

Modern colocation can meet the demands of digital transformation in the public sector

Digitalization in the public sector brings extraordinary demands: maximum security, maximum availability, scalable IT capacities, sustainability and data sovereignty within the national legal framework. This is precisely where colocation data centers come in and provide a solution.

The German Federal Cabinet recently adopted a groundbreaking document: the National Data Center Strategy. The message is clear. Comprehensive digitalization and sufficient data center capacities are fundamental prerequisites for a future-proof and competitive economy and a modern public administration. The document sets concrete goals: By 2030, at a minimum, data center capacities in Germany are to double and those for high-performance computing (HPC) and artificial intelligence are to at least quadruple: And for good reason.

AI as a Growth Driver

According to Bitkom, the total capacity of local data centers already rose to 2,980 megawatts by 2025 – an increase of nine percent compared to the previous year. However, this is far from sufficient. The main drivers of this development are cloud and AI applications as they significantly increase computing and storage requirements.

What exactly does this mean for the public sector? E-government solutions, cloud services and especially citizen-friendly AI applications generate enormous amounts of data that must be processed, stored and secured. Local data centers form the foundation of this modern digital administration.

Not Your Average Customer

Public authorities, municipalities, state and federal administrations have requirements for digital infrastructure that differ significantly from those of private companies. Security, availability, data sovereignty and compliance are a legal obligation and a political necessity.

Anyone processing registration data, social security information or health data is subject to strict national and European regulations. Data sovereignty is therefore essential. Government data must remain within the national legal framework, even if potentially cheaper cloud services from abroad are tempting. For example, under certain conditions the US CLOUD Act allows US authorities to access data from American providers, regardless of where it is stored. This is unacceptable for sensitive government data.

Colocation: The Smart Way

According to Bitkom, the colocation segment experienced particularly dynamic growth in 2025, increasing by 17.5 percent. This puts it in a leading position in terms of growth rates compared to other European countries. But why?

The traditional on-premises data center in government buildings is increasingly reaching its limits. The demands on energy, cooling, physical security and professional operating personnel are enormous and hardly economically feasible for smaller municipalities and districts. At the same time, complete outsourcing to a public cloud is not possible.

Colocation data centers offer a good alternative. They provide professionally operated, highly secure infrastructure where public authorities can run their own hardware or use predefined services. The data always remains within the national legal jurisdiction and control remains with the customer.

Local data centers also provide direct cloud access via so-called cloud-on-ramps, thus offering an attractive environment that strengthens regional economic development.

Geographical proximity is particularly crucial for the public sector. Local or regional colocation data centers enable short connection paths, low latency and rapid physical accessibility – a crucial factor for maintenance, audits and security checks. For time-critical applications such as emergency communications, police systems, or medical infrastructure, every minute counts.

Scalability for Greater Agility

Colocation data centers allow for the rapid and on-demand expansion of capacity without requiring authorities to invest in their own infrastructure. This is particularly important for AI applications: Generative AI, large language models and data-intensive analytics systems demand significant computing power. The National Data Center Strategy addresses precisely this issue.

Secure and Sustainable

In the public sector, security is a multidimensional concept. Physical security, cyber resilience, data protection compliance and business continuity must be considered together. Modern data centers meet these requirements through redundant systems, multiple layers of access control, encrypted data transmission and defined business continuity concepts. Only data centers that demonstrably meet these standards are suitable for sensitive administrative applications.

Sustainability is equally essential for public sector clients. Procurement law, sustainability targets at the federal and state levels and the European Taxonomy Regulation also compel public authorities to consider ecological criteria in their IT infrastructure. Well-positioned providers can score points here with transparent sustainability reports and the

use of renewable energies, including integrated waste heat concepts for municipal heating.

Local Location Strategy as a Strength

Regional data centers strengthen digital sovereignty and promote the local economy—for example, through additional business tax revenue and skilled jobs. Decentralized locations also increase resilience: Outages or cyberattacks on individual locations can be mitigated more effectively.

Andreas Windolph, an expert in digital infrastructure for the public sector at the auditing and consulting firm PwC Germany, succinctly summarizes the strategic dimension: The location of data centers is not an operational decision, but a strategic one with concrete added value for the region, aligned with the long-term economic development strategy of a municipality or state. The consultant recommends considering the entire ecosystem, carefully analyzing location factors and engaging in dialogue with the partners involved.

Digitalization from a single source

The Portus Data Centers Group supports the public sector with high-performance edge colocation services. Since 2020, the company has offered carrier-neutral solutions in Germany and neighboring regions: Hamburg, Munich, and Luxembourg. This enables public authorities to implement data processing close to the point of origin and meet stringent requirements for data sovereignty, low latency and availability.

The locations offer extensive interconnection options, state-of-the-art security concepts (access control, video surveillance, 24/7 monitoring), optional cages, redundant power supplies and efficient cooling systems.

With ISO 27001 certification, site-specific awards and 100% renewable energy the data center operator meets the high standards for security, compliance and sustainability in the public sector.

Conclusion: On-premises data centers in government buildings are increasingly reaching their limits. However, digitalization in the public sector remains feasible. Colocation providers operating within the national legal framework are a viable option as they meet the stringent requirements of the public sector without requiring significant upfront investment.

Source:

<https://bmds.bund.de/service/publikationen/nationale-rechenzentrumsstrategie>

<https://www.bitkom.org/Bitkom/Publikationen/Studie-Rechenzentren-in-Deutschland>

<https://blogs.pwc.de/de/oeffentlicher-sektor-zukunft-gestalten/article/253296/rechenzentren-als-strategische-chance/>