Corporate and consumer users are increasingly embracing hosted information technology solutions that allow users to obtain additional functionality, storage or processing capacity without owning software copies. Instead, users access enhanced software, computing power and data storage by using the Internet. This typically means less upfront investment to users and economies of scale for providers.

While users increasingly embrace cloud computing, data privacy advocates, regulators and lawyers do not see as much perceived risks for privacy and security of personal data. To them, cloud computing means primarily that users do not understand, own or control. As is often the case with respect to legally and technologically complex topics, buzz words and slogans are quickly established and (ab)used to pursue various policy and competitive agendas.

In this article, I am taking aim at a dozen myths that tend to cloud the decision-making process regarding data privacy and the hosted solutions. In conclusion, it is a myth that cloud computing is somehow bad or risky for privacy or that it is a fact that data is far more secure in some clouds than on traditional systems and devices. Challenges are very manageable—if approached reasonably from the vendor and customer side. For illustration purposes, a graphical example of a common application that a multinational enterprise can patch together from decentralized cloud computing vendors is provided: e.g., Workday.

Myth 1: Cloud computing presents fundamentally new and unique challenges for data privacy and security

Fact is that consumers and companies have been entrusting specialized service providers with personal data for decades, payment processors, accountants and various outsourcing service providers; e.g., payroll, call centers. We have made the Internet an integral part of our information society and economy—and the Internet is found of data across geographies, devices and connections. Even the very services and models that are currently promoted for 15 years or so by an up-and-coming industry that initially referred to itself as “application service providers and remotely hosted solutions certainly create challenges—but they are neither new nor unique.
Myth 2: Cloud computing involves more data sharing, and that is inherently bad for privacy

Fact is that transferring data to data processing agents—who process data only on behalf and in the interest of transferring data to data controllers, who use data in their own interest and possibly impair the data subject’s processing agents is so different from transferring to data controllers that German data protection laws define exclude sharing with data processing agents.

Data sharing with data processing agents is not inherently bad or good for privacy—it is neutral. Companies are a legal fiction. When companies use and process personal data, they have to act through human statutory employees, individual independent contractors or employees or contractors of corporate contractors. Important that the individual person who processes the data acts on behalf and in the interest of the data controller in turn complies with applicable data protection laws. It is less relevant for privacy compliance purposes.

For most companies, the switch from internally maintained human resources databases to an external cloud-based sharing or transmission to additional geographies. Most data these days is transferred across geographical boundaries. Traditionally, data has been shared over the Internet, via myriad devices, connections and persons using spreadsheets and e-mailing across legacy systems with varying degrees of data protection to a centralized cloud will not add to the prevalence of data sharing. Usually, it just means more orderly, organized and secure sharing.

Myth 3: Cloud computing is bad for data security

Fact is that employee malice and negligence; e.g., lost laptop, smart phone, etc., causes many data security breaches. Whether personal data is safer on a system secured by the data controller in house or an external cloud provider, it also on the rise. Whether personal data is safer on a system secured by the data controller in house or an external cloud provider.

Returning to the example of a global HRIS, each multinational employer needs to ask itself whether its own IT department is superior to the measures deployed by a specialized vendor that can leverage economies of scale and is motivated by the data of its customers secure. If the vendor has better security measures, systems and processes, then cloud computing will be a good thing if the vendor brings better technologies to the table and helps the data controller manage risk. It can be neutral if the vendor’s cloud system is more secure but the way the customer uses the system k customer does not configure security to properly restrict data to the appropriate users, the customer uses unauthorized or inaccurate data should diminish.

Myth 4: Cloud computing causes additional issues under privacy law because data is transmitted in

Fact is that most companies are already transmitting data internationally because they use the Internet—for e-mail or office locations—or because they have subsidiaries, customers, suppliers or channel partners in other jurisdictions because data is needed in different jurisdictions not because of where the data is stored. With respect to employment, to cause personal data to be transferred across borders to populate the system—whether they host it themselves or not, the risk of unauthorized access or inaccurate data should diminish.

Myth 5: Data in the U.S. is endangered by the USA PATRIOT Act

Fact is that the United States enacted the Uniting and Strengthening America by Providing Appropriate Tools R Act (USA PATRIOT Act) in October 2001, following the September 11 terrorist attacks, to help fight terrorism provide certain additional investigative powers to U.S. law enforcement officials. But:

- These powers are not relevant for most types of data in cloud computing arrangements;
- The government is much more likely to obtain the data directly from the data controllers; i.e., users of cloud computing systems.
If the data controller is not based in the United States and has no strong nexus to the United States, it is interested in the data regardless of whether the data is hosted in the United States; if the U.S. government is interested, it can usually obtain access to the data through foreign government cooperation treaties, regardless of where the data is hosted; similar powers exist in most other countries and data is typically much more at risk of being accessed by the controller based, and the USA PATRIOT Act issue is raised to support unrelated agendas, such as protecting local companies or the information that the U.S. government seeks to fight terrorism and money laundering is not what most corporations are looking for. Returning to our global HRIS example, it seems quite unlikely that the U.S. government would be interested in the data system. Even if the U.S. government were interested, it would more likely turn to the employer first to obtain access to the data subjects and may have additional information, and the government would not need to exercise any jurisdictional complications. The U.S. has treaties with over 50 countries, including Canada, Mexico, Australia, Hong Kong and a majority of the EU Member States assistance agreement with the EU. The cooperation under mutual legal assistance arrangements can include sharing information between law enforcement authorities in the two countries. Similarly, the G8 nations (Germany, France, the United Kingdom and Russia) recently reaffirmed their commitment to enhance the exchange of information and judicial assistance in acts of terrorism. Accordingly, in most cases, even if information is stored outside of the U.S., it is typically much more at risk of being accessed by the government. In some cases, the additional hurdles established by jurisdictional complications will make a difference, but the U.S. bankruptcy court recently refused to hand over e-mails to and from a German resident to the German government because the resident’s privacy was better protected due to the fact that his e-mails were stored in the United States. The German government had access to his e-mail if he had used a German Internet service provider. Most countries around the world have updated their privacy laws to require such information through existing treaties or agreements with the jurisdiction in which the information is stored. In one of the first cases that raised concerns regarding the USA PATRIOT Act in the context of international outsourcing, the British Columbia Government Service and Employee’s Union, sued the British Columbia Ministry of Health Services for contracting out the administration of the province’s public health insurance program, whether they act as data controllers or processors. The U.S.-EU Safe Harbor program has been heavily criticized, with a data protection authority in one German state has even called for a rescission of the program. However, it's important to note that the Safe Harbor Principles expressly state that data processors may participate and achieve adequacy if they comply with the program's requirements. Myths and facts about data privacy in the cloud—A dozen myths and facts.
not seem much more relevant and noteworthy as the occasional buzz around plans by Bavaria to cede from Gi States. Until the European Union or the United States cancels the Safe Harbor arrangement, all data protection are legally obligated to accept that Safe Harbor-certified cloud computing service providers in the United State providers.

Of course, data controllers need to verify that each particular service provider can be trusted with personal dat such provider is based in the United States and Safe Harbor-certified or not certified and based in a Member S relative strengths and weaknesses of data protection technologies and laws across geographies, it is worth rec France and Germany, which historically pride themselves of relatively high data protection law and technology some of which have joined the EEA only recently and do not have much of an information technology industry

As a data protection law practitioner and scholar in both Germany and California, I am troubled by calls for an to the United States by German politicians, singling out highly respected global technology leaders headquarte attacks, while accepting, without any additional scrutiny, the free flow of data in the EEA. Why should a multi HRIS is more secure in Bulgaria and Romania—the youngest EEA Member States—compared to California? Not and policy perspective supports such double standards. Unsubstantiated attacks do not help advance the disc local protectionism and national arrogance.

**Myth 8: Contractual clauses are unnecessary if the service provider is Safe Harbor-certified**

Fact is that the Safe Harbor certification only qualifies a service provider outside the EEA as adequate as a ser be. But, European laws require particular contractual clauses for data transfers to any service provider—whether A company has to take on three hurdles before it may transfer European personal data internationally—into th and use has to be permitted, based on consent, contractual duties, statute, etc. Second, the transfer has to be achieve adequacy if it is not based in the EEA or a country that has been declared adequate by the EU CommiHarbor, a U.S.-based service provider helps its customers over the third hurdle—adequacy—but the Safe Harb as such. Whether a recipient is in the U.S. or in the EEA, the customer has to justify any transfer. In the conte controllers; i.e., recipients that want to use the data in their own interest, data controllers typically have to ob on statutory data transfer obligations. But, when a company transmits data to a service provider, it does not h control over the data via an adequate contractual arrangement. This is where the need for certain particular cc

One option is to sign the Standard Contractual Clauses promulgated by the EU Commission for data transfers I required if the service provider is certified under the U.S.-EU Safe Harbor program, because the Safe Harbor c the alternative would be to implement agreements that satisfy the national law requirements for agreements v promulgated, blessed or prescribed by the various data protection authorities in the 30 EEA Member States va binding such clauses are and whether they will be accepted without questions and scrutiny in data protection e any customer or service provider opting for “self-made” or “national government templates” should be prepare analysis, lengthy negotiations and ultimately a multitude of agreements. By comparison, the European Comm because all EEA Member States are supposed to accept this form as assuring “adequacy,” it is in both parties’ SCC—to preserve the preemptive blessing of the commission regarding adequacy—and one form agreement c

**Myth 9: Data privacy and security law compliance is the provider’s responsibility**

Fact is that data privacy and security laws primarily hold the data controller responsible for compliance; i.e., t relationship. The customer has to ensure that the data made available to the service provider has been legally received notice, filings have been made, etc. The service provider has typically only two duties under data priv customer’s instructions and keep the data secure against unauthorized access. The second duty—data security controller. Therefore, it is important for customer and vendor to reach a reasonable agreement about what lev types of data and who should be doing what. For example, if a customer hires a service provider to store archi encrypted information in the cloud, it may not be necessary for the vendor to invest heavily in security feature data would not typically harm the data subjects. On the other hand, backup copies of credit card transaction ir because such information is actively pursued by hackers to steal identities and commit fraud. Data in an HRIS
information; e.g., U.S. Social Security numbers—a primary target for identity thieves and hackers, even though is of little or no interest to hackers.

If the service provider offers a specialized application for certain types of data that are typically sensitive and take the initiative and either implement certain security measures itself, for example, encryption, or recomme also take the initiative to identify the various compliance obligations that apply to a particular type of data pro these obligations can or should efficiently be handled by service providers and which are better discharged by various compliance obligations on the data controller depend on where the data controller is located, and if the jurisdiction, the data controller will need to educate and instruct the data processor about the compliance requ

**Myth 10: Cloud service providers cannot cede control to their customers**

Fact is that many organizations find it difficult to stay in control over modern IT systems, whether they hire se or whether they host, operate and maintain systems themselves. Even with respect to self-operated systems, support service providers who have to be granted access to the systems and data to analyze performance prol support and maintenance. Most companies find it prohibitively expensive to customize systems—whether self-beyond the configuration options provided by the vendor as part of the standard offering. Consequently, there control that users can and want to exercise over their systems, whether self-hosted or hosted by a provider.

Yet, from a legal perspective, it is imperative that the service provider remains in the role of a data processor controller. If the service provider obtains or retains too much discretion about aspects or details of the process co-controller, which is not acceptable for either party. The service provider would suddenly assume all kinds of notices to data subjects, assure data integrity, grant access and correction requests, submit filings to data pro data retention and deletion requirements, etc. A cloud computing service provider cannot discharge these dat know the data subjects or what data is uploaded into its systems. And, if the service provider did in fact qualif would typically violate statutory prohibitions and privacy policy promises regarding data sharing. Therefore, bc toward an arrangement that keeps the provider limited to the role of a data processor.

In the context of self-hosted systems, it tends to be easier to prove that the provider retains little or no contrc cloud computing scenario, on the other hand, the data resides on servers on location that the provider control: from a data protection law perspective refers to “control” of the data—not “control” of the premises where dat viewed as data controllers merely because they own a building where data is stored and have access and repo law regarding the building and tenant property.

The focus of control regarding cloud computing is to ensure that the customer decides what data to upload, dc otherwise process. This is the case with respect to most cloud computing offerings because the service provide functionality as a service, without any interest, knowledge or influence regarding data types and processing pl hosted HRIS, the service provider does not have any interest to view or use the data that the customer uploa need to provide to access data in order to provide support for technical issues. If the parties contractually and personnel only access data on the system to provide the service and prevent support issues, then the custome customer can be with respect to self-hosted systems.

Nearly, because with respect to self-hosted systems, the customer can monitor and safeguard physical safety many companies outsource premises security in any event to security service providers. To keep the customer provider has to provide key information about storage locations, processing practices and subcontractors. Sorr information based on trade secret protection objectives and this can create friction with respect to the objectiv purposes of data protection law compliance.

To resolve such conflicts and keep the service provider in the “processor” role, vendors could disclose to their processing practices, equipment locations and significant subcontractors with access to the customer’s personal safeguard control and data protection need to be passed on to the subcontractors. In connection with cost-effi computing solutions, it can be very difficult and expensive for providers to accommodate customization requ can also remain in control over data processing if the customer retains a right to receive prior notice regarding
and changes thereto, so that the customer can withdraw data or change the use of a cloud solution in case changes to data. Or, the customer could agree or instruct the provider to update service and technology from time to time condition that the provider will not lessen the security and privacy measures set forth in the agreement. Whether contract termination rights and early termination fees is a commercial point and not prescribed from a data pr

**Myth 11: Vendor has and should accept unlimited liability for data security breaches**

Fact is that service providers may not always be able to limit their liability vis-à-vis the data subjects in scenario customers and not the data subjects themselves. If hackers gain unlawful access to employee information resi may be liable directly vis-à-vis the employees under negligence theories—if and to the extent economic harm liability under a particular jurisdiction’s laws.

But, data protection laws do not prescribe the allocation of commercial liabilities between the parties. Sophistic exposure in various ways in indemnification, limitation of liability and warranty clauses. It is quite common to on whether customer and/or service provider contributed primarily to a breach or resulting harm; whether the contractual obligations, its information security policies and applicable law, and whether a risk materialized the including the customer.

Also, cloud service providers are increasingly mindful that they can be held liable for violations of laws by their for example in the context of uploaded viruses, illegally copied files and pornographic materials. Such risks are to the customer.

**Myth 12: Customer needs to have the right to access the provider’s data centers and systems for ai**

Fact is that customers need to reserve a right to audit the cloud service provider’s compliance measures. But, may not let customers into its data centers or systems because that would impair the security of other custom unnecessarily disruptive and costly. As a compromise, cloud service providers can arrange for routine, compre generally accepted audit firm and make the results available to all customers. If customers demand additional expand the scope of the next scheduled audit, if the customers are willing to pay for the additional effort and t service.

Beyond generally applicable compliance and audit requirements, there can occasionally be additional needs will processing arrangements or industries. For example, European laws implementing the Markets in Financial Ins require that regulated entities perform due diligence on their vendors "when relying on a third party for the pe are critical for the performance of regulated activities, listed activities or ancillary services." But, in the context is important to differentiate what types of data and processing services are within and outside scope. If a regu a hosted solution for human resources data relating to its own employees, this can hardly be considered a "cri services regulations. If the same firm were to outsource core functions such as calculations of its funds values, come into play.

*Prof. Lothar Determann* practices data privacy and technology law as a partner in Baker & McKenzie’s Palo A commerce and computer law at the University of California, Berkeley School of Law (Boalt Hall), Hastings Colle Universität Berlin.