Towards an architecture framework for management platforms in the public sector
– Security considerations in times of transformation –

Nadine BAUMANN,
Substitute Professor Business Informatics with focus at digitalization in the public sector, RheinMain University of Applied Sciences, Wiesbaden, Germany
nadine.baumann@hs-rm.de

Christian SCHACHTNER,
Vice President Education and Sustainability, RheinMain University of Applied Sciences, Wiesbaden, Germany
christian.schachtner@hs-rm.de

Abstract

Objectives: This paper addresses the digital transformation of public administration in Germany, especially in the context of security aspects of digital transformation of public administration. The importance lies in the creation of flexible, secure, and collaborative structures that ensure both efficiency and data protection and promote a sustainable culture of innovation. **Prior Work**: The concept builds on international experience with platform architectures and leading practices from the private sector. The study by Doubrava and Sikes (2022) shows that the use of platform and cloud approaches in public administration is not yet widespread, although the ‘Government as a Platform’ model outlined by Tim O'Reilly (2011) promises considerable efficiency potential. The technical architecture is also based on established security standards (e.g. B. ISO 27001) and principles such as defence-in-depth and role-based access control. **Approach:**The survey was conducted analysing existing platform solutions in the public sector and comparing reference architectures in Switzerland. In addition, empirical experiences from pilot applications, in particular on workflow automation, data integration and user roles, were evaluated. The technical architecture was modelled iteratively based on practical examples and current security requirements. **Results:**The framework enables a clear separation between innovation space, operational data processing, and protected data management. In the open innovation area, employees and external partners can develop digital solutions collaboratively without access to sensitive data. The data plane ensures the integration and automation of processes through automated workflows, role-based access rights and connectors to specialist applications. The protected data centre ensures the secure processing and storage of application data in compliance with the highest data protection and compliance requirements. **Implications:** In terms of administrative practice, the framework means a significant reduction in media disruptions, scalability without infrastructure investments and a strengthening of employees' personal responsibility. Researchers will receive a blueprint for the development of secure, flexible platform architectures in the public sector. For decision-makers, architecture offers a way to reconcile innovation, data protection, and economic efficiency. **Value:**The contribution of the paper lies in the first systematic description and empirical validation of a three-part platform framework for public administration. The combination of an open innovation space, automated data level and protected data centre is new in this form and addresses the specific challenges of administrative digitalization. The framework provides a practical, scalable, and legally secure basis for sustainable digital transformation in the public sector.

Keywords: IT infrastructure framework, data security, platform economy.

1. Introduction

The digital transformation of public administration in Germany is facing enormous challenges, especially with regard to the implementation of the Online Access Act (OZG) and the associated end-to-end digitization of administrative processes. The need to create flexible, secure, and collaborative structures that promote efficiency, data protection, and a sustainable culture of innovation in equal measure is central to current debates [1].

While the private sector has been relying on platform architectures and cloud approaches for years, international comparisons show that public administration in Germany and other countries still has a lot to catch up on. The "Government as a Platform" model outlined by Tim O'Reilly [2] offers a promising framework to leverage efficiency potentials and fundamentally transforming administrative processes.

Challenges continue to exist in the data protection assessment of international cloud solutions (cf. Schrems II ruling) and in overcoming existing IT silos. However, the empirical examples show that a systematic platform approach can succeed in the sustainable digitization of administration. Consistent governance that addresses both technical and cultural aspects is crucial. The implementation of secure platform solutions requires the consideration of regulatory requirements such as the adequacy decision of the European Commission and the GDPR. The storage and processing of personal data has to be placed in countries with an adequate level of data protection. Technical measures such as encryption, two-factor authentication, and regular audits are just as important as organisational measures to raise awareness of data protection and IT security among employees [3].

This article highlights the state of research ("Prior Work") on administrative platforms, draws international comparisons, analyses leading practices from the private sector, and discusses technical and organisational challenges and solutions. A three-part framework for the technical architecture of platform solutions is proposed and discusses the security-relevant aspects as well as the importance of a co-developer culture [4].

2. State of research

The system landscapes in German law enforcement agencies are often characterized by local IT systems with rigid interfaces, which make it difficult to optimise business processes. In a European comparison, however, there are successful examples of efficiency gains through digitized administrative processes. International experience with platform architectures in administration has shaped the vision of a "data highway" for processing applications, and support from smart systems is increasingly coming into focus. At the same time, it becomes clear that platform approaches from the private sector, such as Microsoft Teams and the Power Platform, can serve as a model for public administration to establish innovative governance and an e-government ecosystem.

Tim O'Reilly [2] formed the concept of "Government as a Platform", which aims to provide modular, reusable IT building blocks for government agencies and citizens. The aim is to make administrative services more efficient, flexible and user-centric. Open interfaces, standardised data formats and a clear separation of basic infrastructure and specialist applications are intended to enable the development of an ecosystem that promotes innovation and facilitates cooperation between administration, business and civil society.

While countries such as Estonia or Denmark already established far-reaching platform approaches in administration, their prevalence in Germany and other EU countries is still low [1]. Success factors are in particular:

- central identity services (e.g. X-Road in Estonia)

- Open Standards and Interoperability
- cloud-based infrastructures with strict security and privacy requirements
- fostering developer ecosystems to expand and improve the platform

The technical architecture of modern management platforms bases on international security standards such as ISO 27001 and relies on principles such as defence-in-depth and role-based access control. Examples such as the SaaS solution "eGeKo" from Ategra AG in Switzerland show how high levels of security can be achieved through certified hosting, encrypted connections and two-factor authentication [5].

Challenges in the conceptual framework are the harmonisation of federal structures, the overcoming of data silos and the assurance of IT security and data protection. For the development of a framework for gov platforms, the following functional components are established concerning platform economy:

2.1 Data virtualization and integration

A central element of modern platform architectures is data virtualisation. It enables unified access to heterogeneous and distributed data sources without the need to physically migrate data. Technologies such as Microsoft Dataverse offer corresponding virtualization layers that can integrate both internal and external data sources. Data from systems such as MS Dynamics, SAP or Salesforce are integrated via standardised connectors and made available for applications on the platform [6].

The advantages of data virtualisation lie in the reduction of media disruptions, the simplification of data management, and the facilitation of real-time analyses. At the same time, the basis for data-driven automation and decision support is created. The availability of consistent, structured data is a prerequisite for the use of artificial intelligence (AI) and analytical methods to automate business processes. Research projects can investigate how smart systems provide decision support and automate routine tasks without compromising the control function of the administration [7].

2.2 Granular access control and compliance

Managing sensitive process data requires fine-grained access control. Role-Based Access Control (RBAC) is the dominant model here, assigning access rights based on roles and responsibilities [8]. The implementation is based on international standards such as ISO 27001 and the specifications of the German Federal Office for Information Security (BSI). This ensures that only authorized users have access to certain data and functions.

Gov platforms such as eGeKo from Switzerland also rely on two-factor authentication and certified hosting to ensure the highest security standards. Compliance with data protection regulations, especially in the context of international data transfers (e.g. according to Schrems II), is ensured through hosting in countries with an EU adequacy decision [9]

2.3 Automation and governance

The automation of data flows and processes is a central goal of modern platform architectures. Tools such as Microsoft Power Automate orchestrate ETL (Extract, Transform, Load) processes and integrate governance checks to ensure compliance [6]. Changes to processes are coordinated and implemented in a quality-assured manner via a central Centre of Excellence (CoE).

The platforms offer no-code and low-code editors that enable business users without coding knowledge to automate processes and design workflows. This promotes the enablement of employees and contributes to acceptance and motivation.

The challenges of data protection law, especially in light of Schrems II, offer a broad field of research. Solutions such as eGeKo, which ensure hosting and data backup according to European and Swiss standards (ISO 9001, ISO 27001), can serve as reference models for data protection-compliant platform architectures. Interoperability between different systems and compliance with international standards (z.B. ISO 15489 for records management) are other relevant research aspects [10]. Furthermore, there are proven security mechanisms in the platform architecture to prevent security breaches.

2.4. Zoned architecture according to PBMM standard

A central element for secure processing of sensitive data is the segmentation of IT infrastructure. The application of the PBMM (Protected B, Medium Integrity) standard leads to physical and logical separation of data and systems, so that particularly sensitive citizen data can be processed in isolation [11] The implementation is done dividing the data centre into different zones, each with different levels of security and access controls.

An example is the architecture of Microsoft Azure, in which data is stored in a so-called data lakehouse using network segmentation, role-based access control, and encryption [6]. Segmentation prevents compromised systems to access other zones, thus supports compliance with data protection regulations.

2.5 End-to-end encryption and key management

End-to-end encryption ensures that data is protected from unauthorized access during transmission and storage. Modern platform solutions rely on FIPS 140-2 certified encryption modules and hardware security modules (HSMs) for key management [8].

HSMs enable the secure generation, storage, and management of keys without them ever leaving the protected hardware area. This prevents both internal and external attacks on the key materials and is a key element for meeting compliance requirements such as GDPR and Schrems II [3].

2.6 Compliance-by-design and schrems II

The Schrems II judgement of the European Court of Justice has fundamentally changed the requirements for hosting and data transfer in public administration. Platform solutions now have to ensure that personal data is only stored in countries with an adequate level of data protection (European Commission, 2024).

Compliance-by-design means that these requirements are already taken into account during the architecture planning process. These include geo-redundant storage in certified EU or

Swiss data centres, as well as using encryption and role-based access controls [1]. The "eGeKo" product from Zurich-based Ategra AG, for example, offers encrypted connections, two-factor authentication, and hosting in accordance to ISO 9001:2015 and ISO 27001:2013 [5].

2.7 Platform architecture: From middleware to automation

Platform solutions rely on modular architectures that enable flexible integration of specialist applications and databases [2]. Standardised connectors can be used to connect different systems and consolidate data. Microsoft's Power Platform includes components such as Power Apps (no-code/low-code development), Power Automate (process automation), Power BI (data analytics), and Power Virtual Agents (chatbots). These building blocks enable even business users without coding knowledge to design and automate digital processes [7]. This relieves the burden off the IT department and strengthens the organization's ability to innovate.

2.8 SaaS solutions and workflow management

Software-as-a-Service (SaaS) solutions offer the advantage to not having to operate their own infrastructure and that updates, patches, and security measures are provided centrally by the provider [1]. Browser-based use allows location-independent collaboration and strengthens cross-organizational collaboration. Workflow engines enable the mapping and automation of business processes, including audit-proof archiving in accordance with ISO 15489. The integration of OCR engines and digital signatures accelerates processing and increases traceability [5].

3. Empirical methodology

Due to the different stages of implementation of existing solutions, a reference architecture platform from the Gov sector and an industrial solution such as the Microsoft Power Platform will be used to compare differences in terms of the compatibility of the performance of tasks of public services, in particular with regard to security risks. In the private sector, platform models such as Microsoft Teams and the Microsoft Power Platform have established themselves as central tools for digital transformation. These solutions offer:

- integration of various applications (Power Apps, Power Automate, Power BI, Power Virtual Agents)
- automation of routine processes
- no-code/low-code approaches to engage subject matter experts without coding knowledge
- central governance structures such as the Center of Excellence (CoE) for governance and quality assurance [7].

The Forrester Total Economic Impact Study™ [7] shows that a return on investment of up to 356% can be achieved by using such platforms, especially with digitizing paper-based processes and reducing media disruptions.

SaaS solutions such as "eGeKo" enable easy collaboration, central information overviews, and standardized workflows. Compliance with international security standards and the possibility of location-independent access to data and processes are decisive advantages. In addition, the possibility to develop one's own digital solutions promotes employee motivation and loyalty and creates incentives for disruptive innovations.

The first step of the science mapping method [12] is the definition of clear analysis goals and the development of a comparative framework that includes central comparison criteria and relevant metrics. These criteria are based on the specific requirements of the platform solutions and are organized in a comparison matrix to ensure a transparent and consistent assessment [12].

The survey began with a systematic analysis of existing platform solutions in the public sector. For this purpose, both proprietary and open source solutions used in German and Swiss authorities were considered. Particular attention was paid to the Microsoft Power Platform, which serves as a prominent example of the integration of workflow automation, data integration, and user role management [7].

In addition, reference architectures were compared, as they are established in Switzerland in particular. As an example, the SaaS solution "eGeKo" from Ategra AG was analysed, which convinces with its modular architecture, high data security standards (ISO 9001:2015, ISO 27001:2013), and flexible user management. The selection was made based on the criteria of interoperability, scalability, data security, and user-friendliness.

The descriptive analysis was supplemented by the evaluation of empirical experiences from pilot applications.

The focus was particularly on the following aspects:

- automation of routine processes (e.g. application processing, meeting management)
- integration of heterogeneous data sources
- implementation of differentiated user roles (incl. developer roles for process automation)
- evaluation of the effects on employee motivation and organizational culture

The data based on interviews with project managers, usage statistics, and feedback from user training.

The results are interpreted and critically discussed in relation to the research questions formulated at the beginning. Finally, implications for science and practice are derived and limitations of the study are reflected in order to ensure the comprehensibility and transferability of the findings. The technical architecture was modelled iteratively and practically. The starting point was the requirements from the analysed practical examples, especially with regard to security (e.g. two-factor authentication, encryption), data integration (e.g. connectors to specialist applications), and usability (no-code/low-code approaches). The modelling was carried out in close coordination with current regulatory requirements, especially in the area of data protection [3]

4. Results

The platforms examined enable extensive automation of business processes. The Microsoft Power Platform offers a comprehensive set of tools with Power Apps, Power Automate, and Power BI that supports both the development of custom applications and the integration of existing systems [7]. Similarly, "eGeKo" shows a high degree of flexibility in mapping workflows and the integration of external data sources.

A key finding is the importance of differentiated user roles. The successful introduction of administrative platforms requires a cultural change towards more openness, co-creation and personal responsibility. The training and empowerment of employees to actively shape digital solutions is of central importance here. In particular, the possibility of involving business users as "citizen developers" promotes innovation and personal responsibility [2].

The development of a co-developer culture in which employees can digitize and optimize their own processes is an important success factor for the sustainable digitization of administration. This helps to increase employee motivation and the formation of a co-developer culture. The integration of user feedback and the consideration of regulatory frameworks are crucial for the success of platform projects in the public sector. The promotion of a co-developer culture and the use of modern platform technologies can significantly accelerate the digital transformation of administration.

The following table grid shows strengths and weaknesses based on relevant comparison criteria:

Table. 1. Comparison Matrix Platform Solutions

Criterion	Microsoft Power Platform	Ategra eGeKo
Functionalities	general	domain-specific (public administration)
Usability	UX-Optimized (Mass Process)	user requests (paradigm: reduced to the max)
Integration	maximum	Minimum
Innovation	Adaptive portal framework for maximum data connectivity	Rigid portal frame with integrative import of third-party features
Co-developer culture	Community Developments	adaptive function configuration by authorized users

Source: Own Diagram

Despite technological advances, challenges remain. Particularly with regard to the data protection classification of cloud and platform services according to Schrems II [3] and the integration into existing authority structures [3].

Compliance with data protection requirements, particularly after the Schrems II judgement, remains a central challenge. Data hosting has to take place in secure third countries that have an adequacy decision from the EU Commission [9].

Both platforms examined meet high security standards. While the Power Platform relies on international certifications, "eGeKo" ensures compliance with European data protection requirements through hosting in Switzerland and regular audits. Nevertheless, the data protection assessment – with regard to cloud solutions from the USA – remains a challenge [1].

The scalability of platform solutions and the establishment of effective governance structures are other key factors. Virtual coordination offices such as a Center of Excellence can help to implement changes systematically and with quality assurance. Moving to SaaS models reduces capital costs and allows flexible scaling. The Forrester study puts the return on investment potential of the Power Platform at up to 356%, particularly when replacing paper-based processes [7]. "eGeKo" also offers cost transparency and predictability as an effect of its user-based pricing model.

The combination of an analysis of existing solutions, empirical evaluation, and iterative architecture modelling has proven to be an effective approach.

5. Development of a architecture framework

For research, the frameworks described above offer a blueprint for the development of secure, flexible, and interoperable platform architectures in the public sector. The integration of Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) opens up new fields of research on governance, privacy, and user adoption [1] The analysis of best practices from other European countries provides valuable insights for the further development of digital government platforms.

The surveys can be used to derive requirements for a networked way of working, which serves as a paradigm for action for a three-part framework for platform solutions.

5.1 Collaboration and innovation culture

Platform solutions enable not only internal, but also cross-organizational collaboration. The provision of central wikis, shared document repositories and workflow functionalities promotes collaboration between different actors. Promoting a co-developer culture in which employees implement their own process automation and exchange ideas in communities makes a significant contribution to a sustainable innovation culture [1].

5.2 Flexibility through modular platform architecture

Modern platform solutions such as the Microsoft Power Platform offer a modular architecture that enable to develop data-based applications in a modular system [7]. The integration of Power Apps, Dataverse, Power Automate, Power BI, and Power Virtual Agents creates a flexible environment where both business users and professional developers can design digital solutions. The use of no-code/low-code editors promotes employee ownership and enables rapid adaptation to changing requirements.

5.3 Security and data protection as a cornerstone

Data security and the protection of personal information are central requirements for any platform solution in public administration. The Schrems II judgement and the requirements of the GDPR require that data is stored in secure countries (BfDI, 2023). Solutions such as "eGeKo" from Ategra AG rely on encrypted connections, two-factor authentication, and certified hosting according to ISO 27001 to ensure the highest security standards. A Center of Excellence (CoE) can serve as a virtual coordination point to ensure interface governance for data delivery for digital transformation. Compliance with standards such as ISO 15489 for records management and regular security audits are essential to ensure trust and legal compliance.

In this respect, an architecture framework that distinguishes a clear distinction between innovation space, operational data processing and protected data management derives. In the open innovation area, employees and external partners can develop digital solutions collaboratively without access to sensitive data. The data plane ensures the integration and automation of processes through automated workflows, role-based access rights, and connectors to specialist applications. The protected data centre ensures the secure processing and storage of application data along with the highest data protection and compliance requirements.

The three layers of architecture integration are connected by the following components:

Table. 2. Technical components for the portal framework for the implementation of the architecture framework

Component	Function	Technical implementation
API-Gateway	controlled data exchange between levels	Azure API Management with OWASP-Checks
DevSecOps-Pipeline	Automated Security Testing	CI/CD-Integration of SAST/DAST-Tools
Audit-Logging	traceability of all transactions	SIEM solutions with 360° monitoring

Source: Own Diagram

The introduction of such platform architectures lead to increased efficiency, higher user satisfaction, and a strengthening of the culture of innovation. Through the clear separation of innovation space, operational data processing and data management, the presented framework provides performance provision for specialists in three central areas in a structured way.

5.4 Proposal of an architecture framework for Gov platforms

Thus, the framework enables the following request deployment as a Gov platform architecture:

Innovation space (enabling and co-developer culture)

The open innovation space serves as a collaborative environment in which administrative staff, IT experts, and external partners jointly develop digital solutions. In the open innovation area, employees can also develop digital solutions together with external partners. Access to sensitive data is explicitly excluded, which guarantees compliance with data protection regulations and still promotes creativity and collaboration. The ability to build digital applications in a modular way (e.g., via no-code/low-code editors) lowers barriers to entry and enables broad participation in innovation processes [7]. The promotion of a co-developer culture is essential in order to make digitization in the administration sustainable. No-code/low-code platforms enable subject matter experts to develop digital solutions on their own. This leads to higher motivation, innovative strength, and stronger employee loyalty to the organization.

Operational data processing (interoperability and data management)

The automated data plane forms the backbone of the framework. It ensures the integration and harmonsiation of data from different specialist procedures and external sources. Middleware solutions and connectors, such as those used in the Power Platform or SaaS solutions such as "eGeKo", enable seamless data processing and create the basis for AI-supported analyses and process automation [13]. The data plane is characterized by automated workflows, role-based access rights, and connectors to business applications. This ensures the integration and automation of processes, reduces media disruptions, and enables efficient processing of processes [1].

Harmonizing fragmented specialist applications through middleware solutions such as the Microsoft Power Platform or eGeKo leads to a significant acceleration of workflows. A central element of successful platforms is interoperability: standardized interfaces (APIs) and data formats enable the integration of various specialist procedures and external partners. Systems such as "eGeKo" also offer functions such as workflow management, document management in accordance with ISO 15489, and role-based access for internal and external stakeholders.

Protected data management (Center of Excellence)

The protected data center ensures the secure processing and storage of application data. The highest data protection and compliance requirements are met, for example through encrypted data transmission, certified hosting and regular security audits [5]; [9]. Separating sensitive data from innovation and development areas minimizes the risk of data breaches. The protected data center ensures data protection and information security according to the highest standards (z.B. ISO 27001). Personal data is stored and processed exclusively in countries with an adequate level of data protection (see EU adequacy decision). Certified hosting solutions and regular security audits are essential to meet the legal requirements and ensure the trust of citizens.

This architecture enables pilot projects to be scaled to productive systems while maintaining IT security – a critical success factor for the acceptance of digital government services. The presented framework creates significant added value for public administration:

- Increased efficiency: Automated processes and integrated data streams reduce processing times and sources of error. The introduction of platform architectures enables extensive automation of routine processes. Standardised workflows and digital file management (according to ISO 15489) lead to a reduction in processing times and sources of error. The Forrester Total Economic Impact Study (2023) puts the return on investment potential of the Microsoft Power Platform at up to 356%, especially when digitizing paper-based processes.

- Legal certainty: Legal risks are minimized through compliance with data protection standards and certified infrastructures. Virtual coordination offices such as a Center of Excellence (CoE) ensure the governance and quality of the digital transformation. They provide a framework for continuous improvement and the exchange of best practices. Integrating compliance and data protection requirements into the platform architecture ensures that innovation does not come at the expense of security [1].
- Scalability: The framework is flexible and can be adapted to different management sizes and requirements. SaaS solutions such as eGeKo enable flexible scaling of costs according to the number of users. Investments in infrastructure and maintenance are no longer necessary, which is particularly attractive for smaller authorities. Cost efficiency contributes to the acceptance and sustainable use of the platforms.
- Promoting innovation: Open innovation spaces and low-code/no-code tools enable employees to develop solutions independently. The platforms promote a culture of ‘enablement’: employees get the opportunity to digitize and automate processes on their own responsibility. This not only increases employee motivation and retention, but also promotes competition for the best solutions. The developer role for in-house process automation and the creation of virtual spaces for co-creation strengthen the innovation culture in the long term [2].
- Motivation and retention: The involvement of employees in process design promotes motivation and identification with the digital transformation. Central platforms offer all participants – internal and external – a uniform working environment with common wikis, document repositories and workflow functionalities. This promotes cross-organizational collaboration and creates a full overview of information. The ability to handle meeting management, application processing and communication digitally and securely significantly increases user satisfaction.

6. Conclusion

The digital transformation of public administration in Germany can only succeed if flexible, secure, and collaborative platform solutions are implemented that ensure both efficiency and data protection, and promote a sustainable culture of innovation. The presented framework offers a practice-oriented approach to the development of technical architectures that meet the specific requirements of public administration. The promotion of a co-developer culture and consistent compliance with security standards are key success factors. Hopefully, the implementation of the OZG Amendment Act will be further advanced through innovative platform solutions and an open culture of cooperation.

International research and practice show that platform architectures and cloud approaches offer considerable potential for the digitization of public administration. Success factors include consistent alignment with security and privacy standards, the promotion of interoperability and co-developer culture, and the adoption of best practices from the private sector. The challenges lie in particular in adapting legal frameworks, overcoming federal structures, and promoting cultural change. The vision of ‘Government as a Platform’ is ambitious, but achievable – provided that the administration uses existing international experience and establishes innovation-friendly governance.

The methodological approach, consisting of analysis, comparison, empirical evaluation, and iterative modelling provides a reliable basis for the development of sustainable platform solutions in the public sector. The examples examined show that technical innovation and organizational change need to go hand in hand in order to fully exploit the potential of digitalization.

Despite proven successes, challenges remain, especially in the area of data protection [3] and interoperability between different platforms. The consistent implementation of platform architectures requires not only technological but also organizational changes and continuous qualification of employees.

However, practical experience shows that the introduction of such frameworks leads to measurable efficiency gains, higher user satisfaction, and a sustainable strengthening of the innovation culture. Platform architectures thus make a decisive contribution to the successful digitization of public administration.

The three-part platform framework provides an innovative, empirically validated foundation for the digital transformation of public administration. It addresses key challenges such as efficiency, legal certainty, scalability, and the promotion of innovation. The combination of an open innovation space, automated data level and protected data centre creates sustainable ‘value’ that makes the administration ready for the future.

References

[1] C. Doubrava and V. Sikes, "Cloud-Paradigma in der öffentlichen Verwaltung," *Datenschutz und Datensicherheit - DuD,* vol. 46, no. 1, p. 605–610, 2022.

[2] T. O'Reilly, "Government as a Platform.," *Innovations: Technology, Governance, Globalization,* vol. 6, no. 1, pp. 13-40, 2011.

[3] Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI), "Datenübermittlungen in die USA und Schrems II Urteil," 2023.

[4] C. Schachtner, "On the way to resilient information security management: Business Continuity Management (BCM) for public institutions," *Smart Cities and Regional Development Journal (SCRD),* vol. 9, no. 1, pp. 17-15, 2025.

[5] C. Schachtner, "Besser zusammenarbeiten dank Plattformen," *Innovative Verwaltung,* vol. 46, pp. 43-45.

[6] Microsoft , "Secure a data lakehouse with Azure Synapse Analytics," *Azure Architecture Center,* 2024.

[7] Forrester, "The Total Economic Impact Of Freshworks Freshservice," 2023.

[8] Mercury Security, "Future Of Open Architecture," 2023.

[9] European Commission, "Adequacy decisions," 2024.

[10] D. M. Popa, "A technological and legal investigation into how smart states deploy collective intelligence for security and surveillance purposes," *Smart Cities and Regional Development Journal (SCRD),* vol. 9, no. 2, pp. 77-86, 2025.

[11] Government of Canada, "Data Centre Services Reference Architecture Document," *Shared Services Canada*, 2023.

[12] Appinio Research, "Comparative Analysis: Implementation & Practical Examples," 2024.

[13] O. A. Sarcea, "AI & Cybersecurity – connection, impacts, way ahead," *Machine Intelligence & Security for Smart Cities*, vol. 1, pp. 17-26, 2024.

[14] "Besser zusammenarbeiten dank Plattformen," *Innovative Verwaltung*, 2024.