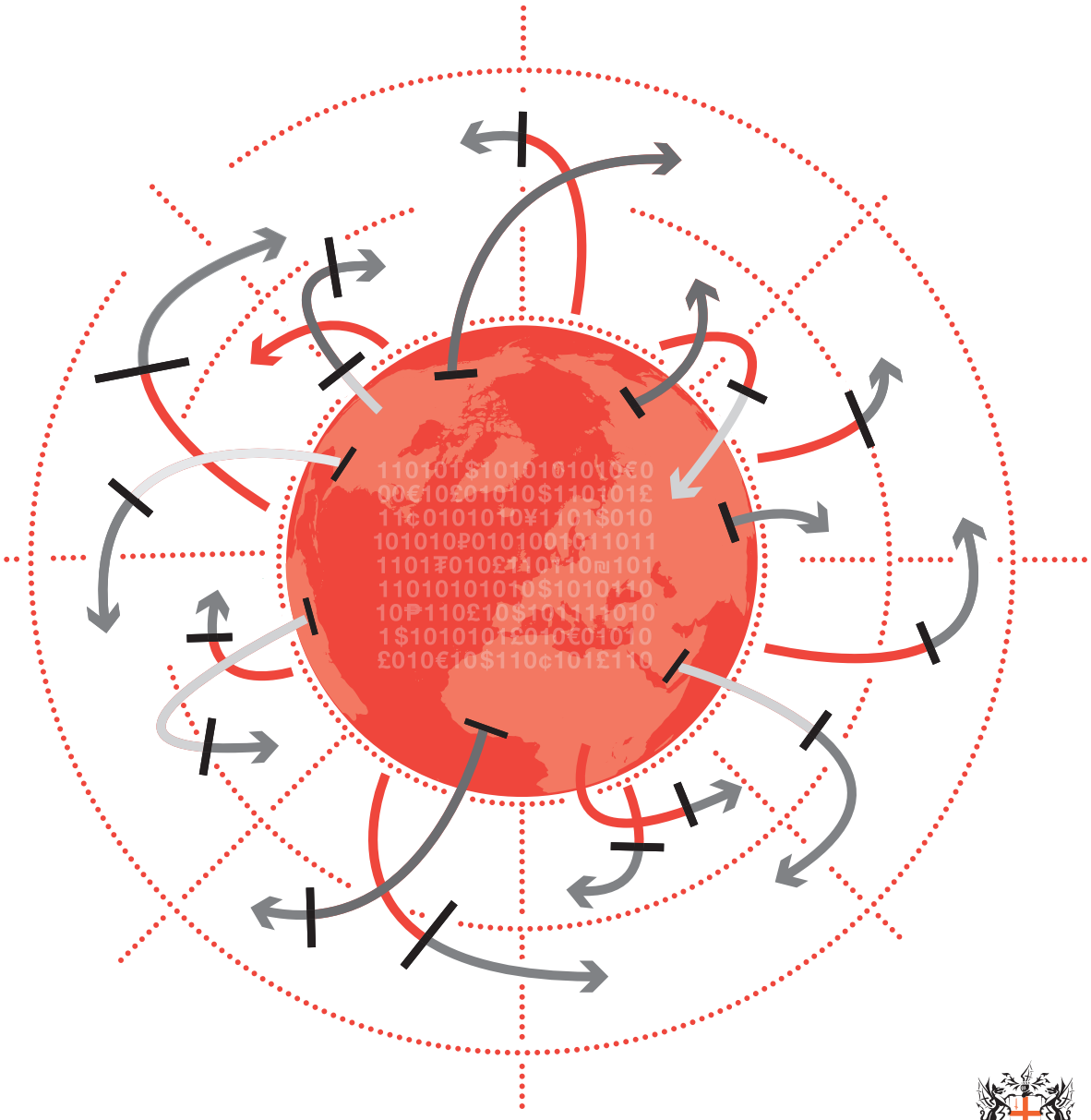
IRSG
INTERNATIONAL
REGULATORY
STRATEGY GROUP

DAC BEACHCROFT

How the trend towards data localisation is impacting the financial services sector

A report by the International Regulatory Strategy Group in partnership with DAC Beachcroft LLP



December 2020

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 DAC Beachcroft

DAC Beachcroft is a leading international legal business with over 2,500 colleagues across offices in Europe, Latin America and Asia Pacific. We also have one of the most comprehensive UK legal networks, operating from 11 locations.

We are a broad-based commercial firm with a strong heritage in insurance, health and real estate. The wide range of other sectors we support includes: construction, financial services, retail, telecoms, technology and utilities.

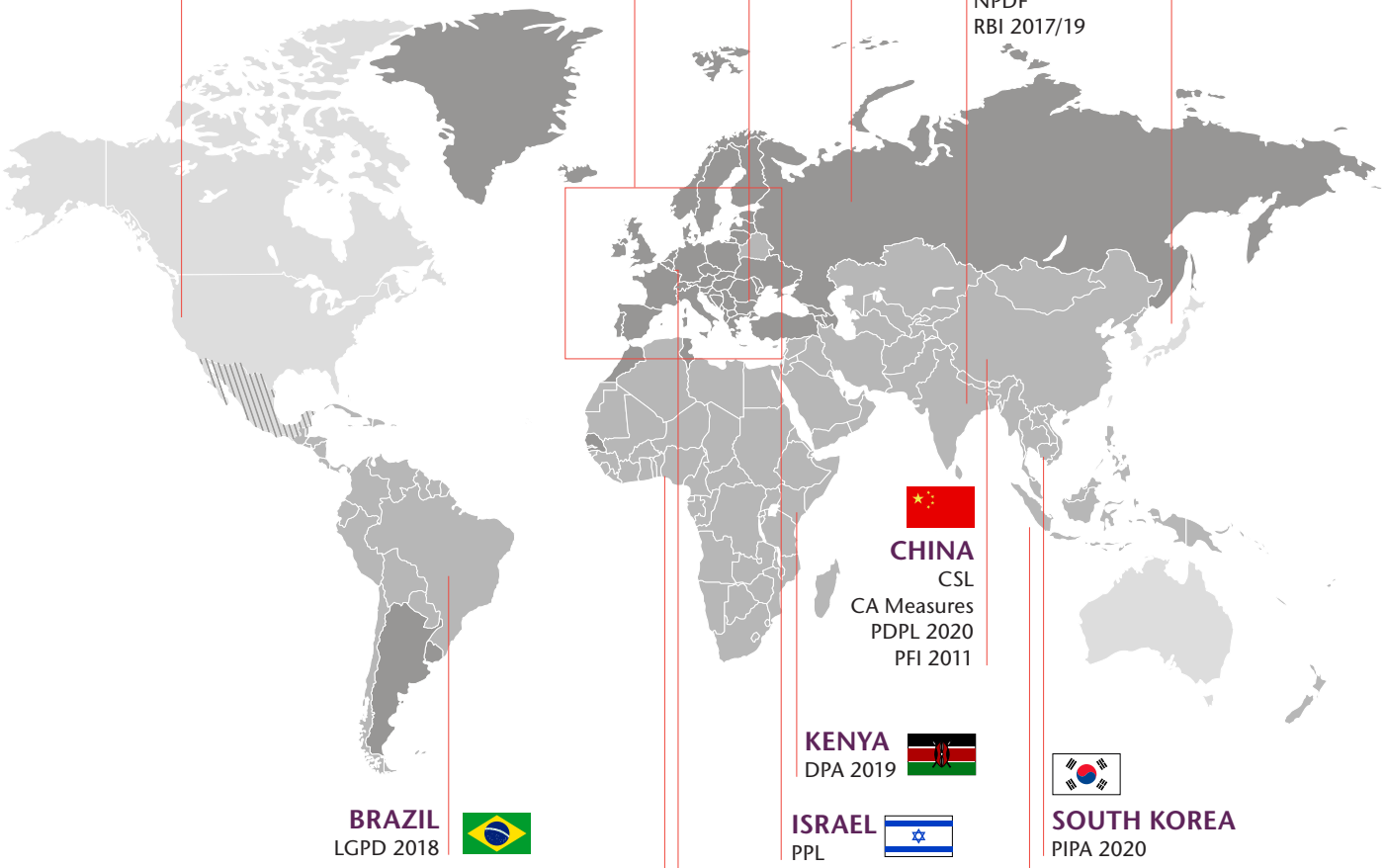
Our purpose is to help clients and colleagues succeed, creating sustainable value. Our vision is for our firm to be recognised for its insight and outstanding commitment to clients.

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

CITY OF LONDON

TheCityUK

The Evolving Global Data Privacy Landscape



CALIFORNIA
CCPA 2018
CPRA 2020

EUROPE
CONVENTION 108
GDPR 2016
FFD Regulation 2018
UK DPA 2018
DORA

TURKEY
EBS 2020
PDPL

JAPAN
APPI 2017

RUSSIA
Federal Law 242-FZ

INDIA
PDPB 2018
NPDF
RBI 2017/19

CHINA
CSL
CA Measures
PDPL 2020
PFI 2011

KENYA
DPA 2019

ISRAEL
PPL

SOUTH KOREA
PIPA 2020

BRAZIL
LGPD 2018

SWITZERLAND
SBA Article 47

LUXEMBOURG
FSA 1993

INDONESIA
GR71 2019
GR82

NIGERIA
NITDA 2013

KEY

CONVENTION 108; Council of Europe and Argentina, Mexico, Morocco, Senegal, Tunisia, Uruguay, Cape Verde and Mauritius

APEC CBPR; Japan, USA, Australia, Canada, South Korea, Mexico, Singapore and Taiwan

CONVENTION 108 and **APEC CBPR**; Mexico

CONTENTS

1 FOREWORD

Vivienne Artz
Chair of the IRSG Data workstream,
Chief Privacy Officer at Refinitiv

In the pre-Covid world, and even more so as we plan toward the post-Covid world, it is clear that data is the enabler of business and digitisation is leading the future for growth, innovation and opportunity. Given the importance of data, whether personal or non-personal data, to the success of the fourth industrial revolution, it is equally important that individuals, businesses and governments are able to readily access quality data, diverse data and in sufficient quantities to inform our ideas, policies and products, and to understand our customers' needs.

More than half of the world's population is online today, making the Internet a critical pillar of the digital economy, enabling businesses, large and small to access local and international markets and to grow. International Internet bandwidth has doubled on a global level between 2016 and 2018[1], largely driven by the free flow of data across country borders.

Trust in data is also paramount to the fourth industrial revolution and the exponential increase in data protection laws across the world in the last decade reflects the desire of individuals and governments to ensure that data is held securely, processed fairly and transparently, and that individuals are able to exercise their rights in relation to data.

The big data and data analytics market alone is estimated to be worth $139 billion in 2020[2] and big data analytics form an increasingly significant and important part of banking infrastructure. In 2019 the big data banking analytics market was worth $29.87 billion[3]. Data insights generated by banks worldwide can offer improved customer services, help bankers create new and more appropriate products for their customers and improve risk management.

While data continues to flow in a seemingly borderless digital environment, we are also seeing an increase in data localisation, a term used to describe a variety of different types of restrictions and requirements imposed by national governments and regulators which require (or have as a consequence) that data, with an increasing trend toward personal data and financial data, originating within a jurisdiction remains, in that jurisdiction.

Continues…

1 According to TeleGeography, Inc, as cited in https://www.deltapartnersgroup.com/data-localisation-information-protection-balkanisation-internet#01

2 Clifford Chance Talking Tech, "*Is the Clock "Tik Toking" on Global Data Localisation?*", accessible at https://talkingtech.cliffordchance.com/en/data-cyber/data/is-the-clock--tik-toking--on-global-data-localisation-.html

3 Mordor Intelligence, "*Big Data Analytics in Banking Market – Growth, Trends and Forecast (2020-2025)*", accessible at https://www.mordorintelligence.com/industry-reports/big-data-in-banking-industry

Data localisation measures can take many forms and the reality and impact of data localisation may be both intentional and unintentional, making it a challenge for even the largest and well-resourced of firms to navigate. Interestingly, the aims of data localisation are often based on arguments similar to those proposed for trade restrictions, such as improved security and regulatory oversight, protecting citizens data and increasing local employment opportunities.

The aim of this report is to provide an overview of the objective of data localisation measures and to outline the different types of restrictions applied by jurisdictions throughout the world to the extra-territorial transfer of data, in the context of the financial services sector. The report further seeks to evidence the practical implications and consequences of such restrictions, and to highlight the key concerns arising out of these restrictions, both regionally and internationally.

We have also proposed recommendations as to how we can navigate this increasingly complex and global issue, and facilitate the continued flow of data in a trusted environment where rights and responsibilities can be accommodated, and the benefits of data flows can be realised for all.

This report has been made possible by the insights we received from across the industry and stakeholders. I would like to thank Rhiannon Webster and the team at DAC Beachcroft for their work with the IRSG in producing this timely contribution on an important issue for the industry.

2 EXECUTIVE SUMMARY

The financial services industry is currently witnessing and responding to increasingly protectionist behaviours across the world in the form of data localisation. "Data Localisation" is a term used to describe a variety of different types of restrictions and requirements imposed by national governments and regulators which require (or have as a consequence) that data, with an increasing trend toward personal data, originating within a jurisdiction remains in that jurisdiction.

The IRSG recognises the important role of industry in ensuring data is secure and protected through internal governance, standards and controls. However, the sector is seeing real changes in the approach to data protection and other related regulation, with businesses no longer able to share data across borders on the same basis as they have done in the past. It is the view of the IRSG that data localisation is not the solution for cross border protection of data and should be resisted.

The aims of this report are to:

- consider the origin of the regulation of extra-territorial transfers, from guidelines to law and the journey towards the current issue of the increasing restrictions on the transfer of personal data across jurisdictions, known as data localisation;
- review the key types of restrictions applied to the transfer of personal data by data protection regimes throughout the world which give effect to the concept of data localisation;
- consider the rise of restrictions on outsourcing and non-personal data flows and how such restrictions have been used to further promote the concept of data localisation;
- analyse and evidence the practical impact of data localisation on the financial services industry; and
- make recommendations and propose alternative measures to data localisation requirements that would better address the concerns raised by national governments and regulators and that have been used to justify data localisation.

Continues…

The context for the financial and related professional services industry:

In recent years, the implementation of data localisation requirements within jurisdictions has increased, which has been driven by a number of concerns surrounding:

- varying levels of protection afforded to personal data across different jurisdictions;
- breach of data privacy and access to data within jurisdictions (e.g. governmental access);
- sufficient and timely access to data for regulators to effectively supervise regulated entities;
- varying standards of data security and breach response obligations across jurisdictions; and
- the impact of foreign businesses on local businesses and markets in which they operate.

With increasing protectionism and a growing lack of trust of other countries, national governments have sought to protect the data of their citizens and address the concerns listed above by implementing various data localisation measures. The members of the IRSG do not consider that measures requiring, or that have as their effect, data localisation are an effective solution to these concerns. Indeed, such measures often given rise to unintended consequences, and may have a contrary impact to that which is intended.

We also see that often data localisation arises not only from intentional protectionism but also as a consequence of otherwise admirable objectives. In particular we have seen an increasing desire across the world for countries to introduce legislation that protects personal data and the rights of data subjects, but these efforts often result in a fragmented approach to data protection across different jurisdictions, which consequently cause increased data localisation due to the difficulties of aligning different data protection regimes.

Summary of key findings:

- **Security is often not increased by data localisation** as businesses subject to data localisation measures cannot benefit from the increased security standards of centralised data centre structures which allow more focussed, consistent and significant investment in data security measures, global outsourcing providers or even foreign outsourcing providers with enhanced data and cyber security tools and their more developed infrastructures. Data is instead hosted in less sophisticated and often therefore more vulnerable local environments with security resources spread across multiple sites.

Continues…

- **Regulatory oversight can also be hampered** as data localisation measures can prevent any regulator from having a full picture of the regulated activity when financial products and services are transacted across borders.

- And contrary to a common rationale for data localisation, **such measures may actually negatively impact local businesses and markets**. The cost of compliance may be too high, which consequently reduces investment in that jurisdiction, detrimentally impacting the local economy and often causing local businesses to close. Restrictions may also have a real and tangible impact for smaller businesses that look to make use of cloud data storage in technologically sophisticated jurisdictions to ensure their data is secure, not only on international businesses whose regularly transfer personal data across borders.

- **Protection of data can be provided instead by use of equivalent standards**. The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) in Europe, and jurisdictions whose data protection regimes echo those provisions in the GDPR, do allow for transfers of personal data outside the originating country if equivalent standards of data protection are in place. However, the concept of "equivalent standards" is fast being replaced with a desire for the importing country to have "identical standards" as the country from whom the data originated.

- Although it seems to be the intention of legislators and regulators to protect the data of the customer by regulating the transfer of data outside the originating country so robustly, in reality, these measures are having a negative impact on the customer.

RECOMMENDATIONS

This report has at its core a recommendation for policymakers to move as close as possible towards mutual recognition of core principles in order to achieve the protection of personal and non-personal data whilst ensuring the continuation of cross border trade and opportunities.

It is proposed that regulators adopt a suggested approach to policy development based on the following principles. These are explained in further detail in Chapter 12.

Continues...

RECOMMENDATION 1 – A principles-based approach to data protection

The IRSG would like to see jurisdictions acknowledging and recognising the adherence to core principles of data protection standards and safeguards across different legal jurisdictions, which can be mutually recognised on a multi-lateral basis and would provide the assurance that data will be sufficiently protected so as to allow the transfer of data. This could be possible by developing standards, using the principles set out in Part Two of the OECD Guidelines[4] as a starting point.

RECOMMENDATION 2 – Regulatory oversight concerns should be addressed by rules on access rather than location

Outsourcing regulations should seek only to ensure that such control of, access to, and ultimately the responsibility for the data remains that of the local regulated entity, and that such is legally documented in the relevant contract with the outsourcing provider.

RECOMMENDATION 3 – Operational resilience should focus on the quality of the outsourcing solution, not its location

An assessment of operational resilience should focus on a qualitative analysis of the measures protecting the data, not its location per se. Ultimately, an outsourcing service provider should not be deemed to be a threat to the operational resilience simply because it is providing the service from another jurisdiction.

RECOMMENDATION 4 – Increased co-operation at an international level

Jurisdictions should work together to recognise that equivalent standards for data protection do not necessarily translate as "identical" standards for data protection. Increased co-operation between regulators in different jurisdictions, perhaps through memorandums of understanding, may ensure that appropriate and proportionate regulatory access to data can be maintained, wherever in the world it is located.

RECOMMENDATION 5 – Use of international trade agreements to remove barriers

Jurisdictions should explore using trade agreements to help stem the flow towards data localisation. The IRSG supports the use of specific trade agreement clauses prohibiting the restriction of cross-border transfer of data. It is encouraging that the recent UK-Japan Comprehensive Economic Partnership agreement (CEPA) contains a shared commitment to allow the free flow of data with no requirement for localisation as a condition for doing business. Policymakers should ensure that any such provisions are modern, forward looking and consider the increased digitisation of services trade.

4 Accessible at http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

3 BACKGROUND

In 1980, the Organisation for Economic Co-operation and Development (**OECD**), in recognition of the increasing amount of personal data travelling cross border, developed Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (the **Guidelines**)[5]. The OECD recognised the importance of harmonisation in ensuring the protection of personal data that was subject to international transfer.

With the Guidelines, the OECD sought to lay out basic rules to govern trans-border data flows. Although they are not legally binding, they are intended to provide a flexible set of principles on which to base data protection legislation or to build into existing legislation and emphasise the need for cooperation between countries in order to strike a balance between protecting the privacy and rights and freedoms of individuals whilst at the same time not creating any barriers to trade and allowing the uninterrupted flow of personal data across national borders. Indeed, the Guidelines actually go so far as to warn against protectionism and data localisation.

The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (as updated in 2013)

PART 4 – BASIC PRINCIPLES OF INTERNATIONAL APPLICATION: FREE FLOW AND LEGITIMATE RESTRICTIONS

16. A data controller remains accountable for personal data under its control without regard to the location of the data.

17. A Member country should refrain from restricting transborder flows of personal data between itself and another country where (a) the other country substantially observes these Guidelines or (b) sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures put in place by the data controller, to ensure a continuing level of protection consistent with these Guidelines.

18. Any restrictions to transborder flows of personal data should be proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the processing.

The OECD produced the guidelines in cooperation with the Council of Europe, which subsequently introduced the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (**Convention 108**). Convention 108 was the first

5 Accessible at http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

legally binding instrument in the area of data protection. Similar to the Guidelines the aim of Convention 108 was to achieve greater unity between members and extend the safeguards for each person's rights and fundamental freedoms, particularly in light of increasing international transfers of personal data.

These two instruments formed the basis for the GDPR (with the principles set out at Part Two of the Guidelines very much echoing the core principles of the GDPR), which again had as one of its aims, facilitating the free movement of such data through the European Union through harmonisation and core principles[6].

However, as we will see in this report, many countries appear to have lost sight of the aims and approaches of these instruments. Across the world, we are seeing increasingly protectionist behaviour and a movement towards data nationalisation in order to protect the data of its citizens.

Such movements were a key driver in Europe behind the introduction of Regulation (EU) 2018/1807 providing a framework for the free flow of non-personal data in the European Union (**the FFD Regulation**)[7]. This regulation has at its centre a prohibition on data localisation requirements on the basis that such requirements hamper and sometimes prevent the exercise of freedom of establishment and the freedom to provide services[8].

Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union

Article 4 – Free movement of non-personal data (defined as any data, not within the scope of the GDPR) within the European Union. Data localisation requirements are prohibited.

Article 5 – The availability of data for regulatory control: public authorities will retain access to data, even when it is located in another Member State or stored or processed in the cloud.

Article 6 – Ease of data portability. The European Union promotes self-regulation in the area of cloud service providers. Providers and regulatory bodies who are encouraged to develop standards and codes of conduct promoting the portability of data.

The FFD Regulation defines a "data localisation requirement" as any "*obligation, prohibition, condition, limit or other requirement provided for in the laws, regulations or administrative provisions of a Member State or resulting from general and consistent administrative practices in a Member State and in bodies governed by public law…..which imposes the processing of data in the territory of a specific Member State or hinders the processing of data in any other Member State*".

In essence, data localisation requires companies that store or otherwise process data to do so in the country where data originates from.

6 Preamble 166 of GDPR

7 Preamble 4 of FFD Regulation

8 Preamble 3 of FFD Regulation

The main drivers for a country imposing data localisation measures or otherwise enforcing measures that have as their effect the localisation of data are usually:

- Concerns about the level of protection afforded to individuals' privacy once the data leaves the country;
- Concerns over data security outside the originating country – including access by foreign governments;
- A concern by local regulators of lack of oversight or access to data when it leaves the country; and
- Support for local businesses.

Concerns about the level of protection and security once the data leaves the country

The case of Schrems II and resultant European Data Protection Board Guidance looked at in more detail in Section 5 of the report is a current example of a data localisation reaction to concerns about the access of foreign governments to citizen's data.

Case study: Localisation as a method of promoting local business in Nigeria

The Nigerian National Information Technology Development Agency (NITDA) released in 2013 (and subsequently amended in 2019) their Guidelines for Nigerian Content Development in Information and Communications Technology (ICT)[9] (the Guidelines). The intention behind the Guidelines was to give effect to the Nigerian government's target to significantly increase the percentage of locally supplied goods and services in the information technology. Amongst other things, the Guidelines require that data and information management firms "[h]ost all sovereign data locally within the country and shall not for any reason host any sovereign data outside the country without an express approval from NITDA"[10]. The Guidelines have as their consequence a restriction on the ability of local information storage firms that Nigerian or other countries' firms may make use of from effecting any transfer of data on their client's behalf.

While neither the Guidelines, nor any other piece of regulation in Nigeria's privacy framework contain a definition of "Sovereign data", the reference relates to personal data generated and collected within Nigeria.

Some information management providers have advocated NITDA's approach as one having the potential to improve confidence in the local technology providers, leading to a boom in domestic ecosystems and economic growth. However, the Guidelines effectively prevent local and international businesses from making use of company or third party data centres located outside Nigeria, which could negatively impact investment and innovation initiatives driven by foreign organisations.

Identical measures are contained in Kenya's 2019 Data Protection Act, which allows the Government to prescribe that certain types of processing shall only be effected through a server or a data centre located in Kenya, based on grounds of strategic interests of the state or protection of revenue.

9 Guidelines for Nigerian Content Development in Information and Communication Technology (ICT), accessible at https://nitda.comepower.com.ng/wp-content/uploads/2020/06/GNCFinale22.pdf

10 See above, Guideline 13.1(2)

Proposed EU initiatives for Digital Operational Resilience for the Financial Sector (DORA)

As part of an ongoing campaign to support the innovation and competition in digital financial services while mitigating associated risks, in September 2020 the European Commission published a draft legislative package which includes a new regulation on digital operational resilience for the financial sector, as well as a draft directive amending existing legislation concerning operational risk and risk management requirements in EU financial services.

The new proposals aim to harmonise the rules for financial services companies around IT risk management. These include requirements around business continuity and disaster recovery; IT incident reporting; digital operational testing, including new obligations around penetration testing. Notably, they also contain stricter rules around management of third-party IT risks.

DORA aims to harmonise the rules concerning the contractual arrangements between third party IT service providers and financial entities. It addresses issues such as audit rights, oversight of sub-outsourcing, data requirements, termination and exit strategies.

Notably, the draft Regulation distinguishes between IT service providers established in the EU and those who have no business presence in the EU. It contains several restrictions on the use of such third-country IT providers, including:

General prohibition on using them as a business-critical provider or sub-contractor. This includes any role of the supplier where its failure can have a systematic impact on the stability, continuity or quality of the provision of financial services[11].

Possibility for regulatory examination of the contracting, sub-contracting and outsourcing arrangements between IT providers and financial services entities, resulting in a recommendation for the financial services entity to refrain from entering into the agreement[12].

Obligation on financial services firms to consider, as a minimum, the below factors, when entering into contractual arrangements with third-country IT providers:

a. the respect of data protection in the third country;

b. the effective enforcement of the law in the third country;

c. insolvency law provisions that would apply in the event of the IT provider's bankruptcy;

d. any constraints that may arise in respect to the urgent recovery of the financial entity's data[13].

Further to the above, the Regulation also requires that any contractual arrangements falling within by its scope, contain as a minimum the locations where the contracted or sub-contracted functions and services are to be provided and where data is to be processed, including the storage location and indication of locations where data is to be processed. The provisions should also mandate the IT provider to notify the financial entity of any changes to these locations.

11 Proposal for a Regulation on digital operational resilience for the financial sector (COM(2020) 595 final), Article 28(2)(9)

12 See above, Article 31(1)(d)(iii) and (iv)

13 See above, Article 26(2)

Establishment in the EU

In practice, while the draft DORA rules stop short of introducing data localisation obligations, they limit the possibility for third-country providers to carry out critical services in relation to financial entities. For such a business to avoid the restrictions imposed in the Regulation, it needs to set up an establishment in the European Union and at all times keep its client updated regarding the physical location of its data storage and other processing activities. The European Commission refers to its approach as a balanced solution to address the systemic impact of ICT third-party concentration risk through a flexible and gradual approach, since rigid caps or strict limitations may hinder business conduct and contractual freedom."[14]

Whilst data localisation requirements may be driven by reasonable policy concerns, including for issues such as national security, there are significant and potentially damaging repercussions associated with seeking to comply with them. In a study commissioned by the European Centre for International Political Economy (ECIPE) the cost of compliance is costing the EU economy $52bn per year whilst the removal of the existing regulations would generate GDP gains of $8bn per year.[15] However, it is not only a compliance issue for the sector. As explained in Chapter 11, data localisation measures also have a negative impact on the customer. Among other things, customers are faced with less choice and therefore higher prices for financial products.

–$52bn/year

+$8bn/year

$52bn/year cost of compliance to the EU economy
$8bn/year GDP gains if existing regulations removed

14 See above, Recital 49

15 ECPE, Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in EU Member States, 2016, accessible at https://ecipe.org/publications/unleashing-internal-data-flows-in-the-eu/

4 OVERVIEW OF THE TYPES OF MECHANISMS

The trend towards localisation can be split into the following main categories:

1. Rules which mean that if you send data to another jurisdiction, you must ensure measures are in place to ensure the same or equivalent standards apply in the jurisdiction of the receiving company/entity as the sending jurisdiction ("**equivalent standard restrictions**");

2. Rules prohibiting transfer unless you have the consent of the individual concerned ("**consent restrictions**");

3. Rules which state certain data cannot leave a jurisdiction at all ("**no transfer rules**");

4. Rules which state that a local copy of certain information must be kept within the country of origin where that information is to be subject to a transfer ("**local copy rules**");

5. Restrictions on outsourcing ("**outsourcing restrictions**");

6. Restrictions on the transfer of **non-personal data** both in terms of specific regulation dealing with non-personal data and also scope creep of both legislation and regulators, expanding their remit to broader categories.

"Equivalent standard restrictions… Countries are increasingly requiring that 'equivalent' means 'identical'."

5 EQUIVALENT STANDARD RESTRICTIONS

5.1 Overview

Equivalent standard restrictions are the best known and most widely used of the mechanisms for restricting (and permitting) the transfer of data. They require that data is not transferred to another country unless that country is recognised as having standards equivalent to the home country for the protection of such data.

On the face of it, the rationale for these restrictions seem sound and the concept of equivalent standards clearly has roots in the legislation and guidelines discussed at Section 3 with their aim of achieving harmonisation across different jurisdictions.

However, as more and more equivalent standards regimes are introduced, we see the practical impact of these mechanisms moving away from this overarching aim, often with the measures for compliance being complex, costly or impractical to implement and therefore organisations are often avoiding undertaking transfers, resulting in greater localisation of data.

The problem arises in the concept of "equivalent". The OECD principles and Convention 108 would likely see "equivalent" as ensuring that different jurisdictions have data protection laws have at their centre a set of outcomes-based core principles or essential elements, with flexibility for changes in technology and other regulation. This would allow for mutual recognition and acceptance of laws across different countries, with different legal regimes and cultures without the need for identical laws to be in place in those countries.

However, what we see instead is a push for more specific, detailed and prescriptive standards of data protection for a jurisdiction to be deemed to protect data to an "equivalent standard", which may run contrary to local legal regimes and other laws and regulations in that country.

As stated above, the practical impact of such restrictions can be to restrict the transfer of data because the requirement is simply too inaccessible or impractical, or there is uncertainty in what "equivalent standards" look like with the result that in either case, the ability to achieve compliance is excessively difficult or impossible. There is no better example of this than the recent Schrems II decision in Europe, the result of which has every company in the EU, and every company in the world which handles EU personal data, questioning if and how they are permitted to transfer data to the US, and indeed any jurisdiction which is not currently on the European Commission's adequacy list.

Case study: Schrems II

Case C-362/14 Data Protection Commissioner v Facebook Ireland Ltd, Maximilian Schrems and intervening parties

Mr Schrems is a Facebook user. Facebook processes user data in the United States and participated in the EU-US "Safe Harbor" programme, which the European Commission had determined provided "adequate protection" for EU user data. In 2013, Mr Schrems lodged a complaint with the Irish Data Protection Commissioner (**DPC**) objecting to surveillance activities undertaken by intelligence agencies in the US. He argued that the law and practice in the US relating to this surveillance meant that there was not adequate protection for personal data transferred from the EU. This complaint was referred to the CJEU, which declared the EU-US Safe Harbor invalid and asked the DPC to reconsider Mr Schrems' complaint.[16]

Following this decision, Facebook, along with most other companies previously relying on the Safe Harbor as offering an adequate level of protection, entered into Standard Contractual Clauses (**SCCs**) to provide adequate protection for the personal data being transferred to the US.

Out of the ashes of the Safe Harbor, arose the Privacy Shield decision adopted by the Commission in 2016. The decision included consideration of law and practice in the US relating to access by US intelligence agencies to EU data and referenced explanations and assurances made by the US (including the establishment of an Ombudsperson, with a remit to review complaints about intelligence service access to EU data) and concluded that the EU – US Privacy Shield, offered adequate protection for EU personal data.

The Commission's decision on SCCs provides that supervisory authorities, such as the DPC, can suspend or prohibit data transfers if it concludes that the law of the country to which the personal data is transferred means that the data importer cannot comply with the obligations set out in the SCCs. Mr Schrems asked the DPC to use this power to suspend or prohibit transfers of his data to Facebook in the US.

The DPC considered Mr Schrems' reformulated complaint and adopted a draft decision, which took the view that US law and practice, allowing US intelligence agencies access to EU data, was incompatible with the EU Charter of Fundamental Rights. The DPC brought proceedings before the Irish High Court, asking it to make a reference to the CJEU, to consider if the SCCs themselves were invalid. The DPC also asked the court to consider whether transfers to the US on the basis of the EU-US Privacy Shield could be suspended because those same laws precluded appropriate protection for EU citizens' personal data.

On 16 July 2020, the CJEU ruled that the protection provided by the EU-US Privacy Shield is not adequate and it is therefore no longer an adequate mechanism for the transfer of personal data from the EEA to the US. The rationale, seemingly mirroring the same concerns raised in relation to Safe Harbor back in 2015, focuses on fundamental concerns with US surveillance law: the "level of protection essentially equivalent to that guaranteed within the EU by the GDPR, read in the light of the [EU] Charter [of Fundamental Rights] cannot be guaranteed [in the US]." The protections for EU citizens in the US are weak because US "provisions do not grant data subjects actionable rights before the courts against the US authorities". The CJEU also concluded that the US Ombudsman, intended to help EU citizens make their case, did not have sufficient binding authority over the US intelligence services.

When considering the SCCs, the CJEU ruled that they remain valid, but on their own may not be enough to ensure an adequate level of protection. Personal data can only be transferred if the importer and the exporter can ensure that the protection set out in the SCCs can be complied with in practice. The judgment implies that supervisory authorities have a role in assessing whether the data is subject to an adequate level of protection. In response to questions received from Supervisory Authorities, the European Data Protection Board (EDPB) issued further guidance in the form of Q&A[17] clarifying that there is no grace period for transfers made under the EU-US Privacy Shield to be changed to a different compliant mechanism.

16 Case C-362/14 Maximillian Schrems v Data Protection Commissioner

17 EDPB, Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, 23.07.2020,, accessible at https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf

European Data Protection Board (EDPB) recent recommendations for data transfers post-Schrems II

On Wednesday 11 November, the European Data Protection Board (EDPB) published its guidance on what these supplementary measures look like in practice. It has published two documents: Supplementary Transfer Measures[18] and Recommendations and European Essential Guarantees [19] for consultation.

Its "Supplementary Transfer Measures Recommendations" set out the steps which should be taken when seeking to make a transfer outside the EEA to a jurisdiction which has not been deemed "adequate" by the EC. The EDPB advises data exporters to take the following 6 steps in order to ensure a compliant transfer.

1. Know your transfers. This involves undertaking a mapping exercise. It may be possible to obtain this information from your Article 30 records. At this point the EDPB refers to other principles in the GDPR such as minimisation and purpose limitation (i.e. making sure the data you are transferring is adequate, relevant and not excessive).

2. Verify the data transfer mechanisms under Chapter V of the GDPR.

3. Assess if there is anything in the law or practice of the third country that may impinge on the effectiveness of the appropriate safeguards of the transfer tools you are relying on, in the context of your specific transfer. This needs to be subjected to due diligence and properly documented. Consider the 4 essential guarantees set out in European Essential Guarantees document.

4. Identify whether there are any supplementary measures required. This is only necessary if the analysis in Step 3 concludes that the law of the third country do impinge on the effectiveness of the safeguards of the transfer tools.

5. Take any formal procedural steps to adopt your supplementary measure. This will depend on the particular Article 46 GDPR transfer tool you are relying on.

6. At appropriate intervals, re-evaluate the level of protection afforded to the data you transfer to third countries and monitor if there have been or there will be any developments that may affect it. The principle of accountability requires continuous monitoring of the level of protection of personal data.

The European Essential Guarantees purport to provide data exporters with guidance on the assessment to conduct in order to determine whether a third country provides a level of protection essentially equivalent to that guaranteed within the EU.

The EDPB considers that the applicable legal requirements can be summarised in four "European Essential Guarantees":

- **Processing should be based on clear, precise and accessible rules;**
- **Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated;**
- **An independent oversight mechanism should exist; and**
- **Effective remedies need to be available to the individual.**

18 Accessible at https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en

19 Accessible at https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en

Complexity and inflexibility

These two documents form a lengthy and, at points, complex framework and methodology for making compliant overseas transfers. A detailed analysis of the practical consequences of this will take some time. The Supplementary Transfer Measures Recommendations are open for consultation until 21 December. The European Essential Guarantees are in final form. At this point, we would highlight the following:

- To make a compliant transfer to a country not on the EU Commission adequacy list, organisations are required to undertake a detailed assessment of the type of data being sent, the access that might be granted to the data when overseas and an assessment of the legal regime in the countries where you are sending the data. This is an incredibly onerous task to ask even the largest of institutions with the deepest pockets for legal advice;

- Annex 2 of the Supplementary Transfer Measures Recommendations sets out a non-exhaustive list of the supplementary measures that could be put in place if the assessment above concludes that a jurisdiction does not provide the level of protection which would be considered acceptable. It contains some insightful case studies where it is clear that strong encryption and pseudonymisation can work as a sufficient measure to ensure a compliant transfer so long as the data remains encrypted and pseudonymised throughout. Although this could be useful in some limited circumstances, in most cases, data needs to be accessible in identifiable format;

- Case Study 6 of Annex 2 uses the example of a cloud service provider which requires access to unencrypted data to perform the service. The EDPB offers no solution to make this transfer compliant if the result of the analysis has concluded that the laws of the third country impinge on rights and protections granted by European data protection laws. One has to assume following Schrems II, that US laws impinge in a way that is not compatible with European data protection law and therefore such a transfer is unlawful.

- Guidance applies with immediate effect and there is no grace period.

At this point in time, one cannot understate the massive ramifications of this guidance on international transfers. If they are approved as drafted, we believe the complexity of making assessments on other jurisdictions and the inflexibility of the suggested supplemental measures, will drive organisations to data localisation as the only option.

5.2 Example jurisdictions

The key example of an equivalent standard regime comes from European data protection law, both from the EU Data Protection Directive and the EU General Data Protection Regulation.

Overseas transfer principles under the EU Data Protection Directive and EU General Data Protection Regulation (GDPR)

Under the old privacy regime in the EU, governed by Directive 95/46/EC (**the Data Protection Directive**), controllers were prohibited from transferring personal data outside the EEA unless the transferee's country afforded adequate protection over personal data. It was for the European Commission to approve particular third countries as providing an adequate level of data protection, taking into consideration the data protection laws in force and international commitments of these countries. As of 2018, when the GDPR came into force, a total of 13 such decisions were made by the Commission[20], including the subsequently invalidated US adequacy decisions – the Safe Harbor and Privacy Shield. In January 2019 Japan was also awarded adequacy status, while adequacy talks with South Korea are ongoing.

The Data Protection Directive provided two further mechanisms by which adequate levels of data protection could be adduced. The first one, Standard Contractual Clauses (SCCs) are model contractual clauses pre-approved by the European Commission which contain commitments for the transferor to ensure an EU-level of protection of personal data. The Commission published 3 sets of SCCs – two for controller-to-controller transfers[21] and one for controller-to-processor transfers[22]. Another mechanism, initially developed by the Article 29 Working Party was Binding Corporate Rules (BCR) - internal data protection policies which allowed for international transfers within the same organisation. The Directive provided that it was for Member States' Data Protection Authorities (DPAs) to authorise transfers made through the use of SCCS and BCR.

The enactment of the GDPR did not amount to an overhaul of the international transfers status quo under the Data Protection Directive. The adequacy decision approach was retained and all adequacy decisions already in force remained valid. The derogations provided for the use of SCCs were also preserved and BCR's were formally recognised in the text of the GDPR. Notably, transfers based on these mechanisms no longer require authorisation from the local DPA.

Adding to the mechanisms prescribed by Data Protection Directive, the GDPR further introduced transfers on the basis of approved codes of conduct and approved certification mechanisms issued by the competent DPA or the EDPB.

20 Andorra, Argentina, Canada (where Canada's PIPEDA applied), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand

21 Commission Decision 2001/497/EC and Commission Decision 2004/915/EC

22 Commission Decision 2010/87/EU

Other derogations set out in the Data Protection Directive, such as consent-based transfers, have continued to be in force under the GDPR, subject to some amendments (e.g. the conditions for 'specific consent'). The GDPR provides an additional derogation, where none of the other derogations apply, that the transfer is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject. However, the GDPR makes it clear that any derogations are intended to have limited application and they are labelled to be "for specific situations" only. They also need to be notified to the local DPA, which is a further restriction on its use.

As more and more countries bring in data protection laws around the world, the majority are following the concepts and terminology of the GDPR and are looking to impose restrictions on overseas transfers. Some examples of these jurisdictions and the particular challenges which are being faced, are set out below.

BRAZIL

Passed in 2018 and entered into force on 18 September 2020, Brazil's new Law on General Data Protection (**LGPD**) replaces and codifies more than 40 existing pieces of data protection legislation in the country[23].

In a GDPR-identical approach, Section V of the LGPD contains the rules on international data transfers. Such transfers are permitted only when the recipient country or international organisation provides an "adequate" level of protection of personal data or where certain contractual documents are in place (the equivalent of SCCs and BCR). There are also a number of derogations from the prohibition, including where the data subject has provided its consent.

The new law grants legal bodies the right to request an evaluation of the level of protection of personal data provided by other states or international organisations by the country's newly-created DPA, Autoridade Nacional de Proteção de Dados (**ANPD**). The factors which the Brazilian regulator will take into account in its assessment are identical to those relating to adequacy decisions under the GDPR.

While the law is already in force, the presidential decree creating the ANPD was only published at the end of August 2020, and the first President Director and Board of Directors were appointed in early November 2020. This list of "adequate countries" to be published by the ANPD is currently awaited.

23 Brazilian General Data Protection Law, 2019, accessible at https://iapp.org/media/pdf/resource_center/Brazilian_General_Data_Protection_Law.pdf (English translation)

JAPAN

The central piece of data protection law in Japan is the Act on the Protection of Personal Information (**APPI**), which received its last substantive overhaul in May 2017[24].

Under APPI, the transfer by a controller of personal data to a third country is only permitted in certain circumstances. Akin to the position under the GDPR, for an entity to transfer personal data to another, situated outside the borders of Japan, for processing, it must be satisfied that the recipient is either:

- Located in a country on a list of countries considered by the Personal Information Protection Commission (**PPC**) as having a data protection regime equivalent to that under the APPI; or

- Specifically adhering to data protection standards providing data protection at the level provided in APPI.

Presently, only countries within the EEA (including the UK) are on the list of countries considered by the PPC as having equivalent data protection standards. If the recipient's country is not on the PPC list, they will need to demonstrate compliance with an APPI-equivalent standard of data protection to enable the transfer. In practice, this could be achieved by the use of SCCs, BCRs, or if the transferee is accredited under APEC's CBPR system.

Alternatively, where the above conditions cannot be met, the controller can rely on the data subject's clear, informed and express consent for the transfer to a third country. For more on the use of consent for cross-border transfers, see Section 6 below.

On March 10, 2020, the Japanese Government published a bill partially amending the APPI. While the changes are expected to take effect from 2021 or 2022, they introduce minor amendments to the legal position regarding international data transfers.

Under the draft bill, where an international transfer of personal data is based on consent, the transferor must provide the data subjects with all relevant information. This includes details about (1) the data protection system of the foreign country to which personal data will be transferred and (2) any specific data protection measures taken by data transferee. Only then, the data subjects will be deemed to have provided informed consent for the transfer. The transferor should also ensure that transferees have in place continuous security measures to protect the personal data, and must provide such information to data subjects if asked.

24 Act on the Protection of Personal Information (Act No. 57 of 2003), accessible at https://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf (English translation)

The Global Ripple Effects of Schrems II

On 24 September 2020, the U.S. Government and Government of Japan released a statement on the conclusion of the 11th U.S.- Japan Policy Cooperation Dialogue on the Internet Economy[25]. In particular, the statement highlights that both countries intend to continue to collaborate with international partners to promote rules that support international data flows, including personal information. In addition, the statement outlines that the two countries reaffirmed their commitment to working together closely to expand participation in the APEC Cross-Border Privacy Rules ('CBPR') system, recognising the CBPR system as a relevant mechanism to facilitate interoperability and create a globally useful and acceptable cross-border data flow scheme.

25 Joint Press Statement on the 11th U.S.-Japan Policy Cooperation Dialogue on the Internet Economy, can be accessed at https://www.state.gov/joint-press-statement-on-the-11th-u-s-japan-policy-cooperation-dialogue-on-the-internet-economy/

ISRAEL

Data protection in Israel is governed by a number of legislative acts, most notably the Protection of Privacy Law, 5741-1981 (**PPL**) and accompanying regulations, as well as the Basic Law on Human Dignity and Liberty, 5752-1992, and the guidelines of the Israeli Privacy Protection Authority (**PPA**).

Under Section 1 of the Privacy Protection Regulations (Cross-Border Transfers of Personal Data from Israeli-Based Databases), supplementing the PPL, controllers cannot transfer personal data outside of Israel, except if the law of the recipient country provides a level of data protection that is no less stringent than that provided by Israeli law. On 1 July 2020, the PPA reaffirmed that it considers EU law as providing such a standard of protection, and therefore, transfers of personal data to all EEA countries, as well as other states affording an EU-level of data protection are permitted[26]. On the same date, the PPA further clarified that despite the UK's departure from the EU, the country would also enjoy such adequacy status, since the country has ratified Convention 108[27].

For transfers to any third countries, transferors can rely on SCCs and BCRs or can obtain the data subject's consent for the transfer. Notably and as alluded above, Israeli law further permits transfers to recipients located in countries which are signatories to Convention 108, which reflect a shift toward mutual recognition of substantially similar protections rather than equivalence.

Continues…

26 PPA, Opinion regarding cross-border transfers of personal data, from Israeli based organizations to organizations based in countries complying with the data protection legislation of the EU, accessible at https://www.gov.il/en/departments/publications/reports/personaldata_the_european_union

27 PPA, Opinion regarding the continuation of cross-border transfers of personal data, from Israeli based organizations to UK based organizations post Brexit, accessible at https://www.gov.il/en/departments/publications/reports/gb_personaldata

On 2 November 2020, the PPA published a report examining how organisations within various sectors comply with the PPL[28]. While the report refers to evidence of "*horizontal deficiencies*" in some sectors, especially in relation to data security in outsourcing, it goes on to conclude that most organisations in Israel maintain a high level of compliance with the provisions of the PPL. Irrespective of the basis of a cross-border transfer, a transferor must obtain the transferee's written undertaking that it has implemented safeguards to protect data subjects' privacy and that it promises to refrain from any onward transfer in its own country or any other country.

An exercise in creative legal solutions

In practice, this restriction on onward transfer in Israeli law prohibits any sub-contracting or outsourcing of services, irrespective of the location of the subcontractor. However, we have seen a variety of approaches taken by international businesses to allow their Israeli entities to take advantage of global outsourcing and IT solutions with onward sub-contracting. These have included putting in place a separate direct written agreement between the local Israeli entity and the sub-contractor. Whilst this approach solves the legal problem it, at the very least, creates an additional administrative burden with the accompanying cost and time implications. Nevertheless, in many cases we have also encountered the additional barrier of providers being unwilling or unable to enter into contractual arrangements with local branches.

CALIFORNIA

While it's easy to assume that countries with GDPR-inspired privacy laws provide for broadly identical Equivalent Standards Restrictions on international transfers, including adequacy decisions, BCRs and SCCSs, one noteworthy exception is the California Consumer Privacy Act 2018 (CCPA), which entered into force in January 2020. While the CCPA affords data subjects a broad range of rights in relation to their data, which are in many ways compatible to those afforded under the GDPR, the law does not contain any provisions restricting the transfer of personal data outside California. Given the influence of the state's technology behemoths and the paramount importance of cross-border transfers to their business models, the lack of provisions restricting international transfers is not surprising.

In reaction to the CJEU ruling in Schrems II, California may seek to apply for an adequacy decision by the European Commission. However, notwithstanding some other substantive differences between the two privacy laws and the present lack of an independent oversight agency to ensure organisations' accountability and compliance with the law, the lack of third-country transfer

28 PPA, Findings of the breadth supervision procedure among the corporate sector: Storage and processing of databases in Israel, accessible at https://www.gov.il/BlobFolder/reports/audit_report_database_companies/he/dtatbase%20compeny.pdf (in Hebrew)

restrictions in the CCPA may prove to be a major, and even insurmountable hurdle for California's attempts to gain adequacy status.

On 3 November 2020, the day of the US Presidential Election and less than a year after the CCPA came into force effect, Californians voted to approve the California Privacy Rights Act (CPRA) which will amend and expand the CCPA. The CPRA strengthens individuals' rights to control the processing of their data by organisations and brings the privacy law in California even closer to a GDPR-compliant standard. Amongst the novelties is the creation of the California Privacy Protection Agency, which will have as one if its main functions the cooperation *"with other agencies with Jurisdiction over privacy laws and with data processing authorities In California, other states, territories, and countries to ensure consistent application of privacy protections"*[29].

While the amendments under CPRA will take effect on 1 January 2023 and enforcement would not commence until July 2023, its new requirements will apply to personal data collected or processed from 1 January 2020 onwards. Should Californian authorities seek to apply for adequacy status with the EU, the enforcement delay could prevent the granting of such status in the next 2 to 3 years, requiring the implementation of alternative solutions for data transfers to Europe in the aftermath of *Schrems II*.

29 Submission of Amendments to The California Privacy Rights and Enforcement Act of 2020, Version 3, No. 19-0021, Paragraph 1789.199.40(i), available at https://oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf

Brexit: The consequences if the UK does not obtain an adequacy decision

The GDPR restricts the transfer of personal data to countries outside the EEA and therefore even though the UK is currently subject to the GDPR and will ensure it is fully adopted into the UK legislature at the end of the current transition period, the UK will become a "third country" when it leaves the EU on 31 December 2020.

It is hoped that the UK will achieve a finding of "adequacy" from the European Commission prior to that date so that transfers of personal data from the EU can continue without further restriction. However, at the time of writing, it is looking unlikely that this will occur in time for 31 December 2020.

The European Data Protection Supervisor (**EDPS**) has commented in its Opinion on the opening of negotiations for a new partnership between the UK and the EU[30] that the UK may benefit from its status as a previous EU Member State and its current compliance with GDPR. However, the EDPS was also concerned with the UK's potential repeal of the Human Rights Act 1998 and emphasised that future regulatory developments in the UK will need to be regularly monitored by the Commission. In March 2020, the Department for Digital, Culture, Media & Sport published an explanatory framework[31] which sets out the UK's data protection legal framework and argues that the UK upholds a high standard of data protection in compliance with the GDPR.

Most recently a letter from the Chair of the EDPB[32] indicated that the organisation is now also concerned with the UK-US Agreement on Access to Electronic Data for the Purpose of Countering Serious Crime (AED Agreement)[33]. The AED Agreement is intended to allow law enforcement authorities of both countries to request access to electronic evidence, including personal data, held by relevant businesses based in the other country, for the purpose of preventing and prosecuting serious crime. It is expected to run in parallel with the existing mutual legal assistance regime, which has been criticised for being slow and inefficient. In the US, the bilateral agreement is implemented through the Clarifying Lawful Overseas Use of Data Act (CLOUD Act).

In its letter, the EDPB expresses concerns that in the event of a conflict between the AED Agreement and the CLOUD Act, especially in relation to data protection, it is not evident that the former will prevail. In comparison, the Chair of the EDPB noted that the EU and the US are also negotiating an equivalent agreement to facilitate the sharing of electronic data and that the EU-US agreement must prevail over US domestic laws, especially regarding onward transfers of personal data. The EDPB also considers it essential that requests made under the Agreement and the CLOUD Act are subject to mandatory prior judicial authorisations. Whilst the AED Agreement does indicate that requests made under its provisions are subject to the "application of domestic law", the EDPB considers the wording is not sufficiently clear.

The EDPB makes the point that the concerns of the EDPB in relation to the AED Agreement will need to be taken into account by the European Commission in its assessment of the UK's adequacy decision application.

The judgement in *Schrems II* makes it clear that US surveillance programme is already considered intrusive by the EU. If the UK's data sharing agreement with the US does not address the EDPB's concerns as set out above, the granting of an adequacy decision to the UK may become difficult. In turn, this brings lack of clarity as to whether EEA businesses could still rely on the SCCs to transfer personal data lawfully under GDPR to the UK. At the time of writing there is also great uncertainty as to whether, in the absence of an adequacy decision on the 1 January 2021, the UK will be able to use the current new draft SCCs. It looks unlikely that the new draft SCCs will be adopted before 1 January and therefore they cannot be incorporated into UK law automatically. It is currently unclear how the UK Government will resolve this problem, and for a period of time, we may have the situation where the UK will be relying on the historic SCCs whereas mainland Europe will rely on the new SCCs.

This current uncertainty in itself could drive further data localisation within the EU.

30 EDPS, Opinion 2/2020 on the opening of negotiations for a new partnership with the UK, 24.02.2020, accessible at https://edps.europa.eu/sites/edp/files/publication/20-02-24_opinion-eu-uk-partnership_en.pdf

31 DCMS, '*Policy Paper: Explanatory framework for adequacy discussions*', 13.03.2020, accessible at https://www.gov.uk/government/publications/explanatory-framework-for-adequacy-discussions

32 EDPB, Letter to European Parliament (OUT-2020-0054), 15.06.2020, accessible at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out_2020-0054-uk-USgreement.pdf

33 Agreement between the UK and United States on Access to Electronic Data for the Purpose of Countering Serious Crime, 03.10.2019, accessible at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_US_6.2019_Agreement_between_the_United_Kingdom_and_the_US_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf

5.3 The challenges of equivalent standards restrictions

Founded on a sound basis, equivalent standard restrictions should be the method through which data can flow internationally. However the high bar put in place by countries as to what "equivalent" means has resulted in the stifling of international data flows. Countries are increasingly requiring that "equivalent" means "identical", in some cases stopping flows completely due to the practical implications of imposing different and prescriptive requirements which may conflict with other legal and regulatory obligations across the world, to flows of data.

Far from producing a consistent framework for data transfers, companies are having to show that their own jurisdictions contain near on identical data protection laws to the countries from whom data was sent, which is an impossible task. Struggling with this requirement, financial services companies with global reach, are seeking to meet compliance with the highest international standard of data protection in the search for consistency and so to be able to avail themselves of all the required equivalent standard mechanisms. But the proliferation of privacy laws and data transfer requirements is demonstrating that the challenge is less about "high standards" and more about "different" or "inconsistent" standards, which leaves companies with the challenge of multiple types of data transfer agreements and requirements. Attempts to strictly comply, and reconcile differing requirements under these evolving requirements comes at a great and strictly unnecessary cost, which is ultimately passed onto the consumer.

"As more and more countries bring in data protection laws around the world, the majority are following the concepts and terminology of the GDPR and are looking to impose restrictions on overseas transfers."

6 CONSENT RESTRICTIONS

6.1 Overview

As has been seen in previous Sections, the EU and many jurisdictions around the world who have adopted a GDPR-style framework for their data protection regimes, do allow for transfers of personal data outside the jurisdiction on the basis of consent of the data subject.

We have included this Section for completeness to note that the types of transfers being made by most financial services organisations are rarely those that can be legitimised by consent.

6.2 Example Jurisdictions

EU and the GDPR

Taking the GDPR-style framework, several jurisdictions have sought to rely on consent as a mechanism to validate the international transfer of data.

Whilst the GDPR does provide consent as a possible mechanism, the definition of consent in the EU under the GDPR, in particular that it must be freely given and can be withdrawn, means that it is unlikely to be a viable mechanism to rely on for the purposes of validating international transfers. This is because, the GDPR standard consent has a high bar to overcome at the outset, and if a customer cannot access a service without providing consent, it is unlikely to satisfy the requirement that it is freely given. In addition, even where a business is able to overcome this first hurdle, a data subject may withdraw their consent at any time, which will not only cause operational difficulties for businesses including the inability to perform know your customer checks and monitoring to comply with financial crime legislation, but may also raise concerns from a customer protection perspective if this leaves them without access to a vital financial product.

The operational difficulty of relying on consent is brought into focus with the example of a financial services business undertaking bulk transfers of data to servers hosting data outside the originating jurisdiction, which may be for the purposes of increased security or efficiency of processing. It would simply not be practicable to undertake such transfers on the basis of consent as it would not be possible to treat individual transfers related to single data subjects differently if a data subject happened to withdraw their consent.

The definition of consent under the GDPR

Consent is defined in **Article 4(11)** GDPR as: *"any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".*

Article 7 GDPR also sets out further 'conditions' for consent, with specific provisions on freely given consent if a contract is conditional on consent.

The GDPR is clear that consent should not be bundled up as a condition of service unless it is necessary for that service.

Article 7(4) states: *"When assessing whether consent is freely given, utmost account shall be taken of whether… the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."*

Recital 43 of the GDPR states: *"Consent is presumed not to be freely given… if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance."*

SOUTH KOREA

In early 2020, the Korean National Assembly passed amendments to three major data privacy laws: the Personal Information Protection Act (**PIPA**), the Act on the Promotion of Information and Communications Network Utilization and Information Protection and the Act on the Use and Protection of Credit Information. The amendments entered into effect on 5 August 2020[34].

PIPA contains a number of separate definitions for specific types of data processing, including ones related to data transfers – the concepts of "outsourcing" and "provision" of personal data. The definitions are alternative to each other: a "provision" occurs when a data transfer is conducted for the benefit and business purpose of the transferee, while "outsourcing" refers to transfers conducted for the benefit and business purpose of the transferor. The difference is substantial – PIPA mandates that the prior consent of data subjects is required when carrying out provisions, whereas transfers involving outsourcing, do not require prior consent.

34 Personal Information Protection Act, No 11990 , 06.08.2013, as amended by Act No 16930, 04.02.2020, accessible at https://www.privacy.go.kr/cmm/fms/FileDown.do?atchFileId=FILE_000000000830758&fileSn=4&nttId=8186&toolVer=&toolCntKey_1

Notwithstanding the above, in cases where the data transfer is to a party located abroad, PIPA mandates that controllers obtain the prior consent of data subjects[35]. Accordingly, for any service providers in the financial services industry and recipients of personal data provided by such companies, the prior consent of South Korean data subjects is required for all cross-border transfers, irrespective of whether such transfer constitutes a provision or outsourcing.

It is specified that consent for the international transfer needs to be separate from any consent for the service. If South Korea were to apply a GDPR standard of consent, such consent would need to be freely given and capable of being withdrawn at any time, which would make its practical application for financial services companies unworkable.

Case study: data localisation as a consequence of requiring consent

In November 2019, after a year-long consultation process, Kenya adopted its central piece of privacy legislation – The Data Protection Act 2019 (**Act**).

Section 48 of the Act provides that for a Kenyan-based entity to transfer personal data overseas, it needs to firstly satisfy the Data Commissioner – the country's DPA, that it has taken all appropriate safeguards in relation to the processing activity and that the transferee is located in a jurisdiction "*with commensurate data protection laws*". The drafting, in its current form, has been subject to extensive criticism due to the lack of clarity and further particulars on the mechanisms which may be available to controllers and processors who wish to satisfy this requirement[36].

Furthermore, under Section 49 of the Act, the processing of sensitive personal data out of Kenya is only permitted with the consent of the data subject. The provision makes it clear that even where consent has been obtained, the Data Commissioner may suspend or reject such transfers or impose any further conditions "*as may be determined*". The legislators have justified these requirements with the need to protect the rights and freedoms of individuals.

36 Privacy International, '*Analysis of Kenya's Data Protection Act, 2019*', 01.2019, accessible at https://privacyinternational.org/sites/default/files/2020-02/Analysis%20of%20Kenya%20Data%20Protection%20Act%2C%202019_Jan2020.pdf

"The GDPR is clear that consent should not be bundled up as a condition of service unless it is necessary for that service."

35 See above, Article 17(5)(3) and Article 39(12)(2)

6.3 The challenges of consent

For entities in the financial services sector it is often challenging to obtain the consent of data subjects in relation to transfers of their data. In many jurisdictions, consent needs to be freely given and cannot be made a condition of the service, where the service could still be provided without the transfer.

Case study: Consent in the fight against financial crime

The challenges of consent were recognised by the UK government in its drafting of the Data Protection Act 2018 after the financial services sector raised their practical concerns. Given the restrictions and the need for explicit consent in order to process of sensitive personal data as part of AML and transaction monitoring, it was clear that consent was not always a practical or feasible possibility. For example, if obtainable, consent may be withheld by the very persons for whom it is most key that processing be conducted. In addition, most firms are subject to financial crime due diligence, screening and monitoring obligations from multiple jurisdictions. Recognising that the processing of this data for these purposes was in the public interest, Section 12 was created in Schedule 1 of the UK DPA 2018 to provide clarity around the processing of certain special category data as necessary for compliance with applicable laws and regulations when it is in the substantial public interest.[37]

37 Data Protection Act 2018, Schedule 1, Paragraph 20

Very often the need for such transfers is linked to the firms' obligations to comply with sanctions screening, anti-money laundering and financial crime legislation, covering onboarding and transaction monitoring obligations. Additional rules may explicitly prohibit informing the individual of processing in the context of any investigations. Moreover, cybercrime and financial fraud, two often interlinked offences, are borderless in nature, and tackling them requires joint co-operation by organisations and law enforcement agencies. Enabling such 'opt-out' processes can create jurisdictional black holes for criminals to exploit. Instead we would recommend a focus on transparency and building customer trust in combination with a principles based approach as discussed in section 12.

7 NO TRANSFER RULES

7.1 Overview

There are a growing number of jurisdictions across the world which are designating certain data as so sensitive or "critical" that there is an absolute prohibition on sending the data out of the country at all. Some jurisdictions such as South Korea and Kenya are purporting to empower the individual to decide if data can be transferred out. In others, even in the absence of specific legislation, the attitude of regulators is driving financial companies operating in the financial sector to have no choice but the keep their data onshore.

7.2 Example jurisdictions

INDIA

India's first comprehensive data protection legislation is currently making its way through the legislative process. The Personal Data Protection Bill[38] (**PDPB**) follows many of the provisions in the EU GDPR, but also includes potentially far-reaching data localisation requirements.

The original 2018 draft required "data fiduciaries" (loosely the equivalent of controllers under the GDPR) to maintain a copy of all personal data in India, except where the government exercised its authority to designate "certain categories of personal data" as exempt from the local storage requirement.

Notwithstanding the requirement to maintain a copy in India, under the 2018 draft, personal data can be transferred outside of India only where data fiduciaries had put in place additional mechanisms, such as model clauses and intra-group data transfer arrangements approved by the Indian data protection authority, or where the relevant individual (termed the "data principal" in the PDPB) provided consent or the government found the receiving country to provide "adequate" protection. These very much mirror the "equivalent standards" concept within the GDPR.

Where the PDPB went much further in terms of data localisation is that it stated that critical personal data, which was to be defined by the government, generally could not be transferred outside of India at all.

38 Bill No. 373 2019, The Personal Data Protection Bill 2019, accessible at https://www.prsindia.org/sites/default/files/bill_files/Personal%20Data%20Protection%20Bill%2C%202019.pdf

Category	Description	Transfer Restrictions
Personal data	Data which is neither sensitive nor critical	No transfer restrictions
Sensitive personal data	Sensitive personal data includes many of the "special categories of personal data" as defined under the GDPR — including data relating to health, religion, sex life, political beliefs, and biometric and genetic data — but unlike the GDPR, financial data is considered to be sensitive.	May be transferred outside of India but a local copy must also be maintained. Any transfers must be subject to certain mechanisms, comparable to those in the GDPR (i.e. guaranteeing equivalent standards") facilitate transfers. However we understand that in most cases data fiduciaries must obtain "explicit consent" in addition to making use of the mechanisms.
Critical personal data	The PDPB permits the government to define certain personal data as "critical personal data," without providing any limitation on the government's power to make such designation	A general prohibition on such data being sent out of the country. However, the PDPB would create an exception to this strict localisation requirement for transfers to countries or organizations deemed to **i.** provide an adequate level of protection; and **ii.** where the state's security or strategic interests will not be prejudiced; or **iii.** in limited circumstances to protect vital interests

The latest draft of the legislation is a slight improvement on this position and introduces three tiers of "data" and the protection varies according to each.

The concern for global financial services companies operating within India is the power given to the government to designate any information as "critical" and therefore prohibit its transfer at all. The concerns around "sensitive personal data" and local copies are picked up in the next Section.

In a Statement on the 2018 draft[39], the European Commission's International Data Flows and Protection Unit labelled the data localisation requirements under the proposed bill "unnecessary and potentially harmful". The Statement adds that as a matter of economic policy, the proposed data localisation approach will create significant costs for companies – in particular, foreign ones – linked to setting up additional processing/storage facilities, duplicating such infrastructure and is thus likely to have negative effects on trade and investment. The Commission concluded that if implemented, these measures might deter foreign investment as foreign clients and companies might prefer to switch the processing of their data to a country that does not impose these types of costly constraints. The US CLOUD ACT is given as an example of ensuring law enforcement authorities' access to data stored abroad without imposing data localisation requirements.

39 European Commission, Consultation on the Personal Data Protection Bill 2018, 29.09.2018, accessible https://eeas.europa.eu/delegations/india/53963/#_ftn2

CHINA

China's current main privacy law – the Cybersecurity Law (**CSL**) was originally enacted in June 2017. The law and subsequent guidance provide specific data localisation obligations on all controllers handing critical data.

Under Article 37 CSL, critical information infrastructure operators (**CIIOs**) must store personal information and "Important data" (a broad concept defined as data which is "*closely related to national security, economic development or public interest*") generated from critical information infrastructures, within the borders of China. While at the time of drafting of this report there has been no formal guidance of which entities are considered to be CIIOs, it is believed that these are companies involved in the finance, energy, transportation, and telecommunications industries.

Additionally to the "No Transfer" rule in the CSL, in April 2020 China's Cyberspace Administration (**CA**) issued Measures for Cybersecurity Review (the "**Measures**"), which took effect on 1 June 2020. The Measures contain supplementary provisions to the CSL in relation to the procurement of "Network products and services" (**NPS**) by CIIOs. They mandate that where the purchase of NPS by a CIIO influences or may influence state security, the entity shall notify the Cybersecurity Review Office, part of CA, which will in turn carry out a comprehensive cybersecurity review before allowing or denying the procurement.

The definition of NPS includes all core network equipment, high-capability computers and servers, high-capacity data storage, large databases and applications, network security equipment, cloud computing services.

On 21 October 2020, the Chinese Government released a draft Personal Data Protection Law (**PDPL**), a comprehensive piece of legislation which, once in force, will overhaul the country's data protection regime. The draft PDPL retains the localisation rules provided in the CSL, but contains a number of proposed mechanisms for cross-border data transfers. These include a newly-established certification regime by CA and the possibility for cross-border data transfer agreements, enabling the transferor to effectively supervise the transferee's compliance with data protection obligations of PDPL[40]. However, the data subject's consent remains a pre-requisite for all international data transfers, regardless of the transfer mechanism chosen[41]. These provisions further compound the data localisation impact of the PDPL in conjunction with the other provisions mentioned.

Under Article 6 of the Notice No. 17 of 2011 by the People's Bank of China Regarding the Effective Protection of Personal Financial Information by Banking Institutions, Personal Financial Information (**PFI**) collected in China must be stored, processed, or analysed in China. Banking financial institutions are prohibited from transferring

40 Article 38 of Draft Law on Personal Information Protection, version of 21.10.2020

41 As above, Article 39

domestic PFI outside of China. Notice No. 17 defines PFI as "*personal information acquired, saved and retained by banking institutions in the course of operating the payments, settlement, financial management, […] or any other intermediary business*" as well as "*personal information generated in the course when clients have business relationships with insurance companies, securities companies, fund companies, futures companies and other third-party institutions through banking institutions*"[42]. The definition encompasses virtually all personal data processed in the provision of financial services.

Unsurprisingly data localisation is the main practical effect of the above provisions. In response publishing of the CSL, in 2018 Apple re-located all data relating to its Chinese customers to China through a partnership with a local data centre operator. Some of the largest global cloud services providers, including Microsoft Azure and Amazon Web Services have also partnered with local service operators to comply with data localisation laws and be able to operate on the Chinese market.

INDONESIA

At present, Indonesia does not have a codified set of privacy rules, but rather a number of separate regulations and laws dealing with specific privacy-related rules. In 2012 the Indonesian Government passed Government Regulation No. 82 of 2012 (**GR82**) – a controversial law which imposed strict data localisation requirements on Electronic System Operators (data controllers of electronic information). Under GR82, all entities providing "Public Services" (a very wide definition including any activities for the purpose of fulfilling goods and services under a state code, subsidy or license) were required (with a 5-year implementation period) to have all their data centres and disaster recovery platforms located in Indonesia.

After many international organisations providing services falling within the Public Services definition struggled to implement the changes, at the end of 2019, the Government repealed GR82 with an amended Government Regulation No. 71 of 2019 (**GR71**). The new law scrapped the concept of "public services" and released any non-governmental entities from the data localisation requirements in GR 82.

In January 2020 Indonesia's president submitted a draft Personal Data Protection Bill to the country's House of Representatives. The Bill provides mechanisms for cross-border data transfers, similar to those under the GDPR. Transfers will be allowed:

- Where the standard of data protection in the recipient country is equal or higher than the one in Indonesia;
- Via the utilisation of SCCs; or
- With the data subject's explicit consent.

42 Section 1(5) of Notice by the People's Bank of China Regarding the Effective Protection of Personal Financial Information by Banking Institutions

In September 2020, the country's Communication and Information Minister expressed hope that the scrutiny of the draft Bill will be completed in November 2020.

Notwithstanding the above, under the Financial Services Authority Regulation No. 38 of 2016 on the Implementation of Risk Management in Information Technology Utilisation by Commercial Banks, if a regulated bank wishes to process customer data to an entity located abroad or establish a data centre or disaster recovery centre outside the territory of Indonesia, it must obtain prior approval by the country's Financial Services Authority. As such, recent developments in Indonesia do not remove the concerns for financial services firms which may result in more data localisation.

7.3 The challenges of no transfer rules

Whether the requirement to keep data onshore is driven by express legislation or by regulator behaviour, rules prohibiting the transfer of data out of a jurisdiction practically inhibit the ability for financial services companies to, amongst other things:

- effectively manage their risk because a patchwork approach to data security and data management has to be maintained, often with only lower levels of protection being achievable at a local level;
- achieve a single customer view, which in some cases presents difficulties when complying with regulatory obligations, as well as potentially causing the customer detriment or at the very least providing a less joined-up service;
- address cyber and financial crime rules, because they are unable to immediately access certain data;
- provide local customers with access to global products and platforms; and
- undertake comprehensive risk management on global clients (for example to monitor credit risk), which depends on a joined up view.

In essence, no transfer rules create a gap between what is required or expected by customers or international regulators and what is practically possible when acting in compliance with local law or regulator custom.

8 LOCAL COPY RULES

8.1 Overview

There are a number of jurisdictions who have fallen short of an absolute prohibition on data leaving the country but have nonetheless imposed restrictions on companies from implementing global solutions to data processing by insisting that a copy of the data is held within the country. This is commonly referred to as data mirroring.

Whilst in practice local copy rules may have the impact of data localisation due to the potential increased costs and administrative burden of maintaining multiple copies of data, they can also be seen as a compromise, essentially providing a workaround to more typical data localisation measures and therefore allowing continued international flow of data.

8.2 Example jurisdictions

 INDIA

As set out in Section 7, India is looking to impose data mirroring requirements to "sensitive personal data". Sensitive personal data includes the categories of data labelled as "special category data" under the GDPR, and in addition, financial information. This, therefore, has far-reaching consequences for financial services companies who will need to ensure that financial data from Indian citizens is held within India, which will likely lead to significant data duplication.

 RUSSIA

Russia brought in requirements of data localisation on September 1, 2015. The key obligation in Russian Federal Law No. 242-FZ states:

"*When collecting personal data, including by means of the information and telecommunication network "Internet" the operator must provide the recording, systematization, accumulation, storage, adjustment (update, alteration), retrieval of personal data of citizens of the Russian Federation with the use of databases located in the territory of the Russian Federation, except for the cases specified in paragraphs 2, 3, 4, 8 of Article 6(1) of [Federal Law No. 152-FZ "On Personal Data"]*"

Interpretations by the Russian data authorities (Minkomsvyaz and Roskomnadzor) indicate that the initial database of Russian personal data must be in Russia however they accept the possibility of having local copies abroad.

The rules apply to all data operators who handle Russian personal data, including foreign data operators without any presence in Russia. The wording of the law is not precise, but the criteria used for asserting jurisdiction over foreign data operators usually focuses on how the data operators' websites are presented; specifically if the website is particularly focused on Russia or Russians.

The Russian government has thus far not engaged in widespread enforcement of the rules however there was one notable enforcement action in 2016, when LinkedIn was blocked in Russia for failure to comply with the data localisation rules. At that point, the Russian authorities did not have the power to fine LinkedIn and exercised their powers by blocking access to the website in Russia. On 2 December 2019, a new law was introduced in Russia to enable substantial administrative fines to be imposed on organizations and individuals that fail to comply with the data localisation requirements. Under this new law, fines for first-time offences for legal entities can be between $16,000 – $96,000, increasing to $288,000 for repeat offences. Fines for responsible managers can be between $1,600 – $3,200, increasing to $12,800 for repeat offences.

Case study: Russian branch of insurer with SAAS and cloud service providers

Many large international financial services companies seek to procure their IT services on a global scale to achieve data processing, security and cost efficiencies. Unlike on-premises software and support where it is clear that local laws must be complied with, SaaS and cloud services providers, making available and allowing their tools to be used globally, do not see it as their obligation to ensure those tools are compliant with the laws in the jurisdictions in which the company planned to use the tool from.

One global insurer procured a Software-as-a-service (SaaS) solution to be used in its key jurisdictions, which were explicitly stated to include Russia. It was only at the point of negotiating the data protection clauses in the contract that it transpired that there was no local infrastructure in Russia to support the use of the tool in compliance with Russian data localisation laws. The SaaS provider said it was the company's obligation to ensure its use of the tool was compliant with the laws of any jurisdiction it was to be used and could offer no local solution.

The service also included technical support from the SaaS provider which could occur from any part of the world. This would entail the transfer of data from the local user to the support staff. Again the SaaS provider claimed it was the responsibility of the insurer to verify where the support will be provided from and ensure such transfer is compliant with the jurisdiction in which the local user is based (which may have localisation laws), before accessing the support.

Negotiations are still ongoing with the provider following escalation of their lack of commitment to comply with local laws and agreeing geographical scope.

Although there is some sympathy for such a position taken by SaaS providers, as often they are blind to the data being put into the solution, in reality, both the vendor and the purchaser of the solution need to be alive to every potential data localisation rule in the world. Those financial services companies purchasing the solutions need to be provided with exact locations of where the data is being stored and processed by the vendor. The vendor needs to be prepared to offer additional local solutions for certain jurisdictions. This obviously increases the cost to the financial services company which is in turn passed onto the ultimate consumer.

8.3 The challenges of local copy rules

Local copy rules such as the ones discussed above, impose significant administration, compliance, infrastructure, service, staff and compliance costs on firms. While not as severe as the data transfer restrictions and limitations on outsourcing as those imposed by jurisdictions which prohibit the transfers altogether, the total cost of compliance may result in firms determining to exit such jurisdictions altogether. The resultant duplication of data also potentially reduces the protection offered to the data, as this creates multiple links in the chain which could be the subject to cyber-attacks and other security breaches.

However, given that the alternative to local copy rules may be full localisation of data, some organisations see local copy rules as a means of facilitating the international flow of data. In practice, for those organisations that can take advantage of these local copy rules, this compromise is welcome.

If the rationale behind local copy restrictions or "data mirroring" is that supervisory authorities and data subjects wish to retain effective access to the data, the same result could be achieved by requirements that mandate effective access rather than mandating onshore copies.

"Local copy rules may have the impact of data localisation due to the potential increased costs and administrative burden of maintaining multiple copies of data, they can also be seen as a compromise."

9 OUTSOURCING RESTRICTIONS

9.1 Overview

There are many examples of jurisdictions imposing restrictions on outsourcing particularly in the financial services industry, which can in turn lead to the implementation of data localisation in practice. Such outsourcing restrictions are often drawn up in local regulations and are seemingly fuelled by the regulators' suspicion that once data leaves their jurisdiction, they will lose the ability to access the data and the possibility to maintain adequate oversight.

Outsourcing restrictions ultimately seek to protect regulatory access to data but can, at times, result in localisation in practice as can be seen from the example jurisdictions below.

9.2 Example jurisdictions

TURKEY

Turkey's new Electronic Banking Services (**EBS**) Regulation[43], which entered into force on 1 July 2020, contains binding provisions related to processing of banking customers; personal data. The new law continues the previous legislative line of introducing onerous requirements for financial institutions wishing to utilise outsourced service providers.

Article 25 of the EBS Regulation, mandates that banks must keep all primary information systems (including all infrastructure, hardware, software and data that enable the execution of banking activities) and all available backups geographically situated inside the country. The same requirement is extended to apply to all providers of information services utilising cloud computing, as well as any other outsourced services.

Moreover, Article 29 of the EBS Regulation contains specific requirements regarding the selection criteria when choosing outsourced developers of products and services related to security and critical information systems. Under the new regime, all products involved should either be produced in Turkey or the developer and/or service provider must have an R&D centre within the country.

43 Regulation on Information Systems of Banks and Electronic Banking Services, 15.03.2020

In a striking example of the practical effect of Turkey's data and infrastructure localisation requirements, in June 2016 the online payment platform PayPal was forced to close its Turkish operations after being refused a new banking license by the country's banking supervisory authority, the BDDK, because of the inability to comply with the rules on data localisation.

PayPal's comment at the time of the announcement provides an ideal summary of the issue with infrastructure localisation: "*We respect Turkey's desire to have information technology infrastructure deployed within its borders, however, PayPal utilises a global payments platform that operates across more than 200 markets, rather than maintaining local payments platforms with dedicated technology infrastructure in any single country*". Also commenting the announcement, Business Insider observed that "*The absence of major alternative payment products like PayPal that don't meet regulatory criteria could encourage citizens in the country to seek out more traditional ways of making payments*"[44], potentially hampering consumers' access to innovative financial services solutions.

SWITZERLAND

The Swiss Federal Criminal Code sets out certain provisions relating to business secrecy and professional secrecy which are also considered to apply to customer personal and non-personal data. It is therefore recommended that written outsourcing contracts bind the supplier to comply with such business secrecy and confidentiality provisions. Any disclosure of data protected under these provisions to a supplier is allowed only with the express prior consent of all parties involved. An identical requirement applies to information protected by contractual confidentiality obligations.

Well-known for its banking traditions, Switzerland benefits from strict regulations regarding banking secrecy. Article 47 of the Swiss Banking Act explicitly protects data belonging to banking customers from disclosure to third parties. If in an outsourcing transaction the customer is subject to banking secrecy, the written outsourcing contract with the supplier must set out any data security requirements and the supplier's obligation to comply with business, banking and professional secrecy rules. Any disclosure of non-encrypted data to a supplier is only allowed with the express prior consent of the banking customer.

Switzerland's legislation contains severe sanctions for non-compliance with the above provisions. A wilful breach of banking secrecy or professional secrecy can lead to not only significant civil liability but also to criminal sanctions involving imprisonment of up to three years or a monetary penalty of up to CHF 1mln. (approx. £846,000). Negligent breaches of banking secrecy may also be sanctioned by a fine up to CHF 250,000 (approx. £212,000).

44 Business Insider Intelligence, '*PayPal is shutting down in Turkey*', 01.06.2016, accessible at https://www.businessinsider.com/paypal-is-shutting-down-in-turkey-2016-6?r=US&IR=T

LUXEMBOURG

The rules governing outsourcing in the financial services sector in Luxembourg stem from the Financial Sector Act of 5 April 1993. The Act defines "professionals of the financial sector" (**PFS**) and contains certain obligations to such persons, including specific rules regarding the provision of 'IT Support Services' and 'IT System Operation and Management Services'.

IT Support Services in the financial sector could be performed by PFS or other individuals (under the strict control and quality assurance by a PFS), in a manner which guarantees the strict protection of confidential information relating to clients. IT System Operation and Management Services must be carried out by IT system and communication networks operators of the financial sector (**support PFS**). Support PFS are entities to which a specific licence has been granted, and are subsequently supervised by the Commission for Surveillance of the Financial Sector (**CSSF**).

Any financial sector outsourcing projects where functions are outsourced to a parent company or a subsidiary must be notified to the CSSF by PFS. However, in outsourcing schemes involving the transfer of data to a service provider external to the corporate group, PFS are obliged to obtain CSSF's prior authorisation before proceeding with the transfer. In practice, this requirement to obtain authorisation has the capacity to seriously hinder business-critical projects requiring urgency, such as data recovery after a cyber incident.

In addition, similarly to the position in Switzerland, PFS and other entities wishing to form an outsourcing relationship will be bound by Luxembourg's strict professional secrecy obligations in Article 458 of the Criminal Code and the financial data secrecy rules under Article 41 of the Financial Sector Act.

9.3 The challenges of outsourcing restrictions

One of the main risks and challenges associated with outsourcing in the financial services industry that relates to the concerns giving rise to data localisation is that of supervisory access. It is contended that outsourcing poses challenges to regulators and their ability to effectively regulate and supervise financial services companies. Amongst other things, one of the reasons for this relates to the perceived lack of control over the processes of, and data held by, the non-regulated outsourcing service provider. Such concerns have drawn the concept of data localisation into ongoing discussions surrounding regulating outsourcing.

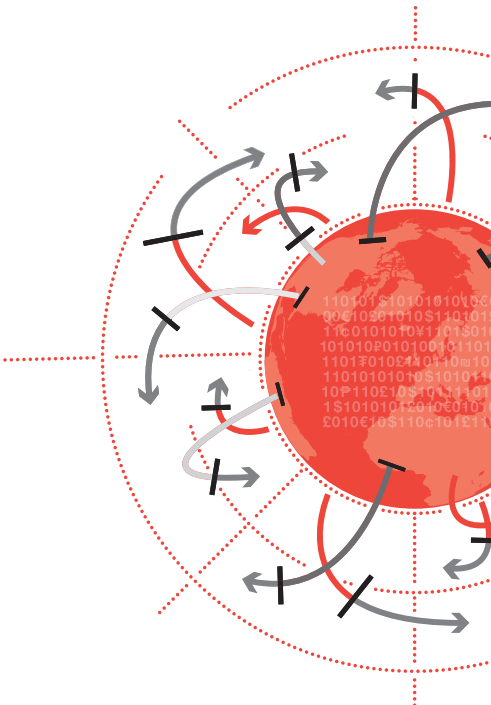
A recent consultation report, the 'Principles on Outsourcing' issued by the International Organisation of Securities Commissions[45] noted that regulators often require the financial services company to retain full regulatory responsibility for the outsourced services and that some regulators may even seek to prohibit outsourcing or impose restrictions

45 International Organisation on Securities Commissions, '*Consultation Report: Principles on Outsourcing*', 05.2020, accessible at https://www.iosco.org/library/pubdocs/pdf/IOSCOPD654.pdf

where they determine that outsourcing introduces "*an unacceptable risk or is critical to the functioning of a regulated entity or the integrity of the market.*" As has been seen in the example jurisdictions, some regulators have determined that the physical location of a financial service company's data can form such an unacceptable risk, as to warrant outsourcing restrictions that practically implement or mandate data localisation as a result.

The consultation report also noted that outsourcing and the storing of data in a cloud may increase risks which make the monitoring of, and reliance on outsourced tasks difficult. Amongst the reasons for this, is "*the uncertainty of the physical location of data*". However, the report also notes that the use of cloud service providers can also mitigate more prevalent data risks enhancing the level of data security as they are often more aware of and are up to date with cyber-security issues and have "*more sophisticated systems to detect cyber-incidents than local data centre providers or individual regulated entities*".

Many outsourcing guidelines, rules and regulations address these concerns by requiring the regulated entity to ensure that the regulators have certain levels of access to the data processed and stored by the outsourcing service provider including access to the outsourcing service providers premises and any other information on the outsourced service. However, the 'Principles on Outsourcing' go further to suggest that the financial services company "*may be required by its regulator to ensure that data is maintained in the regulator's jurisdiction*" or "*that the service provider will provide originals or copies to the regulator's jurisdiction upon request*" and even advocate for the implementation of such measures to ensure jurisdictional access to outsourced data. If jurisdictions are to take the first option they would effectively be mandating data localisation within outsourcing, which for all the reasons provided throughout the rest of this report would be severely disruptive to the financial services industry.



"It is contended that outsourcing poses challenges to regulators and their ability to effectively regulate and supervise financial services companies."

10 NON-PERSONAL DATA RESTRICTIONS

10.1 Overview

There are also an increasing number of jurisdictions which are looking to restrict the transfer of non-personal data outside the originating jurisdiction. Such restrictions can be contained within laws not specific to the regulation of data per se, for example the laws may be seeking to protect national security, sovereignty and integrity.

10.2 Example Jurisdictions

 **India** – non personal data

On July 13, 2020, an Expert Committee within India's Ministry of Electronics and Information Technology published a draft Non-Personal Data Governance Framework for India (**NPDF**)[46], which was open for public consultation until September 2020. In providing the rationale behind the need for non-personal data regulation, the NPDF document lists 4 perceived fundamental benefits of the regulation of such data. These include:

- implementing a modern framework to unlock the economic, social and public value from using data;
- creating certainty and incentives for innovation and to encourage start-ups in India;
- develop a data sharing framework to enable the availability of data for social, public and economic good;
- addressing privacy concerns, arising from re-identification of anonymized personal data.

The NPDF document defines non-personal data (**NPD**) as all data not within the scope of the proposed Draft Data Protection Bill (**PDPB**) (see Section 7.2 above) and other data without any 'personally identifiable information'[47].

Continues…

46 Ministry of Electronics and Information Technology, Report by the Committee of Experts on Non-Personal Data Governance Framework, accessible at https://static.mygov.in/rest/s3fs-public/mygov_159453381955063671.pdf

47 See above. Section 4.1

The NPDF recommends that NDP is classified into 3 main categories[48]:

- **Public NPD**: data collected or generated by government or by any agency of the government in the course of execution of all publicly funded works (e.g. anonymised vehicle and land registration data);

- **Community NPD**: data about inanimate and animate things or phenomena whose source or subject pertains to a community of natural persons. (e.g. anonymised data processed by municipal corporations and public utility companies);

- **Private NPD**: data collected or produced by non-government entities, the source or subject of which relates to assets and processes that are privately-owned by such person or entity, and includes those aspects of derived and observed data that result from private effort (e.g. data which is inferred or derived through the application of algorithms (including AI) and proprietary knowledge).

The NPDF recommends the further categorisation of Private NPD as either General, Sensitive or Critical based on the personal data definitions in the PDPB. The document provides that Sensitive and Critical NPD should be subject to the localisation rules applicable under the Bill. In particular, Sensitive NPD may be transferred outside India, but shall continue to be stored within India (a "Local Copy" rule), while Critical NPD can only be stored and processed in India (a "No Transfer" rule).

The NPDF has been subject to heavy criticism by industry bodies such as the BSA, a global software alliance comprising of the biggest service providers to the financial services sector like Amazon Web Services, CISCO, Microsoft and IBM[49]. BSA's submission on the proposed framework calls on the Expert Committee to remove restrictions on cross-border data flows and eliminate local storage and processing requirements.

Providing background on the importance of maintaining the undisrupted flow of data, whether NPD or personal data, the submission states that: "*The seamless transfer of data across international borders is critical to cloud computing, data analytics, and other modern and emerging technologies and services that underpin global economic growth. Cross-border data flows are particularly important in the context of cybersecurity and data privacy, enabling distributed and compartmentalized data storage, as well as allowing correlation of threat data for more effective cybersecurity defence. Cross-border data flows are also essential to improve data analytics, which can deliver socially and economically beneficial results in situations ranging from digital commerce to responses to natural disasters.*"

48 See above, Sections 4.2 – 4.4

49 BSA Submission on the Report by the Committee of Experts on Non Personal Data Governance Framework, accessible at https://www.bsa.org/files/policy-filings/09102020indiabsanpd.pdf

Against that background, in criticism of the NPDF, BSA state that the prospective law "*would disrupt companies' operations, make it costlier to provide services in India, decrease opportunities for collaboration through data sharing, and increase barriers for competition that are key to ensuring Indian users have cost-effective access to the best products and services. […] The Committee's proposal to import cross-border data flows restrictions and data localization requirements on NPD derived from personal data by anonymization based on the same proposed restrictions and requirements in the PDP Bill unnecessarily complicates the regulation of personal information, would raise costs to businesses in India and deter investment in data-related enterprises and is inconsistent with global norms and practice.*"

 **India** – payments data

There have also been restrictions in India on the transfer of payments data.

In 2017 the Reserve Bank of India (**RBI**) issued a notice to payment systems providers which required that payment data was stored onshore[50].

Subsequently in 2019 the RBI communicated with banks to confirm that they came within the scope of the 2017 notice, so that it did not just apply to payment system operators as had been assumed, and the banks were therefore currently in breach of the requirements of the notice.

The RBI issued formal notice of this in its FAQs on the Storage of Payment System Data51 which also set out other key aspects of the 2017 notice, including the scope of data caught by the notice and details of the limited (24 hour) window for offshore processing of data.

Following the publication of the FAQs there were a series of discussions during the course of 2019 between the RBI and onshore banking to confirm the application of the 2017 notice. The most recent position in respect of the notice's application is that:

- domestic payments data that is processed offshore is to be deleted on any offshore system within 24 hours;
- foreign legs of transactions may be processed offshore and financial crime compliance systems are not expected to be in scope. This is because the RBI subsequently clarified that the only systems that need to be exclusively on-shored are those that store the entirety of the data involved in domestic end-to-end payments transactions (e.g. systems that maintain/process every field in a domestic payments transaction); and
- banks are expected to use panel auditing firms to confirm their approach to dealing with payments data and compliance with the notice.

50 RBI notice on the Storage of Payment System Data https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244

51 FAQs on the Storage of Payment System Data https://www.rbi.org.in/Scripts/FAQView.aspx?Id=130

In addition to being an example of localisation, the moral of this story is that precise scope and compliance implications can be difficult to pin down (for example, what data is caught by the term 'end to end payments data'), which is a time consuming and resource intensive exercise, not to mention the costs of getting it wrong.

More generally, the IRSG understand the actions of the RBI to be a first volley in the broader onshoring push that is expected in the form of personal and non-personal data localisation restrictions.

Stemming the Tide: a European Perspective

In February 2020, the European Commission issued a Communication presenting its concept for "A European Strategy for Data[52]. The Communication outlines the Commission's proposed strategy, having as its key aim the creation of an attractive policy environment at EU level so that, "*by 2030, the EU's share of the data economy – data stored, processed and put to valuable use in Europe – at least corresponds to its economic weight, not by fiat but by choice.*"

The main objective of a data-driven policy environment is the creation of a single European data space – a genuine single market for data, open to data from across the world – where personal as well as non-personal data, including sensitive business data, are secure and businesses have easy access to an almost infinite amount of high-quality industrial data. The instruments at the foundation of this environment are the GDPR, FFD Regulation, the Cybersecurity Act[53] and the Open Data Directive[54].

Highlighting the critical importance of cross-border data transfers, the Commission confirmed that its vision of a common European data space implies an open, but assertive approach to international data flows, based on European values. It recognises that European companies operate in a connected environment that goes beyond the EU's borders, so that international data flows are indispensable for their competitiveness.

The Commission emphasised its intention to be a leader and to support international cooperation with regards to data, shaping global standards and creating an environment in which economic and technological development can thrive, in full compliance with EU law.

52 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0066&from=EN

53 Regulation (EU) 2019/881 on ENISA and on information and communications technology cybersecurity certification

54 Directive (EU) 2019/1024 on open data and the re-use of public sector information

Stemming the Tide: a UK Perspective

In September 2020, the UK Government Published its National Data Strategy (NDS)[55], which was open for consultation until 2 December 2020. The NDS outlines 5 ambitious mission statements by the UK in its strive towards building a work-leading data economy. One of these contains the country's commitment to be a "Champion the international flow of data" by facilitating cross-border data flows. The specific tasks in pursuit of this goal include promises to:

- Work globally to remove unnecessary barriers to international data flows;
- Agree ambitious data provisions in future trade negotiations and use the newly independent seat in the World Trade Organisation to influence trade rules for data for the better;
- Remove obstacles to international data transfers which support growth and innovation, including by developing a new UK capability that delivers new and innovative mechanisms for international data transfers;
- Work with partners in the G20 to create interoperability between national data regimes to minimise friction when transferring data between different countries.

The NDS also confirms that the UK will seek an adequacy decision by the European Commission after the end of the Transition Period.

55 DCMS, '*Policy Paper: National Data Strategy*', 09.09.2020, accessible at https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy

10.3 The challenges of non-personal data restrictions

Increasingly ad hoc regulations for various subsets of data whether personal or non-personal data are adding to the complexity of seeking to comply with the myriad of laws and rules governing the transfer of personal data, which in turn is driving localisation.

It is worth pointing out that in reality within financial services companies, data is often not separated into personal and non-personal data and all data is held to the same standards, on the same software, and on the same hardware. While there might be a legal discrimination between personal and non-personal data, the practical reality is somewhat different. Therefore, if a law applies to one particular subset of data, the measures that to apply it (such as encryption or retention requirements) in many cases need to be applied to the whole set of data whether personal or not.

11 IMPACT OF DATA LOCALISATION LAWS ON THE FINANCIAL SERVICES INDUSTRY

11.1 Background

The increasing implementation of laws and regulations that promote or have as their effect data localisation within various jurisdictions, creating obstacles to the flow of data across borders, raise particular issues for the financial services industry.

All industries which operate on an international scale will have to circumnavigate their way through varied, and at times competing, data protection legislation for each of the jurisdictions within which they operate. However, for the financial services industry, this is a particular challenge as consumers, both retail and commercial, expect global solutions. The free flow of data between entities in various jurisdictions, not least within financial services groups, is of paramount importance to the financial services industry, the continuing globalisation of finance across the world and the industries future development.

Globalisation, and in particular the need to be able to support cross-border commerce and trade by supplying cross-border services, has placed new emphasis on the financial infrastructure of the world, so much so that the operations of the largest groups in the financial services industry are inherently international. Even the smaller entities within the industry rely on the larger groups to transact or provide services internationally to its customers in foreign jurisdictions. It is evident that for the economy to function and evolve alongside globalisation, the financial services industry must remain interconnected and this itself means that data has to be able to flow internationally, across borders and continents.

Data localisation measures consequently limit firms' ability to channel global capital and liquidity flows into a market, and limits their ability to support local businesses' activity outside the local market.

From the simple concept of a UK citizen holidaying in Brazil who needs to use their money abroad or acquire it via a local ATM machine, or needs to rely on their travel insurance purchased from a UK insurer to cover medical expenses incurred in Brazil, to a global corporate wishing to provide its employees with access to a global travel product, money and data need to be transferred and used across the world in real-time in the 21st century. This societal shift has in part driven the financial services industry towards globalisation as the most efficient way to provide financial services and meet the demands and expectations of its customers, providing them with ready access to their money and various financial products across the world.

In conflict to this increasing globalisation, financial services companies are subject to increasing layers of laws, guidance and regulatory oversight, which are placed on top of existing laws governing the use and transfer of personal data and, as has been seen in this report, these increasingly stray into restrictions on data transfers. Often rules and guidance from local regulators that inhibit the free flow of data stem from a desire to ensure that the relevant local financial services regulator can maintain adequate oversight of the regulated entity. However, in our view, many go much further than necessary when mandating local copies of certain information or restricting data transfers in the various forms explored in this report and may in some cases actually prevent or hinder a joined-up risk management approach. Indeed, regulatory oversight, or access to data for regulatory supervision or law enforcement, has been claimed as a reason for the introduction of data localisation restrictions within the financial services industry[56]. National regulators fear that their ability to access data beyond their borders may be weakened by the territorial limits of their powers, and as such see the ability to require a local copy of data as a way to retain territorial access to such data. However, this can be readily addressed by placing obligations on those handling local data to ensure access can be achieved in their inter-group or third party contracts with service providers.

Consequently, data localisation laws quite often lead to financial services companies having to implement complex and unwieldy operational "workarounds" in multiple jurisdictions in order to comply with the requirements of that jurisdiction. One example of this is the need to use local software provider solutions or data stores in a country, for the processing and storage of local data or local copies. These may not meet corporate or third country standards, may not be sufficiently scalable, or may not even be available or viable options. In addition, this entails additional time and money being expended by the financial services company and its key personnel to set up and maintain these local operational workarounds. The consequences of this are set out in more detail below.

11.2 Complexity of layers of regulation – stifling local investment

The combination of traditional data protection laws and financial services regulation which also encroaches on the topic form a complex web of laws and guidance, to which only the largest of financial services companies with the most sophisticated of legal teams or size of budget for legal spend, could hope to navigate. Even then, those companies would need to consider if such an expense on compliance is worth the investment. This often leads to a viability question, as the members of IRSG have reported many instances of weighing up the cost of compliance vs local revenue. Sometimes it has still been worth investing in the jurisdiction but in other situations it has not.

56 Institute of International Finance, '*Data Flows Across Borders*', 03.2019, accessible at https://www.iif.com/Portals/0/Files/32370132_iif_data_flows_across_borders_march2019.pdf

Case studies: a balancing exercise of the cost of compliance against revenue opportunities

A member of the IRSG told of the complex assessment undertaken when its financial services group wanted to enter the Russian market. The business had to assess whether the potential business revenues over 3 years covered the cost of compliance with data localisation rules which mandated a local server. In this situation, the decision was taken to go ahead with the entry into the Russian market.

Conversely, a global insurer looking to consolidate its servers worldwide had to take the decision to close its branch in Liechtenstein as the professional secrecy laws there prohibited such an off-shore storing of the data and the provision of local data storage was considered cost-prohibitive when compared to the revenues generated by that branch. The Liechtenstein branch closed at the cost of local employment.

When assessing such viability, financial services groups have sought to predict the future by itemising and calculating the local cost compliance before weighing it against the present and potential revenue of the local operations.

Some African countries when considering recent proposals to update their data protection regimes looked at the use of data localisation requirements before receiving feedback from international businesses that this would deter them from entering their respective jurisdictions. It was contended that implementing data localisation requirements would have inhibited overseas investment, which in turn could have disrupted the economic development and modernisation of their respective markets. Such data localisation has been shown to hinder economic development particularly in developing countries where economic modernisation is often sought after.[57]

57 M. Badran and R. Tufail, '*Economic Impact of Data Localization in 5 Selected African Countries, an empirical study*', 21.06.2018, accessible at https://pic.strathmore.edu/wp-content/uploads/2019/03/PIC_RANITP_Economic_Impact_of_Data_Localization_in_5_selected_African_Countries.pdf

At times, such additional costs also flow down to product pricing which leaves the local customer to pick up these costs and be at a comparative disadvantage to the financial services companies' customers in various other jurisdictions that do not require such data localisation.

11.3 Complexity of layers of regulation – navigating risk and compliance

Whilst such regulations layered together can create huge complexities for financial services companies operating within any particular jurisdiction, they can also deter some from entering many jurisdictions, and not only for financial reasons.

The more complex a web of laws and guidance is in any given jurisdiction, the more tailored the financial services companies' operations have to be for that jurisdiction, which may cause wider problems from a risk management perspective. It makes it almost impossible to draw up and implement group-wide policies and operational when the operating conditions of each jurisdiction vary dramatically. This forces the largest financial services companies operating across jurisdictions to take a bottom-up approach to risk management and compliance, which makes it difficult for international and senior managers within these companies to effectively manage global risks and operations. With the added complexity of multiple layers of regulation it is quite often difficult for financial services companies to build a complete picture of the compliance requirements within a relevant jurisdiction. As will be seen from the case example below, despite financial services companies' efforts to comply with such a complex web of requirements, it can be difficult to do so in practice.

"Data localisation laws quite often lead to financial services companies having to implement complex and unwieldy operational *workarounds*."

Case study: Turkey

Amendments to Turkish Banking Law No. 5411 at the beginning of 2020 introduced some general requirements regarding banks' handling of confidential customer data. In accordance with these provisions, in March 2020, the country's Banking Regulation and Supervision Agency (BRSA) introduced the EBS Regulation (see Paragraph 9.2 of this report for more detail). The EBS Regulation grants BRSA authority to prohibit the transfer of customer confidential information or banking secrets with third parties established abroad, as well as to make decisions regarding the primary and backup information systems used by banks.

It is important to highlight that the conditions under Article 9 of Turkey's Personal Data Protection Law (PDPL) – approval by the DPA, explicit consent, transfer to the "safe country" list, as well as the binding corporate rules announced by the DPA could not be relied for the transfer of customer confidential information to third parties abroad without the specific instruction or request from the customer.

The exceptions to these restrictions on international data transfers are limited and only apply where the transfer is mandated by Turkish law or necessary for the work of a government ministry.

In this context, any banking entity wishing to transfer customer information abroad can only do so if both conditions have been complied with:

- It has received the customer's instruction for the transfer or a request under the Banking Law; and
- It has complied with the requirements of Article 9 of PDPL.

At the beginning of September 2020 the country's privacy authority – Turkey's Personal Data Protection Board (**DPB**) published a new decision in relation to international data transfers. In this instance, a company within the automotive industry was fined 900,000 Turkish Liras (approx. £90,000) for a transfer of personal data outside of the country without the data subject's express consent and in the absence of any other justification. It is noteworthy that the controller sought to rely on Convention 108 in attempted justification for transferring the data to a state which, like Turkey, was a signatory to the document. The DPB disagreed with the approach and ruled that being a party to Convention 108 might be taken into consideration as one of the criteria during the assessment of "safe countries" by the DPA, but the countries that are party to the Convention cannot be automatically deemed as countries which have an adequate level of protection, without any further evaluation. This example demonstrates the lack of clarity regarding the implications of Convention 108's effect on international data transfers.

The requirement to obtain the customer's consent for most data transfers in the course of providing a financial service in Turkey creates obstacles in the operation of international financial businesses in the sector.

11.4 Regulatory oversight inhibited rather than maintained

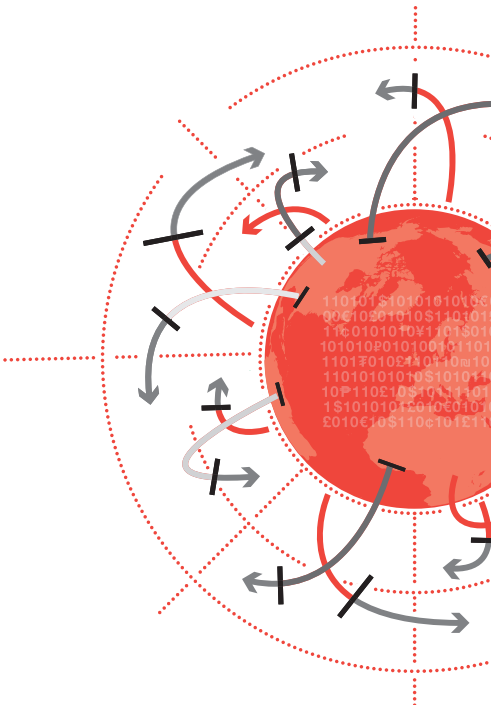
Many national regulators fear that once data has left the borders of a jurisdiction, they may not have the power to access it. The imposition of data localisation requirements within the financial services industry may in fact hamper their regulatory oversight.

For example, where an international financial transaction involves a jurisdiction mandating data localisation, each financial services company and each respective regulator will only have sight of the half of the transaction that takes place in their jurisdiction, which deprives the authorities of an overall understanding of the transaction and any other financial implications such as tax implications. Such practices would also inhibit the financial services industries' stringent anti-money laundering and fraud procedures, increasing the risk that criminals rejected in one country, succeed in another.

This in turn gives rise to the conflicting demands of financial services regulation and can often cause tension between local, foreign and international legislation, and local, foreign and international regulators. Moreover, such a movement towards data localisation works contrary to the wider policy agendas of recent decades to promote international cooperation amongst regulators when dealing with financial services companies that operate across various jurisdictions, which has supported and, at times, even promoted the globalisation of the financial sector. Notably, the founding of the Financial Stability Board to assist with the effective regulation of the now-global financial economy and the global financial services companies operating within it has worked to oversee, promote and facilitate the cooperative regulation of the financial sector by national regulators.

GOOGLE
MICROSOFT
93%
CLOUD

The US-based Microsoft and Google control approximately 93% of the global market for cloud-based Office Suite solutions.



Case study: United States v Microsoft Ireland

In December 2013, during an investigation into a drug-trafficking case, a United States magistrate judge issued a warrant under the Stored Communications Act of 1986 (SCA) requiring Microsoft to produce all emails and information associated with a Hotmail account hosted by the company. While the information was held on Microsoft's United States servers, the emails were stored on a server in Dublin, Ireland.

Microsoft complied with providing the US-stored account information but refused to turn over the emails stored in Ireland, arguing that a US judge has no authority to issue a warrant for information stored abroad.

The US Government contested the refusal, arguing that in a case where Microsoft, as a US-based company, could access data stored elsewhere from within the United States, that act of disclosure of the data will take place in the United States and that this was not an extra-territorial act and therefore permissible under US law. The subsequent litigation took over 5 years and eventually reached the Supreme Court.

Commenting on the legal issues on data localisation posed by the case, the Harvard Law Review observed that "*The idea that there is an inherent sovereign interest in the ones and zeros stored on one's soil is increasingly hard to support. Data, after all, is highly mobile; it is divisible, meaning that a single email account may be broken up so that the bodies of emails are stored in one location and the attachments in another, potentially in a place far from the account owner. The country where the data is stored may not have any connection to the account holder or to the particular crime being investigated.*"[58]

However, while a judgement was awaited, shortly after the oral hearings, Congress introduced the CLOUD Act (see page 24 of this report). Among other provisions, the CLOUD Act modified the SCA to specifically include cloud storage platforms utilised by communication providers in the United States regardless of where the cloud servers may be located. The bill was supported by both the Department of Justice and Microsoft. A new warrant was issued, identical to the 2013 one which was complied with and the Supreme Court rendered the case moot and vacated it.

As of February 2020, the US-based Microsoft and Google control approximately 93% of the global market for cloud-based Office Suite solutions[59].

58 Jennifer Daskal, '*Microsoft Ireland Argument Analysis: Data, Territoriality, and the Best Way Forward*', 28.02.2018, accessible at https://blog.harvardlawreview.org/microsoft-ireland-argument-analysis-data-territoriality-and-the-best-way-forward/

59 As per https://www.statista.com/statistics/983321/worldwide-office-365-user-numbers-by-country/

11.5 Data security and cyber threats

Often the incentive for imposing data localisation rules is to keep data secure. However, as is the case with the approach of keeping money safe by storing it under your mattress, this approach is often misguided.

Very often, local data storage services do not have the budgets, resources or facilities to compete with internationally recognised global service providers in terms of data security. As such, a requirement that data is stored locally may actually, and is likely to, result in local data being held and processed by firms with less rigorous security standards.

Furthermore, where a global solution can be used to store the data, firms are able to focus their resources and attention on ensuring the security of that data store, wherever it is based. Where there is a requirement to hold data locally, or even regionally, it dilutes the IT security spend and divides and fragments the resources that can be

applied to data security. It can also unnecessarily duplicate the data and increase the number of access points to the data, which increases the risk exposure and potential failure of data security.

All of this leaves the data stored locally more vulnerable to data security failures, breaches and cyber-attacks. As such, imposing data localisation as a means of keeping data secure often achieves the reverse in practice.

Following on from this, data localisation can result in fragilities with the financial services industries cybersecurity and threat response capabilities by limiting the ability of financial services companies to share information from one jurisdiction with other countries and regulators, which inhibits the identification and prevention of global security threats.

Ultimately, customers' and consumers' personal and financial data needs to be sufficiently protected against global security threats and this would be best achieved by a financial services company through the concentration of its resources and in leveraging a global solution for its data store with enhanced data security features, which cannot often be replicated on a local level. Fragmenting and duplicating the data, as data localisation and local copy rules require, would almost certainly lead to more fragile data stores with less sophisticated data security features and increased exposure to data security breaches.

Case study: Data localisation impacting data security

By way of example of the absurd unintended consequences of data localisation measures, one member was looking to implement data loss prevention software in Luxembourg, which clearly has as its purpose ensuring the security of data, but as the provider of the software was a global provider which meant that implementation of the software would be mean transfer and storage of data outside of Luxembourg, implementation was prevented by Luxembourg's data localisation rules, therefore leaving the local data without the benefit of the protection of the data loss prevention software.

11.6 Impact on the customer

Although it seems to be the intention of legislators and regulators to protect the data of the customer by regulating the transfer of data outside the originating country so robustly, in reality, these measures are having a negative impact on the customer.

Consumers not empowered by the offer of consent
As we have explained, some jurisdictions think they are empowering consumers by saying that data can only be transferred with the consent of the data subject. However, financial organisations simply cannot rely on consent to restrict or allow the transfer of data between countries, as this is and would be unworkable in practice. If consent becomes a condition of providing the services, it is a meaningless tool for empowering consumers in practice.

Less choice of service provider in country
Data localisation is leading to the undesirable consequences that it is only the large cash-rich organisations who can afford to compete in local territories with stringent data localisation rules. It is only those companies who have the internal resource to scope out the requirements of each locality and if necessary make the investment of local infrastructure to house the data and resource to manage the data. This leads to a lack of local competition.

Less able to access opportunities external to their regions
Stemming from the point above, customers are unable to access opportunities external to their region and they will not have access to products and services which might be more suited to their needs at a more competitive price. In reality, services provided in a country may be less innovative due to the restrictions in place as to where the data can reside.

Higher prices for financial products
The cost of compliance, whether it's having to provide local infrastructure, or simply navigating the myriad of personal and non-personal data restrictions on transfer, is ultimately passed onto the consumer. The viability question of the cost of compliance vs local revenues can be adjusted from a non-viable position to a viable position if the cost of the financial product is adjusted to absorb the cost of doing business including the additional cost of compliance in that jurisdiction. Ultimately, this leaves the local consumer in a worse-off position.

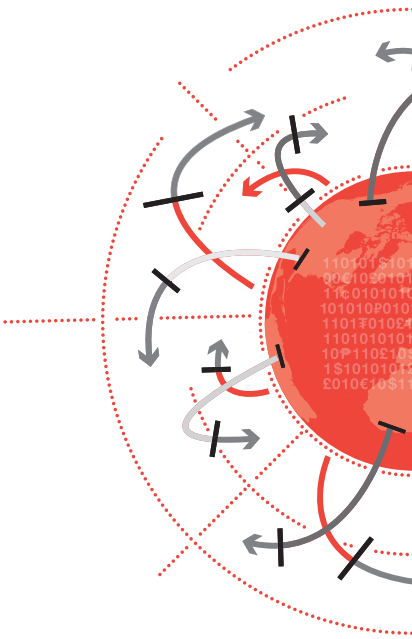
Impacting the customer journey and the potential for a single customer view
Customers and regulators often demand that global financial institutions have a complete consolidated picture of a customer's interactions with the company, often referred to as a "single customer view". In order to achieve this, businesses need to be able to access and share data more freely across jurisdictions. Data localisation laws can cut across this desired view and result in a disjointed customer journey and failure to meet regulator requirements.

11.7 Impact on the insurance distribution chain

The UK (re)insurance and long-term savings industry is the largest in Europe and the fourth largest in the world. As an inherently global industry, it is extremely important for the (re)insurance and long-term savings sector to continue to be able to transfer personal data internationally, in order to carry out a wide range of functions, including underwriting and claims handling.

The transfer of data across borders may be within a multinational group operating across a number of jurisdictions, as part of an outsourced function, as part of a reinsurance arrangement, as part of data storage arrangements, such as location of servers and cloud services, between insurance companies and intermediaries, or to an international organisation, as defined in GDPR Article 4.

Restrictions on the ability to transfer data cross border could have a significant detrimental effect on (re)insurance firms, (re)insurance intermediaries, policyholders and wider society due to the impact on the ability to offer cover, which may be caused by for example: difficulties in obtaining information so that policyholders can be checked against international sanction lists; difficulties in checking aggregations of cover on the same policyholder; difficulties in complying with know your customer checks and monitoring obligations and risk management; and limitations on the ability to use intra-group service hub offices that are outside of that particular jurisdiction to help with the management of that business (for example policy administration and claims support).



"Imposing data localisation as a means of keeping data secure often achieves the reverse in practice."

12 ADDRESSING THE CONCERNS WHICH ARE LEADING TO "DATA LOCALISATION" THROUGH OTHER MEANS

It is the view of the IRSG that the concerns which are driving data localisation, are:

- **concerns about the level of protection afforded to individuals' privacy once the data leaves the country;**
- **concerns about the data security outside the originating country – including access by foreign governments;**
- **concerns about potential lack of regulatory supervision once data has left the country; and**
- **a desire to support local businesses.**

The above problems are not being solved by data localisation. Such concerns would be better addressed by laws which: (1) from a data protection perspective, are based on mutual recognition of similar standards on a multi-lateral basis rather than prescriptive equivalence standards which require the extra-jurisdictional application of laws on third countries; and (2) from an outsourcing/regulatory oversight standpoint, are concentrated on sufficient access to the data and operational resilience, rather than a focus on where data is located.

12.1 A principles-based approach to data protection

RECOMMENDATION 1

The IRSG would like to see jurisdictions focussing on identifying agreed shared principles and standards of data protection as set out in long standing and established principles such as Part Two of the OECD Guidelines[60] as a starting point.

This is rather than mandating that entities in countries importing personal data are subject to laws which require near-identical data protection laws to the originating jurisdiction.

Exporting data controllers should be given more freedom to make their own assessment of whether sufficient safeguards are in place under a risk based approach where the nature of the data, destination of the transfer and type of processing as well as other safeguards can all be appropriately assessed.

60 See no 4 above

12.2 Regulatory oversight concerns should be addressed by rules on access rather than location

RECOMMENDATION 2

We strongly support arrangements that ensure authorities have access to the data they need. However, whilst regulators fear that their access to its regulated entities data could be stifled by outsourcing arrangements, in practice this is rarely true. A local regulated entity almost always seeks to ensure that it has control of its data in all forms, whether stored in its local jurisdiction or elsewhere.

It is the view of the IRSG that outsourcing regulations should seek only to ensure that such control of, access to, and ultimately the responsibility for the data remains that of the local regulated entity and that such is appropriately reflected in the relevant contract with the outsourcing provider. The data that is being accessed must actually be necessary to those authorities, statutorily. This may require technical focus and agreement within markets. Another avenue, as an alternative to formal regulation of access, is for access arrangements to be agreed through dialogue with regulators or even through contractual arrangements with internal and external service providers.

To date, the approach in the UK (with relevant FCA guidance) and at a pan-EU level (with the EBA's Guidelines on outsourcing arrangements) has been to require that the firm ensures that the relevant competent authority is able to effectively supervise the firm through requiring provisions to be included in the written agreement between the local regulated entity and the outsourcing provider. These provisions not only include access to the regulated entities data but also the cooperation of the outsourcing provider (indirectly and/or directly) with the regulator in relation to information requests as well as rights of access to the outsourcing providers premises for regulatory audits. Such provisions ultimately protect the regulators against the fear that their access to regulated entities data could be stifled by outsourcing without mandating data localisation.

The IRSG supports this approach and would welcome other jurisdictions adopting this position.

12.3 Operational resilience should focus on the quality of the outsourcing solution, not its location

RECOMMENDATION 3

In addition to guidelines, restrictions and regulations, and given the increased use of outsourcing in the financial services industry, some financial regulators have turned their attention to operational resilience on the whole. The Financial Conduct Authority (FCA) in the UK is one such regulator.

In December 2019, the FCA issued a consultation paper[61] which seeks to address concerns amongst regulators relating to operations as a whole including the use of outsourcing. Whilst the consultation paper itself and the proposed amendments to the FCA Handbook do not mandate data localisation, its purpose is to ensure that regulated

61 Financial Conduct Authority, '*Building operational resilience: impact tolerances for important business services and feedback to DP18/04*', accessible at https://www.fca.org.uk/publication/consultation/cp19-32.pdf

entities review their own operational resilience and address any vulnerabilities that are exposed. One of the factors to be considered when setting impact tolerances is "*any potential loss of confidentiality, integrity or availability of data*." In an example of resources that might support a financial services group's important business services, the paper explains that the group will make each firm self-sufficient in terms of data storage by creating separate primary and back-up data centres in each jurisdiction.

This guidance therefore encourages a form of data localisation by implying that local data storage is more resilient. In reality, the use of global data service providers often provides a greater degree of data protection. Ultimately, an outsourcing service provider should not be deemed to be a threat to the operational resilience simply because it is providing the service from another jurisdiction.

An assessment of operational resilience should focus on a qualitative analysis of the measures protecting the data, not just its location.

12.4 Increased co-operation at an international level

RECOMMENDATION 4

IRSG Members have noted that in the UK Government's National Data Strategy (**NDS**)[62], it outlines 5 ambitious mission statements by the UK in its drive towards building a world-leading data economy. One of these contains the country's commitment to "[c]hampioning the international flow of data" by facilitating cross-border data flows. Specifically the UK promises to:

- work globally to remove unnecessary barriers to international data flows;
- agree ambitious data provisions in future trade negotiations and use the newly independent seat in the World Trade Organisation to influence trade rules for data for the better;
- remove obstacles to international data transfers which support growth and innovation, including by developing a new UK capability that delivers new and innovative mechanisms for international data transfers; and
- work with partners in the G20 to create interoperability between national data regimes to minimise friction when transferring data between different countries.

62 Department for Digital, Culture, Media and Sport, Policy Paper on National Data Strategy, 09.09.2020, accessible at https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy

There are now more than 120 countries, two-thirds of the world, with privacy laws[63], but as this report shows, we increasingly have multiple and differing standards rather than a more level playing field. The IRSG believes that regulatory co-operation should be promoted to ensure greater consistency. All of the recommendations in this report would be better achieved by increased co-operation at an international level, for example:

- jurisdictions working together to recognise that equivalent standards for data protection does not necessarily translate as the "same" standards for data protection; and
- co-operation between regulators in different jurisdictions, perhaps through memorandums of understanding, to ensure that appropriate and proportionate regulatory access to data can be maintained, wherever in the world it is located.

Case study: the United States – Singapore Joint Statement on Financial Services Data Connectivity

In February 2020, US Treasury Under Secretary for International Affairs, Brent McIntosh and MAS Deputy Managing Director, Jacqueline Loh, met in Singapore to discuss the, importance of data connectivity in financial services. The Under Secretary's speech[64] lays out the Treasury's views on how governments, market participants, and other stakeholders should deepen their cooperation to ensure the benefits of cross-border data flows in financial services are realised. Consistent with these efforts to deepen cooperation, at the conclusion of their meeting, Under Secretary McIntosh and Deputy Managing Director Loh issued a joint statement[65] on the importance of data connectivity in financial services.

64 Address by Under Secretary McIntosh, 06.02.2020, accessible at https://home.treasury.gov/news/press-releases/sm900

65 United States – Singapore Joint Statement on Financial Services Data Connectivity, 05.02.2020, accessible at https://home.treasury.gov/news/press-releases/sm899

PRIVACY LAWS

2/3 WORLD

"There are now more than 120 countries, two-thirds of the world, with privacy laws." [63]

63 DFIN Solutions, '*The Evolving Data Privacy Landscape: GDPR, CCPA and Similar Data Protection Laws*', 31.03.20, accessible at: https://www.dfinsolutions.com/insights/article/gdpr-ccpa-and-US-data-privacy-laws

12.5 Use of specific trade agreement clauses prohibiting the restriction of cross-border transfer of data

RECOMMENDATION 5

Digital trade is increasingly important. Half of services trade is digitally enabled, and Covid-19 has only accelerated the trend towards e-commerce[66]. Despite this, restrictions on digital trade have doubled in ten years[67].

The IRSG supports the use of specific trade agreement clauses prohibiting the restriction of cross-border transfer of data. It is encouraging that the recent UK-Japan Comprehensive Economic Partnership agreement contains a shared commitment to allow the free flow of data with no requirement for localisation as a condition for doing business. Under the agreement Japan cannot restrict a UK financial service supplier from transferring data from Japan (and vice versa), and, subject to certain regulatory safeguards, UK financial services suppliers cannot be obliged to store financial data in Japan.

The UK-Japan CEPA is step in the right direction in terms of fulfilling the digital objectives of the financial and professional services sector in a free trade deal, however, it is essential to ensure this high standard is replicated in trade agreements going forward. The ASEAN/APAC countries are leading the way in this regard, with many of the recent trade deals in the region containing comprehensive provisions on data. For example, the New Zealand-Chile-Singapore Digital Economy Partnership Agreement (**DEPA**)[68] and Australia-Singapore Digital Economy Agreement (**DEA**)[69]. Similarly, the joint statement between the Monetary Authority of Singapore (**MAS**) and the U.S. Treasury specifically supports cross-border data flows by financial services firms.

Policymakers should ensure that any such provisions are modern, forward looking and consider the increased digitisation of services trade. Due to the rapidly changing nature of digital trade, flexibility is required. In addition to including the relevant clauses within the agreements, policymakers should also commit to cooperation through regulatory dialogue to address issues as arise.

66 Data Free Flow with Trust (DFFT), "*Paths towards Free and Trusted Data Flows*", p.8, World Economic Forum, June 2020, available at: http://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20_Flows_2020.pdf

67 VOX, Centre for Economic Policy Research (CEPR) Policy Portal, "*The cost of data protectionism*", 2018; World Economic Forum, "*Exploring International Data Flow Governance*", White Paper, 2019.

68 Accessible at https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-concluded-but-not-in-force/digital-economy-partnership-agreement/

69 Accessible at https://www.dfat.gov.au/trade/services-and-digital-trade/Pages/australia-and-singapore-digital-economy-agreement

13 CONCLUSION

Many of the explicit moves towards localisation, such as local copy rules, restrictions or limitation on data transfers, or measures which have an outcome of increased localisation, such as requiring equivalent standards, are put in place with the aim of increasing the level of protection provided to personal (and non-personal) data.

As this report demonstrates, often such measures have unintended consequences, for example, creating friction in the free movement of data, with moves to keep data within a jurisdiction or a region, impeding local business by making the jurisdiction unattractive for inward investment, increasing the administrative burden on companies seeking to operate in that jurisdiction as they often have to take a patchwork approach to compliance, or indeed actually having a detrimental effect on the security of the data. These unintended consequences ultimately have a negative effect on the individuals whose rights the relevant legislation and regulation were designed to protect. Ultimately it creates a confusing picture for individuals trying to understand how their personal data is used in what is a global economy, and a global reality of the digital world.

The report also shows that while we may make legal distinctions between personal and non-personal data, the reality is that the impact of measures often designed to protect data, or to encourage the development of local opportunities in relation to data, is that it in many cases adversely impacts all data, whether personal or non-personal. This is due to the reality that data is processed by applications which contain both personal and non-personal data, and in the digital world, the two are inter-mingled and are often mutually co-dependent. For example, the ability to access a system processing index data requires a unique identifier which is usually attributed to a specific login or user. It is difficult to contemplate a system or process which is wholly exclusive of any sort of personal data element. So when we legislate to protect data, we need to consider the impact based on the reality of how data is used in the digital world. The cloud has enabled unique opportunities for both SME's and global enterprises to operate beyond their borders to serve customers and access new markets. Many of these innovations are customer driven, and provide customers with ready access to their funds and services, wherever they are or wherever they need the services to be delivered. Data localisation measures introduce legal and regulatory barriers to the digital work, which have been shown to impose barriers to these opportunities for both individuals and businesses.

Continues…

The report suggests that regulators and legislators should first consider their overarching aims and concerns, which include, as above, ensuring the protection of data, as well as access to data by regulator as required. These aims and concerns can be resolved by means other than localisation of data, including focussing on assurances around the access to data rather than localisation, and encouraging cooperation between regulators to avoid the need for legislative measures to impose physical restraints on the location of data.

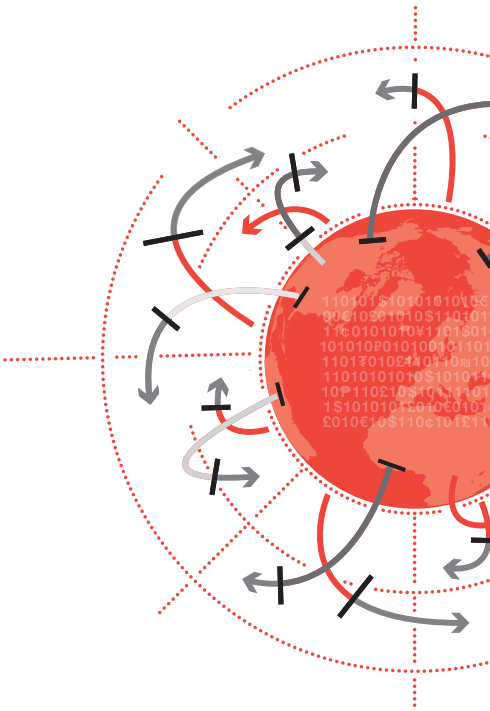
As nations across the world plan how we re-emerge from the global pandemic, and how to help businesses grow, it is important to remember that the future is increasingly digital, and data is the driver of digital businesses and innovation. The opportunity is for countries to recognise the importance of embracing an outcome focussed approach to data which protects data (whether personal or non-personal) while allowing it to cross borders. This approach allows countries to do things differently, but to recognise other regimes which achieve a similar result, and so build on shared outcomes and objectives, rather than focussing on legal differences. Focussing on accountability rather than control of data will help countries to collaborate and build a stronger digital future where cooperation on outcomes can build trust in data.

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:

AFME
AIMA
Bank of America
BNY Mellon
CBI
Citi
Clifford Chance
Credit Suisse
DLA Piper
Fidelity
FLA
Freshfields
HSBC
IA
Invesco
IBM
JP Morgan
Lloyds Banking Group
London Stock Exchange Group
Marsh Ltd
Morgan Stanley
Nasdaq
PIMFA
Refinitiv
Standard Chartered
techUK
UK Finance

For further information about this report, please contact:

IRSGsecretariat@cityoflondon.gov.uk



IRSG
INTERNATIONAL
REGULATORY
STRATEGY GROUP

DAC BEACHCROFT

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