Bus Inf Syst Eng
https://doi.org/10.1007/s12599-026-01020-1

INTERVIEW

Interview with Bernie Wagner on "Digital Sovereignty: Building a Completely Independent European Cloud."

Walter Brenner · Barbara Brenner · Benjamin van Giffen

Accepted: 18 August 2026
© The Author(s) 2026

Strengthening Europe's digital sovereignty can only be achieved if new providers — particularly of cloud services — emerge in Europe that rely largely on European components, store their data exclusively in Europe, and are subject solely to European jurisdiction. Schwarz Digits, an integral part of the Schwarz Group — which includes the retail chains Lidl and Kaufland, among others — has set itself the goal of building a digitally sovereign European cloud infrastructure to serve as a counterweight to American and Asian providers. For this reason, Schwarz Digits will invest several billion euros in a data center near Berlin as the foundation for a digitally sovereign infrastructure. Against this backdrop, we interviewed Bernie Wagner, Chief Sales Officer of Schwarz Digits. The editorial deadline for this interview was June 30, 2026.



W. Brenner · B. Brenner (✉)
University of St. Gallen, St. Gallen, Switzerland
e-mail: barbara.brenner@unisg.ch

B. van Giffen
University of Liechtenstein, Vaduz, Liechtenstein

Schwarz Digits follows the principle of being its own first customer: it first develops and uses its digital infrastructure internally and only offers it to the external market once it has been professionally tested and proven stable. Before joining Schwarz Digits, Wagner was Managing

Published online: 21 September 2026

Director of Google Cloud Germany. From 2013 to 2021, he was responsible for sales in Germany as Senior Vice President Sales at T-Systems International. Throughout his career in the IT industry, Wagner has built an extensive network in areas such as cloud, cybersecurity, and modern telecommunications technologies.

BISE: How would you define digital sovereignty? How is it different from autarky and protectionism?

Wagner: For us at Schwarz Digits, digital sovereignty means first and foremost "freedom of choice" — that is, the right to choose and having the independence to do so. It is about us, as a company, deciding for ourselves where our data is stored, how it is processed, and who has access to it. Sovereignty means being able to get up from the negotiating table, at any time, when a provider's terms no longer suit you. We draw a clear distinction between this and autarky, or protectionism. We are not saying that technologies from other countries should be excluded, or that we should isolate ourselves. In a globally interconnected world, that would nearly be impossible. But a healthy dose of pragmatism doesn't hurt here, either.

BISE: What effects of a lack of digital sovereignty do you encounter in your daily work? How do you view statements of Chief Information Officers who claim to have fallen into an almost insurmountable dependency on a few, typically American, providers, a phenomenon known as "vendor lock-in"? According to CIOs, this dependency very often manifests itself in price increases that they regard as unjustified.

Wagner: At the time, we were confronted by our software provider with unreasonable price increases, without any corresponding improvement in performance. On top of that, we lost control: our provider could neither guarantee us exactly where our data was stored, nor what would happen to it — for instance, whether it would be used to train third-party AI models. Under laws such as the US CLOUD Act of 2018, American providers have become subject to extraterritorial jurisdiction, which could have potentially given US authorities access to our data. An inability to switch providers in the cloud domain jeopardizes a company's ability to survive in a crisis. This is what is known as vendor lock-in. That was the very reason for us to build a completely independent European cloud infrastructure with STACKIT.

BISE: What effects will the increased use of artificial intelligence, especially generative artificial intelligence, which is primarily offered by American hyperscalers, have on the digital sovereignty of European countries?

Wagner: Data is the essential fuel, the "oil" of the twenty-first century, and indispensable for artificial intelligence. The greatest danger is feeding our exclusive European domain and industry knowledge into the generic language models of American hyperscalers. In the worst case, if this highly specific knowledge drains away, then we are training our global competitors' models and losing our greatest asset. What we are talking about here is the danger of outright "data colonialism". In order to prevent these outflows and protect intellectual property, we rely on digitally sovereign, domain-specific AI applications.

BISE: The selection of suitable suppliers will play a major, perhaps even decisive, role in strengthening digital sovereignty. Will a criterion such as "strengthening digital sovereignty", or something similar, appear in public-sector tenders in the future?

Wagner: The state has a particular duty to lead by example here and, moreover, it has considerable leverage. From an economic standpoint, it makes no sense for public tax money to flow almost exclusively to US hyperscalers, especially when it comes to storing sensitive government data there. We would therefore like to see politicians adjust the public purchasing rules in a way that strengthens domestic providers and allows the state to function as an anchor customer. The criterion of "digital sovereignty" must play a central role in public tenders. In Germany, for example, the Federal Government recently passed the so-called Public Procurement Acceleration Act which anchors the concept of digital sovereignty — which was previously barely tangible in legal terms — as a qualitative criterion in public procurement. Thereby it creates the legal framework to actively favor bids for open-source solutions and sovereign IT architectures in public procurement. In addition, the Federal Office for Information Security recently published a modular catalogue of criteria, the C3A (Criteria enabling Cloud Computing Autonomy), giving additional guidance. At the European level, we see similar developments with the publication of the EU Commission's Cloud Sovereignty Framework in October 2025 and the proposal for the Cloud and AI Development Act (CADA) which was presented by the European Commission a couple of weeks ago.

BISE: What is your view on open-source software as an important component for strengthening the digital sovereignty of companies in Europe? In this context, what significance does the "European Sovereign Stack Standard" — which relies heavily on the use of open-source software — have?

Wagner: For us, open-source software is a critical building block for overcoming dependencies and "vendor lock-in". Our own cloud, STACKIT, is built fundamentally on open standards such as OpenStack and Kubernetes. The decisive advantage of open source is the transparency that comes with it. The source code can be inspected and is not an uncontrollable American "black box," where it is impossible to know if digital backdoors exist. Projects such as the Federal Government's "Germany-Stack" are the right answer to geopolitical risks here. Their goal is to

create a federated and mutually reinforcing technology ecosystem that spans the entire value chain — from microelectronics and cloud infrastructure to AI and software — offering a German-European alternative. But these projects need sovereign infrastructure and components to achieve their goal of reducing existing dependencies and strengthening digital sovereignty.

BISE: What effects do you expect European and national regulation of the digital economy to have on the digital sovereignty of companies and public administrations in Europe?

Wagner: In principle, we welcome European regulations such as the GDPR or the EU AI Act, because they protect our liberal values and people's privacy. However, at the same time, innovation in Europe needs a certain space in order to develop freely. Regulation must be designed in a pragmatic, proportionate, and application-oriented way. If we manage that, European data protection and values-based AI can become a genuine export success and a global competitive advantage.

BISE: What impact or significance does the European Commission's new Technological Sovereignty Package have for Schwarz Digits?

Wagner: We strongly welcome the EU Commission's Technological Sovereignty Package and its proposal for the Cloud and AI Development Act (CADA). As a digital infrastructure provider and pioneer for technological independence in Europe, we regard this step as a milestone on the path toward a self-determined, viable European data space. Cloud sovereignty is an indispensable foundation for digital sovereignty—an issue of exceptional strategic relevance given the growing hybrid threats and Europe's dependence on non-European technology monopolies.

The CADA draft and its tiered approach to defining Sovereign Cloud Services reflects this necessity. In particular, the higher levels—which mandate not only EU control but also comprehensive technological sovereignty—align with the standard of performance that we have already successfully established in the European market with STACKIT, our sovereign cloud infrastructure.

This European initiative correlates closely with pioneering standards at the national and corporate level, and in our view represents their logical extension at the level of EU policy. In its entirety, we've published the European Sovereign Stack Standard (ES^3) which builds on the EU Commission´s Cloud Sovereignty Framework follows the same core principles as CADA and has analogies to the C3A standard put forward by the Federal Office for Information Security (BSI). This interlocking creates a harmonized framework that finally offers the public sector and regulated industries the legal and investment certainty they urgently need.

We particularly welcome the formal adoption of the "Open Source First" principle in the EU Open Source Strategy as part of the Technology, as well as the planned establishment of a European cloud federation. These instruments serve as powerful levers for consistent prevention against technical vendor lock-in — in turn, efficiently pooling European computing capacities, and accelerating sovereign access to state-of-the-art AI platforms and models.

Funding Open access funding provided by University of St.Gallen.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

Publisher's Note Springer Nature remains neutral with regard tojurisdictional claims in published maps and institutional affiliations.