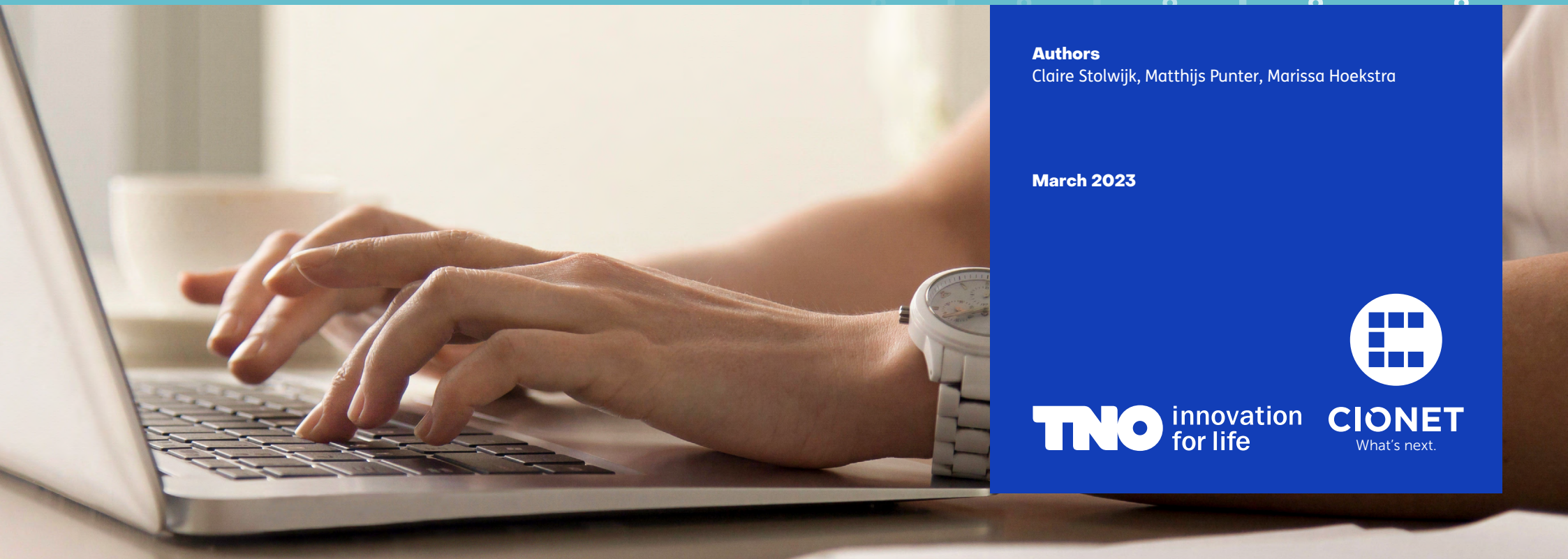
Paper

Digital sovereignty: How Europe takes back control

The opinion of European digital leaders



Authors
Claire Stolwijk, Matthijs Punter, Marissa Hoekstra

March 2023

TNO innovation for life

CIONET What's next.

1 Introduction

Literature defines digital sovereignty as *having control over the design and usage of digital systems*[1].

Data is become a primary resource of value in the emerging global digital economy. CIOs are helping their organisations and value chains to become digitalised and 'data-driven' as part of their digital transformation programme. Digitalisation and 'data-driven' approaches resulted in a lot of advantages such as improved digital cooperation, costs savings, more transparent and resilient value chains, new business models etc.

At the same time there are disadvantages and risks: companies are increasingly dependent on a limited number of Big Tech suppliers and geopolitical actors can (mis)use digital technology and data to gain power. Legal initiatives such as the US Cloud Act or the Chinese Surveillance Legislation that give access to European data abroad are a cause of concern.

A cyber arms race is ongoing using a wide range of techniques, from blunt nation-state cyber attacks on critical infrastructures to sophisticated social manipulation tactics.

To stimulate the advantages while mitigating the disadvantages and risks, European and national authorities clearly define and impose 'digital sovereignty' regulations, including severe penalties for non-compliant use of data.

To make Europe more digitally sovereign, initiatives such as the International Data Spaces (IDS) and Gaia-X have started the work on pan- European trusted data infrastructures. In addition, legislation was adopted by the European Union on topics such as digital platforms, data governance and AI.

But how is this all affecting individual companies? And how can CIOs make a difference?

We discussed this matter with 20 CIOs from 7 different European countries within the CIONET communities.

Most of them are working for private companies (61%) and some of them for public organisations (33%), the minority is active for public-private initiatives (6%) (see Table 1).

Descriptive statistics	
Number European countries involved in the study	7
Percentage of respondents that have digital sovereignty in their strategy	22%
Percentage of respondents that do not have digital sovereignty in their strategy	78%
Percentage of respondents from a public-private organisation	6%
Percentage of respondents from public organisations	33%
Percentage of respondents from private companies	61%

Table 1. Descriptive statistics.

1 Based on: https://www.uu.nl/sites/default/files/Moerel%2C%20Timmers%20%282.0%29%20-%20Preadvies%20Staatsrechtconferentie%202020.pdf.

2 State of play

The CIOs we interviewed view digital sovereignty most often from the perspective of data. In many cases they take the perspective of control over infrastructure. In some cases they take the perspective of strategic autonomy from vendors.

We expected that resilience (cybersecurity, business continuity, etc.) would be the main driver. In our interviews CIOs indicated that the added value of data sharing is actually the key driver for them.

Risk management remains however important. This was especially mentioned by public organisations and organisations in the financial sector. It was particularly important for organisations that are part of the European NIS-list working on critical physical infrastructures (such as ports, utilities, the energy sector etc.).

Although everyone indicated digital sovereignty is of high importance for the current and future digital strategy, the topic as such is for most organisations (over 75% of the organisations we interviewed) not yet an explicit part of their current strategic roadmaps.

3 Key findings

Key findings from discussions with the CIOs relate to:

- **The strategy for digital sovereignty is driven by the added-value of data**: when organisations have a digital sovereignty strategy, it is primarily driven by the added-value to the organisation.
- **Cloud technologies of hyperscalers are commonplace**: Most organisations are already using cloud technologies for line-of-business applications. Most of them are using hyperscaler-infrastructures for their move to the cloud. This goes hand in hand with the trend that more and more data will be shared within and between these organisations and put in the cloud.
- **Technical and cost concerns are currently driving cloud based digital infrastructures**: pragmatic technical and cost concerns are the main drivers of the current digital infrastructure set up for companies. This is often still a hybrid cloud approach, meaning that part of the data is stored in the cloud and part of it still resides on-premise or in private cloud environments. Many CIOs indicated that this will evolve as more critical and sensitive data will be put in the cloud in the future.
- **Limited assessment of new European legislation on data**: only a few CIOs we interviewed indicated that they had already performed an explicit assessment of new European legislation (such as the Data Act, Data Governance Act, Digital Service Act, ...). This is surprising as the impact can be similar to the introduction of GDPR, making it a compliance risk. In addition, new legislation on digital intermediaries and the mandatory provisioning of IoT-data can also provide new opportunities for the data economy as a whole and for individual companies.

4 How digital sovereignty can impact businesses

We asked CIOs about their main concerns regarding the potential lack of digital sovereignty and current European approaches that aim to address this. In the interviews the following topics were mentioned:

- **Span of control of CIOs for managing an increasingly complex digital landscape**: CIOs we interviewed raised concerns about the controllability of their digital landscape: the dependency on external infrastructures increases, data is shared between multiple stakeholders and at the same time data become more pervasive and critical to the business. This creates a more dynamic and complex situation, which can go beyond the current span of control of CIOs of individual companies.
- **Missing business opportunities as not all digital technologies have a global reach**: Global business coverage of organisations - especially for multinationals - often requires global reach of digital technologies. This is currently limiting the market potential of smaller (European) cloud and data sharing offerings. Currently only larger providers of digital technologies, with a similar multinational reach, can provide the required level of service.
- **Lock-in effects of new digital infrastructures**: CIOs worry that it is easy to get access to a certain cloud platform or supplier, but expensive and difficult to get out and move data from one supplier to another. There is a risk for future lock-ins. CIOs want to be able to make informed choices, facilitate transitions, migrations and maintain control when outsourcing their digital infrastructure and data sharing services.
- **CIOs regret there are no real European alternatives with a relevant scale yet**: Cloud solutions based on European initiatives, such as Gaia-X, still need to find their way to the market. For many applications there is no viable European cloud offering at the moment. CIOs indicated that they are following these developments with interest and that this position could change in the future.
- **Doing nothing is not an option**: some CIOs indicate that 'doing nothing' is simply not an option as it will have a negative impact on:
  - The earning power of their organisations – today.
  - The ability to stay innovative – affecting future earning power.
  - The wider impact that a lack of digital sovereignty will have on democratic and European norms and values, such as privacy. This is impacting corporate social responsibility in the digital realm.
- **New approaches are necessary to deal with the increasing complexity due to**:
  - New and increased legislation, as well as constant changes in international regulations. CIOs of large corporates have legal experts in-house, but many smaller organisations do not have this expertise and are expected to involve external experts.
  - Higher frequency of cyber-attacks, requiring dedicated specialist countermeasures.
  - Global geopolitical instability that plays an increasing role via digital technology, which is affecting companies as well.
  - The dependency on increasingly complex digital infrastructures which was mentioned before.

5 Solutions: finding an open approach to digital sovereignty

The value of data comes very often from sharing it: making it part of business processes, involving other partners having new algorithms, introducing new applications for the workforce, customers or suppliers, etc. Being sovereign in a walled-in garden is therefore not a realistic option for most CIOs.

This is also true on a European scale. It is recognised by the CIOs we interviewed that developing secure data-sharing infrastructures across Europe can restore Europe's digital sovereignty and boost European businesses. At the same time: digital 'walls around Europe' should be avoided too, since many organisations involved in our discussions need to be able to operate on a global level. The diversity amongst European countries can however influence the cooperative approach to come to a trusted data infrastructure (e.g. protectionists versus countries focusing on cooperation).

Developing the necessary technologies and having a leading legislative framework does however provide an opportunity for Europe to become a global hub for data sharing – similar to the effect that GDPR has had on privacy measures worldwide.

6 How to get there?

There is not one single solution, but various actions need to be taken by several stakeholders. Mitigating risks and grasping opportunities is important for long term digital sustainability.

For **CIOs** it is important to:

1. **Create a digital sovereignty strategy** based on the value of data to ensure:
   - Collection, sharing and usage of data within the organisation and with partners.
   - Sufficient protection of key data assets.
2. **Manage complexity** by:
   - Strengthening in-house capabilities.
   - Cooperation with other companies to handle the complexity.
3. **Assess the new opportunities that European digital legislation might bring**, but at the same time: check compliancy.
4. **Introduce a balanced cloud strategy**: that indicates which data can be shared through which cloud infrastructure based on:
   - Additional requirements for high-critical systems.
   - A multi-vendor strategy, as it is likely that a single-cloud-strategy is unsustainable in the long term (data sharing with third parties, mergers & acquisitions, legal requirements, etc.). A federated approach for cloud and data sharing could play a key role in such strategies.

For **policy makers**:
Some CIOs see policy makers as enablers and catalysts in strengthening the digital sovereignty of Europe.

They recommend the **EU to strengthen its digital sovereignty, but it must at the same time balance this with concerns for the values that underpin the Union and its businesses**. That will require a complex balancing act.

There is a potential to turn Europe into the 'Switzerland' for data sharing. Having a trusted internal data economy could turn Europe in a go-to place for data sharing and digital infrastructures: secure and trusted, enabling organisations to collaborate on a global scale.

Authors

Claire Stolwijk
Senior researcher & consultant

claire.stolwijk@tno.nl

Matthijs Punter
Senior researcher

matthijs.punter@tno.nl

Marissa Hoekstra
Researcher

marissa.hoekstra@tno.nl

TNO innovation for life

CIONET
What's next.

Context

This paper was written as part of the Digital sovereignty project of TNO. For this paper TNO and CIONET cooperated to conduct 20 interviews with CIOs from 7 European countries. CIONET is the community of CIOs, Digital Leaders and IT executives in Europe, UK, USA, Australia and LATAM.

Project number: 060.55452/01.01

tno.nl