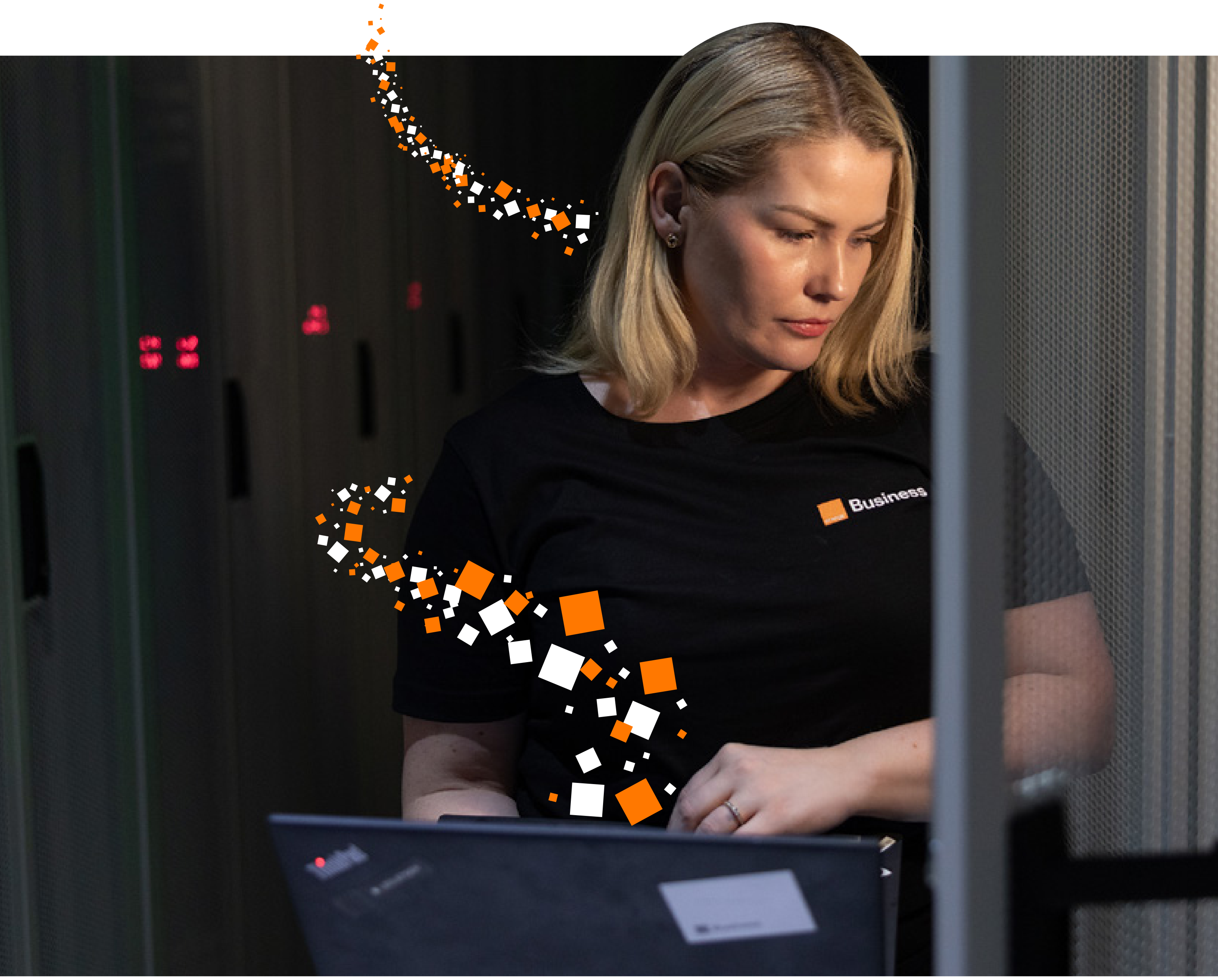
Digital Services



Sovereign Cloud

Everything you need to know about data sovereignty, local regulations and EU laws.

orange™ Business

Introduction

48%
of the respondents indicated that "data sovereignty and industry compliance had a major impact on discussions about their future IT architectures".

According to a survey from International Data Corporation (IDC), data sovereignty and compliance have become significant factors shaping the selection and design of IT decisions. Almost half of the respondents (48%) indicated that "data sovereignty and industry compliance had a major impact on discussions about their future IT architectures".

These days, technology is evolving faster than regulations — but it won't be that way forever. As data privacy regulations become stricter, it's important for companies to have future-proof data infrastructures that can adapt to whatever changes come their way.

This is why data sovereignty is so important in the strategic planning of IT infrastructures.

If you want to learn about data sovereignty, you've come to the right place. In this eBook we'll explore the concept of data sovereignty and explain why it's so crucial in a digital present (and future). We'll look at the EU's view on data sovereignty, the technical aspects that support it, global comparisons, and highlight some potential future trends and challenges within data sovereignty.

Our aim is to give you everything you need to know about data sovereignty, EU regulations, and future trends in data storage. So, with that said, let's get started.

Contents

04 About data sovereignty
06 The importance of data sovereignty
08 The European view on data sovereignty
10 Technologies behind data sovereignty

About data sovereignty

So, what does data sovereignty really mean?

Data sovereignty is about protecting the integrity and security of data while complying with the laws and regulations that apply. If a company or nation has data sovereignty, it means they have full control over their own data. They have the right to decide where their data is stored, how it is used, and who has access to it. Data sovereignty has evolved as a response to increased digitalization and globalization. As the world becomes increasingly digital and interconnected, the flow of data across international borders has intensified. This cross-border data flow poses a variety of challenges for both companies and countries, who realized they needed a strategy to manage their data in a way that protected their interests and sovereignty.

Standardization of data sovereignty

For companies, data sovereignty means that they must comply with the laws of the countries in which they operate. This can include regulations regarding data privacy, security, and storage. Companies need to develop data management strategies that not only respect the laws of each country but also protect their own business interests. This might involve decisions about where to store data physically and how to architect

their data systems to comply with different regulatory environments. For countries, the issue of data sovereignty is tied to national security, economic competitiveness, and the protection of citizen's rights. A country might enact data sovereignty laws to ensure that its citizens' data is stored within its borders, thus subject to its own privacy and protection laws. This can be seen to maintain control over its digital assets and safeguard against external influences or exploitation.

Data sovereignty has evolved as a response to increased digitalization and globalization.

The importance of data sovereignty

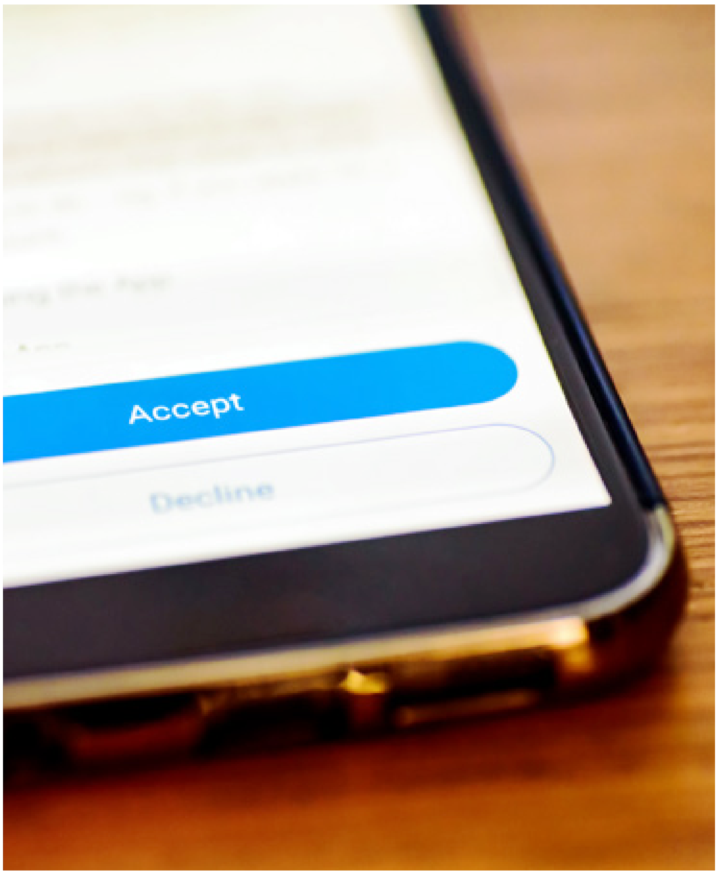
Now that we’ve briefly gone through what data sovereignty means, let’s talk about why it’s so important.

One of the most critical aspects of data sovereignty is data security.

Data sovereignty is central to protecting both the individual's and the organization's privacy and rights. As the use of personal and business-related data increases, actively ensuring the protection of this data from misuse or unauthorized distribution becomes crucial. By having control over their own data, organizations can ensure that it is used in accordance with their ethical and legal principles. Over 100 countries now have laws related to data sovereignty. These global regulations pose a significant challenge for companies operating across borders, as they must navigate and comply with a multitude of different data protection laws.

Security and compliance with data sovereignty

One of the most critical aspects of data sovereignty is data security. By implementing data sovereign cloud services and infrastructure, organizations can enhance the security of their data. This means that data is stored and managed in a way that aligns with the highest security standards, reducing the risk of data breaches and loss.
Data sovereignty also plays a crucial role in ensuring compliance with laws and regulations, such as the General Data Protection Regulation (GDPR) in the EU. These laws mandate organizations to safeguard personal data and adhere to strict data handling rules, making data sovereignty essential for avoiding costly fines and sanctions.



Practical management of data sovereignty

To manage data sovereignty effectively, companies and organizations need to make deliberate choices about the technology and infrastructure they use to store and manage their data securely. In the past, this has meant that on-prem logging services and security aspects have been important considerations when striving for data sovereignty.
But today's data lives in the cloud, which means cloud-based solutions that guarantee high security and compliance within certain jurisdictions are gaining importance. Sovereign cloud solutions are particularly attractive for organizations that want the flexibility and scalability of cloud services while meeting stringent data protection standards. These cloud solutions, equipped with strong security protocols and compliance mechanisms, provide companies with a means to handle data sovereignty complexity without sacrificing availability or performance.

Over
100
countries now have laws related to data sovereignty

The European view on data sovereignty

The European Union (EU) and European Economic Area (EEA) have unique views on data sovereignty that are embedded in their overarching data protection regulations and rules.

EU data protection laws

The EU has taken the lead globally by introducing some of the most comprehensive data protection laws, with GDPR as the flagship. This regulation plays a pivotal role in the concept of data sovereignty, ensuring that control over personal data remains within the hands of the individuals to whom it belongs.

GDPR

GDPR's primary objective is to fortify and unify personal data protection for all individuals within the EU. But this is not limited to the borders of the EU; any company that processes the data of EU residents must comply, making its reach truly global. The regulation empowers individuals with greater autonomy over their personal information. It mandates that organizations obtain explicit consent from individuals before collecting their data, and they must be clear about how this data will be used. And this consent must be as easy to withdraw as it is to give, ensuring individuals can easily reclaim control of their personal data.
GDPR is the beginning of a new era of corporate responsibility, where organizations are held accountable for the data they handle. Complying with GDPR requires meticulous data reporting and transparency, obligating companies to disclose data collection methods, processing practices, and sharing protocols with individuals and regulators. This transparency is essential because it allows individuals to understand how their data is being used and provides them with choices about its use.
In relation to data sovereignty, GDPR is a critical component. Data sovereignty is the concept that digital data is subject to the laws of the country in which it is located. GDPR ensures that the sovereignty of personal data is respected and maintained within the EU's jurisdiction. It also affects how data is transferred outside the EU, insisting on equivalent levels of protection to safeguard data as it crosses borders.

European Data Act - rules for a fair and innovative data economy

The European Union (EU) has initiated the rollout of new legislation, the EU Data Act (the Act). The Data Act, which came into force on January 11, 2024, is part of the EU's efforts to foster a more competitive and innovative data economy. With the enforcement date scheduled for September 2025, this regulation will have profound implications for businesses by influencing how they manage, share, and protect their personal and non-personal data. It is crucial for businesses to fully understand the Act's provisions to take proactive steps to ensure compliance and leverage new opportunities. The new rules define the rights to access and use data generated in the EU across all economic sectors and will make it easier to share data, in particular industrial data. The Data Act will ensure fairness in the digital environment by clarifying who can create value from data and under which conditions. It will also stimulate a competitive and innovative data market by unlocking industrial data, and by providing legal clarity as regards the use of data.

NIS 2

NIS 2, or the Network and Information Systems Directive 2, is a crucial aspect of the EU's view on data sovereignty. This legislation focuses on ensuring that member states have robust cybersecurity systems in place.

NIS 2 brings a proactive approach to supply chain security by addressing the heightened risk of cyberattacks through third-party services. It requires companies in essential sectors to not only fortify their own cyber defences but also to ensure that their suppliers comply with stringent cybersecurity standards. This directive is vital in safeguarding data sovereignty by preventing cyberattacks that could compromise the integrity and security of vital data infrastructures.

EU policies and initiatives

In addition to data protection laws and NIS 2, the EU has launched various policies and initiatives that bolster data sovereignty. These measures include guidelines on data sharing, regulations on data storage locations, and enforcement of rigorous security protocols for businesses. The overarching aim is to foster a secure and accountable digital ecosystem within the EU.

For businesses, these policies mean that they must engage actively in establishing secure data practices, thus reinforcing trust and integrity in the digital marketplace. These initiatives also position the EU as a leader in digital rights, setting a global standard for data sovereignty and cybersecurity.

Schrems II case

A significant milestone in the data protection domain is the Schrems II case. This legal case, involving Austrian Max Schrems and Facebook, had a profound impact on data protection and data sovereignty within the EU.

In July 2020, the EU Court of Justice decided that the Privacy Shield agreement, which previously regulated the transfer of personal data between the EU and the USA, was no longer valid. This decision was based on concerns that US authorities could have unrestricted access to European citizens' data without adequate guarantees for privacy and data protection.

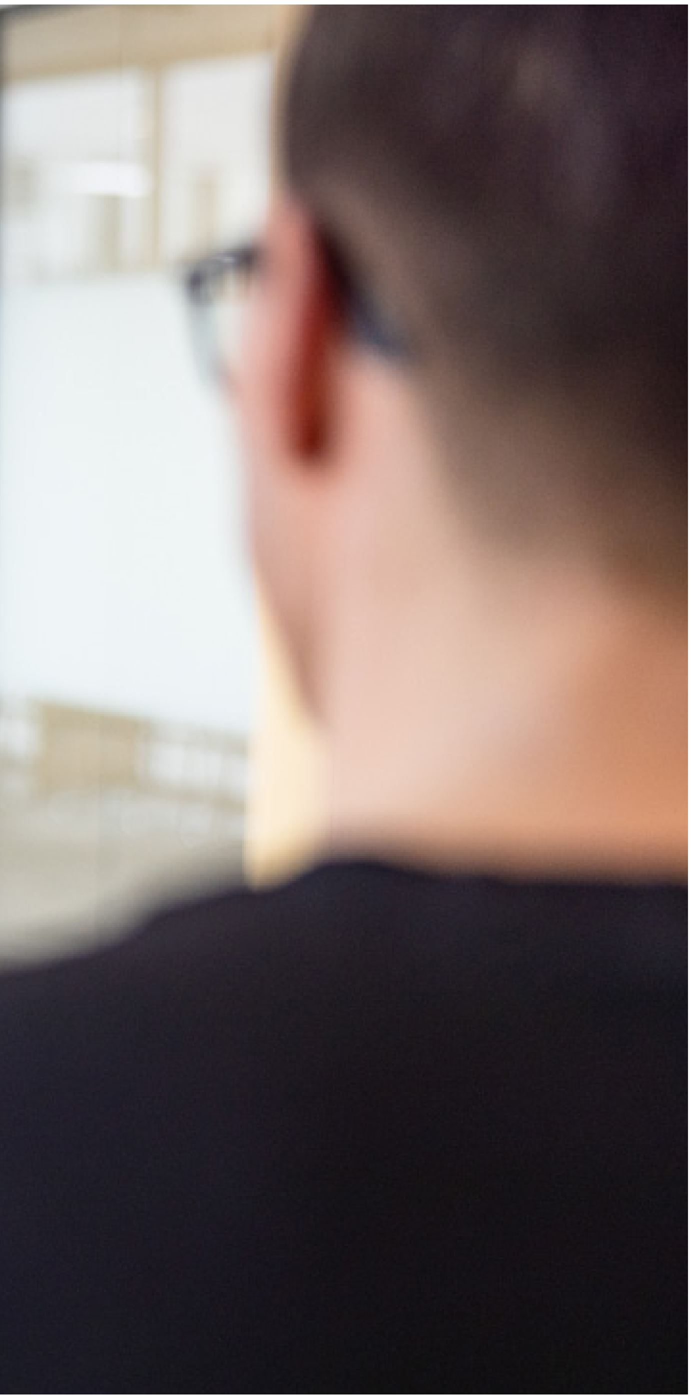
The Schrems II case emphasizes the necessity for data leaving the EU to meet GDPR's strict data protection criteria.

The verdict has forced organizations to review and modify how they transfer data, ensuring they follow EU laws. It has also sparked wider debates about international data transfer mechanisms and the need for strong data protection agreements in line with the EU's dedication to personal data security.

For companies, the Schrems II ruling highlights the importance of GDPR compliance and the risks of international data transfers. It affirms the EU's view that privacy and data protection are essential rights. Agreements on data transfer must respect these rights to preserve data sovereignty.

Technologies behind data sovereignty

In this chapter, we'll explore the technology and infrastructure that form the backbone of data sovereignty. We'll look at the tools, solutions, and strategies that empower organizations to uphold data sovereignty and security in a digital landscape.



01 Sovereign clouds

Sovereign clouds are a type of cloud service designed to meet specific legal, regulatory, or policy requirements related to data localization, sovereignty, and protection. They account for the need to store and manage data within specific jurisdictional boundaries.

Benefits of sovereign clouds:

- ✓ **Legal and geographic data localization:** Data is stored and managed within defined geographic boundaries, in compliance with local laws and regulations.
- ✓ **Customized data protection mechanisms:** Sovereign clouds offer tailored solutions to meet specific data protection and privacy requirements, including advanced encryption methods and strict access controls.
- ✓ **Regulation compliance:** These cloud services are designed to comply with strict data protection regulations such as GDPR, making them ideal for organizations needing to ensure full compliance.
- ✓ **Transparency and control:** Users gain increased transparency and control over where and how their data is stored and managed.

02

On-prem logging services

A key component in data sovereignty is the use of on-prem logging services. These services enable the collection, storage, and analysis of log data on-site, within the organization's own data centres or server environments. This is particularly important when the organization wants to have full control over its logs and avoid sharing sensitive information with third parties.

Benefits of on-prem logging services:

✓ **Full control:** You retain complete control over your logs and data, which is crucial for data sovereignty.

✓ **Security:** By keeping log data internally, you can ensure that sensitive information doesn't fall into the wrong hands.

✓ **Customization:** On-prem solutions can be tailored to your specific needs and requirements.

03

Data centres and private cloud

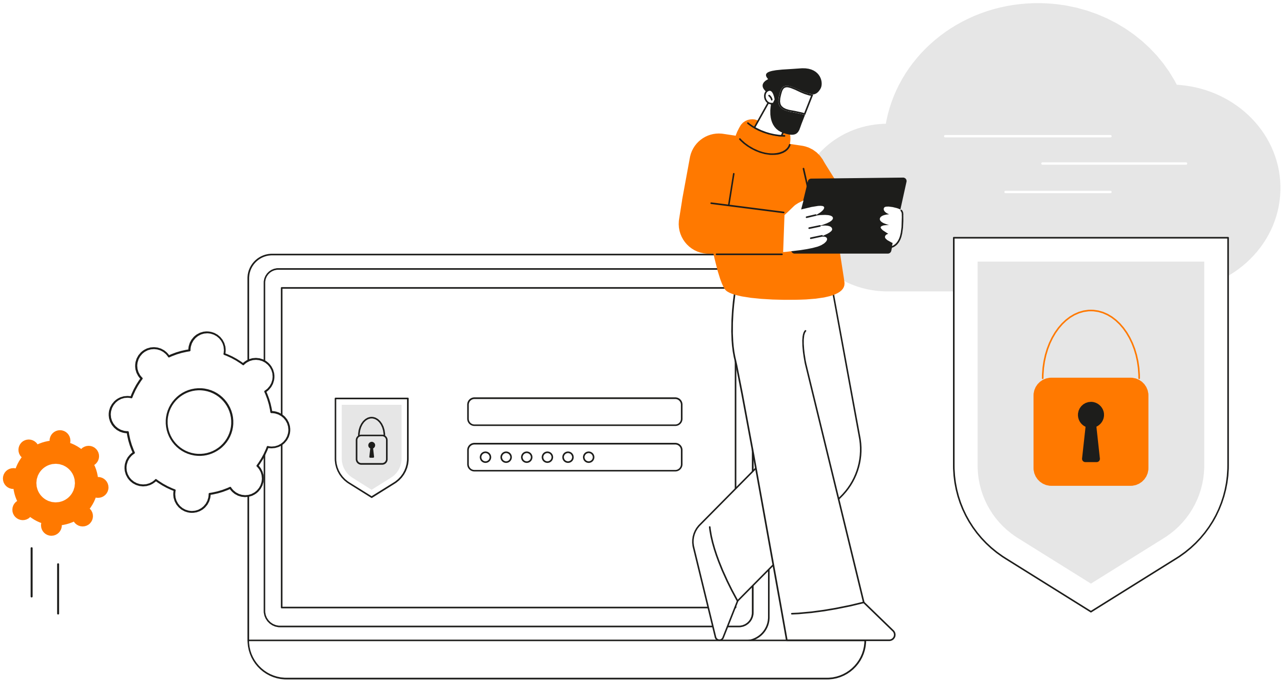
Data centres and private cloud services play a central role in ensuring data sovereignty. These infrastructures enable the storage and management of data in a secure manner and in compliance with the necessary regulations.

Key aspects of data centres and private cloud:

✓ **Security:** These environments are designed with a focus on security and the protection of sensitive information.

✓ **Physical availability:** Data centres and private cloud platforms provide strong redundancy/failover capabilities to guarantee consistent data and minimise downtime.

✓ **Compliance:** Using these infrastructures can help you meet the compliance requirements necessary within your industry and jurisdiction.



04

Security aspects

Security is a central aspect of data sovereignty. Protecting data against unauthorized access, data breaches, and other threats is of utmost importance. Here are some security aspects that organizations should consider regarding data sovereignty:

- ✓ **Encryption:** Use of strong encryption to protect data at rest and in transit.
- ✓ **Access control:** Limit access to data only to authorized users and systems.
- ✓ **Data backup:** Regular data backup and restoration to prevent loss.
- ✓ **Threat detection and prevention:** Implement systems and measures to detect and prevent threats in real time.
- ✓ **Education and awareness:** Encourage staff to be aware of security risks and educate them on best practices.

> **A strong technical foundation for data sovereignty requires integrating state-of-the-art security technologies, comprehensive policy enforcement, continuous monitoring and training, and strategic data governance mechanisms. With this foundation in place, you can not only defend against cyber threats but also foster a culture of data privacy and regulatory adherence.**

Conclusion

We hope that this e-book has provided you with new insights and knowledge about data sovereignty. Keep exploring the world of data sovereignty, and if you have any questions or want to know more, please contact us.

Orange Business Sovereign Cloud

As a leading player in digital transformation, data protection and data sovereignty, Orange Business understands the importance of local compliance. Our Sovereign Cloud service is designed to meet the needs of organizations striving to maintain control over their data while complying with local regulations and requirements. We have local control of all our data centres, meaning your data is always in compliance with local data regulations. customers have always demanded that their data stay locally.

With Orange Business Sovereign Cloud, you can securely store and manage your data while accessing powerful tools and services to optimize your operations. We continuously work to ensure that our service aligns with the latest laws and regulations, allowing you to focus on your business without compromising data sovereignty. Orange Business also provides a full range of managed services

Do you have any further questions?

Interested to learn how Orange Business can help your organization achieve secure and compliant data management? Contact us today for more information.

Digital Services

Digital Services is a business line within Orange Business, contributing to reliable and successful digital transformation for many organizations. Our joint mission is to help customers innovate and drive their business strategies in key digital domains, including Cloud, Customer Experience, Workspace, and Data & AI.
We assist them on their digital journey by providing advisory, end-to-end solutions, managed services, and professional services to ensure our customers' success. We are digital natives, with innovation at the core of our business, which makes us a reliable partner close to our customers, leading them in their digital transformation challenges.

We support a wide range of industries in the private sector as well as the public sector. We have built a significant level of experience and understanding over the last 30 years in industries like Finance, Insurance, Life Sciences, Healthcare, Manufacturing, Travel & Transportation, Retail, and the Public Sector.
As always with Orange Business, our customers trust us for delivering end-to-end, sovereign, and sustainable solutions to turn their Operational Experience, Employee Experience and Customer Experience into business value.

Find out more how we can help you with your projects on:

digital.orange-business.com

Follow us on

orange™ Business