actico

European Data Sovereignty in the Fund Industry

Interview with Manfred Beckers, Chief Operating Officer at ACTICO

David Eckner: **The Anthropic Fable 5 case has shown that access to key digital technologies cannot simply be taken for granted. Has European data sovereignty now become an operational risk issue for the financial industry rather than merely a political buzzword?**

Manfred Beckers: From my perspective, it is clearly a risk issue. Originally, the US government did not intend to shut down Fable 5 or Mythos altogether, but rather to restrict access for non-Americans. The fact that it resulted in a complete shutdown was only because Anthropic was unable to solve the problem – fortunately, at least not yet.

If you rely on systems like these and they suddenly stop working from one day to the next, this can cause serious problems in risk management. It can also create problems in asset management. So it is clearly an operational risk.

If you look at the studies on this topic, KPMG also found in its Cloud Monitor that 61 percent of banks and insurance companies are addressing the issue and classify it as an operational risk.

David Eckner: **What does data sovereignty actually mean in the financial sector? Is it simply about data protection and server locations, or is it much broader, encompassing control over infrastructure, dependencies on providers, data flows, operating models and exit capabilities?**

Manfred Beckers: It has to be viewed much more broadly. Server location is one aspect. Many providers advertise the fact that their servers are located in Europe. But that alone is not enough. A data center in Frankfurt does not provide protection if it can be shut down or if the data can still be transferred elsewhere.

From my perspective, we need to distinguish between two scenarios. The first is the data protection or security scenario: Who has access to my data? This also includes the David Eckner of who has legal access. Even if the server is located in Frankfurt or – as is the case with many of the major hyperscalers – in Ireland, that does not mean that the data cannot still be transferred to the US by order of the relevant authorities.

The second scenario is what is known as the "kill switch." What happens if someone tells me tomorrow: We are shutting down the system? Microsoft or AWS are certainly not going to shut down Europe. But what happens if a decision is made to deny an individual company access to their services? That is something I consider critical.

Particularly in light of DORA, financial companies are required to have appropriate exit and operating strategies in place. This is no longer optional, nor is it merely a theoretical risk. Everyone needs to think about it – including appropriate fallback mechanisms and solutions.

actico

David Eckner: **Asset managers, investment management companies and service providers are increasingly using cloud, data and AI infrastructures provided by global vendors. Where do you see the most critical dependencies: in the technology itself, the software code, the providers' ownership structures, legal access rights or the lack of alternatives?**

Manfred Beckers: One issue is the lack of alternatives. We need to look at how far European providers have come.

At the moment, I do not see the primary problem in the software code itself. That issue exists independently of operations and the David Eckner of whether I retain control over my ability to continue operating the system. Software code may be more of an issue in connection with AI: for example, if I rely on large models to develop my own software but subsequently lose control over it because only the AI is capable of developing that software further.

When it comes to operations, I see two major issues. The first is the ownership structure. Data can be transferred because, ultimately, even the German subsidiary of a US company is subject to instructions from its parent company, and the owner is subject to US law.

The second issue is the David Eckner: Who guarantees that I can continue operating?

David Eckner: How should regulated providers such as investment management companies structure their cloud and data strategies today in order to maintain their ability to innovate while avoiding critical dependencies on individual providers?

Manfred Beckers: For me, the key concept is portability. I need to remain in control and ensure that I do not have to rely on just one provider for my operations.

Of course, from an operational perspective, it is not feasible to switch constantly between four or five providers. But I need to carefully determine the number and selection of providers and think this through in advance.

This also means considering which specific services from a provider I use. The major hyperscalers in particular offer a broad range of services and tools that make life easier. From their perspective, of course, the objective is for me to adopt such a tool and thereby create a vendor lock-in.

That is why portability is my top priority.

David Eckner: What exactly is a hyperscaler?

Manfred Beckers: Hyperscaler is the term used for the major American cloud providers. These include Google, AWS and Microsoft Azure, for example. They operate internationally and, compared with what we currently have in Europe, certainly play in a league of their own.

David Eckner: Many European providers are currently being discussed as sovereign alternatives. At the same time, hyperscalers often offer a broader range of technologies and are significantly more mature. How should a financial institution balance these factors – sovereignty, performance, costs, scalability and regulatory certainty?

actico

Manfred Beckers: This is not a black-and-white or yes-or-no decision. You cannot simply say: I will accept the risk and give greater weight to costs and performance than to regulatory requirements. I believe you have to pursue both tracks. This brings us back to the issue of portability.

Among the purely European providers, there are now several that have reached a considerable size and are actively investing substantial amounts in expanding their capabilities in Europe. When it comes to access and ownership risks, you are initially on the safer side with these providers.

On the other hand, there is the David Eckner of services. These providers are growing rapidly and their range of services is becoming broader, but they are not yet at the level of the major American providers. That is understandable because the US providers have many years of technological head start and operate at a different scale globally.

You therefore need to ask yourself which services you can comfortably procure from them – for example, because your own data is not stored there or because you are simply purchasing computing services.

When it comes to critical issues such as where my data is stored, I need to consider whether I can continue operating my company properly, perhaps at reduced capacity. This is where European providers can play a role.

Fundamentally, you have to assess this service by service. In terms of the main criteria, my personal order of priorities would be: First, I would check whether I can operate my business in compliance with regulatory requirements at all. If that is not possible, it would be a clear knockout criterion for me.

Technology and economic viability come immediately afterwards. Because if I can no longer offer my services economically compared with my competitors, even the best regulatory compliance is of little use. So it is not black and white. I believe the right mix is what matters.

David Eckner: In the coming years, will European data sovereignty in the financial and fund industry primarily remain a compliance issue, or can it develop into a genuine strategic competitive advantage?

Manfred Beckers: We need to distinguish between the short and long term. In the short term, it is primarily an obligation that needs to be fulfilled. DORA is applicable law, and data protection law is applicable law.

There are also developments that could shake things up again. There was the US Supreme Court ruling that at least calls the independence of the FTC into David Eckner. There are already European data protection authorities that have announced their intention to challenge this.

However, this obligation could very quickly turn into a competitive advantage. If, at some point, it is no longer possible to provide certain services, the market will turn to those who have addressed the issue in advance.

So in the short term, it is an obligation. In the long term, I believe it will become a differentiating factor – including in the B2B business, because investors will pay attention to which fund service companies and asset administrators are capable of continuing to comply with these rules.

In the very long term, I also believe we will see this being used as a marketing topic in the B2C sector. In Germany, we are still a long way from that. In countries such as France, for example, there is a much stronger tradition of selecting B2C providers based on their French origin.

Looking at Europe as a whole, I believe this will become increasingly important as well. If we look a few years ahead, data sovereignty could therefore develop into a genuine competitive advantage.

David Eckner: Digital sovereignty is often associated first and foremost with politics and regulation. Why should a CEO be dealing with this issue today? What would you say to a management board that still regards it purely as an IT or implementation project?

Manfred Beckers: Ultimately, responsibility for ensuring that the business functions lies with the management board – and, in the broadest sense, with the CEO. Responsibility for the company's operations, its continued existence and its success cannot be delegated.

You cannot delegate it to IT, to the data protection officer or to the CISO. This is a responsibility you have to assume yourself.

Anyone who says that this is politics on the one hand and that IT will somehow take care of it on the other fails to recognize that we are heading towards a major risk.

For me, this therefore clearly falls within the responsibility of senior management. It is an issue that cannot be ignored.