Cloud Computing May Violate German Data Privacy Laws

The term “Cloud Computing” is generally used to describe services through which a company accesses software applications, databases, infrastructure and related services via the Internet or other networks. The use of Cloud Computing is growing substantially worldwide due to the cost savings and other benefits it provides. Due to concerns regarding personal data protection and transfers, German data protection authorities want to impose tougher restrictions and requirements on both Cloud Computing and other outsourcing arrangements involving personal data. Companies need to ensure that they are complying with these strict new requirements. Failure to comply with these laws may result in substantial fines, civil lawsuits and reputational damages.

The German Data Protection Authority’s Statements

The Data Protection Authority of the German Federal State of Schleswig-Holstein (the Unabhängiges Zentrum fuer Datenschutz Schleswig-Holstein – “ULD”) recently published on its website a white paper that covers data privacy aspects of Cloud Computing. The opinions expressed in the ULD’s paper are not legally binding on companies operating in Schleswig-Holstein or other German federal states. However, the ULD’s published views indicate the manner in which the ULD will view and examine Cloud Computing arrangements. The ULD views may also influence data protection authorities in other German states. In the paper, the ULD expresses concern that many transfers of personal data in connection with Cloud Computing arrangements will not satisfy requirements under German data privacy laws. The ULD called out “Public Clouds” in particular, but the concerns are not limited only to Public Clouds.

The German Data Protection Act (Bundesdatenschutzgesetz – “BDSG”) implements the EU Data Protection Directive. Section 11 of the BDSG specifically addresses requirements that data controllers must follow regarding data processors. Section 11 previously did not apply to data controller to data processor transfers outside of the European Union. Now, however, the ULD has taken the position that Section 11 does apply to transfers of personal data outside of the European Union. The result is that, according to the ULD, reliance solely on the EU standard data transfer clauses (one of the more common means for accomplishing a compliant data transfer) for data controller to data processor transfers in a Cloud Computing engagement is not enough to satisfy German data privacy laws. In addition to the standard clauses, data controllers will also have to comply with Section 11 requirements of the BDSG.

Regardless of whether the Cloud Computing provider is located inside or outside of the European Union, the ULD demands that companies using Cloud Computing services must take adequate measures to safeguard the
integrity and security of the personal data processed. For example, companies must include contractual provisions with Cloud Computing service providers in accordance with the criteria for data controller/data processor relationships (Auftragsdatenverarbeitung) set forth in Section 11 BDSG – regardless of the location of the Cloud Computing provider or the services.

In addition, according to the ULD, companies or qualified external third parties must exert “regular control” over whether Cloud Computing providers observe the restrictions of the BDSG. The control must cover the processor’s technical and organizational measures used to protect the data. Neither the BDSG nor the data protection authorities provide any extensive guidance on what regular control means, or how it will be interpreted. The ULD has suggested that companies can do this in at least two ways: they can obtain expert advice, in the form of audits or certificates provided by external experts, that the service provider observes the legal restrictions; or they can obtain a binding guarantee declaration by the service provider in which the service provider provides a comprehensive commitment to obeying the obligations imposed by the law.

Data Transfer to Countries Outside the European Union

When personal data is transferred outside of the European Union in connection with the Cloud Computing services, in addition to complying with Section 11 of the BDSG, the transfer must be accomplished by one of the permitted means. One widely used method is to employ the EU-approved standard clauses for transfer of personal data. Until recently, the Safe Harbor Agreement was also a permissible means of accomplishing personal data transfers from the European Union to the United States. However, German data protection authorities recently announced that they no longer regard Safe-Harbor certifications of US companies as a stand-alone basis for fulfilling German data privacy standards. (For more information about the stricter requirements set out for German companies regarding the Safe Harbor certification, see http://www.mayerbrown.com/publications/article.asp?id=9156&nid=6.)

The ULD gave examples of situations in which Cloud Computing arrangements could satisfy the German data protection and transfer laws. Please note that the ULD requires that the requirements of Section 11 of the BDSG are also to be satisfied in these arrangements. Some of the examples, however, bear little resemblance to actual business practices and Cloud Computing service offerings.

1. OPTION OF TERRITORIAL RESTRICTION
A Cloud Computing provider may offer its customers the option to restrict data processing to countries which are part of the European Economic Area (EEA) or the European Union.

2. ADEQUATE LEVEL OF PROTECTION PURSUANT TO THE EU COMMISSION
Cloud Computing services may be provided in and from any jurisdiction for which the EU Commission has deemed to have an adequate level of protection pursuant to Sec. 4b Subsec. 2 Sent. 3 BDSG.

3. STANDARD CONTRACTUAL CLAUSES PLUS ADDITIONAL MEASURES
The company using the Cloud Computing services may comply via (i) use of standard contractual clauses and (ii) satisfaction of the requirements of Section 11 of the BDSG. As mentioned above, use of the standard clauses was thought to be sufficient to accomplish a compliant data transfer.

There are questions regarding the ULD’s view and application of Section 11 of the BDSG to data transfers outside of the European Union. Previously, Section 11 was thought to apply to
data processing within the European Union, and not to transfers of personal data for processing outside of the European Union. The ULD’s application of Section 11 to data processing outside of the European Union extends the prior reach of Section 11. Despite these questions, other German state data protection authorities are likely to share the ULD’s view and enforce these requirements.

4. QUESTION OF APPLICATION OF BINDING CORPORATE RULES

Though Binding Corporate Rules (BCR) have previously applied to intercompany and multinational affiliated company transfers of personal data, the ULD has suggested that BCR might be adapted to cover non-affiliated processors. This view is not yet officially approved by the EU Article 29 Working Group (the EU advisory body that coordinates data protection activities among the EU member states), and its application and use for transfers to third-party processors, including Cloud Computing providers, remains to be seen.

What Your Company Should Do

If you have existing Cloud Computing service arrangements, or other outsourcing arrangements involving personal data from Germany, you should review these arrangements with counsel to ensure that they continue to meet the requirements of the German data protection authorities. If you are considering entering into a Cloud Computing service arrangement involving personal data from Germany, you should review the ULD requirements with German lawyers to ensure that you structure the arrangement, contracts and control measures in a manner that satisfies the new and changed requirements under German data protection laws. You should also monitor the developments both in Germany and other EU countries. As the use of Cloud Computing increases, other EU data protection authorities are certain to provide their opinions and guidance on personal data protection and Cloud Computing.

Other Related Data Protection Developments in Germany

The ULD white paper is only one of several recent developments in personal data protection. There have been several scandals involving large German companies disregarding binding BDSG provisions. Recently, the joint coordination committee, in which all German data protection authorities align their regulatory actions (the so-called Duesseldorfer Kreis), passed strict control requirements for companies transferring personal data to Safe Harbor-certified data recipients in the United States. In addition, the German government is currently preparing new legislation regarding employee data protection.

Generally, the importance of data privacy as one major part of corporate compliance in Germany has increased substantially during the last few years – and it can safely be assumed that this trend will continue. As a consequence, companies operating in Germany need to stay current with these developments, and review their data privacy compliance programs.

For more information about this subject or if you have any further questions regarding the above please contact your regular contact or one of the attorneys listed below.

**Tim Wybitul**  
+49 69 79 41 2271  
twybitul@mayerbrown.com

**Dr. Andrea Patzak**  
+49 69 79 41 1067  
apatzak@mayerbrown.com

**Dr. Guido Zeppenfeld**  
+49 69 79 41 2241  
gzeppenfeld@mayerbrown.com
Cloud Computing May Violate German Data Privacy Laws

Mayer Brown is a leading global law firm serving many of the world’s largest companies, including a significant portion of the Fortune 100, FTSE 100, DAX and Hang Seng index companies and more than half of the world’s largest investment banks. We provide legal services in areas such as Supreme Court and appellate, litigation; corporate and securities; finance; real estate; tax; intellectual property; government and global trade; restructuring, bankruptcy and insolvency; and environmental.

OFFICE LOCATIONS
- Asia: Bangkok, Beijing, Guangzhou, Hanoi, Ho Chi Minh City, Hong Kong, Shanghai

ALLIANCE LAW FIRMS
- Spain (Ramón & Cajal); Italy and Eastern Europe (Tonucci & Partners)

Please visit our web site for comprehensive contact information for all Mayer Brown offices. [www.mayerbrown.com](http://www.mayerbrown.com)

This Mayer Brown publication provides information and comments on legal issues and developments of interest to our clients and friends. The foregoing is not a comprehensive treatment of the subject matter covered and is not intended to provide legal advice. Readers should seek specific legal advice before taking any action with respect to the matters discussed herein.

IRS Circular 230 Notice. Any advice expressed herein as to tax matters was neither written nor intended by Mayer Brown LLP to be used and cannot be used by any taxpayer for the purpose of avoiding tax penalties that may be imposed under US tax law. If any person uses or refers to any such tax advice in promoting, marketing or recommending a partnership or other entity, investment plan or arrangement to any taxpayer, then (i) the advice was written to support the promotion or marketing (by a person other than Mayer Brown LLP) of that transaction or matter, and (ii) such taxpayer should seek advice based on the taxpayer’s particular circumstances from an independent tax advisor.

© 2010. Mayer Brown LLP, Mayer Brown International LLP, Mayer Brown JSM and/or Tauil & Chequer Advogados, a Brazilian law partnership with which Mayer Brown is associated. All rights reserved. Mayer Brown is a global legal services organization comprising legal practices that are separate entities (the Mayer Brown Practices). The Mayer Brown Practices are: Mayer Brown LLP, a limited liability partnership established in the United States; Mayer Brown International LLP, a limited liability partnership in England and Wales; Mayer Brown JSM, a Hong Kong partnership, and its associated entities in Asia; and Tauil & Chequer Advogados, a Brazilian law partnership with which Mayer Brown is associated. “Mayer Brown” and the Mayer Brown logo are the trademarks of the Mayer Brown Practices in their respective jurisdictions.