

Ensuring the
Ability to Act:
*A Guide to Digital
Sovereignty*

BEST PRACTICE GUIDE

Opportunities and Dependencies: The Path to Digital Sovereignty in Switzerland	03
Seven Measures for Digital Independence in Your Company:	04
1. Open Source Alternatives	04
2. Technology Made in the EU	05
3. Data in the Cloud	06
4. OnPrem Instead of Cloud	07
5. Hold Partners Accountable	08
6. Develop Exit Strategies	09
7. Co-management and Diversification	10
Conclusion and Outlook	11
Contact	13

Opportunities and Dependencies: The Path to Digital Sovereignty

In our networked and data-driven world, digital sovereignty has evolved from a buzzword to a strategic success factor for companies. Close integration with partner companies, the use of cloud services, and data-based business models offer enormous opportunities. However, these must also be critically examined:



Foreign dependence

96% of EU companies rely on digital technologies and services from abroad – especially from the US and China¹



Supporters

84,4% of IT decision-makers favor European digital products for critical in-frastructures, but only 20% are in the process of switching²



Concrete strategy

Only 21% of companies have developed a concrete strategy for digital sovereignty³



Strategic goal

87% of companies see digital independence as a strategic goal, but 79% are critically dependent on a few, mostly non-European providers⁴

According to a study by adesso and the Handelsblatt Research Institute, a lack of skills, a shortage of skilled workers, and high costs are still slowing down the expansion of digital sovereignty in many places.³

Digital sovereignty is becoming increasingly important, especially in times of global uncertainty, growing cyber threats, and complex regulatory requirements.

Maintaining control over one's own information, infrastructure, and digital processes is crucial in order to avoid dependence on third-party providers, platforms, or geopolitical interests. The goal is to secure one's own ability to act, minimize risks, and remain competitive in the long term.



1 Digital Sovereignty 2025 | Study Report | Study 2025 | Bitkom e.V.

2 1753185101-myra-state-of-digital-sovereignty-2025.pdf

3 First „Digital Sovereignty Index“ from adesso shows: Four out of five companies without a strategy as a key topic of digitalization | Wirtschaft Digital BW

4 New Bitkom study on digital sovereignty

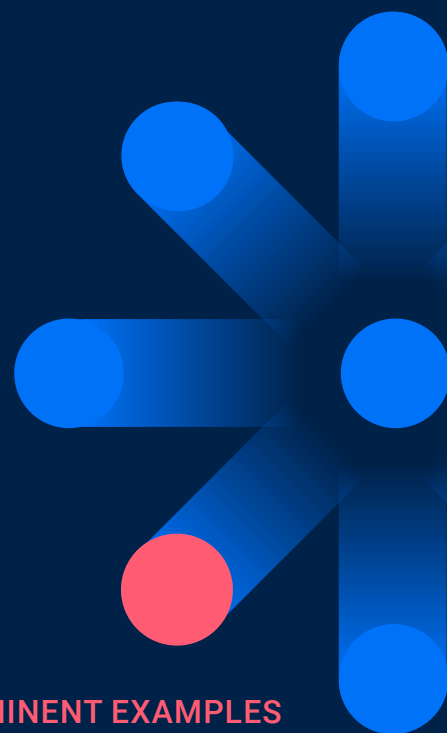
5 First „Digital Sovereignty Index“ from adesso shows: Four out of five companies without a strategy as a key topic of digitalization | Wirtschaft Digital BW

Seven Measures For Digital Independence in Your Company:

1. Open Source Alternatives

The lion's share of the software used in everyday office life comes from large corporations with sometimes one-sided and/or restrictive licensing models. Those who rely entirely on individual ecosystems (walled gardens) can very easily be pressured by these providers. You can avoid this by using free open source software:

- ✓ **Saves on licensing costs**
- ✓ **Avoids dependencies on individual manufacturers**
- ✓ **Is often more secure thanks to consistent review of the code base and improved traceability**
- ✓ **Offers support from large online communities**



PROMINENT EXAMPLES
of successful, professional open source solutions include Libre Office, GIMP image editing, Linux OS, Mozilla Firefox browser, and Thunderbird mail client.

2. Technology Made in the EU

Data sovereignty stands and falls with the jurisdiction of the technology partner. If a technology partner is forced by its government to hand over data, even the most securely worded contractual agreements won't help. The only thing that works here is choosing the right provider. The EU and its associated states have the world's strictest regulations in terms of:

- **Data protection**
(GDPR, TISAX, DORA)
- **Consumer protection**
(Digital Fairness Act, Digital Services Act)
- **Due diligence obligations**
(EU Data Act, EU Supply Chain Act, EU Due Diligence Act)

Software and services from EU countries are therefore generally a good investment for protecting your data and infrastructure when it comes to legal certainty and justiciability. This is particularly true when choosing a cloud provider. Even if the servers of the data centers are located in the EU, **the location of the company's headquarters is crucial.**



3. Data in the Cloud

Data storage in a cloud should not rely solely on security by the provider. Even those who only use cloud services within the EU with its strict data protection regulations should consider the following:

Encryption

Data security requires that even the cloud provider has no access to plain text data. Companies that encrypt data demonstrate responsibility and strengthen trust in their digital processes.



Deletion concepts

After termination of the contract, it must be ensured that your data has actually been deleted.



Approval concepts

The use of cloud services requires reliable and well-thought-out authorization and approval concepts. The principle of „as much as necessary, as little as possible“ applies here.



These measures already allow a certain degree of security and independence to be achieved.





4. OnPrem Instead of Cloud

Cloud services are particularly appealing due to their convenience and scalability. However, using them means entrusting your data to other companies. If you don't want that, you should consider returning to on-premises for the following advantages:

- ✓ **No third-party access to sensitive digital resources**
- ✓ **Often more cost-effective solution in the long term**
- ✓ **Faster problem solving by your own employees**



However, for on-premises solutions to be successful, companies must invest in the necessary expertise and technical equipment within their organization in good time.

5. Hold Partners Accountable

Digital sovereignty can only be achieved if companies not only secure their internal processes and systems, but also consistently hold partner companies accountable. Upstream and downstream technology and service partners play a crucial role in the processing of sensitive data and the provision of digital infrastructure. It is therefore essential to establish clear contractual regulations on data processing and storage as well as security standards.



Transparency

Demand complete transparency from your partners in this regard.



Disclosure

Insist on disclosure of subcontractors and their locations in order to identify and assess potential risks from foreign legal access – such as through the CLOUD Act or similar regulations – at an early stage.



Protection

Ensure that contractual agreements explicitly regulate protection against unauthorized access by third parties and stipulate binding mechanisms for information security, such as encryption and access controls.



Verification

Confirm contractually regular audits and certifications (e.g., ISO 27001) to verify compliance with the promised standards.



6. Develop Exit Strategies

Companies evolve, and it can happen that technology or service partners no longer meet your requirements for secure and legally compliant handling of your data. There are many reasons for this: changed business models, security incidents, lack of transparency, or even geopolitical developments. To remain able to act in such cases, it is advisable to identify alternatives for all business-critical systems and services at an early stage, as well as developing exit strategies.

The strategy should include clear processes and responsibilities so that a change can be implemented structured and with minimal disruption.



Task 1

Conduct regular inventories to check where in the company you use which services and what alternatives are available.

Task 2

Create a process that defines both the procedures for a service/technology change and the responsibilities.

Task 3

Set deadlines for data deletion by your previous partner and request proof of complete deletion.

7. Co-management and Diversification

Digital sovereignty means operating independently of individual software solutions. Therefore, companies should not allow themselves to become dependent on a single provider, but rather focus on diversification. Using several compatible systems simultaneously increases reliability and enables companies to remain operational in the event of disruptions or limitations of a single solution.

Co-management supports this approach through:

- **Simultaneous management across different platforms**
- **Flexibility in the IT infrastructure in accordance with the „best of breed“ concept**
- **Avoiding lock-in effects, i.e., dependence on individual manufacturers**

By combining diversification and co-management, companies retain control over their digital processes and can respond more quickly to changes, whether for technical, economic, or regulatory reasons.

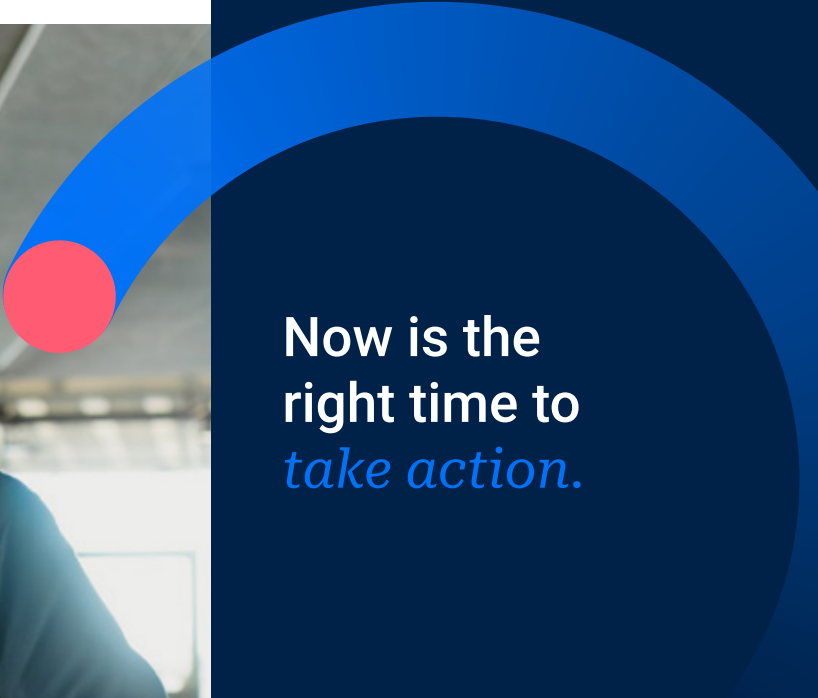


Conclusion and Outlook

Digital sovereignty is not a one-time project, but an ongoing process that requires strategic thinking, technological expertise, and organizational clarity. Companies that set the right course today will secure the independence and flexibility they need tomorrow to respond confidently to changing situations.



Review your existing digital dependencies, define clear goals for greater digital self-determination, and implement them consistently.



**Now is the
right time to
*take action.***

About baramundi software GmbH

baramundi software develops unified endpoint management for the central administration of PCs, mobile devices, and servers. It automates software distribution, simplifies patch management, and creates transparency in the network. baramundi thus makes a significant contribution to IT security and frees up resources.



Any Questions?

Feel free to make an appointment with us.

In a personal meeting, we will explain how baramundi software can help you achieve greater digital independence with its unified endpoint management solution.



Get in Touch.

*We look forward to
hearing from you!*



Making IT Admins Smile



baramundi software GmbH
Forschungsallee 3
86159 Augsburg, Germany
+49 821 56708-380
request@baramundi.com



+43 1 928 0136 0010
request@baramundi.com



+41 77 280 49 79
request@baramundi.com



+39 340 8861886
request-italia@baramundi.com



+48 735 91 44 54
request@baramundi.com



+44 2071 93 28 77
request@baramundi.com



baramundi software USA, Inc.
30 Speen St, Suite 501
Framingham, MA 01701, USA
+1 508 861 7561
requestUSA@baramundi.com



+49 821 56708-390
request@baramundi.com