WHITE PAPER

DATA SOVEREIGNTY:
THE IMPERATIVE FOR ACTION

November 2019

HDR | Hurley Palmer Flatt Group

FOREWORD

Robert Thorogood
Executive Director

At a time when businesses are already being challenged by political upheaval, technological advancement and environmental concerns, another front is developing at pace: the safety and sovereignty of data.

Data is widely recognised as one of the most valuable materials of our future, but legal constraints around where it should reside and how it can be used have serious implications for how businesses use and store their increasing volumes of information.

The current legal framework exists to protect individuals, organisations and countries, but the landscape is fraught with pitfalls.

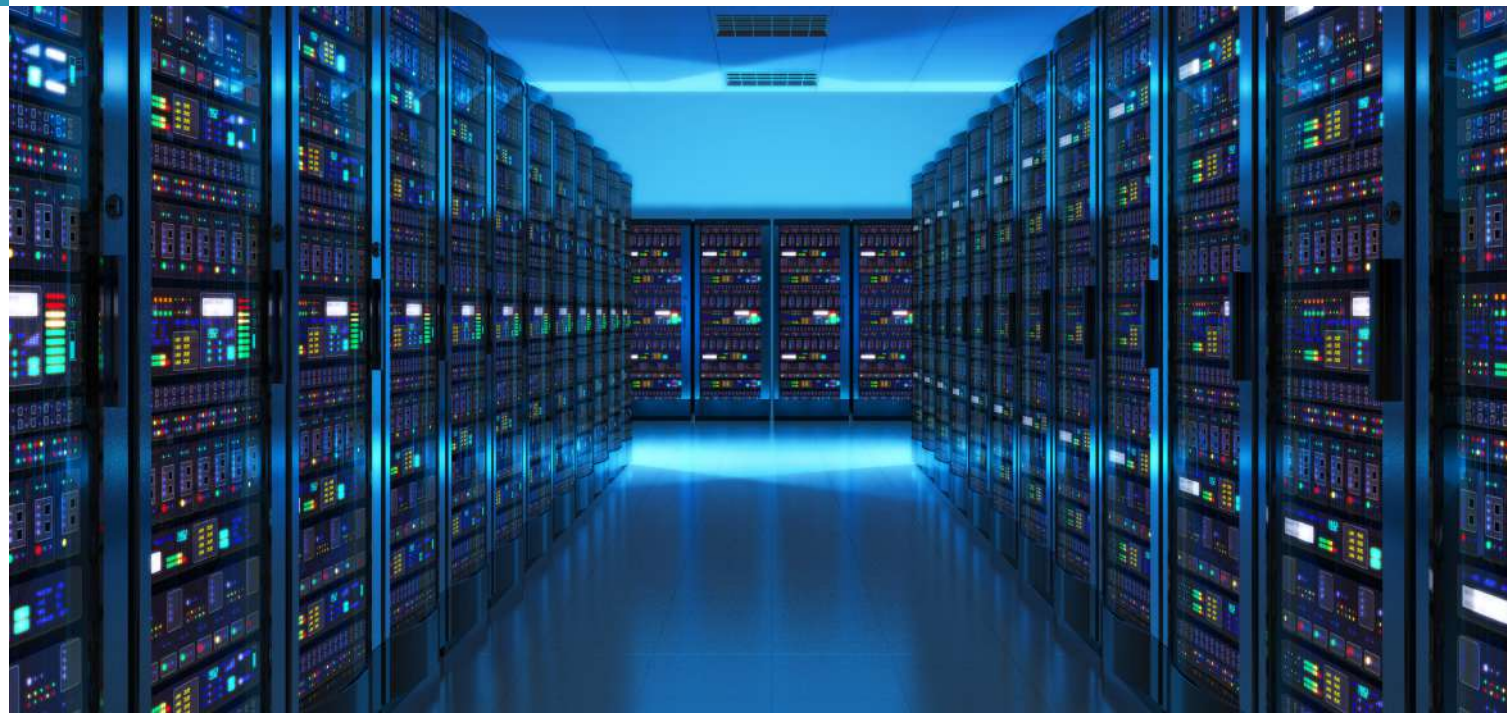
For this reason it is imperative that organisations to give the management of data their fullest attention.

This white paper aims to crystallise and inform on the issues around data sovereignty. It aims to raise key considerations so the issue can rightly find a place at the centre of business leaders' conversations.

Data sovereignty is an ever-evolving topic and we continue to monitor developments, particularly with countries or areas in the process of defining their control of data. We also welcome greater clarity as it is only then that organisations can make plans on how to arrange their data and how to use it within the various legal frameworks.

We aim to update businesses further as the legal framework is finalised and comes into force.

In the meantime, we welcome your questions and debate.



Data Sovereignty: The Imperative for Action

The concept that data may be subject to the laws of more than one country - and the fact that those laws are ever changing - presents mounting responsibilities and challenges for organisations.

Rapid advancements in digital and mobile technology, increasing global connectivity, and the proliferation of cloud services have made the global economy a seamless ecosystem.

Within this ecosystem is the ability of organisations to collect, manipulate and monetise unprecedented amounts of personal and confidential data, which is heightening concerns about citizens' privacy and cyber security.

In this frenetic landscape, in which huge amounts of data are harvested, stored and analysed 24 hours a day, governments have moved with uncommon swiftness to provide statutory instruments that seek to regulate the flow of information.

This has included the assertion of 'data sovereignty', in which governments enforce their own privacy laws on data stored within their jurisdictions. It is a rebuff of sorts to the global economy, a reimposition of sovereign interest.

For businesses, this has created a raft of compliance obligations and strategic imperatives, as well as the need for informed decisions about where their data is stored, how that data is managed and protected when shared across borders, and how IT systems are set up.

Data sovereignty vs residency and localisation

For businesses that collect private and confidential data, the challenge is to ensure that data privacy is not put at risk when shared across borders.

However, before they can devise appropriate strategies to mitigate risks and compliance burdens associated with data sovereignty, it is important to clarify what we are considering:

- Data sovereignty is frequently used interchangeably – and incorrectly – with 'data residency' and 'data localisation'.
- Data residency is when an organisation specifies that its data will be stored in a geographical location of their choice, for example, if a company wishes to take advantage of a favourable tax, legal or regulatory regime.
- Data localisation comes with legal obligations. It requires that data created within a country's borders remain in situ. Data localisation laws generally require that a copy of data be held within the country's borders, usually to ensure that the host government can audit data on its own citizens without having to contend with another government's privacy laws.

In some countries, the law is so strict as to prevent data crossing the border at all, most notably Russia's On Personal Data Law (OPD-Law) which requires the storage, update and retrieval of data on Russian citizens to be limited to data centres within the Russian Federation.

Data sovereignty is a concern for companies that believe their data has less protection when it's hosted overseas.

What does data sovereignty mean for business?

The rapid take-up of cloud-based data storage exposes companies to issues of data sovereignty. With the rising popularity of cloud computing, data sovereignty issues have become a greater focus for companies concerned about threats to the integrity and security of their data.

Data sovereignty becomes an issue when a company's data servers are located outside the country in which the business is domiciled, and governments insist that this data is subject to the laws of the country in which it is collected or processed.

A lack of proper due diligence often results in data servers being located in countries without the express concurrence of the client company. Those servers are consequently subject to the laws of the country in which the data resides.

When data is stored digitally with a cloud service provider the provider might store the data in multiple countries, making that data subject to the privacy laws of more than one country.

Data sovereignty can unexpectedly become an issue even if a business does not have direct operations overseas. Many businesses have customer service call centres located offshore which will be in receipt of customers' personal information. That is sufficient to place that information under the purview of foreign privacy laws.

If an Australian multinational company sends personal information to a branch office or processing centre in

the United States, where that information is stored, the information is subject to US laws irrespective of the provenance of that information or the fact that the company is domiciled in Australia.

A risk posed by data sovereignty is that an organisation's personal data could be subpoenaed by a foreign government. Data stored in the US, for example, could be subject to a subpoena to give law enforcement agencies access to a customer's information, such as personal information, credit card details, financial records and health records.

The ready solution to falling prey to data sovereignty risks would seem to be obvious: ensure that sensitive data is stored on home soil, but even that approach is not so straightforward.

When data is stored through a cloud service, the provider may store the data overseas. Data stored overseas becomes subject to the legal jurisdiction and privacy regulations of another country. This doesn't just happen when a business chooses an overseas service provider; the same problem can arise with a local cloud services provider.

Mitigating data sovereignty risks

Businesses need to have a robust and comprehensive data security strategy and vigorous internal procedures to protect and secure data. The onus is on businesses to understand how their data is stored, who owns it and how it moves.

Even when using a local service provider, it is best for a business to verify where its data will be stored. If using an overseas provider, then establish where the data will be located – it may be another country.

Businesses also need to:

- Ensure that their cloud service provider will not replicate data onto servers in other countries
- Ensure that the data stored overseas is done so according to local laws.
- 'De-identify' data before storing it in the cloud. (De-identification is removing people's identity from the data.)
- Ensure that their cloud service provider has insurance to cover data breaches.
- Back up their data before moving it offshore, as a loss of data can be catastrophic for the business.

Furthermore, if using a data centre, where is the data going to be stored and who owns the data centre? A company's data may be in a data centre in the UK, but if this data centre is owned by a US-headquartered company, then the US Government may have the right to access that data under the CLOUD Act (see below).

Who owns the data? Organisations may not be aware of the ownership rights over data stored in different countries. Data that was protected by strong privacy laws in the EU may not be protected in a different jurisdiction. This can make legal challenges to data access hard to defend.

Data gravity, data sovereignty and the cloud

'Data gravity' is a metaphor introduced into the IT lexicon by San Francisco software engineer Dave McCrory in 2010. The idea is that data and applications are attracted to each other, similar to the attraction between objects that is explained by the law of gravity. As data sets grow larger and larger they become more difficult to move. So, the data stays put and applications and processing power moves to where the data resides.

Analytics in the cloud: even higher barriers

Barriers become even more challenging if you want to run analytics in the cloud on data stored in the enterprise, or vice-versa. These new realities for a world of ever-growing data sets suggests the need to design enterprise IT architectures in a manner that reflects the reality of data gravity. Alternatively, companies could consolidate their data in a cloud platform where the analytics capabilities reside (and which includes data sovereignty guarantees).

The legal framework

Australian Privacy Principles (APP)

APPs are a set of principles that govern how a business is to deal with and store personal information. They set out the circumstances under which a business may collect data from their customers.

The APPs outline how and when other entities can access this data. They instruct businesses on how this data may be used and for what purposes. They also set out the disclosure requirements businesses have to comply with when sharing personal information for secondary purposes. (Source: LawPath)

APPs now include rules for handling data sovereignty.

General Data Protection Regulation (GDPR)

The European Union's GDPR covers data protection for EU citizens. The GDPR also addresses the transfer of personal data outside the EU and European Economic Area (EEA). It supersedes the Data Protection Directive.

With the advent of the GDPR, organisations have reviewed their data sovereignty requirements and capabilities.

Besides the 'right to be forgotten' provision of the GDPR – the right for individuals to have personal data erased – the most prominent provision is that relating to data sovereignty.

The GDPR requires that all data collected on citizens must be either stored in the EU, so that it is subject to European privacy laws, or within a jurisdiction that has similar levels of protection. It applies to both data controllers and data processors.

Countries such as Russia, China, Germany, France, Indonesia and Vietnam require that their citizens' data must be stored on physical servers within the country's borders. They argue that it is in the governments' and their citizens' interest to protect personal information against any misuse, especially outside of each country's jurisdiction.

Data sovereignty and the courts

Litigation often spans country borders, but how is eDiscovery and data sovereignty handled when data is generated and stored outside the US? Many countries have laws that stipulate that data created in a particular country must also be stored in that same country.

However, during a lawsuit's legal discovery phase, supporting content can be requested no matter where that data is stored. A landmark case in 2013 collided head-on with country data sovereignty and corporate rights. US law enforcement sought data on a user of Microsoft services in relation to a drug trafficking case; Microsoft argued that the data in question was located exclusively in a data centre in Ireland and argued that the data were not subject to US jurisdiction.

A federal court issued a warrant under the Stored Communications Act against Microsoft for both personal user data and email. Microsoft challenged the warrant but lost. Microsoft appealed to the US Second Circuit Court which froze the warrant until a decision could be handed down.

While the case was awaiting judgment by the US Supreme Court, the US Congress passed the Clarifying Lawful Overseas Use of Data (CLOUD) Act (2018). The Act states that companies must provide information properly requested by law enforcement "regardless of whether such communication, record or other information is located within or outside of the United States".

The passing of the Cloud Act finally decided the question of the federal courts and cross-border eDiscovery. Microsoft issued a statement in support of the CLOUD Act. [Source: Archive360]

Brexit: in or out?

All countries in the EU benefit from what might be called the 'free movement of data'. This currently applies to the UK in the same way that it does to the other 27 members.

However, when the UK leaves the EU, it may or may not still be included in this 'free market' in data. Current EU data protection legislation states that "special precautions need to be taken when personal data is transferred to countries outside the European Economic Area that do not provide EU-standard data protection".

If data sovereignty isn't included in any finalised Brexit deal, or if the "no deal" scenario eventuates, then UK businesses could be directly affected. Post-Brexit, the UK would no longer be covered by data agreements between the EU and other countries, such as the EU-US Privacy Shield Framework.

If the EU does not grant "equivalency" to the UK post-Brexit, the safest thing to do when it comes to data sovereignty issues is to make sure that data is migrated to UK-based data centres. This will mean that it will be subject to UK data protection legislation post-Brexit. [Source: Access]

Around the world

Vietnam

Vietnam's Law on Cybersecurity came into force on January 1, 2019. The law seeks to regulate data processing methods of technology. Online service providers subject to the new law will be required to store the personal data of Vietnamese end-users in Vietnam for the legally prescribed time, and surrender such data to Vietnamese government authorities upon request.

Personal data in this context includes personal information such as name, date/place of birth, ID numbers, address and phone number as well as job title, health status, medical records and biometrics.

Data created by a user (for example, uploaded information and synchronisation or input from devices) and data regarding the relationships of a user (for example, friends and groups with which an individual interacts) are also covered by data localisation requirements.

Personal data must be stored in Vietnam for as long as the service provider continues to provide the covered services, while data created by users and data regarding the relationships of users must be stored for a period of at least 36 months. [Source: Hogan Lovells]

India

In August 2019, India's Minister for Communications, Sanjay Dhotre, announced that he had tasked the government's Centre for Development of Telematics (C-DOT) to continue the "indigenisation of technology and products". Noting that India is one of the largest data-consuming nations, he said: "To cope with the increased data requirement, our telecom networks [will] also need new technology. C-DOT will have to work towards achieving this ... the dream of building India cannot be fulfilled without indigenous technology and manufacturing."

The Indian government is developing a national e-commerce policy which will include initiatives to enhance India's data sovereignty.

UAE

The UAE is poised to introduce a data protection law, similar to the EU's GDPR, as part of a three-year National Cybersecurity Strategy. As part of the 2020-2025 strategy 60 initiatives will be implemented.

The strategy has also identified information and communication technology as 'critical infrastructure' for development. Mohammad Al Zarooni, Director of Policies and Programs at the UAE Telecommunications Regulatory Authority, explains: "Part of the strategy is that data privacy is crucial to the cyber [sector] and the UAE is regulating and drafting a data protection law. We will look at the best practices performed worldwide. GDPR will be one of the inputs to it."

Priority areas include: enhancing cybersecurity laws, regulations to address cybercrimes and developing a cybersecurity standard for SMEs. Policy frameworks for the Internet of Things, cloud computing and artificial intelligence are in the drafting phase.

China

In May 2018, China introduced the National Standard of Personal Information Security Specification. The standard provides guidelines to assess whether a company has met the requirement of "implementing technical and other necessary measures to protect personal data" as required under the China Cybersecurity Law (2017).

Although not mandatory for companies to adopt, it is viewed as a 'soft law'. Following the close of public consultation in March 2019, China's National Information Security Standardisation Technical Committee has foreshadowed the introduction of new regulations to address "data subject consent" and revised data breach reporting standards involving sensitive personal data.

Revisions to China's Cybersecurity Law will include guidelines for the appointment of Data Protection Officers for companies whose principal business involves the processing of personal data. No time-table has been announced for the introduction of the changes.

CONCLUSION

In the digital economy, organisations are information-rich. They have never possessed such extensive reserves of personal data nor have they been closer to their customers as a result. Digital consumers have benefited from customised product and service offerings, enhanced customer experiences and the ability to intimately engage with their favourite brands across multiple platforms.

But with the ability of organisations to collect unprecedented amounts of data across multiple technology platforms comes great responsibility, and challenges – not least compliance obligations and strategic imperatives, as well as the need for informed decisions about where their data is stored, how that data is managed and protected, and how vendors are chosen.

How well organisations deal with the risks posed by data sovereignty is the latest challenge in the digital transformation of the economy. ◆

HDR | Hurley Palmer Flatt Group

HDR | Andrew Reid

HDR | Bradbrook Consulting

HDR | Concentre Consulting

HDR | Hurley Palmer Flatt Group Companies

hurleypalmerflattgroup.com