



Digital Sovereignty

Adapting to a challenging
digital landscape

 tietoevry

This white paper, presented by Tietoevry, explores the increasingly important rise of digital sovereignty, and outlines several key steps that organizations and businesses can take to either embark on or gather momentum in their cloud journeys.



Contents

The path to digital sovereignty	3
Data Sovereignty	4
Sovereign Cloud	4
Overview of Digital Sovereignty, Data Sovereignty and Sovereign Cloud	4
Unpacking the emergence and relevance of digital sovereignty	5
Data is power, but extracting its full value is a challenge	5
Untangling the regulatory maze	7
Outlining the journey towards digital sovereignty	9
Sovereign cloud – the enabler for achieving Data Sovereignty	9
A roadmap to sovereign cloud – a step-by-step guide	11
The potential of Sovereign cloud in different industries	14
The road towards digital sovereignty starts now	15



The path to digital sovereignty

In a growing data economy where organizations are increasingly moving their business to the cloud and leveraging the full potential of data, there is a clear dilemma: How can you work collaboratively, grow, and innovate, within the global digital marketplace while complying with new and evolving regulations? It's in this context that digital sovereignty has gained powerful momentum. In fact, the idea of digital sovereignty, and the related topics of data sovereignty and sovereign cloud (as we shall soon see) have been around for a while. However, they have increased in both popularity and relevance through the rapidly growing amounts of data, challenging cybersecurity landscape, global political turmoil, and changes in international regulations of recent years.

So, what is digital sovereignty? In the digital economy, cloud services are becoming increasingly important

to be able to use, transfer and store data in a way that is safe and secure. In this emerging landscape, digital sovereignty is about how a state regulates and exercises control over the technology and services in use there. It's concerned with keeping sensitive data secure and enabling businesses, organizations, and individuals to enjoy greater autonomy over their digital assets and data. Simply put, it's about controlling where the data resides, where it flows, and who has control over it.

With the above information in mind, it's easy to see the broad societal implications and importance of digital sovereignty – and why organizations need to pay attention. Before digging even deeper into some of the underlying factors driving organizations to ensure their digital sovereignty, it's worthwhile taking a brief look at two related concepts: data sovereignty and sovereign cloud.

Data Sovereignty

Data Sovereignty relates to the rules and reference architectures that can help safeguard some of the fundamental principles of digital sovereignty:

- Data residency (where the data is stored),
- Data jurisdiction (who has legal control of the data)
- Data protection (the ability to store and process data in secure ways)
- Data independence and mobility (the ability to use, store and transfer data freely)
- Interoperability and portability (the ability to exchange and make use of data)

Sovereign Cloud

Sovereign Cloud can be seen as an enabler of data sovereignty. It's a set of new and dynamic cross-/multi-cloud solutions designed to answer to new sovereign policies, balancing collaboration with compliance, and bringing together insight, innovation, growth, and security.

Overview of Digital Sovereignty, Data Sovereignty and Sovereign Cloud

Digital Sovereignty		
Strategic initiatives and directions Control data assets and personal data Act independently in the digital world Access proactive mechanisms and offensive tools to foster digital innovation	Data Sovereignty	
	Key principles Data Residency Data Jurisdiction Data Protection Data Independency and Mobility Interoperability and Portability	Sovereign Cloud
Policies and Regulations from EU (e.g. EU Digital Strategy for Data, Digital Markets Act, Digital Services Act, Data Governance Act, Data Act, AI Act)	Rules and Reference Architecture (e.g. Gaia-X, certifications for specific countries and segments, ENISA Certification Schema, CISPE)	Enablement Improve security Improve compliance Improve control Become future proof Fuel innovation
		Different choices of sovereignty in a cross-cloud environment



Unpacking the emergence and relevance of digital sovereignty

Data is power, but extracting its full value is a challenge

The modern data economy is growing at a rapid pace. The EU Commission estimates that the volume of data produced in the world will increase from 33 zettabytes in 2018 to an expected 175 zettabytes in 2025. Every 18 months, the amount of data is doubling. At the same time, according to EU's estimates, the value of the data economy will increase to over €550 billion by 2025, representing 4% of the overall EU GDP.

This means that data is power – and that moving your business (or parts of your business) to the cloud has become imperative for both nations and organizations across different industries. Whether you're running a small e-com business working with a variety of customer data, or working in a multinational corporation tracking multiple sources of data, access to cloud-stored data

is increasingly important. The untapped potential of leveraging that data is staggering, with some estimates stating that 80% of all industrial data is never used. One of the reasons that organizations are not using, or getting the full value out, of their data is the digital security landscape that has emerged over the last ten years.

During that time, the challenge of where to store data and how to move it from one place to another securely – particularly across borders – has become increasingly critical. Over that same period, European organizations and businesses have been storing more and more data in cloud data centers, often provided by American tech giants such as Google, Microsoft, or Amazon, who dominate this space. Currently, no European player makes the global top 20 list of the most powerful tech companies – a data point that is supported by the fact that 92% of the data produced

in the Western Hemisphere is stored in the US. With the amount of metadata that the American cloud providers are collecting being much greater than many people realize (the collection is often automatic and may include data such as IP addresses, credentials, as well as logging and diagnostic reports) the question of how to store, transfer, and use data in safe and secure ways has never been more important. In addition, changes in the global political landscape as well as new security challenges such as an increase of cyberattacks, are also driving companies to bring their data “closer to home” to increase control and sovereignty.

The proliferation of data and the emergence of new cloud solutions in recent years have also increased the value and potential of technologies such as Artificial Intelligence (AI). While AI and other adjacent technologies have the power to help societies and organizations revolutionize the way they think, act, and work (e.g. through automation and smarter use of data), concerns have been raised about certain governments and organizations using AI systems for morally questionable aims. One such concern is the alleged use of AI technologies by certain authoritarian governments to pilot social scoring systems with the aim of implementing social control at scale, something that has come under intense scrutiny from both the EU and the US. Such movements have posed questions about how AI can be used to its full potential, while safeguarding the fundamental rights, security, and integrity of organizations and individuals. With data being the world’s most inexhaustible resource and the fundamental fuel for AI, the explosion of new AI systems has also led to an increased importance of ensuring the sovereignty of data. Both US and other global cloud players are active in developing new, emerging AI systems and technologies, while also having control over a multitude of data from many sources. As a consequence, it has become even more important for organizations to understand where their data is stored, how it flows, and who controls it.



As a response to the above forces, many countries and industries have already established new regulations that require companies to store, process, and manage data safely and responsibly in line with domestic law. EU regulations, such as GDPR, Data Act and Data Governance Act, are all meant to control, safeguard, and enable the flow of data across borders. In a similar vein, the emerging EU AI Act will create a set of rules for developing and using AI-driven products, services, and systems in the EU, and consequently will limit how data can be used by such technologies.

Given the drive towards increased integrity and privacy for both individuals and organizations of recent years, these developments are natural. Nevertheless, as we will soon see, parallel developments, not only in the EU but also in other parts of the world, have rendered the regulatory landscape more complex and difficult to navigate.

Before we dig deeper into how organizations can accelerate their cloud journeys while remaining digitally sovereign, we should take a closer look at the regulatory landscape and explore a few examples of the regulations and rules that are shaping the playing field in the digital economy.

Untangling the regulatory maze





The introduction of the **General Data Protection Regulation (GDPR)**, which came into effect in 2018, set-off a flurry of new EU-centered and cross-Atlantic regulations. Being the toughest privacy and security law in the world to date, the GDPR set a new precedent for data protection regulations and laws across the globe.

As a way to create an improved framework for securely transferring personal data from the EU to the US, the **EU-US Privacy Shield** came into effect in 2016. However, four years later, in 2020, the Court of Justice of the European Union (CJEU) declared the Privacy Shield invalid, due to concerns about the surveillance by US state and law enforcement agencies. This verdict later came to be colloquially known as Schrems II. **Schrems II** would have significant implications for the use of US cloud services and has irreversibly changed how companies and legislators approach data transfers and user privacy. In practice, the Schrems II ruling meant that customers of US cloud service providers must themselves verify the data protection laws of the

recipient country, document its risk assessment, and confer with its customers. In 2019, one year before the Schrems II ruling, US authorities introduced the **US Cloud Act**, which immediately came under intense scrutiny from organizations within the EU, since EU-based companies who are using a US cloud provider to store/manage their data would be legally obliged to share electronic data with US authorities in the event of a serious crime investigation in the US.

A way forward for cross-Atlantic regulations

As a consequence of the growing uncertainties surrounding the regulations intended to protect and bring legal certainty to data transfers across the Atlantic, the US and EU announced the ambition to update the Privacy Shield agreement in 2022. Based on the dependencies of global data transfers for enabling growth and innovation in both the EU and the US, solving these challenges is of high interest and importance for both parties. The new **EU-US Data Privacy Framework** is to be adopted by the EU commission, and is expected to be effective before the

Privacy and data protection	Rise of Digital Sovereignty	Regulations and frameworks	New juridical landscape
<p>2016–2019</p> <p>GDPR EU-US Privacy Shield US Cloud Act Schrems II (2020)</p> 	<p>2020–2021</p> <p>Digital Sovereignty for Europe 2020 EU Strategy for Data EU Digital Decade Strategy</p> 	<p>2022–2023</p> <p>EU-US Data Privacy Framework EU Governance Act EU Data Act EU Digital Services Act EU AI Act EU Digital Market Act EU Cybersecurity Act ENSIA Cloud Security Certification</p> 	<p>2024</p> <p>Regulations reviews and entrance into laws Sustainability regulations and standards</p> 

summer of 2023. The new framework will help ensure that sensitive and critical data is protected from misuse, and provide a trusted environment to enhance digital sovereignty for organizations in Europe and across the globe.

In parallel to developments of EU-US regulations, the EU has introduced a number of regulations to safeguard the digital landscape and promote the secure use and sharing of open data (such as industrial data) in Europe. In line with EU's overall European Strategy for Data, the **EU Data Governance Act** aims to increase trust in data sharing, strengthen mechanisms to increase data availability, and overcome technical obstacles to the reuse of data. While the Data Governance Regulation Act creates the processes and structures to facilitate data sharing, the **EU Data Act** clarifies who can create value from data and under which conditions. The Data Act ensures fairness by providing rules regarding the use of data generated by Internet of Things (IoT) devices.

With the increasing cybersecurity threats of recent years, the EU has also launched several regulations and initiatives to safeguard the security and privacy of EU citizens and organizations. The **EU Cybersecurity Act** is one such initiative. The act increased operational cooperation at EU level and supported the coordination of the EU in cases of large-scale cross-border cyberattacks and crises. In addition, the act introduced an EU-wide cybersecurity certification framework for ICT products, services, and processes.

As touched upon earlier, the proliferation of data and the increasing number of new AI systems have also given rise to new, emerging regulations. The main one is the much talked about **EU AI Act**. The goal of the AI Act, which is expected to be finalized this year, is to regulate AI applications and align them with EU's overall values and fundamental rights. The Act is also intended to be a predictive tool that allows both societies and businesses to continue to grow and innovate within the digital economy by reaping the full benefits of AI technologies, in ways that are safe and secure.

So, with this new-found knowledge of the regulatory landscape, you might ask: How should my organization act? How do we make sure that we can stay compliant with regulations while achieving the benefits of moving to the cloud? How can we become more digitally sovereign and what are the steps to get there? Thankfully, these are exactly the kind of questions we will delve deeper into in the coming chapter.



“ How can we continue to work collaboratively, to grow and to innovate, within a global digital marketplace while complying with new and evolving regulations?

Outlining the journey towards digital sovereignty

Sovereign cloud – the enabler for achieving data sovereignty

Given the regulatory landscape that we have painted above, the question that many CXOs, regardless of whether they're heading up an international bank or spearheading a public sector organization, will ask themselves is: How can we continue to work collaboratively, grow, and innovate, within a global digital marketplace while complying with new and evolving regulations? With the increasing importance of moving their business to the cloud while extracting the full value of data, many CXOs are under pressure to find solutions that can help improve competitiveness and deliver on business and growth goals, while also ensuring security, privacy and sovereignty of critical data. In this context, there are

a few key things to consider. As we have already seen, the emerging regulatory landscape has kept certain industries and companies from transitioning to the public cloud, since businesses and organizations would commonly have a hard time complying with regulatory demands. Thankfully, solutions are now being worked on to make it easier to exploit and unlock the full value of the increasing amounts of data, while adhering to the demands posed by various regulations. This is where sovereign cloud comes in.

As we saw earlier, sovereign cloud is one of the key enablers for becoming digitally sovereign. Sovereign cloud offers increased security, compliance, and control, and a means of future-proofing your business



Data residency

that the data is stored and processed on servers that physically reside inside the country of origin.



Data sovereignty

that the data is in compliance with privacy and integrity laws in the country of origin.



Jurisdictional control

that the data is under control by the laws of the country of origin and not by any other third-party country.

and driving innovation. Let's dig a bit deeper into what a sovereign cloud solution does, before outlining a number of key steps for organizations and businesses to accelerate their cloud journeys in a secure and sovereign way.

At the core, sovereign cloud is about protecting and unlocking the value of critical data. A sovereign cloud solution helps ensure that all data, including metadata, stays under one jurisdiction and prevents foreign access to data under all circumstances. Considering some of the challenges we have touched upon above, this is more important than ever before.

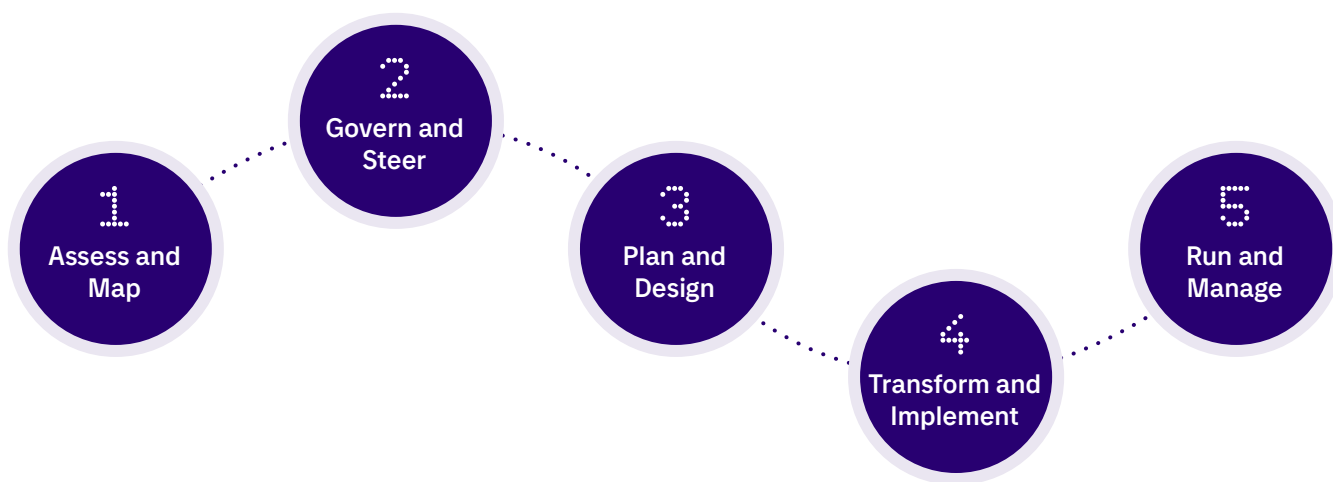
A sovereign cloud solution provides a trusted and secure environment for storing, processing and transferring data across borders in a safe manner. Sovereign clouds are mature and well-established solutions that are part of an emerging multi-cloud landscape. They also provide core benefits of cloud such as agility, security, and automation, by helping organizations and businesses put the right data, in the right cloud, with the right level of sovereignty.

A roadmap to sovereign cloud – a step-by-step guide

Sovereign cloud should be a core part of any multi-cloud strategy, intended to pair security and compliance with business growth and innovation.

Before outlining our step-by-step guide towards adopting a sovereign cloud solution, it's worth emphasizing that such a transition demands an understanding that

not all data is the same and that there are differences between clouds. The clouds have different values, and organizations should consider using their various strengths and capabilities, side-by-side, to reap the most benefits out of their data. So, to future-proof your business, your organization needs data classification and a multi-cloud strategy that can secure safe data flow across different environments and ensure business continuity. This strategy must comply with global, local, regional, and industry-level regulatory requirements.

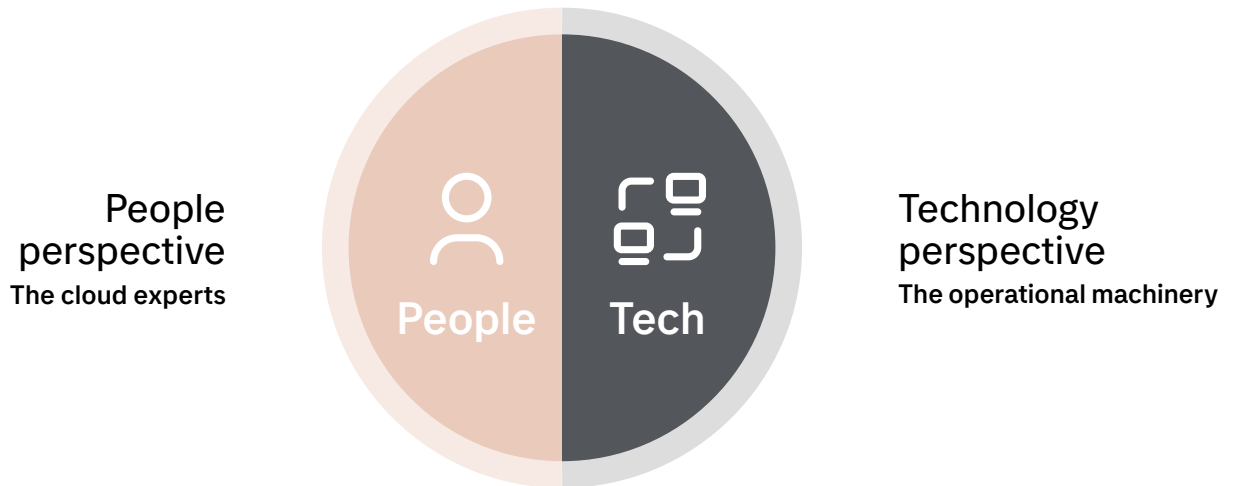


This journey toward sovereign cloud starts now. Here are a few key steps that organizations and businesses should consider to become more digitally sovereign.

- 1. Assess and Map** – A good first step is to classify your data and map the application usage of that data. In addition, assessing current data locations and applications. A few useful questions to ask are: How can our data be categorized? How and through what applications is our data used? Where is our data currently stored and where does it flow? Is any of our data transferred outside the EU?
- 2. Govern and Steer** – As a second step, you should create a Chief Data Privacy Officer role and set-up the right data governance and data policies, both organizational and technical, that will guide you going forward.
- 3. Plan and Design** – As a third step we suggest defining future data flows, data architecture and future infrastructure needs. Given our earlier data classification, how will that data flow going forward? What data architecture will allow us to reap the maximum benefits of our data, while ensuring security and sovereignty? What future infrastructure needs can we foresee?
- 4. Transform and Implement** – In the fourth step, it's time to execute on the planning of previous steps and deploy the right data and workloads in the Cloud.
- 5. Run and Manage** – The fifth and final step is all about running the sovereign cloud solution. To extract the maximum value of the solutions, it needs to be updated and new workloads need to be added to ensure efficiency and privacy, and unlock cloud innovation.

Tietoevry Sovereign cloud

A holistic solution leveraging people expertise and technological power



Tietoevry's sovereign cloud solution helps organizations and businesses put the right data in the right cloud with the right level of sovereignty, while getting access to the values from running their business on the cloud. All this is done in a simple, automated and industrialized way, using capabilities powered by both humans and technology – a symbiosis of people and machine. Let's have a closer look at how Tietoevry uses these two complementary strengths to deliver a holistic solution, and how it can help organizations and businesses through the roadmap sketched above.

People – The cloud experts

The expertise of people is at the center of any cloud journey, from the beginning to the very end, ensuring a simple and adequate design phase, a smooth migration, and regulatory compliance, while generating business value. At the beginning of the cloud journey, people and their knowledge are essential to evaluate the baseline. What are the key categories of data? Where, how and by whom is the data used? Those kinds of questions, although seemingly simple, require both knowledge and experience to properly address.

As the cloud journey moves into governance and steering, people are key to setting the right data governance structure and defining policies that will guide how organizations and businesses use the cloud. In this context, there is no one-size-fits-all solution, and it's important to understand the capabilities, needs, and goals of the organization in question.

In terms of planning and design, people's expertise is important to gauge what the future will look like. Through experience from multiple projects and scenarios, our people have the skills and abilities to define future data flows, set up a data architecture, and anticipate infrastructure needs relevant for the unique needs of each and every organization or business.

People are also essential to any successful migration to the cloud. A well thought-through plan and preparation are nothing without good execution. Also, people are essential to ensure continuous security and compliance monitoring while running the application in the cloud, also making sure that applications are kept up-to-date with the latest versions.

In short, people are the experts that make the cloud journey simple, helping businesses and organizations realize and maximize the value of their cloud journeys by setting transformation frameworks and best practices, being there to ensure a smooth migration to the cloud and adhering to the expectations on security and safety.

People are also an integral part of building and using technology in a purposeful and responsible way. Technology is a double-edged sword that can be used to do both good and bad, and that's why we rely on the experience and judgement of our people to help build, deliver, and run solutions in a way that's responsible for both customers and society.



Technology – The operational machinery

Our technology is what powers the sovereign cloud solution, complementing and amplifying the work done and experience held by people. Our technology not only represents the fundamental cloud infrastructure that allows the solution to run and function, it also includes the capabilities that enable the solution to be updated and new workloads to be added, while continuously ensuring efficiency and privacy.

The infrastructure part of our technology is the foundation for any cloud transformation, and usually comprises of a mix of Tietoevry's own cloud services together with clouds from hyperscalers, such as Microsoft, Google, and Amazon. In addition, it's usually a mix of private, hybrid and public clouds. On top of the cloud infrastructure, the sovereign cloud solution runs on a unified platform that simplifies operations and management of sovereign apps and data. The platform allows governance of a multi-cloud solution, capacity/workload management in real-time, and can help automate the entire IT landscape for an organization or business. Our customers can rest assured that the data and applications that reside on our sovereign cloud solution is always compliant and in line with regulatory requirements. If a specific data set needs to reside in a specific geographical location and be subject to locally

governing law, that data set will never be moved to a public cloud. However, not all data is created equally, and with our sovereign cloud solution you get the perfect mix of private cloud and public sovereign cloud capabilities, and any combination of them.

An important capability of a cloud platform is AI and Machine Learning. The benefits of AI and Machine Learning are many, but from an operational standpoint the increased operational efficiency enabled by predictive and dynamic insights with higher accuracy, faster decision-making, increased visibility and faster root-cause analysis, stands out.

As we have seen, the perspectives of people and technology complement each other. People are important for ensuring a smooth and successful cloud journey from start to finish, while the technology provides the technical foundation that allows business and organizations to run, manage and improve their cloud solutions.

Let's have a look at how the combination of people and technology can help organizations and businesses across different industries make the most out of their data and cloud journeys, while staying safe and secure – with the help of a sovereign cloud solution.

The potential of sovereign cloud in different industries

Public sector

Challenge

With continuous changes in regulation and the need for secure cloud services to keep sensitive national data in safe hands, public sector organizations have had a longer adaptation period to the usage of cloud.

Solution

With Tietoevry sovereign cloud, public organizations can start adapting most of their services into the cloud, ensuring compliance with regulations and standards while keeping the data safe with security clearances and under local jurisdiction.

Values

- Accelerate modernization
- Provide safe cloud applications and services to the public
- Avoid data governance breaches
- Simplify cloud operations, data control and compliance

Utility

Challenge

Providing secure utility services to the public while complying with ever-changing regulation demands is a burden. The nature of the sector, with its public origins, creates a slow modernization process with the unavailability of national and secure cloud services.

Solution

With Tietoevry sovereign cloud, utility companies can adapt most of their services into the cloud and develop new applications and services to optimize delivery and client experiences while ensuring simplified cloud management and regulation compliance.

Values

- Accelerate modernization
- Provide safe cloud applications and services to clients
- Avoid data governance breaches
- Simplify cloud operations, data control and compliance

Banking

Challenge

With banks being holders of a multitude of private information, privacy and security is essential for all banking systems. However, because of new regulations and growing cybercrime, adapting to the cloud and securing services is becoming increasingly challenging for the banking sector.

Solution

With Tietoevry sovereign cloud, the banking sector can breath easier with simpler cloud management and regulation compliance. Information is kept in secure and national data centers, ensuring sovereignty.

Values

- Pivot business value faster
- Ensure end-to-end trust with new services
- Avoid data governance breaches
- Simplify cloud operations, data control and compliance

SaaS

Challenge

Accessing customers in sectors such as banking, public and utility companies has always been tough for SaaS businesses, because compliance with both the standards of the customers and local regulations ever-changing nature is a difficult challenge.

Solution

With Tietoevry sovereign cloud, SaaS companies can start presenting their solutions to entities they have previously not been able to. New clients can enjoy the compliance sovereignty brings to the table.

Values

- Seamlessly integrate both public and sovereign cloud users into customer portfolio
- Provide secure services for existing clients
- Avoid data governance breaches
- Simplify cloud operations, data control and compliance

The road towards digital sovereignty starts now

As we saw in the previous chapter, the value of adopting a sovereign cloud solution can be considerable for organizations across different industries. Regardless of whether you're a global bank, a local public sector organization, a utility company, or a SaaS player, Tietoevry's Sovereign cloud solution can support different use cases and scenarios, depending on the level of sovereignty needed, allowing organizations to cope with the ever-changing regulations while boosting innovation and growth, and decreasing time-to-market for new cloud native services.

With the digital landscape becoming increasingly complex, moving your business to the cloud while leveraging the copious amounts of data is becoming increasingly important. Now is the time to update your cloud strategy to match the current regulatory maze. Making sovereign cloud a foundational part of that strategy will help accelerate your journey towards becoming digitally sovereign – and help you reap the full benefits of the cloud.

Digital Sovereignty and Sovereign Cloud pages

Learn more about digital sovereignty:
www.tietoevry.com/digitalsovereignty

Find out more about our sovereign cloud solution:
www.tietoevry.com/sovereigncloud

Overview of regulations mentioned (went into force)

GDPR (2018)
US Cloud Act (2019)
Schrems II (2020)
EU-US Data Privacy Framework (2022 – planned) – https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_7632
EU Data Governance Act (2022) – <https://digital-strategy.ec.europa.eu/en/policies/data-governance-act>
EU Data Act (2022) – <https://digital-strategy.ec.europa.eu/en/policies/data-act>
EU Cybersecurity Act (2022) – <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act>
EU AI Act – <https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence>

For the futures we know, and the ones yet to be discovered

Tietoevry creates purposeful technology that reinvents the world for good. We are a leading technology company with a strong Nordic heritage and global capabilities. Based on our core values of openness, trust and diversity, we work with our customers to develop digital futures where businesses, societies, and humanity thrive.

Our 24,000 experts globally specialize in cloud, data, and software, serving thousands of enterprise and public-sector customers in more than 90 countries. Tietoevry's annual turnover is approximately EUR 3 billion and the company's shares are listed on the NASDAQ exchange in Helsinki and Stockholm, as well as on Oslo Børs.

Contact us

Wenche Karlstad

Growth Partner Executive & Head of Digital
Sovereignty Initiatives
wenche.karlstad@tietoevry.com

Francisco Romero Gotor

Lead Service Owner, Sovereign Cloud
francisco.romerogotor@tietoevry.com

For more information, please visit
www.tietoevry.com/techservices

