

**The first step towards  
digital sovereignty**



# Digital sovereignty to safeguard strategic autonomy

In today's digital world, organizations are increasingly dependent on non-European data services and technologies, for example by using public cloud services. Due to rising geopolitical tensions, this dependency entails certain risks. At the same time, this situation creates the momentum to invest in the development of innovative European alternatives that contribute to digital sovereignty in a sustainable manner.

## What is *digital sovereignty*?

There is no universally accepted definition of digital sovereignty in the market yet. KPMG's interpretation of digital sovereignty focuses on achieving and maintaining strategic autonomy and control over data, the applications in which it resides and the underlying IT infrastructure it is hosted on – aligned with legislation, regulations and geographical context. This includes everything from design and procurement to implementation and usage.

Digital sovereignty encompasses all aspects of data and technology, from the raw materials

used in technology to connectivity, cloud services and AI. It offers organizations a unique opportunity to gain full control and ownership over their own data and technology.

In recent times, various new legislation has been introduced to promote digital sovereignty within Europe. As a result, strategic autonomy and control over data and technology are becoming increasingly relevant.

This raises a crucial question for organizations: *to which degree do we need digital sovereignty?*



## The unique opportunity of *digital sovereignty*

The changing geopolitical context creates uncertainty, increasing the desire to reduce dependency on non-European technology and services. This does not mean that non-European technology or cloud services can no longer be used altogether, but it does emphasize that there is a need to act in a united and collective manner within the EU. More and more organizations are adapting their policies to prioritize the interpretation and realization of digital sovereignty.

This creates an opportunity for European organizations to deliver technology and services that provide autonomy, stability and resilience for vital infrastructures. They can meet the requirements to process and store data within European borders, by a European entity and within the European sphere of influence, thereby guaranteeing data privacy and accessibility.

The applicability of digital sovereignty applies to all components of the IT environment, from the raw materials of this technology to connectivity, cloud and AI. European IT services are still partly fragmented in this field. The way in which these components relate to each other can be seen as a 'technology Tetris'. The ongoing European initiatives are intended to create standardized architectures to connect these components to each other.

## The first step towards *digital sovereignty*

Organizations often look for a first step to materialize digital sovereignty.

This first step consists of gaining insight and overview: *which non-European suppliers and providers is the organization dependent on and how large are these dependencies?* Based on this, the risks of this dependency for the organization are mapped, also regarding legislation and regulation.

This is followed by answering the question: *how sovereign do you want to be?* – partly based on the organization's risk appetite. Consequently, a series of scenarios are developed in which alternative solutions are presented. These scenarios contain information on the possibility, probability and necessity of an exit from non-European suppliers. The preferred scenario forms the basis for determining the ambition and associated measures.

A next step is to implement the measures from the preferred scenario. These often consist of further detailing exit strategies and plans, and carrying out pilots with European (open-source) alternatives.

By taking these actions, organizations can take a first step towards digital sovereignty and seize the opportunities associated with it.



## Insight and overview



## Risk analysis



## Scenarios and measures



## Implementation and realization

# Contact

## More information?

Want to talk more about taking the first step towards digital sovereignty?  
Contact our experts:



**Deborah Hofland**

Partner Public Sector

[hofland.deborah@kpmg.nl](mailto:hofland.deborah@kpmg.nl)

+31 (0)70 338 2421



**Joost Groosman**

Partner Digital Transformation

[groosman.joost@kpmg.nl](mailto:groosman.joost@kpmg.nl)

+31 (0)20 656 8176



**Johan Noltes**

Senior Manager Digital Transformation

[noltes.johan@kpmg.nl](mailto:noltes.johan@kpmg.nl)

+31 (0)20 656 8012



[www.kpmg.nl](http://www.kpmg.nl)



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2025 KPMG Advisory N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee.

All rights reserved.