EPiC Series in Computing

Volume 105, 2025, Pages 180–187

Proceedings of EUNIS 2024 annual congress in Athens

Digital Sovereignty – Results from the ZKI Survey in DACH

Malte Dreyer[1]
[1] Humboldt University
malte.dreyer@hu-berlin.de

Abstract

The annual ZKI top trends survey for 2024 had a focus on Digital Sovereignty (DS) and asked about the views on aspects of DS, Open-Source-Software, Clouds, Collaboration Structures and Security. This article illustrates the survey results and discusses key issues and outcomes.

1 Introduction

The Strategy and Organization working group of the ZKI Association conducts an annual survey on the most important topics and trends of IT institutions from universities and research institutes. The survey results are intended to help keep an eye on important developments, topics and best practices and to keep pace with the extensive topics of digitalization and the rapid renewal of technologies and also to gain suggestions for further development at one's own institution.

The core survey addresses the most important topics and changes in the survey year in a standardized form. In addition, individual focal points that concern many institutions are surveyed each year. For 2024, the focus questions were in the area of digital sovereignty:

- Questions on the dimensions of digital sovereignty and the role of Open-Source-Software, cloud services and partnerships.
- Issues relating to IT security and cyber-attacks.

The survey also asks about IT governance models and the CDO and CISO positions. It is completed by CIOs, data center managers, IT directors and people in similar roles. In 2024, 180 universities from Germany, Austria and Switzerland took part in the survey

R. Vogl, L. Desnos, J.-F. Desnos, S. Bolis, L. Merakos, G. Ferrell, E. Tsili and M. Roumeliotis (eds.), EUNIS 2024 (EPiC Series in Computing, vol. 105), pp. 180–187

2 Summary

The topic of "digital sovereignty" (DS) is becoming increasingly important for universities and research institutions due to the concentration of service provider structures, rising license costs, data protection and IT security considerations, changing and unpredictable framework conditions and sustainability aspects. The topic revolves around the question of the extent to which institutions can decide on the use of digital resources, data and infrastructures themselves or must accept changes from the market. For universities, digital sovereignty more specifically means the extent to which they can retain self-determination over their digital technologies, systems and data and thus maintain their freedom of teaching and research.

The German Council of Science and Humanities has also taken a position on the topic with its publication "Recommendations on the sovereignty and security of science in the digital space"* . In its recommendations, the Council assigns particular importance to the science system with regard to the promotion of digital sovereignty and recommends using existing competencies and cooperation structures in a targeted manner to increase digital sovereignty.

IT centers are required to interpret the topic of digital sovereignty for themselves and to derive concrete measures and develop strategies to promote a sustainable positioning of their service portfolio. The topic was discussed in the ZKI working group in 2023 and various dimensions were identified as to how the issues surrounding digital sovereignty influence the strategy and actions of IT centers† . This gave rise to the idea of selecting "Digital Sovereignty" as the focus topic for the upcoming Top Trends survey in order to gain a broader overview of how Digital Sovereignty is already being promoted at universities and which fields of action the topic is associated with.

The main questions on the topic of digital sovereignty in the survey were:

- In your opinion, what are the most important dimensions or areas of responsibility that make up the "digital sovereignty" of your university?
- What role do open-source technologies play in your efforts to achieve digital sovereignty?
- What role do cloud services and infrastructures outside your organization play in implementing your digital sovereignty strategy, and how do you secure them?
- What partnerships and collaborations does your institution maintain with other universities or research institutions to strengthen digital sovereignty?
- What measures has your organization taken to ensure the security and integrity of its IT infrastructure?
- According to which standard is the information security management system ISMS developed at your institution?
- Have you integrated a service provider for incident response?
- How do you assess the risk of cyberattacks on your facility?

Summary of the answers

The answers show how complex the topic of digital sovereignty is and they illustrate that extensive activities already exist at universities. Particularly noteworthy here are the far-reaching collaborations at all levels, not only at the level of service provision, but also in the cooperation for the development of topics, for support services and for platforms for direct exchange. In addition to answers on specific operating models, such as on-premises, university clouds, external clouds or SaaS, the location of operations within Germany or Europe is listed as a core criterion in connection with data protection

* German Council of Science and Humanities (2023): Recommendations on the sovereignty and security of science in the digital space; Cologne. https://doi.org/10.57674/m6pk-dt95

† Examples of aspects of DS that are often not directly assigned to the topic are rental licenses for access points or storage solutions as well as demands for standardized interfaces in the area of classroom technology.

challenges. A focus on contract design with external service providers, exit strategies, multi-vendor approaches and the need for open interfaces are also frequently mentioned.

The results show that there is a very differentiated and reflective attitude towards the use of cloud services. This complex of issues goes hand in hand with transparent control over the decision-making process for the use of software and the procurement of licenses in line with policies. A close connection with the accessibility and introduction of innovative technologies is also frequently mentioned, which would otherwise not be feasible for many universities due to the shortage of staff and specialists. There is a clear desideratum here for additional collaborative approaches in order to make such innovative topics available to more universities, at least in cooperation between universities, within the framework of alliances or in working groups.

In addition to the operating and contracting forms, there are many mentions aimed at establishing alternatives for existing products. Open-source policies are a frequently described approach for resolving vendor lock-ins or avoiding them in the future. The vast majority of responses give open-source software (OSS) a major role or have established an open source first policy. In addition to technological independence, the greater flexibility and adaptability of open-source approaches are also emphasized. In contrast, acceptance problems are also mentioned when using OSS.

Last but not least, the demand for data sovereignty also relates to the data security of their own infrastructure, meaning that IT security issues are a necessary prerequisite for the digital sovereignty of the institutions. In this context, most responses describe increased activities for the development of an ISMS (Information Security Management System) and BCM (Business Continuity Management) or the development of in-house personnel capacities and the involvement of external services for these purposes. These change processes are accompanied by extensive technical measures, e.g. in the areas of identity and access management, network security and securing the basic infrastructure for virtualization.

In this area, cost considerations are also increasingly mentioned as a motivation for committing to the topic of digital sovereignty in light of the lack of budget increases or even budget cuts. Conversely, this means that many universities also expect concrete cost benefits from a stronger commitment to digital sovereignty.

3 The Views on Digital Sovereignty

The question received 233 responses from 97 universities. The answers are distributed as follows.

Category	Number of mentions
On-premises operation	34
Open-source software	31
Establishment of alternatives	18
Exit contracts for cloud providers	11
Technological independence	10
Data sovereignty and data protection	9
Implementation of standards	9
Collaboration/cooperation	8
Operating models and data control	7
Cloud strategy	6
Software strategy	5
In-house development and innovation	5
Challenges during implementation	5
Digital skills and resources	4

This question reveals a complex and multifaceted perspective on digital sovereignty across several thematic areas, reflecting the challenges and strategies in a higher education context. In terms of operating models and data control, the focus is on avoiding vendor lock-ins, ensuring sovereignty over data, and establishing standards for the sovereignty of individual providers. This includes strategies for exiting contracts with cloud providers and ensuring data processing complies with EU and German regulations. The software strategy emphasizes the adoption of open-source software, fostering multi-vendor approaches, and strengthening open-source communities. Technological independence is another critical dimension, stressing the importance of reducing reliance on external providers and implementing standards to ensure technological self-reliance.

Other key areas include cloud strategies, which balances between cloud-based and local operations, advocates for open interfaces, and explores cross-university private clouds along with exit strategies for cloud providers. The enhancement of digital skills and resources is seen as vital, aiming to foster digital competencies among students and staff, explore alternative approaches to independence, standardize measures, and provide internal training. Implementation challenges, such as the difficulties of on-premises operations and the constraints posed by staff shortages or lack of operational alternatives, are also highlighted. Collaboration and cooperation are emphasized, focusing on partnerships with other universities and involvement in software selection and provider negotiations. Lastly, data security and protection are critical, with an emphasis on increasing security awareness among IT managers and addressing resource limitations, while in-house development and innovation focus on building internal development skills and considering in-house software solutions.

4 The Role of Open Source

There were 116 responses to this question from 98 universities, which can be broken down into the following categories.

Category	Quantity
Limited or subordinate role	16
Weighing up the advantages and disadvantages	15
Open-Source First	14
Flexibility and adaptability	14
Cost management and budget restrictions	12
Independence and avoidance of vendor lock-in	8
Professionalization and support	8
High priority and active use	6
Lack of use or acceptance	4
Security and compliance considerations	4
Specific areas of application	3
Complementary use to commercial software	3

The answers on the role of open-source technologies revealed a diverse range of perspectives and practices among institutions, reflecting the complex landscape of open-source integration in academia. Notably, many institutions adopted an "Open Source First" strategy, prioritizing open-source technologies in their operations and highlighting the flexibility arising from open-source. Many responses indicated a limited or subordinate role of open source, often attributed to resource limitations or a lack of expertise. In contrast, some responses showed a balanced view, weighing the pros and cons of open source versus proprietary software for individual applications.

Open source was also valued for providing independence from specific software vendors and as helpful for avoiding vendor lock-ins. Professional support for open-source technologies was another area of emphasis. However, there were also mentions of a lack of use or acceptance of open source, often due to insufficient staff or skills, and concerns regarding security and compliance. Specific areas of application for open source, such as web services or learning management systems, were highlighted, along with its complementary use alongside commercial software. The survey also uncovered differences between large and small universities; larger institutions emphasized the significant role of open source, historical importance, and increased support costs, whereas smaller universities focused more on cost aspects, security testing, and functionality versus maintenance costs. Specific projects and products like BigBlueButton, Bitwarden, BookStack, Docker, Linux, Nextcloud, OpenProject, OpenStack, Suricata, and Znuny/OTRS were mentioned, underlining the varied and practical applications of open-source technologies in university environments.

5 The Role of Cloud Services

There were 106 responses to this question from 88 universities with the following distribution.

Category	**Quantity**
Security & data protection challenges	13
Large roll	12
Irrelevant	8
Small roll	8
Increasingly important	7
Within the scope of cooperations	7
Contract management challenges	7
Enabling technology access	6
As part of a multi-cloud strategy	5
Solution approach for personnel & specialist shortage	5
Lack of awareness of the problem	4
Training & awareness	3
Enabling better service levels	2
Only with existing provider flexibility	2

A significant portion of responses highlighted security and data protection as major challenges in implementing cloud services. For many institutions, cloud services play a major role in their digital infrastructure and strategy, while for others, they are deemed irrelevant or play only a small, specific role. The growing importance of cloud services was also noted, indicating an increasing reliance on these technologies. The use of cloud services in the context of cooperations, particularly among universities, was highlighted, as well as challenges in contract management, including the complexity and difficulties involved.

Cloud services are also recognized for enabling access to advanced technologies and facilitating multi-cloud strategies involving several providers. They are seen as a solution to staff and specialist shortages in some cases, although there is also a noted lack of awareness of the problems and risks associated with their use. The need for training and awareness in cloud service usage was emphasized, along with the benefits of improved service quality and provider flexibility. Differences between larger and smaller universities were also observed; larger universities tend to focus on community cloud solutions, using services from major providers like AWS, Azure, Google, and DFN, as well as other universities. Smaller universities, on the other hand, emphasize scalability and availability, the need for

training and awareness, data protection issues, and the challenges associated with contract, cost, and support management. Despite the limited number of contracts for cloud services, these are highly relevant for the universities. Several specific products and organizations were mentioned in this context, including BigBlueButton, COSINEX procurement portal, DFN, FAUbox, iCAS, Jitsi, Microsoft 365, MATLAB, Microsoft Azure, Microsoft Exchange, Microsoft Sharepoint, Microsoft Teams, Overleaf, SAP, SWITCHcloud, VEEAM, and Zoom, underscoring the wide range of cloud services utilized in academic settings.

6 The Role of Cooperation and Collaboration

This question was answered by 89 universities with 111 responses. The answers can be categorized as follows.

Category	Quantity
Regional and nationwide cooperation	16
Participation in specialized alliances and projects	13
Cooperation in special areas	11
Membership in IT networks and associations	10
Specific university partnerships	10
Regular exchange and coordination	10
Cooperative software and infrastructure projects	10
No partnerships or cooperations	9
Informal exchange of experience and personal contacts	9
Formation and use of cooperatives and associations	7
Use of shared resources	6
International and national trade associations and initiatives	6
Initiatives for digital research infrastructure	6
Exchange of cloud and IT services	5
Cooperation in the field of high-performance computing	4
Cooperation for emergency and crisis situations	4

Collaborations can be broadly categorized into regional and nationwide cooperations, focusing on specific geographic areas. Participation in specialized alliances and projects is also prominent, involving specific goals or themes such as IT security or research information systems. Additionally, memberships in IT networks and associations, like ZKI, DFN, and OSBA, indicate an institutional commitment to being part of larger digital and IT communities.

Specific university partnerships are mentioned, highlighting bilateral collaborations, while regular exchange and coordination between institutions underpin many of these relationships. Cooperative software and infrastructure projects are a significant category, demonstrating collaborative efforts in technology development and infrastructure enhancement. Interestingly, some universities report having no relevant partnerships, suggesting a range of engagement levels across the academic spectrum. Informal exchanges and personal contacts also play a role, providing less structured but valuable opportunities for collaboration.

Further, the formation and use of cooperatives and associations are geared towards strengthening digital sovereignty, and the shared use of resources, like cross-university services for backup and cloud storage, underscores the practical benefits of collaboration. Involvement in international and national professional associations and initiatives, such as AcoNet and Gaia-X, extends the scope of collaboration

beyond national borders. Digital research infrastructure initiatives further emphasize the strategic importance of digital technologies in academic research. Exchanges of cloud and IT services, such as the DFN cloud, highlight the operational aspects of these partnerships.

Specific cooperations in high-performance computing show a focus on shared technological resources and expertise, while cooperation for emergency and crisis situations illustrates a proactive approach to managing unforeseen events. Notable mentions include ACOmarket, Bavarian Digital Network, BMBWF, CAMPUSonline, DFN Cloud, European University Alliances, GWDG, and the LRZ, each representing different facets of digital collaboration in the academic world. These varied partnerships and collaborations reflect a dynamic and interconnected academic environment, where shared knowledge, resources, and initiatives play a crucial role in advancing educational and research goals.

7 Measures to Ensure Security and Integrity

The question was answered by 86 universities with 133 responses.

Category	**Quantity**
IT management and governance	14
Personnel and resources	14
Firewall and network security	11
Emergency planning and response capability	8
Awareness and training	7
External services and partnerships	7
Security measures and audits	6
Authentication and access control	5
Compliance and standards	4
Virtualization and infrastructure management	2

A structured approach to IT security management is emphasized, with the establishment of an Information Security Management System (ISMS) and Business Continuity Management (BCM) being crucial. Compliance with governance measures is noted as vital for ensuring the stability and resilience of IT systems. In terms of personnel and resources, the development of specialized capacities for IT security and the promotion of IT security skills at all levels are recognized as necessary to address growing security challenges.

The survey also underscores the importance of firewall and network security, including the implementation of next-generation firewalls, advanced antivirus solutions, geoblocking, and web application firewalls (WAF), to strengthen defenses against network attacks. Contingency planning and response are crucial for efficient handling of security incidents, while awareness and training programs, such as phishing simulations, are essential to enhance the human aspect of cybersecurity.

Collaboration with external services and partnerships, like working with a Security Operations Center (SOC), is seen as beneficial for improving incident detection and response capabilities. Regular security audits, penetration tests, and vulnerability scans are fundamental for identifying and addressing security gaps. Authentication and access control methods, including multi-factor authentication (MFA) and two-factor authentication (2FA), alongside strong password policies, are effective in preventing unauthorized access. Compliance with security standards like ISO 27001 and BSI, and adherence to GDPR requirements, are also highlighted as best practices.

In terms of virtualization and infrastructure management, a potential switch from VMWare to alternatives like OpenStack, Proxmox, or Ceph is considered for cost advantages and flexibility. However, challenges in migration and compatibility issues are noted. Ensuring a hardened and redundant structure for all central IT resources is critical for operational security.

Several products and organizations are mentioned in relation to these themes, including DFN-Cert, eduroam, eduVPN, GrayLog Enterprise Security, Greenbone, ISO 27001, NIST, next-generation firewalls, Palo Alto, Proofpoint ET Pro Rule Set, Proxmox, Ceph, Semperi's Purple Knight, Sentinel One, Sophos, Suricata, VMWare, and Web Application Firewalls (WAF). These references indicate a wide range of tools and services utilized by universities to bolster their IT security and governance frameworks.

8 Author biographies

Malte Dreyer is the Director of the Computer and Media Service of Humboldt University Berlin, Germany. Within several major German, European and international projects he isactive in the areas of digital research infrastructure, research information, service management, cloud services, virtual research environments and software architecture across many scientific disciplines.

Providing advise on software architecture, he is a member of several technical boards. Malte Dreyer’s interests now are in the field of IT governance, information security management systems, scalable information management architectures and infrastructures in the intersection of organisational perspectives on ICT from data centres and information management organisations, both in the area of research infrastructure, as well as for digital learning architectures.