



The Drive to Digital Sovereignty in Europe

A 10 point plan to realise success on the
world stage

Cementing Europe's place in the world means achieving an open, digitally-autonomous and sovereign economy. While growth, productivity and innovation are crucial to achieving this, realising the vision of becoming a powerhouse on tomorrow's world stage will be based on competition and the integrity of European data transparency.

Influencing sovereignty in Europe

It was the focus of our recent Sovereign Cloud Day. An event organised by VMware, hosted in Brussels and one that involved some of the most prominent and influential figures on the subject of European sovereignty. The event was attended by around 200 people in-person and an additional 200 participants joining virtually. The attendees comprised EU Delegates, Cloud Provider Partners, Customers, and Service Integrators, making it a diverse and influential gathering.

The event featured four notable keynote speakers. Pearse O'Donohue, Director, Future Networks, DG CONNECT, European Commission, opened the event and addressed the absence of a clear definition of sovereign cloud while emphasising the strong connection between data sovereignty and the EU's overall vision of genuine strategic autonomy. Carme Artigas Brugal, Secretary of State for Digitisation and Artificial Intelligence, Government of Spain touched on the importance of recognising that the issues at hand go beyond just cloud and data and Sylvain Rouri, Chief Sales Officer, OVHcloud, talked about the importance of understanding the underlying layers of technology. The keynotes were closed by Alfredo Nulli, Head of Portfolio – Innovation and Center of Excellence, TIM Enterprise, who discussed the challenges and objectives of designing a government-controlled cloud infrastructure.

The speakers collectively covered what the EU has experienced in recent years, the numerous challenges that have exposed vulnerabilities in IT infrastructure, particularly cloud, and the notion of a Sovereign Cloud. And while the individual perception of the Sovereign Cloud differed, all agreed that there hasn't been a more critical time to look at data security and privacy in the cloud, prompting the EU to seek greater control over its digital assets, with the main 10 takeaways summarised below.



A 10 point plan to realise success on the world stage

1. Make it easy for businesses to move to and between clouds

By the end of this year, the EU expects that cloud computing should be worth about [€560 billion](#) to the European economy. But nevertheless, in 2021 only [41% of EU businesses](#) were using the cloud, while an objective under the EU's [digital decade program](#) is to have 75% of all businesses by 2030 using cloud computing. The need to accelerate cloud adoption is clear but, in order to achieve this, it must be made easier for businesses to move to and between clouds.

Being locked into a multi-year contract with a cloud provider and not consuming resources in the way they anticipated, hampers the ability of the business to move quickly. Instead, organisations should be able to consume cloud at the right pace to meet their spend commitment, avoiding unnecessary expenditure and allowing them to tap into required data sets when needed. Organisations don't want to have to plan their entire cloud journey upfront; they want the freedom to adapt as their business needs evolve.

To achieve success, organisations must be able to take control of where their data resides - without compromising sovereignty or compliance, and the choice of providers to manage it. This means developing a simplified process for those who want to transition from on-premises to the cloud, especially for SMEs and businesses that don't necessarily have the resources to make the switch. Here, the technology industry should be setting the standard for others to follow. Failure to take any leap of faith will result in that €560bn opportunity going elsewhere.

2. Improve open interoperability standards

This needs to be backed with open interoperability standards on which a digital economy can be founded. Without this, there is no secure data exchange or the ability to monetise sovereign data. At the moment the EU is reluctant to regulate this and is, instead, looking to the ICT industry to evolve standards that have worked on in the past. However, Pearse O'Donohue made clear that if, for competitive advantage reasons, companies or sectors do not adhere to the expected standard, then the commission will intervene.

This is all underpinned by the [Interoperable Europe Act](#), which was published in November 2022 and designed to substantially reinforce cooperation around interoperability among public administrations in the EU. This is a critical development and its enactment needs accelerating because the range of benefits from improved interoperability and public sector cooperation is extensive: There is an obvious reduction in cost, time, energy and unnecessary administrative burden for citizens, businesses and the public sector itself. Indeed, a 2022 study by the [Joint Research Centre](#) estimates annual cost-savings credited to cross-border interoperability range between €5.5 and €6.3 million for citizens and between €5.7 and €19.2 billion for businesses.

3. Insist on data localisation

There are countries, like China and the US, who operate large cloud solutions under their legal jurisdiction, wherever they are located in the world and can demand to have access to data - in some cases without even going through the mutual assistance facilities which exist between countries. It is that situation which means that we need to be assertive and lead the European Union to insist on data localisation, where there is a guarantee that that data cannot be subject to extra territorial legislation.

For instance, the [Data Governance Act](#) requires data intermediaries to take all reasonable measures to prevent the international transfer or governmental access to non-personal data held in the EU that could create conflict with EU or national law. The reasoning behind these measures is not meant to be punitive but to ensure that the rigorous rules that the EU is putting in place to create a marketplace for industrial data cannot be bypassed simply by residing outside the bloc.

4. Achieve operational autonomy

The ambition of the EU is to achieve an open but autonomous cloud market, which means data should be stored and processed in the European Union under the principles, values and norms of the region. We have seen an evolution in offerings from the big technology providers, ensuring the development of commercial solutions in response to European aspirations. However, only European data that is located and processed in data centres located in Europe and managed by national citizens will deliver operational autonomy.

If Europe is to secure a flourishing business sector, growing tax revenues, rising prosperity, a functioning democracy and rule of law it will need decentralised digital technologies. It is why there has been [targeted funding](#) and support for developing technologies such as quantum computing, blockchain, human-centric artificial intelligence and secure cloud services hosted on European infrastructure - all of which will be the bedrock of a sovereign digital Europe.

5. Accelerate the adoption of edge

One of the strategic targets for the EU Digital Decade involves “10,000 climate-neutral, highly secure edge nodes to be deployed in the EU, distributed in a way that will guarantee access to data services with low latency”. While an ambitious target, we must accelerate the adoption of edge to go further, faster because edge computing and sovereignty go hand in hand, as edge makes it easier to know where data resides and who governs it.

From autonomous vehicles to traffic management applications, edge computing solutions are considered one of the driving forces behind the fourth industrial revolution. However, in order to ensure successful implementation of edge computing in Europe, there are several key strategies to consider, including the creation of a set of unified standards that can be applied across different countries and organisations, and connectivity, which is paramount for a successful edge computing deployment where latency is a key factor to run the service and take decisions in real time. This means that businesses must invest in high-speed internet connections and deploy wireless networks to ensure that all parts of the edge computing system are connected.

6. Achieve consistency

Regulators, lawmakers, business decision makers, citizens all have different influencers and drivers - which means the journey to sovereign cloud is both long and nuanced. We have to learn and relearn how cloud legality works to remove confusion and ambiguity and encourage speed and simplicity. Even though there is consensus regarding the need for Europe to achieve a higher degree of technological autonomy and build its own independent future, member states have approached the idea of digital sovereignty differently and have abstained from defining its exact scope or premise.

In [Denmark](#), for instance, the debate has received little attention, which suggests a certain degree of scepticism regarding the value of approaching digital issues under the purview of digital sovereignty. On the other hand, [Estonia](#), mirroring its own success in the digital arena, appears to be more enthusiastic about the possibilities “digital sovereignty” offers in creating a fully digitally enabled nation. Finally, for [the Netherlands](#), digital sovereignty is reflective of wider security concerns in terms of national security and economic security.

7. Embrace open source

Against the hyperscalers in the cloud, open source can give Europe a chance to create and maintain its own, independent digital approach. This is because the concepts of open source and digital sovereignty are both based on freedom, choice and flexibility. Because open source technologies are available to anyone but owned exclusively by no-one, they guarantee the neutrality, fairness and transparency of the strategy for digital autonomy, a process of continuous innovation and the contribution to the development of skills vital for competitiveness, resilience and control in Europe.

The very nature of open source software means data can be shared between government agencies, citizens and businesses in a simple and reliable manner, which is a prerequisite for European sovereignty. As a result of this openness and transparency, those businesses or governments using open source software are better positioned to adopt emerging technologies more quickly and thus accelerate their competitiveness. Finally, the global nature of open source communities makes them resistant to geopolitical disruptions between different jurisdictions.

8. Clarity over the role of AI

Industry has responded to Artificial Intelligence (AI). Investments have increased dramatically and while it is not the be-all and end-all of the tech resurgence, because of its increasingly mainstream adoption, future-proofed decision-making will rely on clear guidelines over its usage and the data it learns from.

The EU has, in many ways, been a frontrunner in data regulation and AI governance. The [EU AI Act](#) establishes a set of rules for developing and using AI-driven products, services, and systems within the EU. The Act is modelled on a risk-based approach that moves from unacceptable risks (e.g., social credit scoring and use of facial recognition technologies for real-time monitoring of public spaces), to high risk (e.g., AI systems used in hiring and credit applications), to limited risk (e.g., a chatbot) to little or no risk (e.g., AI-enabled video games or spam filters). While AI systems that pose unacceptable risks are outrightly banned, high-risk systems will be subject to conformity assessments, including independent audits and new forms of oversight and control. Limited risk systems are subject to transparency obligations, such as user-facing information when interacting with a chatbot. In contrast, little or no risk systems remain unaffected by the AI Act.

The priority is to make sure that AI systems used in the EU are safe, transparent, traceable, non-discriminatory and environmentally friendly and that AI systems should be overseen by people, rather than by automation, to prevent harmful outcomes.

9. Get developers to understand data classification

We have to get developers to understand data classification – most developers, if not all, aren't engaged with privacy frameworks nor understand the classification of data consumed. Open Source products with default passwords still end up in production solutions and the market still has occasional traits of the Wild West we're looking to get away from. Ultimately, achieving sovereignty is predicted on flexibility, choice, control guardrails and security in the cloud and this needs to be baked-in at a developer level.

Companies must ensure their data classification strategy conforms to their internal data protection and handling practices and reflects industry standards and customer expectations. To enforce proper protocols and protect against data breaches, the protected data must be categorised and sorted according to the nature of its sensitivity. A recent [Forrester study](#) commissioned by Capital One confirmed getting this right remains an issue. In a survey of data management decision-makers, nearly 80% cited a lack of data cataloguing as a top challenge. Almost 75% saw a lack of data observability as a problem.

10. Act of the acts

We need a sovereign cloud capability as a landing spot for everyone to understand the EU legislations and acts and how they affect activity - both today and in the future. Right now, these evolving legislations are affecting cloud strategy and purchase decisions, which, in turn, is impacting business spend and investment. Europe needs the clarity and certainty of knowing what is coming and to create the capacity to prepare accordingly. The upcoming [Digital Product Passport](#) (DPP) is a good example.

Announced recently by Ilias Iakovidis, Adviser at DG CONNECT, European Commission, the DPP is a first-of-its-kind regulatory circularity tool to create transparency and unlock circularity within the EU by sharing product information across the entire value chain - everything from data on raw material extraction to production and recycling. Starting in agriculture and e-vehicles, the ambition is bold and should be commended as the need for sustainable production becomes clearer with each passing year. But the impact for businesses is going to be huge in terms of the data and information they'll need to process.

A cloud-smart strategy

The governance required to control data has to start now. If it does not, we will be behind in the blink of an eye because, according to [Statista](#), data is going to more than double in the next five years and there will be further challenges associated with where it comes from and how it is captured, processed, managed and monetised. All of which underlines the importance of organisations being 'cloud-smart' and working with, often, multiple cloud providers that negate getting locked-in or tied to things that potentially are going to cause problems in the future whether that's through regulation or simple repatriation.

A sovereign cloud framework isn't the end goal here. It is the starting point of a new digitally-based future for Europe that can unlock endless possibilities for businesses, citizens, governments and nations. However, while it must be built to capitalise on the opportunities in the future, it must also be reflective of the digital economy we are in today.

We must consider what is strategic for both the EU union and each independent nation to build a secure, trustworthy and resilient digital infrastructure that safeguards our data, protects our citizens and boosts our economy. Achieving this isn't for any one company or government to solve. Action needs to be taken from many players in the European ecosystem and there is much work to do in order to deliver digital sovereignty in Europe.

To visit [News & Stories](#) for more stories about Sovereign Cloud, [click here](#).

Find out more about VMware's Sovereign Cloud initiative, [click here](#).

Join our dedicated LinkedIn group to follow updates: [click here](#).

Find your closest Sovereign Cloud Service Provider: [click here](#).



