern technology.

Customers have, since Covid-19, embraced an exponential shift toward digital information, services, payment and delivery, all of which is predicated on cross-border data flows.

On the financial side, digital payments are increasingly replacing both cash and cheques – reopening a contemporary but previously subdued debate as to the place of both in society. Businesses, workforce, consumers, and the myriad of stakeholders in the modern economy are embracing digital communication, digital development, and digital innovation, leveraging the benefits of speed and ease of access, delivery, lower costs, greater choice and innovative solutions.

The clear push for digitisation, combined with access to the best tools, employees, systems, and practices, on an international scale and facilitated by laws and regulations that support the free flow of data and encourage co-operation, has the potential to advance growth for the financial services sector at an extraordinary rate and to deliver sought after benefits to customers. Increased globalisation, technological improvement, and digital upskilling are stimulating a vibrant and dynamic market in which opportunities and ideas progress from initial concept to market at significant speed.

Data analytics optimises the customer experience – enabling firms to develop tailored products, reduce the cost of offerings, and develop more accurate and affordable pricing. In Asia, younger digital native consumers who are mobile expect tailored and personalised services driven by data analytics whereas in Europe there is a divergence between those who want a tailored experience and those who want to retain more control of their information. Compliance functions can assess data to proactively identify risk areas, model interventions to correct issues, and avoid customer detriment. Regulatory reporting and transparency are enhanced by the responsible and accurate use of data.



Working together to share data and ideas means customers can benefit while companies can grow their existing customer base, explore different markets, and even tackle issues including environmental, social and governance concerns on a wider scale. The financial services sector can offer leadership and support in such endeavours.

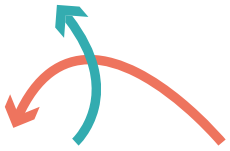
Collection and analytics of data is also of vital importance to facilitate

6 UK digital identity & attributes trust framework: updated version – GOV.UK (www.gov.uk) (last accessed 4.8.2021).

economic survival and recovery from the pandemic and plays an essential role in facilitating an Environmental, Social and Governance (ESG) focussed recovery. Without access to data at a global level and the insights it can provide, ESG ambitions will not be realised as data enables transparency and accountability and helps to inform progress.

24/7/365 customer focused services require a resilient web of suppliers and services with access to the information they need

In our increasingly connected world, it is unlikely that projects or solutions involving the processing of data assets will be confined to only one territory or one legislative framework. At the most basic level, use of cloud storage solutions (whether proprietary or third party), file sharing sites and communications tools generally involve the access to and sharing of data with servers and providers which may be located beyond a firm's home state. In many industries, including financial services, complex flows of data are frequently in motion to facilitate legal and regulatory reporting and compliance, as well as customer service delivery and similar activities.



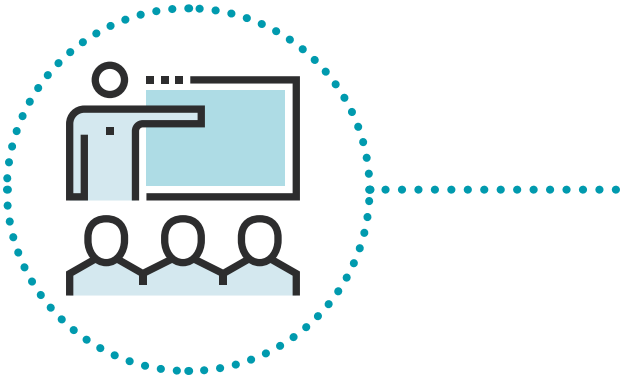
At the most basic level, use of cloud storage solutions (whether proprietary or third party), file sharing sites and communications tools generally involve the access to and sharing of data with servers and providers which may be located beyond a firm's home state.

The financial services sector has a relatively unique position on a global level – underpinning the provision of goods and services on an unprecedented scale. For example, exchange of billing data enables telecoms providers to permit and charge for the use of their communication plans overseas. Use of traveller's cheques is rapidly diminishing, as the payments industry can track and enable the international use of national bank cards. Potentially fraudulent transactions can be identified and frozen based on the collation and analysis of transaction history, location, and similar data.

In the financial services sector, customers are looking to firms, including insurance market participants, to offer products and services across multiple jurisdictions and marketplaces. Customers are mobile and expect to receive the same standard of service, and access to the same products, regardless of their own location. To meet the demand for a seamless, interconnected offering, our view is that financial institutions must think globally, not locally, and must develop the systems and controls necessary to achieve this outcome.

A common thread joining all firms, regardless of size, sector, or location, is the need to comply with relevant data legislation, regulation, and guidance. The responsibility is on companies to ensure that data can be shared safely and securely. Managing international data transfers and their attendant risks, without frustrating progress or impeding growth, is proving to be a highly complex exercise. One respondent to our survey noted that increasing regulation surrounding international data transfers has the beneficial effect of forcing *"organisations to have a better understanding of [the] customer data journey, which will facilitate transparency"*. However, it is becoming increasingly costly, operationally challenging and resource intensive to comply with the myriad of different, and sometimes conflicting, laws, regulations, and guidance, such that financial institutions' global digital initiatives are compromised, and, in some instances, strict compliance with all requirements is perceived as unachievable. Change is needed.

International data transfers occur at all points in a client relationship, from onboarding to termination. At the outset of the relationship, firms need to ensure that Know Your Customer ("KYC") processes are followed. This involves the collation, review, and analysis of a client's personal data (potentially including sensitive or 'special category' material) in conjunction with any relevant public or proprietary non-personal data (both of which may relate to multiple jurisdictions eg a resident of Morocco opening a bank account in the UK) which may affect client acceptance. Client identification information could be sent to a UK institution before being transferred to an affiliate or overseas provider for the completion of necessary checks and analysis. Enquiries may also need to be made of credit reference and similar agencies, which may again require the transfer of personal data. Significant concerns raised in our survey were *"timeliness to on-board"* clients, as well as any *"impact on annual requirements for on-going due diligence."*

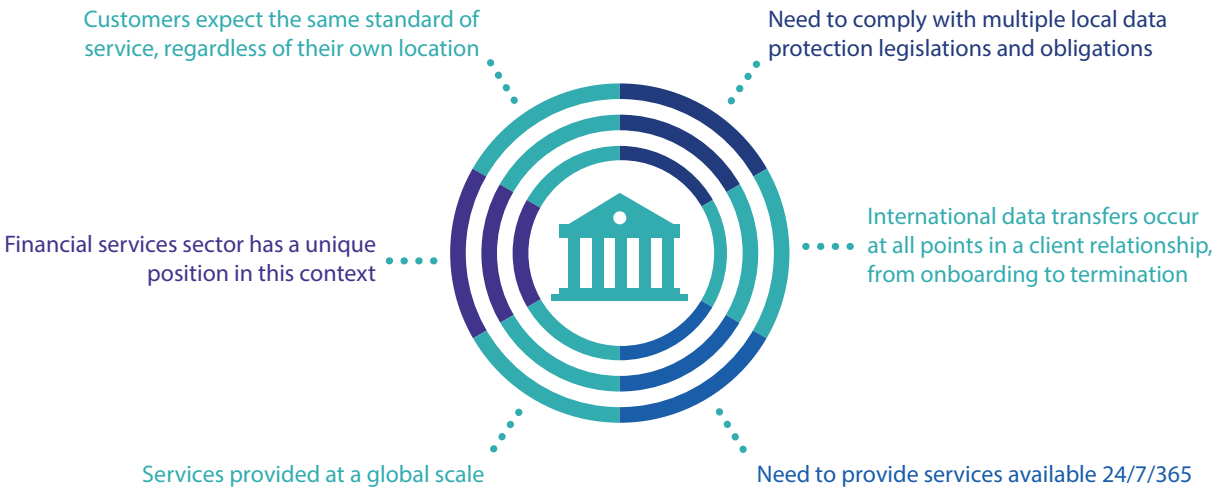


Following onboarding, repeated transfers of personal and non-personal data will be made in the course of customer relationship management and security, product design, marketing, and client services. Data storage rarely occurs in-house for a range of reasons including specialist data storage, security and processing available from specialised vendors and the facilitation of global engagement. Even where processing is directed by internal employees, there are significant benefits to collaborating with group companies, service partners, outsourcing or technology providers which offer up to date services and security, and which are based in a different jurisdiction.

Companies operate best when they can leverage skills and expertise which may be spread across the world. Within a global group, expertise in HR, finance, marketing, technology and other specialisms may be located in a variety of geographical locations. Data needs to be accessible by those in multiple jurisdictions in order for those colleagues to support evolving business models, and to meet customer needs and expectations.

In a global economy, financial firms are a key linchpin of the 24/7/365 model to enable their customers to operate and to meet their regulatory obligations. Data must flow globally and continuously to support these businesses in providing their goods and services to their customers. Constructing a web of suppliers and services which 'follow the sun' ensures that firms in this sector can serve their clients' needs and expectations. Yet in doing so they must be mindful of the obligation to recognise and manage the intrinsic supplier, cyber and compliance risks. In some cases, segregation and other data management will be needed – increasing operational complexity and involving additional and potentially significant cost.

Figure 2

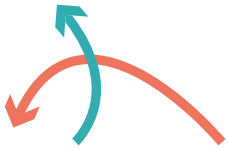


4.1 Cross-border data analysis plays a critical role in stopping financial crime – including funding for terrorism

Money laundering processes and sanctions checks are a mandatory part of the robust governance, effective risk procedures and adequate internal control mechanisms required by law and enforced by regulators. Even firms who manage this process internally rely on third party tools and data sources to assist them with meeting their obligations. For many firms, however, this is a process for which leveraging third party expertise and data is a necessity. Whether performed internally or externally, when onboarding a new client, financial institutions often need to access data from one or even multiple jurisdictions, process that data in another, and potentially store the data and outcome of the processing in yet another place.

Conflict and inconsistency between legislative approaches to data sharing in pertinent jurisdictions can easily impede the free flow of data – impacting the accuracy and utility of any findings while also placing institutions at risk of non-compliance with one or more sets of rules. An inability to share intelligence on individuals, companies, sources of wealth, legal proceedings and other processes risks the creation of unhelpful echo chambers in which undeserved reputations persist. Impediments to AML and similar processes prevent bad actors being identified and dealt with in a timely manner and are harmful to society at large.

As referenced by the FFIS Survey Report of August 2020[7], the voluntary sharing of data across trans-national public-private partnerships is vital to the fight to disrupt *"financial crime threats as diverse as organ trafficking and the illegal wildlife trade, to terrorist financing"*. The quality of regulatory reporting is demonstrably improved by such



Money laundering processes and sanctions checks are a mandatory part of the robust governance, effective risk procedures and adequate internal control mechanisms required by law and enforced by regulators.

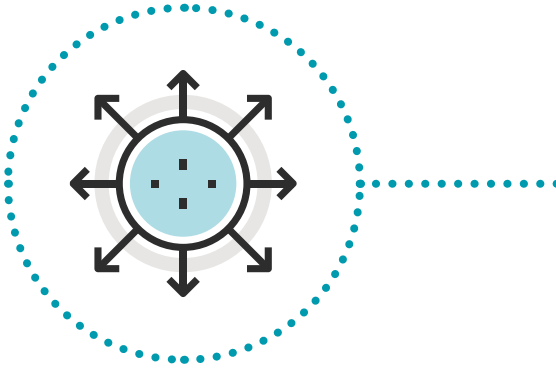
7 Maxwell, N (2020) Future of Financial Intelligence Sharing (FFIS) research programme: 'Five years of growth in public–private financial information-sharing partnerships to tackle crime'

collaboration, with the FFIS reporting that public–private partnerships focused on organised crime are many times more likely to provide disclosable, actionable intelligence for law enforcement agencies. Partnerships are at present small in scale but have vast potential for expansion if provided with appropriate resourcing.

Combatting financial crime and complying with sanctions are global issues, and success demands a coherent and cohesive approach at an international level. Despite some successes, the FFIS Survey Report found that less than 1% of the proceeds of financial crime are currently recovered. Relevant data must be able to move freely across borders if the global community is to successfully exclude bad actors from accessing and using legitimate financial systems to launder the proceeds of their criminal activities.

Jurisdictions with opaque financial sectors and strong or state-mandated banking secrecy obligations, have long been viewed as safe havens for those who would take advantage of the protection they afford. An absence of clear reporting, transparency as to beneficial owner identification, and oversight, provides opportunities for money laundering, tax evasion and other criminal enterprise.

Prohibitions on pooling data naturally inhibit monitoring and surveillance activities, a situation that can be exacerbated by additional restrictive legislative and regulatory rules governing specific relationships, such as employee legal protections that vary between states. Rules implemented historically to prevent a specific harm may, in the context of rapidly evolving data and technological capabilities, particularly increased remote working, need to be reassessed and their scope potentially refined. If data cannot be combined and analysed by appropriate parties under proper conditions, it may result in a proliferation of safe spaces for wrongdoing, provide opportunity for arbitrage for criminals, and defeat the objective.



4.2 Developing people's potential should not face geographical restrictions

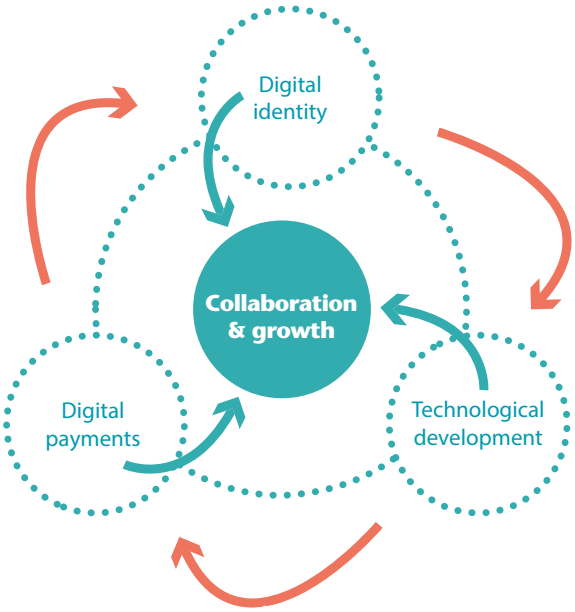
Advancement and innovation are reliant not just on technological opportunity and the availability of data, but also on access to the requisite skills and experience. Horizon-scanning and anticipation of market trends is not simply a matter for computer analysis or application of an algorithm. People, each providing their individual perspective as informed by their distinct cultural and societal norms, are crucial participants in the process. Attracting and engaging diverse talent is a recognised critical element of sustainable innovation.

As demonstrated by the Covid-19 pandemic, virtual working is not only feasible but can even boost productivity. Early indications are that a fundamental shift has occurred in working practices, with continued hybrid working both sought after by employees and now more readily facilitated by employers. Collaboration amongst geographically disparate teams, both nationally and internationally, occurs seamlessly

through new and improved technologies. Documents can be viewed and amended by multiple parties in real time, while 'face-to-face' access to colleagues is as simple as 'pinging' them through a video-conferencing app.

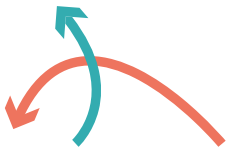
Although physical movement may have been inhibited by recent world events, the movement of data continues and has increased, and the transformation of operations to embrace remote working and new technologies has broadened possibilities for the sector in terms of workforce structuring. To access the leading experts and deepest experience, it is imperative that firms are able to continue to provide individuals and suppliers in other countries with access to personal and non-personal data. We support a framework which would deliver the data conveniently to those who need access, while encompassing sufficient organisational and technological safeguards to protect rights, freedoms, and legitimate interests.

Figure 3



improving connectivity leads to better prospects

Improved data flows also have knock-on benefits for emerging countries and economies. Already, digital trade has enabled enterprises in developing countries to increase their access to the export markets – the internet has made market access easier, enabling suppliers to reach new and often wealthier markets. Digital communications and modern data sharing have improved access to talent, knowledge, skills, and inward investment, enabling accelerated growth for those markets through access to the global economy. Improved data flows support financial inclusion – enabling global markets to reach new customers and transform the quality of life of people in developing countries. Geographical remoteness and inexperience are no longer significant barriers to participation by cutting edge outfits with new ideas. External experts can be identified regardless of their location, and with suppliers tapping into resources worldwide.



Geographical remoteness and inexperience are no longer significant barriers to participation by cutting edge outfits with new ideas.

However, there remain multiple impediments to progress, both practical and technological. Data flow restrictions, whether in the

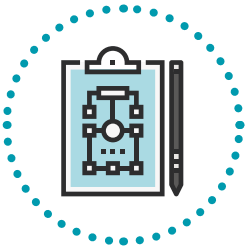
form of intentional barriers to the export of data or as side effects of protective policies, are one factor impeding market access and reducing the availability of high-quality cross-border options for firms and their customers.

Data flow restrictions may force collaboration to occur via joint ventures or require participants to obtain licences – increasing delays, costs and bureaucracy with little to no positive impact on services offered or customer experience. Partial and total prohibitions on the export of data, software or algorithms, as well as obligations on business partners to provide copies of source codes and other proprietary data before permitting a partnership to operate within a territory, all operate to dissuade joint operations and alliances and investment into those territories.

For developing economies to participate fully in the opportunities that modern technologies provide, and to benefit from the huge opportunities for financial inclusion opened up by FinTech and digital trade, more advanced economies and their business communities must provide resources and guidance to enable developing economy market participants to put in place highstandard data governance. Capacity building at an international level will increase competition, not least as regards the race to improve the security of data handling processes.

The creation and recognition of appropriate data standards based on outcomes, with universal application, will aid in the realisation of this aim. In contrast to localised and protectionist approaches, working together as a community to implement minimum acceptable standards will build trust and facilitate safe and reliable data flows.

4.4 Strengthening regulatory compliance benefits consumers and society



Barriers impeding international data transfers are often implemented in the expectation that they will protect local markets and enable better regulatory oversight. However, the Financial Stability Board Report on Market Fragmentation (2019)[8] has warned that applying undue restrictions on data transfers may have the opposite effect.

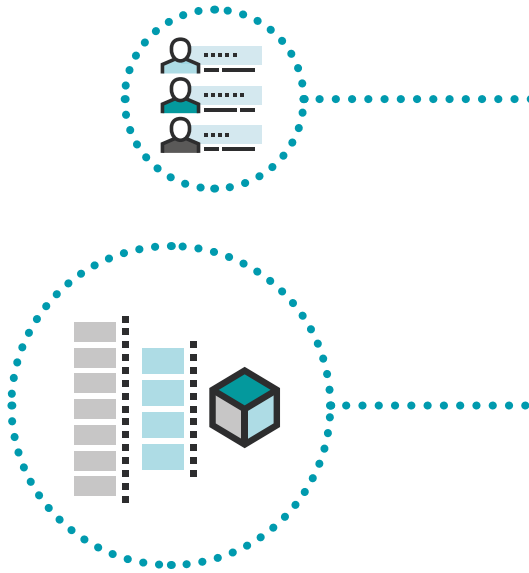
As set out previously, data localisation rules dissuade collaboration and investment. Rather than having the opportunity to access and implement best practices and technologies, local providers may be limited to local solutions which may be of lower quality and do not benefit from the improving influence of competition. Less choice means fewer options, with less impetus and opportunity for improvement and less competition.

The impact of barriers to data flows on cybersecurity and protections for customers is of great concern. Disparate security protocols and

8 Financial Stability Board Report on Market Fragmentation – 4th June 2019 (last accessed 17.09.2021)

technologies, applied to multiple yet separate pools of data of varying confidentiality and sensitivity, inevitably result in a fragmented approach to security. Such an approach will inevitably lead to loopholes, lacunae, and vulnerabilities. Resolving problems and securing data is more difficult when different standards and protocols are being followed, and the data is fragmented and duplicated to meet localisation requirements. The net result, and one we hope can be avoided in the longer term, is a headache for an institution's compliance departments, as well as an increased risk of regulatory failings.

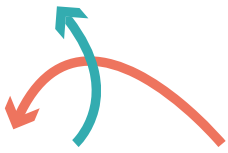
Data localisation requirements also, ultimately, do not better protect data. Data which needs to be made available internationally in order for a service to be provided still needs to be accessed. Barriers to transfer either delay provision of the service or prevent customers from accessing it at all. It is a misconception that data residency obligations provide better protection for data and connected rights. Protection is instead achieved via thoughtful, outcomes-based attitudes to and regulation of how and why data is shared.



Governments are fully aware of the benefits that free flow of data with trust offers. Comparable data protection laws and governance requirements have been enacted across multiple jurisdictions, often aligned to the EU GDPR and encouraged by the prospect of obtaining one or more data protection adequacy decisions. A philosophy lauding the protection of data is developing across multiple regions, often founded in local and cultural mores but also significantly shaped by the existing, predominant legal frameworks. Differences do exist, however. Certain regimes and approaches covering data processing are sufficiently distinctive that mutual recognition and free flow of data between those areas currently is unlikely to be viewed as acceptable

Data protection frameworks remain in their infancy and should not be viewed or approached as fixed in their scope or rules. There is scope for improvement, which could minimise the potential for significant repercussions as a result of data localisation provisions. A focus on raising worldwide data security standards, combined with taking a holistic approach to assessing the adequacy of a region's data laws, is preferable to a rigid approach in which risks and benefits are not adequately weighed.

Further, the markets, regulators and governments should seek to incentivise and encourage openness, cooperation and communication regarding the handling of data sharing, while seeking to minimise formalities, documentation, and unnecessary constraints.



Data protection frameworks remain in their infancy and should not be viewed or approached as fixed in their scope or rules.

SECTION 3
HOW MORE DIGITAL TRADE WOULD HELP FINANCIAL BUSINESS PROVIDE BETTER CUSTOMER SERVICE

3.1 Interconnectedness leading to higher quality customer services in the Financial Services sector

Enhanced reliability of data transfers stimulates an increased interconnectedness between, and consistency across, financial institutions. A unified approach helps to facilitate greater transparency of and access to products and enables the switching of financial products and services, thereby promoting customer choice and enhancing competition. Open banking benefits consumers – helping them to manage their own accounts efficiently and streamlining their interfaces with the sector.

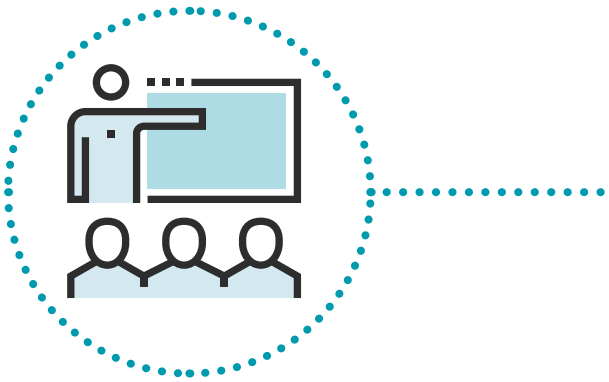
If harnessed correctly, processes such as client onboarding can be condensed without lowering the accuracy of the checks performed. The benefits of data sharing include improved decision-making processes, access to prodigiously large sets of information, capability to leverage information that has been created and/or cleared by other financial institutions, effective systems oversight and the generation of higher quality customer services and greater consumer choice.

Data sharing activities between financial operators fall into three distinct groups:

A **incoming data**, which includes data received or bought from other financial institutions, and which can be used to obtain a clear understanding of a specific situation and support better decision-making;

B **outgoing data**, which comprises all data shared with business partners outside the financial sector, in order to improve capabilities or develop new services; and

C **data pools** – collaborative datasets which are amassed within a specific virtual space and comprised of data emanating from different financial institutions.

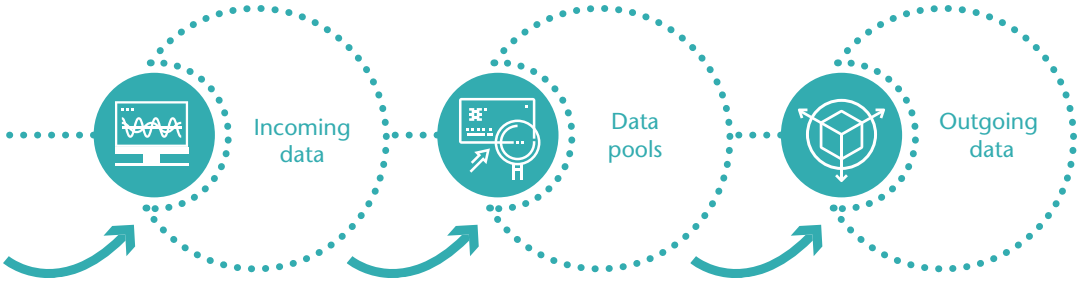


Technological data sharing applications are commonplace within the sector. Application Programming Interfaces (APIs) are the most

frequently used, being protocols that allow services to communicate and exchange information online. The use of APIs increased dramatically in Europe over the past 5 years, following the introduction of the Payment Service Directive in January 2016.

The interconnectedness resulting from the use of APIs has enhanced trust in the market and in financial services sector data sharing activities. For example, banks have been able to provide assistive services such as customer protection against compulsive online gambling, and other problematic behaviours, to the benefit of both individuals and society.

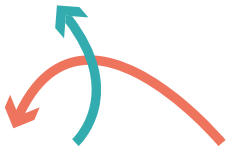
Figure 4



3.2 Business customer view: raising funds and borrowing for investment – equity and debt

The development of data transfers and data sharing practices between financial institutions is an incredibly powerful instrument for business customers as well, especially when it comes to access to funds. Equity financing and debt financing are the primary types of financing companies can use to raise capital for business needs. In both cases, the ability to access relevant information across borders is key for both parties: for companies to access funds, and for financial institutions to perform credit risk assessments.

Access to shared information about stakeholders, companies and their credit risk scoring can help investors to obtain financing rapidly and help financial institutions to make their internal processes quicker and more efficient. The financial markets rely on robust and timely access to data to operate effectively, transparently and to appropriately manage risk.



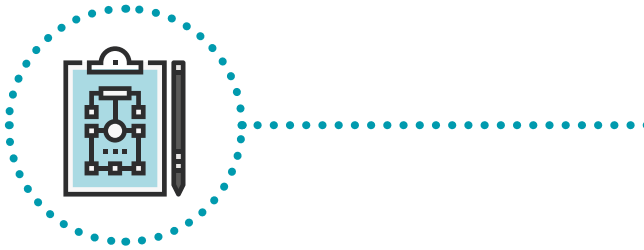
The development of data transfers and data sharing practices between financial institutions is an incredibly powerful instrument for business customers as well, especially when it comes to access to funds.

3.3 Customers require access to funds across the world: both in the form of a local branch and via electronic means

Digital financial services does not stop at borders, meaning banks, insurers and other financial entities must take into account customers' need to access funds, products and services from different countries. If we look at the expectations of the sector, significant issues include increasing connectivity for businesses, creating cross-borders payment services, and enabling cross-border access to funds. Data localisation

services, and enabling cross-border access to funds. Data localisation and transfer restrictions act as barriers, preventing companies from implementing measures to meet these expectations.

Clients expect services to be provided worldwide at the click of a button. Customers use mobile banking services via smartphones or other portable devices, and their expectation is that the services are available everywhere and at any time. An ability to provide services worldwide not only meets customers' needs located in developed countries, but also helps the development of commerce in developing countries.



To enable customers to benefit from global services, financial institutions are increasingly required to comply with localisation measures. This may involve obtaining authorisation to access a local market or ensuring that international data transfers are performed in a specific way or via a specific method. Co-ordination between the private and public sectors on the development of harmonised standards and protocols for data transfers is crucial to enable timely and safe data transfers for customers and financial institutions.

3.4 Customer journey mapping and its link to payments (and other complex transactions)

The evolution from "online banking" to "mobile banking" requires financial institutions to re-design their customer journeys to meet customers' demands and needs, knowing that the easier to use their systems are, and the more demonstrably secure, the more they will be able to meet customers' needs and maintain customers' trust. All of this is predicated on the ability to transfer data.

Applications and access portals continue to evolve. Trends in the sector show that there is ongoing attention to the development of customer-centred solutions, enabling customers to make and receive payments even without accessing their mobile banking, such as user-generated payment links. While practical for users, such payment solutions complicate the user journey, potentially involving international data transfers and exposing deposit holders and credit providers to technological and cybersecurity risk.

3.5 Open Banking

The term "open banking" refers to the process to open-up services across different banks or financial institutions. It provides a secure digital environment by which banks and other financial institutions can share data and make services available to third parties explicitly authorised by the customers.

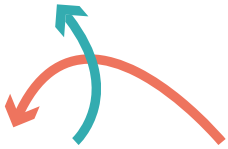
The view within Europe is that it has been pioneering in this sector: putting in place the vision presented by the European Commission

after the 2007 economic crisis. The evolution of open banking services has increased competition and innovation in the financial sector market, stimulating organisations to develop new consumer-centred services. Outside of the EU however the view is that the EU is not setting a good example for open banking, in that places like China have been drafting open banking and data protection laws in parallel and so are able to align the two and make them work together; whereas Europe's open banking laws are being drafted in more of a vacuum and so are perceived to not work together in practice.

Interaction between banks and financial institutions in general is granted via the use of APIs, which enable interconnectedness between operators.

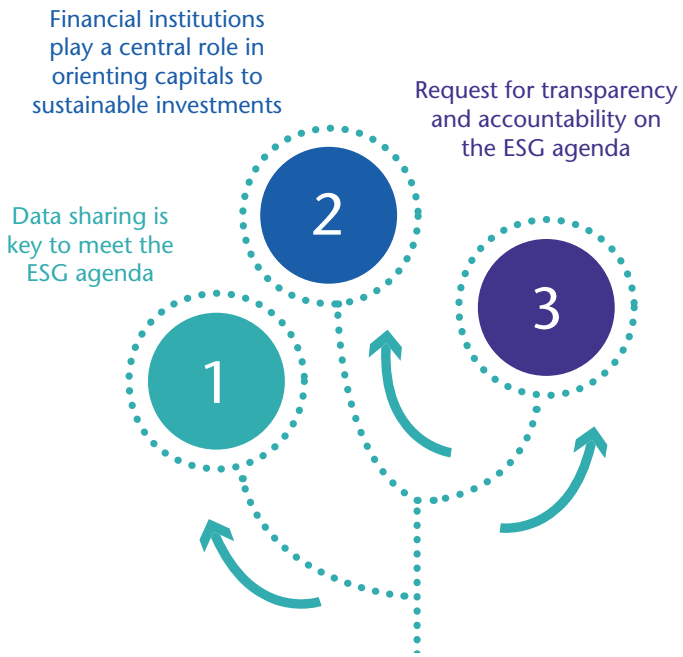
During the COVID-19 pandemic, the digitalisation processes have been accelerated all around the globe, including the financial services sector which has used its capacity and resource to make key investments in digitisation. We expect that reliance by individuals on cash payments will continue to reduce, and society will evolve to a cashless (and ultimately cardless) position, where the interconnectedness of banks and financial institutions will be more central and important than ever.

The identification of standardised requirements for the security of international transfers of data will be crucial to ensure the "ubiquity" of banking services around the world.

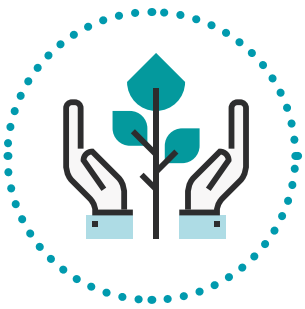


The evolution of open banking services has increased competition and innovation in the financial sector market, stimulating organisations to develop new consumer-centred services.

Figure 5

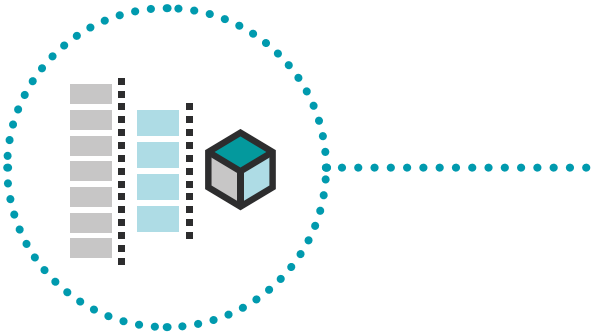


3.6 Environmental Social and Corporate Governance (ESG) agenda



Financial institutions, because of their central role in modern society have a key role in orienting investors and capital to projects and initiatives which focus on sustainability and socially responsible behaviours and demonstrating their own credentials through transparent reporting. The potential exists for the sector to help with

growth and development of new and more sustainable business models.



Access to data is key to meet the ESG agenda and to the ability of organisations to provide the necessary metrics to support claims of sustainability and impact. Professional and financial services are steadily developing frameworks focused on addressing these issues, from modern day slavery to diversity and equal representation[9]. However, these frameworks have developed organically and assess a wide and differing variety of metrics. The lack of a global set of standards and agreement on the necessary quality and content of supporting data makes claims of sustainability and social impact vulnerable to allegations of unreliability and potential 'green washing'.

In order to be able to assess whether a company is investing or taking enough care about their ESG strategy, it is important to collect sufficiently detailed information covering multiple metrics. Government can encourage and support the development of socially sustainable finance by the provision of appropriate incentives, and by ensuring that data management regulations do not prevent the responsible access to and use of data for such purposes.

Sustainability assessments can also provide an insight into future performance. A 2005 Report argued that *"integrating ESG considerations into an investment analysis so as to more reliably predict financial performance is clearly permissible and is arguably required in all jurisdictions"*[10]. The 2020 RIAA benchmark report found that responsibly managed funds are outperforming traditional funds; proactive consideration of social risks tends to result in improved financial resilience, not least by avoiding the brand damage that flows from a misstep.

Modern investors and the media take an active interest in the ESG agenda and demand transparency and accountability. It is through the review, analysis and supply of appropriate data that firms can demonstrate corporate and employee bona fides.

Both personal and non-personal data are relevant to any ESG focused assessments. The sector needs to be clear as to how such data requirements should be handled, in particular when data from disparate jurisdictions needs to be compiled and analysed – the ability to transfer data efficiently is key.

3.7 Artificial Intelligence (AI) innovations

The financial services sector deeply relies on the use of technology and is constantly looking to introduce new solutions to improve their services, making them safer, more convenient, and efficient for the benefit of its customers.

9 See Accelerating the S in ESG – a roadmap for global progress on social standards (IRSG).

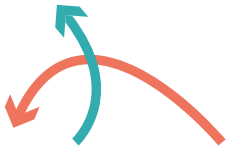
10 Freshfields Bruckhaus Deringer, 2005. A legal framework for the integration of environmental, social and governance issues into institutional investment.

AI is the biggest contemporary technological challenge for financial institutions and, aside from the telecoms and media industries, its adoption is most progressed in the financial services sector. The McKinsey Global Institute in 2018 estimated that AI could add around 16 percent to global output within 12 years – a process that has only been accelerated by the recent pandemic[11]

Development of appropriate AI-focused regulation is necessary – and will need to live coherently alongside rules on international data transfers. The EU, UK and China have clearly set out their ambitions in relation to innovative uses of data and development of AI with many international businesses using research and development centres in China and the US to develop AI and other technologies.

AI permeates internal and client facing activities – automating repetitive and mundane tasks, enabling more efficient use of resource, more effectively enabling risk management, and opening up new options for market and business growth. AI software is reliant on the interaction of algorithms and large datasets, whereby the machine learns to recognise a specific activity or behaviour and react accordingly. Data is a core component of AI.

Without the free flow of data with trust, AI policies are unlikely to realise their potential. Barriers to data transfers will also create a barrier to the diffusion of AI across the world, and instead create barriers to AI diffusion globally. Due to *"its scale and complexity, AI R&D is particularly [collaborative]. It often involves multidisciplinary teams in multiple locations. It relies heavily on open source software, global publications, shared data, and distributed computing."*[12]



AI is currently used by financial institutions for a great number of tasks, including credit checks, chatbots, task automation, fraud detection, predictive analysis, marketing, or trading.

AI is currently used by financial institutions for a great number of tasks, including credit checks, chatbots, task automation, fraud detection, predictive analysis, marketing, or trading. AI is revolutionising the way customers, companies and financial institutions manage their finances with immediate (or near immediate) responses on loan/mortgage eligibility and providing responses to customer queries in real time. Customer service bots are available 24/7 to provide assistance to customers when it is convenient for them, rather than only during standard working hours.

The potential of this technology seems unlimited, and AI will undoubtedly alter many aspects of our daily lives. However, the integration of AI into financial services poses privacy and data ethics concerns, not least due to the use of automated decision-making processes. The problem of bias being built into algorithms, either due to programming, or due to the AI learning from datasets which contain hidden biases, is real.

To tackle the issues, the sector is investing in the development of strong and robust data ethics framework, such as UK Finance's Ethical Principles for Advanced Analytics and Artificial Intelligence in Financial

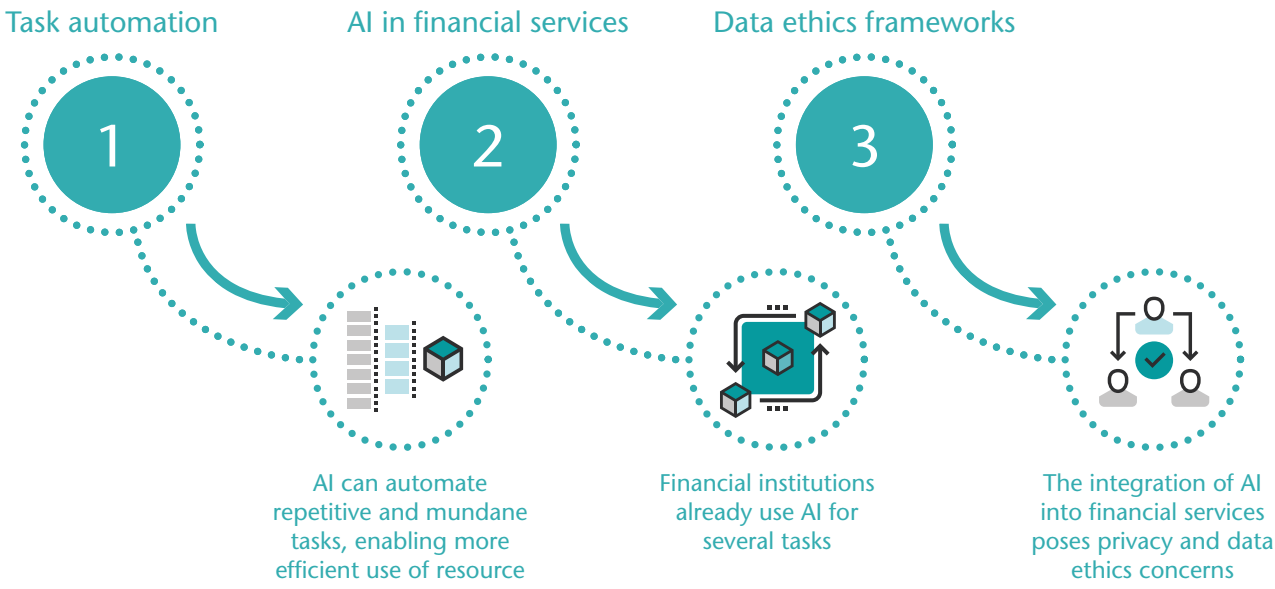
11 Notes from the AI Frontier, September 2018, mckinsey.com

12 Ibid.

Services[13]. Supporting these frameworks, we also need robust, good quality datasets. Inevitably, these will need to be drawn from multiple jurisdictions if the technology is to achieve the best outcomes.

There are moves at state level to begin to tackle this issue. For example, the EU has proposed an AI regulation which puts forward a nuanced regulatory structure. Some uses of AI would be prohibited, while others will be subject to varying levels of regulation based on risk. It will be important that any regulation of AI and the data sets it uses is coherent and does not stifle innovation – a matter that needs to be handled and led carefully.

Figure 6



13 https://www.ukfinance.org.uk/system/files/AAAI-Principles-FINAL.pdf

CONCLUSIONS

Improved rule making is achieved when the means of security compliance that is shaped to meet the problem at hand is dynamic and dialogue based. Our economies, businesses and societies are dependent on data to operate effectively and efficiently. This is becoming ever more important as we transition from industrial based economies to a digital based global economy.

The digital economy and digital society is global, and is dependent on access to data to ensure its effective and efficient operation.

Data needs to be accessible safely and consistently 24/7/365 to support governments and businesses to meet the expectations of their citizens and customers.

Consistency in treatment of data is essential to ensure data protection and prevent misuse of data.

However, achieving compliant data sharing is increasing complex, costly and risky and the current mechanisms are heavily focused on legal, binary and simplistic data transfer scenarios (i.e. via contracts (suitable only for simple commercial arrangements) or adequacy assessments (of which there are very few, takes years to implement and can be revoked)), which do not reflect the reality of multiple, ongoing data access and sharing at scale.

A new approach to facilitating data sharing needs to be developed, one which is fit for the digital economy rather than the industrial economy.

Our recommendations are:

1. Increasing data legitimacy recognitions for third countries as an interim measure based on outcomes rather than comparisons of data laws.
2. Supporting the adoption of codes of conduct, certifications and other mechanisms which all sectors can develop which are relevant and global in scope. A self-service approach relieves the burden on regulators and promotes an accountability approach to compliance which is better understood by individuals.
3. A multi-lateral approach of mutual recognition based on independent standards which builds bridges rather than walls between jurisdictions to facilitate fundamentally similar data outcomes and promote data protection practices while recognizing different cultural perspective on privacy and the value of data will encourage consistency in data sharing and support innovation and economic growth.

CONCLUSIONS...

A new approach to enabling data sharing is key for firms to:

- deliver on their ESG objectives, and to provide the transparency and accountability required by shareholders and customers;
- address their regulatory and legal obligations in relation to the fight against financial crime;
- facilitate access to equity and debt markets and investment opportunities;
- provide transparency and supporting accountability frameworks;
- innovate robustly;
- meet customer needs and expectations;
- leverage diverse and global talent; and
- support global supply chains and helping to manage risk.

Financial services is key to helping facilitate the global economic recovery, and in the global digital economy, this is reliant on timely access to data. Facilitating safe and practical methods to ensure data is protected needs new tools to be developed to support the reality of global and dynamic data flows.

The current approach is creating excess friction, complexity, risk and opacity for all concerned. We need to move from a legalistic and binary approach to a multi-lateral approach based on mutual recognition to promote high data standards focussed on outcomes.

The IRSG wishes to thank the members of the workstream which have overseen the production of the Report. Please note that this report should not be taken as representing the view of any individual firm which took part in the discussions:

ABI
AIG
Bank of America
Barclays
BNY Mellon
Citi
City of London Corporation
Clifford Chance
Credit Suisse
DLA Piper
Fidelity
Freshfields
HSBC
IA
IBM
Invesco
JP Morgan
KPMG
Lloyds Banking Group
Lloyd's of London
LSEG
M&G plc
Marsh UK & Ireland
Mastercard
Morgan Stanley
Nasdaq
PIMFA
PwC
Standard Chartered
techUK
TheCityUK
UK Finance
Zurich

The IRSG is grateful to those organisations not listed above who also gave their time to discuss the content of this report during its preparation.

For further information about this report, please contact
IRSGsecretariat@cityoflondon.gov.uk

IRSG
INTERNATIONAL
REGULATORY
STRATEGY GROUP

KPMG Law

The International Regulatory Strategy Group (IRSG) is a practitioner-led group comprising senior leaders from across the UK-based financial and related professional services industry. It is one of the leading cross-sectoral groups in Europe for the industry to discuss and act upon regulatory developments.

With an overall goal of promoting sustainable economic growth, the IRSG seeks to identify opportunities for engagement with governments, regulators and European and international institutions to advocate an international framework that will facilitate open and competitive capital markets globally. Its role includes identifying strategic level issues where a cross-sectoral position can add value to existing views.

TheCityUK and the City of London Corporation co-sponsor the IRSG.

CITY OF LONDON

TheCityUK