Cyberfort

WHITE PAPER

Overcoming Data Sovereignty Concerns in the Cloud

INTRODUCTION

White paper overview

In this article Cyberfort cloud experts discuss why data sovereignty is in focus for many IT leaders and their Cloud teams.

It starts by exploring why your organisation should be concerned about data sovereignty in cloud environments. Then provides recommendations for how IT leaders and Cloud teams can manage, maintain and control data in their cloud operating environments.

Why should your organisation be concerned with Data Sovereignty?

Lawful use

Secure access and availability

Organisational continuity

What are the challenges faced by IT teams with Data Sovereignty in the Cloud?

Compliance with local country regulations

Global data flows and sharing of data

Cyber Security risks

Cloud vendor storage locations

Building the right business case for investments in cloud and managing cost

Understanding where you need specialist Cloud Service Provider support for Data Sovereignty

Why use a specialist provider to help with Data Sovereignty in your cloud operating environment?

Understand where your data is being stored, managed and processed in the cloud

Identify if a data localisation strategy is required for your cloud requirements

Make sure sensitive data is identified and classified correctly

Put in place best practices for staying up to date with regional laws and regulations

Review your existing and future cloud vendors to ensure the right levels of security for data is in place and your customers are able to access data when they need it

Introduction to data sovereignty

Data Sovereignty has come sharply into focus over the past 12 months in the cloud computing space. The rise of AI and its underlying models of LLM's and Machine Learning, IoT, and Edge Computing, all require and rely on data being identified, processed and managed correctly so organisations can extract the benefits from these technologies.

Many organisations have seen the technology areas identified above as putting extreme pressure on their cloud computing resources. But it isn't just the physical resources under pressure. Those who are responsible for cloud computing are having to review the storage, management, processing and transit of data in relation to regulatory requirements including GDPR, EU ePrivacy directive, California Consumer Privacy Laws (CCPA and CPRA), The Australian Privacy Principles (APP) and The Japan Act on the Protection of Personal Information (APPI).

Data sovereignty due to the regulations highlighted above is fast becoming one of the most important areas to review and address for IT leaders as it relates to:

- **Protection of Individual Rights -** Ensuring that individuals have control over their personal data and can exercise their privacy rights.
- **National Security -** Protecting national security interests by regulating the storage and processing of sensitive data within a country's borders.
- **Economic Consequences -** Organisations who undertake tasks across borders need to make sure they are compliant with local laws regarding data management or face fines and potentially losing customer/employee trust.
- **Data Localisation -** Data sovereignty allows countries to retain control over their data infrastructure and ensure compliance with local regulations. This reduces reliance on out of country data storage providers and helps to mitigate risks associated with cross-border data transfers.

Before we move further into the article it is crucial to distinguish between data sovereignty, data localisation and data residency. All of these three topic areas hold close relationships to each other. But there are some subtle differences:

- **Data sovereignty -** The idea that a country or jurisdiction has the authority and right to govern and control the data generated within its borders.
- **Data localisation -** The practice of requiring that certain types of data be stored and processed within a particular country or jurisdiction.
- **Data residency -** The physical location where data is stored.

Data Sovereignty plays a significant role in data localisation and data residency. If organisations are not focused on their data sovereignty strategy, they could be leaving themselves open to fines, customer and employee complaints about how their data is being used and cyber security risks.

Why should your organisation be concerned with Data Sovereignty?

Data sovereignty is increasingly being seen as important in the cloud computing world as it relates to and ensures laws and regulations applicable to data are observed. Data and how it is used, stored and moved in transit is now at the forefront of not only Data Management and IT teams but it is also on the board agenda as well. The reason for the change in importance of data sovereignty is due to the increased risks associated with it and the rules and regulations put in place by every government across the world. When reviewing data sovereignty in an organisation, concerns generally fall into 3 areas:

Lawful use

Pretty much all countries and regions across the world have created data protection regulations covering security, privacy and storage in relation to the location of physical data storage. The main example often quoted when discussing data sovereignty from a legal perspective is the EU's GDPR law. The regulations regarding data sovereignty in the legal area of data sovereignty include website visitor data and product usage data. If organisations do not comply with these regulations it can lead to complex legal issues and impact operational and financial performance.

Secure access and availability

Do you know who is accessing sensitive data cross the organisation? Personal, financial and intellectual property is all types of data which needs to be controlled from an access and availability perspective in regard to security. Regional laws may also vary and cover someone's privacy in terms of their data collected and how it is securely stored as well.

Organisational continuity

With data stored in public cloud environments sometimes organisations find their data is being stored in other country locations. This can create issues in terms of access and availability to data if an outage should occur in an offshore location. Additionally, issues could occur in terms of jurisdiction. For example, what are the laws for keeping data in one country vs another, if the data is being transited between two different countries what are the attack risks from a cyber security perspective? All organisations therefore need a local facility to backup and store their data in case of a worst-case scenario where data is hacked, lost or stolen from their cloud computing environments.

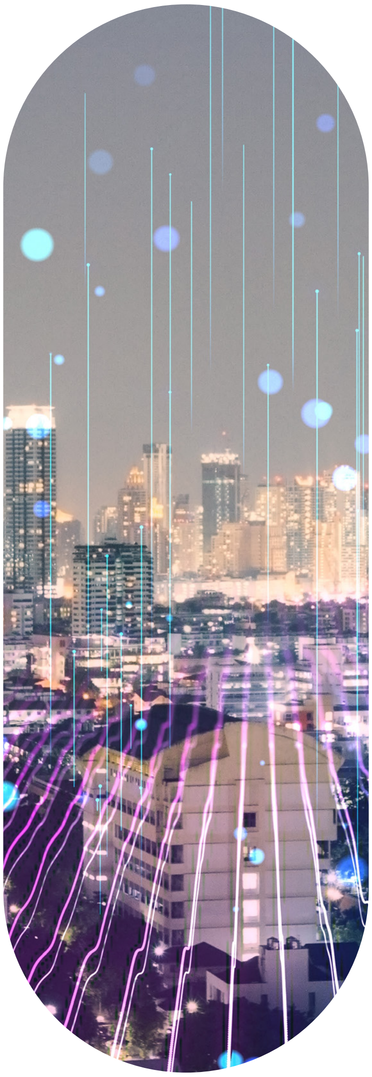
What are the challenges faced by IT teams with Data Sovereignty in the Cloud?

When reviewing Data Sovereignty requirements and an organisations cloud computing environments it is clear there are many challenges which need to be addressed. In the next section of this paper, we identify the most common challenges regarding this topic area, impacts on an organisations cloud strategy and provide advice on how to build a better data sovereignty approach for the future:

Compliance with local country regulations

Most countries have laws in place which require that certain types of data is stored and processed within their jurisdiction. This is often a challenge for organisations who want to use cloud computing across multiple regions. It often adds layers of cost and complexity to cloud computing which may not have been considered as part of the original business case for moving data to the cloud. For example, if using a public cloud an organisation needs the right legal and data management advice on what data can be stored and what data can be moved between each region. If these skills do not exist it could mean not being compliant with local regulations. Which then leads to further cost considerations as investments will need to be made in local datacentres and infrastructure to remain compliant.

A practical way to address this challenge is to first of all undertake an audit of where data in cloud environments is being stored, processes and in transit. Then classify it and review the relevant local laws and regulations in relation to the data. Following this step review your Cloud Service Providers agreement and assess if they are placing your organisation at risk with their data storage facilities. If IT teams do find there is a risk, they should start to review data localisation options with a Cloud Service Provider who has local datacentres for the local country they would like to store data in.



Global data flows and sharing of data

Data sovereignty can make it difficult to transfer data across country borders. For those organisations who have a significant public cloud presence this could result in increased costs and complexity as they will need to factor in legal and security checks on where data is stored, used and protected in transit across different jurisdictions.

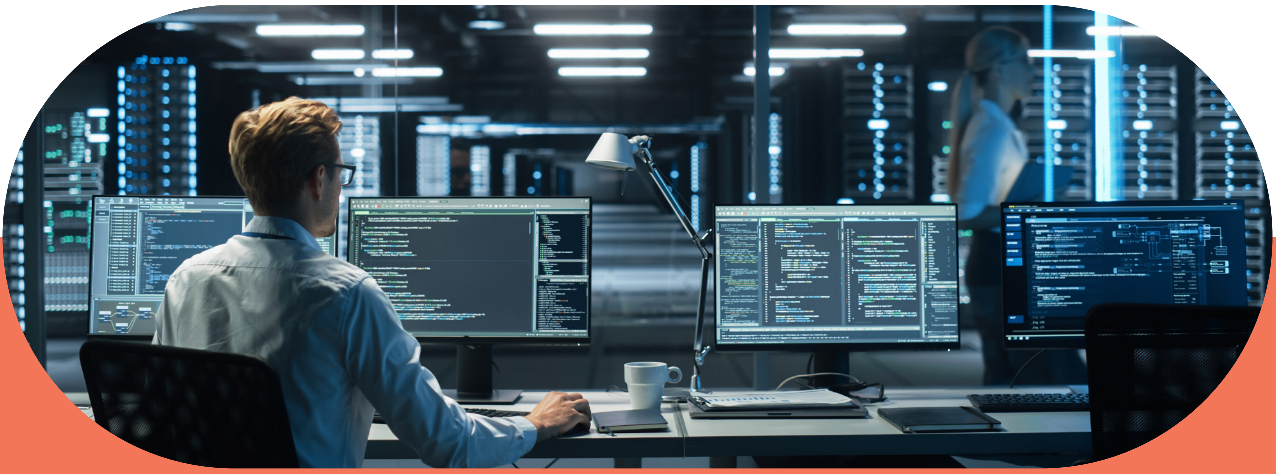
To overcome the challenges with global data flows in relation to data sovereignty, it is recommended a full data audit is undertaken of where data being stored, processed and managed in the cloud. From the audit those responsible for cloud computing in their organisations can identify where data is not being stored, processed or managed in a compliant manner against different country regulations.

If data is identified as crossing country borders a business case should be created to evaluate what the most cost-effective options are for storing, processing and managing the data. For example, should you invest in legal and data management expertise in specific geographic locations or would you be better reviewing your Cloud Service Providers and asking them about their data residency options. If data is going to be transferred across borders still and data residency isn't an option, then a data localisation strategy should be created and communicated to those responsible for data which is being transferred and used in different countries.

Cyber Security risks

By not having the right data sovereignty approach in place as part of an overall cloud strategy could lead to cyber security risks. For example, if data is stored in a location where security is not fully considered or the jurisdiction has lower levels of security requirements in terms of storing, managing and processing data, cyber criminals could be looking at these countries to proactively attack their data. In turn if data is compromised it could lead to financial penalties, operational disruption and reputational harm.

Cloud teams need to check their Cloud Service Providers storage locations, understand the data sovereignty protection laws in place and examine if they meet the organisations expectations. If the countries data protection laws do not meet your organisations expectations plans should be put in place to move the data to a safer location where better security controls and visibility are in place.



Cloud vendor storage locations

A common theme running throughout this article is public cloud and the locations data is stored in the public cloud. The public cloud providers physical storage and processing locations have to be considered as part of the wider cloud strategy. Secondly if data privacy laws for a specific country require data resides within a user's jurisdiction, organisations need to make sure this data is identified and plan with their Cloud Service Provider on where this data needs to be stored, managed and how it should be moved in transit.

Moving forward those who are responsible for data in the cloud must make sure they are reviewing all regulations vs cloud service providers storage locations. If this isn't happening changes in regulations could be easily missed and potentially leave the organisation open to unforeseen regulatory action which could incur additional costs associated with the cloud.

Building the right business case for investments in cloud and managing cost

To make sure the right data sovereignty approach is in place will require a supporting financial plan. Additionally, identifying and classifying the types of data being used in the cloud other cost considerations as part of the data sovereignty business case should include budget for access to legal and data management skills, cyber security measures and training for employees on the different laws and compliance measures they need to be aware of and manage in their roles.

The data sovereignty business case should be forward looking. As discussed earlier in this article global/local regulations regarding data are complex and changing. Inevitably any change in local laws will require reviews of the cloud strategy to happen and investments needing to be made to keep data safe, secure and compliant. The final part which needs to be reviewed and included in the business case is how your organisations cloud computing will scale and the pressures it will put on the data management and cloud teams. Budget will need to be available to assess a variety of scaling options and include what the extra costs may be incurred by the organisation if they have to manage several cloud providers.

Understanding where you need specialist Cloud Service Provider support for Data Sovereignty

It is clear from the challenges, potential impacts and steps needing to be taken for the right data sovereignty strategy to be created and put in place that this is not an easy task. Many organisations do not possess the right skills or have the resources available to them to create, deliver and manage an end-to-end data sovereignty plan in relation to cloud computing.

At Cyberfort we are increasingly witnessing organisations requiring specialist support in this area. But before you ask your existing Cloud Service Provider for help in this area there are some steps to be taken:

1. **Gain an understanding of where data is being stored, processed and managed in the cloud today and what data will need to be managed in the future. Key questions which should be covered as part of this step include:**

- What is the current situation with cloud in the organisation, is data being stored, managed or processed in public, private or hybrid clouds?
- What access and security measures are currently in place for cloud and are they fit for purpose?
- Will you require support for different edge devices which are using data across borders?
- Should you be thinking about data localisation if budgets do not exist for specialist legal and compliance expertise if data is stored, processed and managed in different jurisdictions?

2. **Define what the future looks like in terms of storing, managing and processing data in the cloud. Put in place a roadmap to highlight the regulatory compliance measures which are likely to change and how this is going to potentially impact the organisation in terms of:**

- Your future cloud choices.
- Supporting IT infrastructure.
- Legal and data management skills required.
- Budgets to support and your objectives for cloud and data management.

This will help your organisation to have a clear view of the challenges ahead and where 3rd party specialist support may be required.

3. **Once a clear understanding of the challenges relating to data sovereignty are defined you can then assess where gaps exist and assess your Cloud Service Providers against technical, financial, and compliance-related needs. As part of this step, you can also review their migration services, physical datacentre locations, and service regions. Following this an informed decision on if your Cloud Service Providers are meeting your data sovereignty requirements can be made and understand where specialist support may be needed.**

Cyberfort

SERVICES

Helping your business create, manage and deliver Secure Cloud services

Cyberfort Cloud

- Secure multi-tenant cloud
- Infinitely scalable
- Software-defined networking model
- Integrated backup included
- No ingress/egress charges
- Feature-rich optional native capabilities available

Private Cloud

- High performance dedicated platforms
- Compliant to regulatory & security requirements
- Proven technology stacks
- Secure UK Data sovereignty
- Tailored solutions
- Fully managed
- Certified engineers

Public Cloud

- Azure Managed Cloud
- AWS Managed Cloud
- Performance and cost optimised design & management
- Total cost of ownership calculations
- Build validation services
- Multiple billing options
- Flexible support levels from certified engineers

Hybrid Cloud

- Enterprise cloud
- Managed data protection
- Business continuity
- Managed connectivity
- Solution design
- Integrated platform with native Public cloud tooling and services

Cost certainty

Secure and compliant

Tailored cloud

High performance

Managed support

Skills on-demand

Cyberfort Secure Cloud Customers

ev qolcom DIGISEQ ADL SMARTCARE NEXUM™ B

Cyberfort

PARTNERSHIPS

Helping your business create, manage and deliver Secure Cloud services

Market-leading Technology Partnerships

Infrastructure, networking and connectivity

JUNIPER NETWORKS · Lenovo · DELL · FUJITSU

Platforms, data management and storage

Azure · vmware · aws · Microsoft · veeAM

NUTANIX · debian · Red Hat · kubernetes · ceph

Security and management

FreeBSD · elastic · HAPROXY · A10

Why use a specialist provider to help with Data Sovereignty in your cloud operating environment?

Answering the questions in the previous section and assessing where you need a specialist Cloud Services Provider to support your data sovereignty strategy could be the way forward for your organisation. From our own experience at Cyberfort the right accredited Cloud Servies Provider should be able to help you with developing a bespoke data sovereignty solution for your organisation.

For example, as part of data sovereignty in our cloud services we help customers:

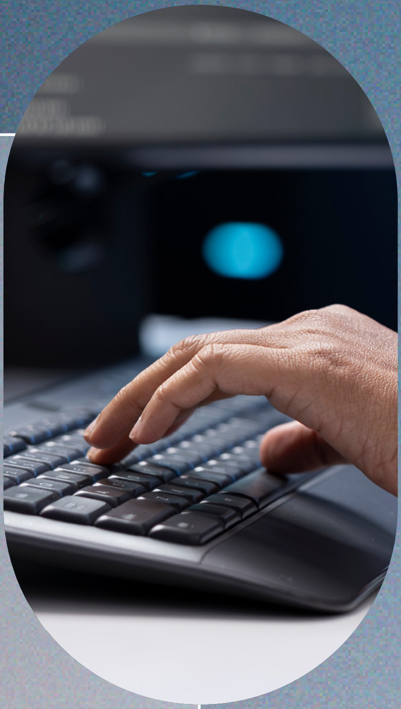
- Understand where their data is being stored, managed and processed in the cloud. We work with our customers to identify the physical locations of their cloud datacentres, review the relevant regulatory frameworks for their industry and what local laws may apply. Then we provide recommendations on different cloud strategies and if a data localisation strategy is required for compliance purposes.

- Identify if a data localisation strategy is required for an organisations cloud requirements. We provide advice on how storing data within a specific country will help to achieve compliance and put in place the right levels of security to protect data as it transits from the cloud back into onto on premises infrastructure and across country borders.

- Make sure sensitive data is identified and classified correctly. We then put in place the right security controls and policies to manage and protect this type of data in the cloud and ensure it meets ethical and legal guidelines. Additionally, we provide regular reviews back to customers on how the data is being used and highlight if there are any regulatory changes happening which could affect how their data is being stored, managed and processed in their cloud operating environments.

- Review their existing and future cloud vendors to ensure the right levels of security for data is in place and customers are able to access data when they need it. We also assess where different cloud vendors are storing data and if there are any compliance issues which could arise.

- Put in place best practices for staying up to date with regional laws and regulations. The world of data compliance is in constant change and evolving. Regularly reviewing the different regulatory compliance measures and validating if the cloud strategy is still relevant from a compliance perspective is crucial. By adopting this proactive approach to monitoring regulatory changes in relation to data in the cloud means organisations are not suddenly surprised by changes or have to make drastic changes which could affect operational and budget performance.



CONCLUSION

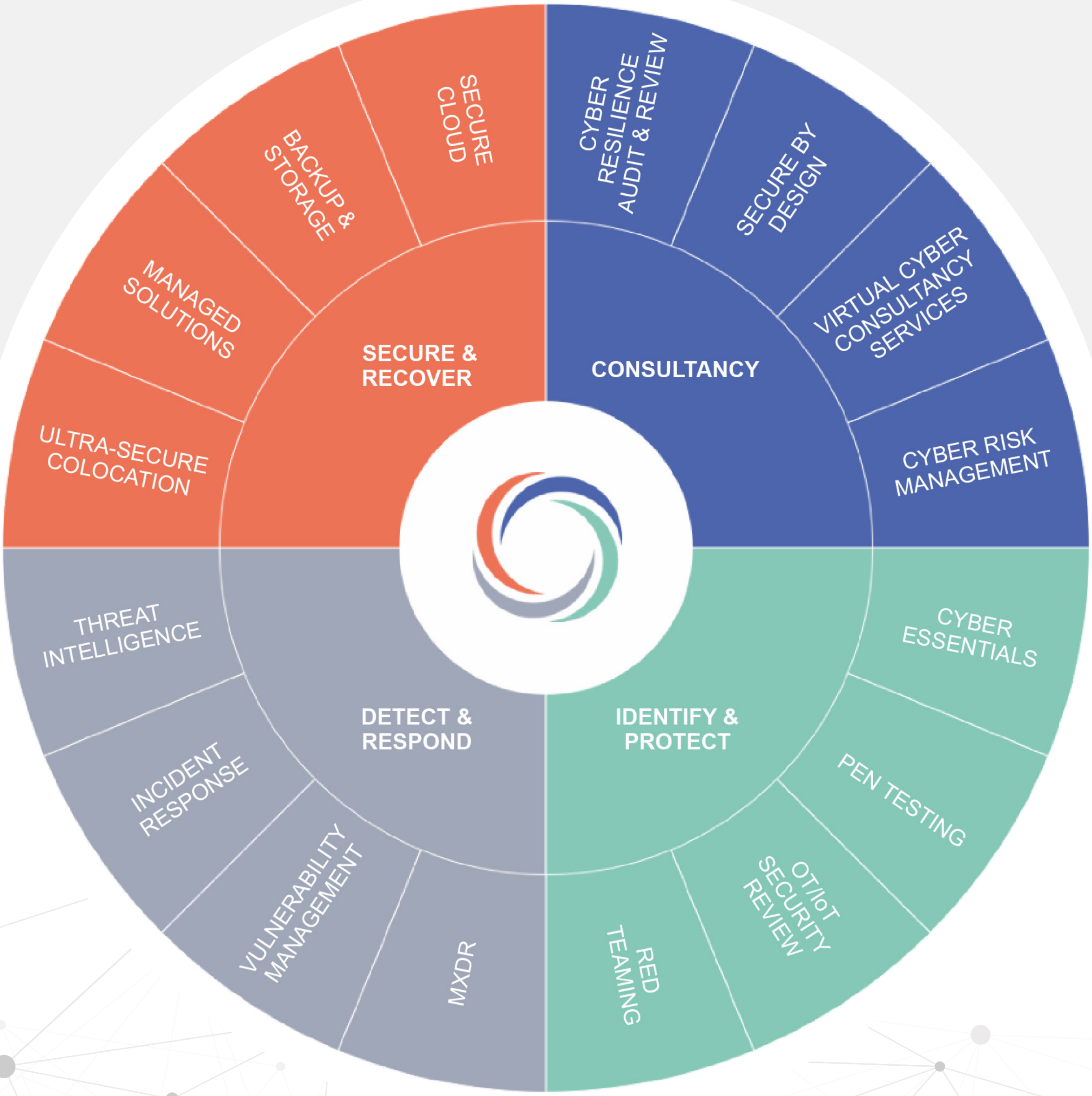
Final thoughts

In this article we have discussed why data sovereignty is in focus for many IT leaders in 2024. It is clear that data sovereignty is not just a passing phase within cloud computing. It needs to be a key consideration as part of any organisations cloud strategy both now and in the future.

Those organisations who take the time to understand the different regulatory compliance measures, legal, financial, and operational impacts of data sovereignty will find themselves in a better position to manage, store and process their data as their cloud environments scale in the future.

Discover more about Cyberfort's all-encompassing Cyber Security Services

Cyberfort Services Portfolio



Find out more about how Cyberfort can help your organisation

At Cyberfort we provide a range of customers with all-encompassing Cyber Security Services. We are passionate about the cyber security services we deliver for our customers which keeps their people, data, systems and technology infrastructure secure, resilient and compliant.

Our business offers National Cyber Security Centre assured Consultancy services, Identification and Protection against cyber-attacks, proactive Detection and Response to security incidents through our security operations centre and a Secure and Recover set of Cloud solutions which keeps data safely stored, managed and available 24/7/365.

Over the past 20 years we have combined our market leading accreditations, peerless cyber security expertise, strong technology partnerships, investment in our future cyber professionals and secure locations to deliver a cyber security experience for customers which enables them to achieve their business and technology goals in an ever-changing digital world.

For more information on our Secure Cloud & Cyber Security services please contact us at the details below:

+44 (0)1304 814800

info@cyberfortgroup.com

Or visit us at: https://cyberfortgroup.com

We look forward to working with you