5 Things to Know About Sovereign Cloud

Cloudian, Inc. 177 Bovet Road, Suite 450, San Mateo, CA 94402
Tel: 1.650.227.2380 | Web: cloudian.com | Contact Cloudian

Introduction

British mathematician and data scientist, Clive Humby, once said that data is the new oil. By the end of 2020, there was an estimated 44 zettabytes of data in existence – the equivalent of 1.7MB of data generated every second by every person on the planet for a year – and with the rise of smart technology and the Internet of Things (IoT), that figure isn't going to stop growing any time soon.

With so much data at our fingertips, organisations are only just beginning to scratch the surface of data analytics and the power to unlock richer insights into just about every aspect of our lives.

Data has the potential to improve both public and private sector services, driving greater efficiency, reducing risks, boosting profitability, and revealing trends that will help us plan for the future.

As the data economy grows, unlocking that value needs to be balanced against keeping personal data safe and secure, and complying with national data privacy laws. While it may be tempting to move data to a public cloud, it's important for businesses outside of the United States to be aware that data hosted in the United States or on infrastructure owned by US companies, for example, will be under US jurisdiction, according to the 2018 US Cloud ACT, which may clash or contradict with the privacy laws in the country where the data was collected.

The rise of sovereign cloud

Data sovereignty and sovereign clouds are not new concepts, but in this emerging landscape they've taken on a new significance. As organisations generate exponential volumes of unstructured data, it's important for managed service providers and/or cloud services providers (xSPs) to be able to offer broad, end-to-end cloud services that are scalable, cost effective, and secure.

When it comes to the storage layer, sovereign data must reside on-premises in the country it was collected and must be protected by national laws and jurisdictional controls of that country. As compared to block storage and/or file storage, object storage is a much more affordable and scalable platform that xSPs can deploy to achieve this.

xSPs also need to embed data protection as a default service into the cloud stack with disaster recovery, backup, encryption, and micro-segmentation capabilities to secure workloads. For smaller providers, storage-as-a-service (STaaS) and backup-as-a-service (BUaaS) are becoming increasingly popular to address the storage and backup requirements of their customers on a subscription model, however these often have hyperscale endpoints, breaking sovereign capabilities.

With on-prem private cloud storage technology, MSPs can position themselves as a viable alternative to hyperscalers to help customers take control of their data with comprehensive data sovereignty strategies and fully compliant sovereign clouds.

So, what are the five most important things xSPs outside the US need to know about sovereign clouds? Read on to find out.

Data Sovereignty Requirements for UK and EU Managed Service Providers

As organisations generate exponential volumes of unstructured data, it's important for Managed Service Providers (MSPs) to be able to offer broad, end-to-end cloud services that are scalable, cost-effective, and secure.

This in-depth white paper covers the 5 most important things MSPs in the UK and the EU need to know about their data in the era of sovereign cloud:

1. **Privacy Regulations**
2. **Residency**
3. **Sovereignty**
4. **Protection & Management**
5. **Security**

Data needs to be stored on-premises in the country it was collected to be protected by national laws. For this purpose, object storage is a more affordable, scalable solution than block or file. MSPs also need to embed data protection into the cloud stack with backup, encryption, and micro- segmentation capabilities to secure workloads.

For smaller providers, storage-as-a-service (STaaS) and backup-as-a-service (BUaaS) are becoming increasingly popular to address the storage and backup requirements of their customers on a subscription model. With on-prem private cloud storage technology, MSPs can position themselves as a viable alternative to hyperscalers to help customers take control of their data.

So, what are the five most important things MSPs in the UK and the EU need to know about sovereign clouds? Read on to find out.

1 Data privacy regulations

In recent years, the way companies and government authorities collect and use customer data has been in the spotlight. People have become more aware of who they're sharing data with, and what it might be used for.

While there's a growing appetite for more personalised services, customers want assurance that their data is secure, and want visibility of third-party access before they're willing to share personal information.

In addition, Cybersecurity is a growing concern. Threats are becoming more sophisticated, and criminals are quick to take advantage of any opportunity. When more businesses pivoted to remote working in response to the pandemic in 2020 for example, there was a 20% increase in hacking attempts.

High profile cyberattacks on household brands have also hit the headlines. In March 2020, British high-street pharmacy, Boots, was forced to suspend loyalty card payments when customer passwords were stolen, and the 2020 attack on the European Medicine Agency revealed a sinister motive to undermine public trust in the Moderna COVID-19 vaccine.

In response to the rising threat of cyber-attacks and higher demand for transparency and security around customer data, many countries have passed data privacy laws and regulations such as the European Union's General Data Protection Regulation (GDPR), and the UK's Data Protection Act (DPA) 2018.

Data privacy across borders

When a business operates across borders, complying with regional, national, and global data privacy regulations becomes more complex. Not only are these laws constantly changing, but new legislation may bring additional challenges, and there are questions around how regulators will enforce existing requirements.

There's also the issue of compelled access, which occurs when law enforcement or a government agency demands access to data via legal means.

The CLOUD Act

In 2018, the Clarifying Lawful Overseas Use of Data (CLOUD) Act came into force in the US to govern cross-border access to data. It was drafted in response to a case involving emails stored in Ireland but controlled by Microsoft, a US-based service provider. The CLOUD Act resolved the issue of this data being outside the US border by stating that Microsoft is subject to US jurisdiction and may be compelled to disclose data as part of the legal process, regardless of where the emails were stored.

Both the EU and UK have equivalent laws: the UK's Crime (Overseas Production Orders) Act 2019, and Article 49 of EU GDPR legislation.

Schrems II

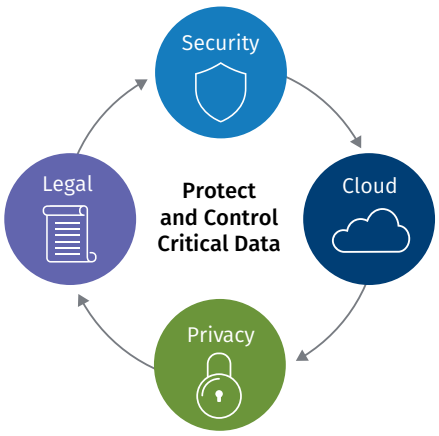
Another significant development was the Schrems II decision concerning the transfer of data between the EU and US. In this landmark case, the EU Court of Justice ruled that the EU-US Data Protection Shield was invalid due to concerns around surveillance by US state and law enforcement agencies.

Schrems II now requires European companies to conduct individual assessments of each data transfer to a non-EU country to ensure compliance.

Although the UK has formally left the EU, Schrems II currently still applies. That means UK businesses need to find alternative safeguards to the Data Protection Shield to protect data flows between the UK and US.

These laws seek to control how personal information is stored, processed, and shared by organisations, businesses, or the government. If data is stored in the public cloud, however, it may be stored across multiple data centres in multiple different countries and be subject to the regulations of the country where the data is hosted.

Sovereign cloud offers a solution to enterprises for complying with data privacy regulations by storing the data in the country where it was collected.



2 Data residency

Data residency refers to the physical location where data is stored. Data sovereignty, on the other hand, means that data stored in a particular location is subject to the laws of that location.

Understanding the difference is crucial to ensure compliance – by storing your data on-premises in the UK, data will have the legal protection of the UK courts, but it must also comply with UK legislation. Embedding an adequate storage and data protection solution into the cloud stack is important to secure data in line with UK regulations.

Where data is stored and processed may be dictated by policy, regulatory, tax, or performance reasons. Some countries, such as France, have national policies in place that require data to be stored in the European Union. Germany also requires data to be stored nationally or in the European Union depending on the type of data involved.

By using a hyperscaler, businesses have control over the boundaries of their data, where it's used, and which cloud services are enabled. Hyperscalers often provide self-service tools so companies can deploy, manage, and secure their infrastructure in line with government or industry requirements.

> **"An information monopoly is a danger that must be taken seriously."**
>
> *- Simon Hansford, CEO of UKCloud*

However, hyperscale public clouds provide places for data to be stored and processed, but the big name hyperscalers based in the US often host data in the United States. In addition, some services offered by hyperscalers span multiple regions, increasing the risk of data leaking across a sovereign border. There's also a risk that resident data can be accessed by a foreign authority under a compelled access order (for example, where the hyperscaler is under US jurisdiction, and therefore the CLOUD Act).

Customer data vs account information

It's important to note that hyperscalers make a distinction between customer data and account information. Customer data (e.g. name, address, contact number) is generally fully controlled by the business that collected it and covered by their terms of agreement with the cloud provider. Meanwhile, account information is managed separately and governed by its own privacy statement.

While customer data may be resident in one country, account information and metadata might be held somewhere else and be under different jurisdiction. It's not uncommon to find a clause stating that personal information may be stored and accessed from multiple countries in the fine print of the terms and conditions. This is especially likely if the hyperscaler delivers technical support from a different country to where the data resides.

The amount of information collected is often much broader than customers realise and can include metadata such as network IP, device, diagnostics, and other logs that the individual doesn't have visibility of.

This presents an opportunity for MSPs to assure customers that they can provide greater transparency and security than hyperscalers, and with distributed on-prem object storage, unparalleled scalability, and affordability.

3 Data sovereignty

As discussed, data sovereignty refers to data being subject to the privacy and governance laws of the country where the data was collected. Therefore, an individual may have two sets of privacy policies protecting their data if the data centre hosting it is in a different country to where data was collected. This affects the national government's right to access that data.

Sovereign cloud simplifies matters by storing data in the country where it was collected. Data will therefore be subject to the laws of that country, and other jurisdictions will have no authority over it. This sidesteps the complexity of overlapping or contracting legal requirements.

In some cases, there may be a need for cross-border data flows, and this can be addressed with hybrid and multi-cloud strategies. To enable data sovereignty across borders, concepts such as virtual data spaces are emerging. The International Data Spaces Association (IDSA) is a coalition of more than 120 companies who are developing a global standard and certification process to support the data economy.

The goal is to facilitate data exchanges between trusted partners, across borders, and between clouds while still maintaining sovereignty, to accelerate collaboration and innovation.

Europe's GAIA-X framework also provides foundations for a European cloud to help repatriate data from the US and China and regain data sovereignty within the union. The project aims to deliver next-generation infrastructure and security standards to decentralise and federate data. It's expected to increase the level of cloud adoption across Europe, which is currently lower than 50% in many European countries.

4 Data protection and management

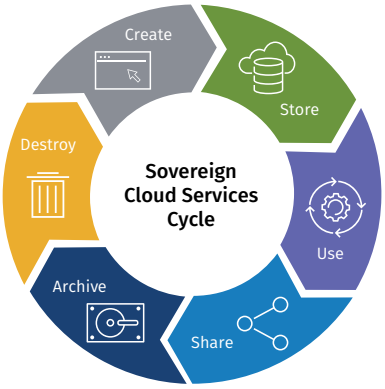
The data economy is an exciting prospect, but data protection needs to be front of mind in any cloud project. Around 64% of organisations cite compliance, auditing, access, and data protection for business continuity, as the biggest security challenges when it comes to cloud computing.

In EMEA, the main regulation concerning data protection is GDPR. Article 25 of the act requires data protection measures to be designed into the development of business processes for products and services, including making sure that personal data is protected from leaks and exfiltration.

Consumers need businesses to demonstrate transparency, integrity, protection, and security at every stage before sharing personal data. MSPs can add value to customers by helping to establish a robust data protection strategy to assure consumers that their data is well protected. They can also act as the designated data protection offer, under Article 37 of GDPR. This requires a person with expert knowledge of data protection laws and practices to ensure the company is monitoring compliance with regulations.

Here are 10 components of a good sovereign cloud data management strategy:

1. **Data lifecycle management** – a framework to standardise data processes across the organisation from collection, to storage, and deletion.
2. **Data risk management** – identify and assess all risks that may affect the data, including which legislation it's governed by.
3. **Data backup and recovery** – as part of a sovereign cloud, data should be backed up and recovered on-premises in the country of origin.
4. **Data access management controls** – ensure controls are properly implemented and maintained so only authorised users can access, use, or transfer data.
5. **Data storage management** – ensure data is stored or archived correctly in line with how often it will be accessed.
6. **Data breach prevention** – cyber security measures include data encryption, antivirus software, ransomware protection, and hardware and software security.
7. **Confidentiality, integrity, and availability** – known as CIA, these are key components that must be maintained to ensure data is protected.
8. **Policies and procedures** – these define data protection activities and how they're implemented. They must be well documented.
9. **Standards and regulatory compliance** – these are vital when establishing a sovereign cloud. Thoroughly research national and industry requirements.
10. **Monitoring and reviewing** – this provides visibility into all data activities, risks, and controls to improve protection and ensure rapid response to risks.



It's important to make sure all key stakeholders understand the data management strategy to ensure high levels of security and compliance and that all data is tracked thoroughly. Conducting a risk analysis can help identify and resolve threats before they impact customer data and will help with GDPR Article 35 compliance.

Embedding on-premises object storage in the cloud stack not only increases security, but its rich feature set also reduces the complexity of complying with regulations and keeping data safe from cyber-attacks. It can also be integrated with other leading data protection and public or private cloud solutions to offer customers unrivalled performance at an affordable price.

Unlike hyperscalers, MSPs have the flexibility to create more bespoke offerings when it comes to security, giving customers greater control to prioritise what matters most to them, and what they want their sovereign cloud to look like.

5

Data security

Growth is a high priority for organizations across EMEA. To succeed, executives are leaning heavily on technology, with a large percentage undertaking digital transformation initiatives.

Naturally, with a greater emphasis on digitization, there's heightened concern about data breaches and ransomware attacks. In fact, 47% of global CEOs were extremely concerned about cybersecurity in 2021, which puts it second only to the pandemic in terms of risks to business growth.

It's no surprise that data security has reached new levels of importance in every industry. Compliance with security regulations has never been more important. Comprehensive data security should include immutable storage services to ensure data can't be accessed, modified, or removed. If an organization's firewall is breached, having immutable backups is the last line of defense. It often means the difference between paying millions of dollars to criminals in vain hopes of unlocking vital data or simply rehydrating locked backups and carrying on with business.

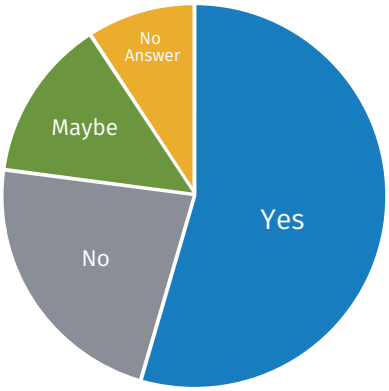
GDPR also requires companies who hold or process personal data to put appropriate technical and organizational measures in place to keep personal data secure, which can be achieved with encryption.

The role of managed service providers

As more companies accelerate their cloud strategies, they're increasingly relying on MSPs to help them implement data security and protection and comply with data privacy legislation around the sharing and storing of customer data.

Managed service providers need to consider data security and data protection as part of their sovereign cloud offering for enterprise customers. This includes securing data in-flight and data at-rest, providing data immutability, and demonstrating that they meet compliance requirements at a jurisdictional level. Customers need to be able to control and implement security features in line with their individual requirements, which is something that public cloud vendors are unable to offer.

MSPs can increase efficiency by using a multi-tenanted approach without compromising on security, allowing multiple users to share a single backup and storage infrastructure with quality-of-service controls to ensure consistent service levels.



Of the UKI MSP IT leaders Cloudian surveyed in Nov 2021, 55% said their customers are requesting Sovereign Cloud capabilities.

The benefits of sovereign cloud

Sovereign clouds may be set up differently depending on business needs and location, but they must ensure that the company can define boundaries for and maintain complete control and sovereignty over its own data.

The data economy offers a huge opportunity for innovation in the UK, and sovereign clouds can help to both protect and unlock the value of critical data in several ways:

- Greater control over data
- Better security
- Simplified compliance
- Future-proofing infrastructure
- Fueling innovation

Reducing vendor lock-in

Establishing a sovereign cloud also reduces dependency on foreign vendors and hyperscalers. This doesn't mean businesses can't use hyperscalers. A multi-cloud strategy can empower them to leverage the right cloud for the right workload and take advantage of the breadth of services offered by these providers. However, sovereign cloud enables customers to move applications and data where needed as their business evolves, which reduces vendor lock-in.

One approach is to establish a common architecture across sites to enable seamless portability and interoperability when migrating workloads between sites or onto and off the cloud. This can also be achieved by enabling container-based applications that can be deployed on any cloud infrastructure using Kubernetes as an abstraction layer. In either case, it is essential that the object storage of choice has high S3 compatibility, so that the on-prem, sovereign cloud storage is speaking the same language as the public cloud for easy data mobility.

Object storage and sovereign cloud – what to look for

Object storage is what makes the cloud durable, scalable, and feature-rich. An on-prem object-storage that can offer equivalent storage capabilities is therefore a requirement for highly secure sovereign cloud environments. Look for an object storage that is highly compatible with the S3-API, the de-facto cloud api standard, with a fully native implementation that eliminates gateways and access layers. This means MSPs can add value to customers by assuring them that sensitive data will be properly managed, secured, and controlled in line with GDPR requirements.

To achieve this, a sovereign cloud should be deployed in at least two nation data centres, with secure and private network connectivity and the ability to isolate the environment from the public internet.

Secure object storage

Comprehensive data security should include immutable storage services to ensure data can't be accessed, modified, or removed. Write once, read many (WORM) allows you to protect data for the retention period specified by the customer, while policy-based data protection features enable off-site replication.

You should also look for object storage that enables you to secure the solution at a system level, even disabling root access to make the solution impenetrable. To be sure you have this, look for security certifications including FIPS 140-2 and Common Criteria, and compliance with SEC 17a-4, FINRA, CFTC, IDW PS 880 (German), OR SS 957ff (Swiss), and NIST 800-88.

All of these security features create an added layer of protection against ransomware attacks, which increased 800% during the pandemic, and were cited as "the most immediate danger to UK businesses," by the head of Britain's National Cyber Security Centre, Lindy Cameron.

Enhanced data protection

Another important requirement for sovereign clouds is data encryption, which is crucial for cross-border data transfers. Look for high S3 API compliance and automatic data verification and encryption.

SSE/SSE-C and Keysecure can support third-party key management systems to keep data secure at rest. HTTPS protects data in transit during upload and download requests, and encryption should be able to be managed at bucket level.

Data immutability protects backups from encryption by ransomware and assures restore in the event of an attack. S3 object lock is quickly becoming the standard for implementing data immutability for cloud storage. Look for a built-in S3 object lock integration between your object storage and backup providers. This makes it as easy as checking a box and setting a date to lock a bucket away from ransomware access. A seamless integration between the right data protection provider and the right object storage can also allow large data sets to be backed up and restored quickly and easily, enhancing recovery point objects and recovery time objectives while increasing performance.

Optimising costs

Object storage is a scalable solution that can enable service delivery at a fraction of the cost of public cloud, allowing MSPs to generate more than 50%* in potential profit margins. Subscription models such as storage-as-a-service (STaaS) and backup-as-a-service (BUaaS) mean that more providers can benefit from this growing market with storage that grows in line with demand.

STaaS also simplifies storage management by handing responsibility for infrastructure, maintenance, facilities, and operations over to a trusted object storage partner.

Of 22 UKI MSP IT leaders surveyed in Nov 2021, 46% said true MSP cost optimisation must include all the following:

- Reduced capital expenditure with less spend on hardware and data centre space
- Storage capacity on demand
- Protection against infrastructure damage due to physical disasters
- Enhanced availability and business continuity

This is particularly beneficial for MSPs with 500 or fewer employees, who can then focus on boosting revenue, improving customer satisfaction, and increasing profits.

Meanwhile, BUaaS is expected to grow at a compound annual growth rate of 26.6% until 2024, offering MSPs the scalability, confidence, and cost savings to focus on more strategic activities.

Conclusion

Sovereign clouds are becoming increasingly important to simplify protecting customer data in the growing data economy. They take the complexity out of complying with national regulations around data residency and data sovereignty, while making vast quantities of data available for analytics to drive a more intelligent and predictive approach to innovation.

xSPs are uniquely positioned to provide a cost-effective, bespoke alternative to hyperscalers for their customers, as part of either a hybrid or multi-cloud strategy. With national and regional privacy laws changing and evolving all the time, xSPs need to position themselves as experts in the field and combine this knowledge with the best technology to create a robust and secure cloud stack.

S3 object storage from Cloudian is a great fit for sovereign clouds built on VMware Cloud because it's fully integrated, scalable, secure, and integrates with enhanced data protection solutions at a price point that enables MSPs the margin they need to compete with hyperscalers. By leveraging STaaS and BUaaS, even the smallest MSP can create viable, affordable sovereign cloud offerings for its customers.

Supporting your journey to cloud

We've discussed the five things you need to know before establishing a sovereign cloud, but what are the next steps?

Finding the right partner to support sovereign cloud strategies is key to success. VMware and Cloudian meet all the sovereign cloud prerequisites described in this paper. xSPs can gain competitive advantage by helping customers take control of their data with comprehensive data sovereignty strategies and fully compliant sovereign clouds. We offer white-glove support for both hardware and software, and we have teams located around the globe to provide region-specific advice.

Our alliances with vendors such as AWS, VMware, and Veeam mean our scalable, S3-compatible object storage integrates seamlessly into the cloud stack, giving xSPs robust and reliable end-to-end solutions they can count on to grow with them in the future.

Learn more about Cloudian at cloudian.com

Cloudian, Inc. 177 Bovet Road, Suite 450, San Mateo, CA 94402
Tel: 1.650.227.2380 | Web: cloudian.com | Contact Cloudian