WHY CLOUDS AREN’T ALL THE SAME.

Cloud computing is booming. Especially in public clouds. But CIOs and CEDs have to tread carefully when picking public clouds, lest the booming they hear becomes the ear-shattering din of data theft instead of the soothing hum of a secure, profitable business. Here’s what to look out for.

Public clouds are big business. According to the Cloud Monitor published by Hitakom and KMDD, over one-fifth (21 percent) of German companies use public cloud services. Last year, only 16 percent did.

That blistering pace seems to continue, too. The German e-commerce association, and Arthur D. Little, a consultancy, forecast that public cloud services will grow as much as 40 percent a year until 2019 — making it a turbo segment, in their words. They expect the growth to fuel demand for IT integration solutions and onsite customer service — as well as improved legal certainty and better data protection.

CUSTOMERS PREFER GERMAN DATA PROTECTION LAWS

Those last two items are absolutely critical for Schwaiger, a German mid-market enterprise. The Bavarian communications company provides a full suite of home automation solutions: from solar power alarms to WiFi speakers in the living rooms right down to humidity sensors in the basement. Its devices send data to a data center where it can be accessed by homeowners with a smartphone or tablet app. “Data protection and data security are top priorities for us,” said Bernd Wana, the head of IT at Schwaiger. “Trust is crucial in home automation. That’s why we wanted to switch our entire system to a provider who met the most stringent standards possible.” The entire process initially went through a foreign-based data center. However, many customers wanted the security afforded by German data protection laws, widely regarded as among the strictest in the world. And these laws only apply if the company’s headquarters and the cloud provider’s data center both are located in Germany. Schwaiger thus migrated its entire HOME/DYOU home automation solution to the Open Telekom Cloud, hosted at Deutsche Telekom’s highly secure data centers in the German state of Saxony-Anhalt.

“WE WANTED TO SWITCH OUR ENTIRE SYSTEM TO A PROVIDER WHO MET THE HIGHEST STANDARDS POSSIBLE.”

Bernd Wana, Head of IT, Schweiger

THE OPEN TELEKOM CLOUD

1. CUT COSTS

Growing start-ups like Octopus benefit heavily from the Open Telekom Cloud’s pay-per-use model. There are no fixed costs, providing more financial leeway to invest in business expansion.

2. SAVE TIME

The Open Telekom Cloud is ready quickly. Octopus’s cloud, for example, was up and running after one week and one technical call. New digital business ideas can be implemented quickly at minimal risk in a public cloud. That was a reason for start-ups like Octopus to self-service portal for configuring the product. Users simply configure their own applications, and the applications. Larger organisations like another aspect: the Open Telekom Cloud’s automation dashboard. It lets users activate hundreds of virtual servers in a flash.

3. STAY FLEXIBLE

The Open Telekom Cloud is based on OpenStack. Being a true open source architecture for cloud computing, it allows customers to quickly and painlessly switch providers. That avoids vendor lock-in. OpenStack supports fast changes to alternative cloud services, too.

Three questions answered by Hans Markus Wuff, IT law expert at SKW Schwarz, a highly regarded law firm with more than 25 IT and data protection attorneys.

It’s still not clear what data protection requirements apply to cloud services. Why is that? Are the laws especially unclear for German organisations using foreign-based cloud services? The problem arises when you transfer personal data to foreign servers. Data transfers within the European Union (EU) or the European Economic Area (EEA) are generally uncomplicated since § 4b of the German Data Protection Act (Bundesdatenschutzgesetz, BDSG) grants preferences to countries in these regions. Once the data leaves the EU/EEA, though, the law requires data recipients to ensure an adequate level of data protection. Companies in the US, for example, rarely offer this level of data protection and so German enterprises can’t store personal data on US servers. An exception was carved out by the Safe Harbor Privacy Principles jointly adopted by the European Commission and the US Department of Commerce. However, the European Court of Justice (ECJ) overturned the Safe Harbor Privacy Principles in October 2015. German data protection authorities had responded quickly since data protection authorities threatened to issue a decision on sanctions at the end of January 2016. Many organizations that failed to act by that deadline (e.g. by adopting standard EU contract clauses) were faced with fines of up to EUR 50,000. It wasn’t an idle threat, either — some firms were indeed fined. Now we have a successor agreement, the US Privacy Shield. However, I expect to see the legal risks lurk outside Germany.

Cloud computing is booming. Especially in public clouds. But CIOs and CEDs have to tread carefully when picking public clouds, lest the booming they hear becomes the ear-shattering din of data theft instead of the soothing hum of a secure, profitable business. Here’s what to look out for.

Three questions answered by Hans Markus Wuff, IT law expert at SKW Schwarz, a highly regarded law firm with more than 25 IT and data protection attorneys.