THREE REASONS TO GO WITH 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 implemen-ted quickly at minimal risk in a public cloud. One feature appeals to start-ups like Octopus: a self-service portal for configuring the product. Users simply configure their servers and upload their applications. Larger organizations 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.

data center both are located in Germany. Schwaiger thus migrated its entire HOME4YOU home automation solution to the Open Telekom Cloud, hosted at Deutsche Telekom's highly secure data centers in the German state of Saxony-Anhalt.

Does that mean that data from a lowly basement sensor really belongs in a German cloud? Yes, in some cases, according to Hans Markus Wulf, an attorney and partner at SKW Schwarz (see interview). Even foreign companies agree – including Swiss-based Octopus Cloud Inc. Its cloud service helps companies with complex software licensing for Microsoft SPLA or VMWare vCAN by generating licensing reports at a keystroke – a process that otherwise takes hours or even days to complete. The Swiss start-up has opted for the Open Telekom Cloud, largely for its superior data protection and data security. And so even international customers know their data is in excellent hands at German data centers. Clearly, this cloud offers more.

<Contact> *frank.strecker@t-systems.com*
<Links> *cloud.t-systems.com/open-telekom-cloud*
www.t-systems.com/solutions/cloud-security

Interview

LEGAL RISKS LURK OUTSIDE GERMANY.

Three questions answered by Hans Markus Wulf, 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 organizations 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 preferential treatment 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 had been 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 companies had to respond quickly since data protection authorities threatened to issue a decision on sanctions at the end of January 2016. Any organizations that failed to act by that deadline (e.g. by adopting standard EU contract clauses) would face 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 Privacy Shield and the standard EU contract clauses land before the ECJ soon since nothing substantial has changed since the 2015 ruling. The use of US servers will, in my view, remain on shaky legal ground for years to come.

Do you think public cloud services pose other typical legal risks?
Public cloud services have the drawback that users don't know where their data is stored. Obviously, this doesn't apply to private clouds or to providers who situate all their servers in Germany. Another risk is cyber attacks, which are easier to launch against a public cloud. To reduce this risk, organizations should entrust their data and applications to large hosting providers with advanced defense systems.

How can organizations ensure their cloud services comply with data protection laws?
Organizations should make sure that all data identifying specific employees or specific customer or supplier contacts is stored on servers located in the EU/EEA, preferably in Germany, since these regions have the strictest security standards. Moreover, they should use cloud providers who already have valid security certifications (such as ISO 27018) recognized by regulators in preparation for the EU General Data Protection Regulation, since the certifications will become absolutely essential for cloud computing in 2018.

Read the full interview at
www.t-systems.com/interview-drwulf