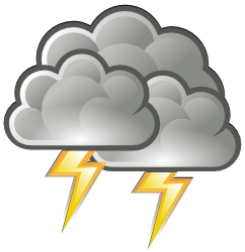
DBSC Infoletter Datenschutz-Praxis ▶ 2013-05

Schlechtes Zeugnis für Cloud Service Anbieter



Die deutsche Niederlassung der international tätigen Anwaltskanzlei Bird & Bird hat im März 2013 die 12-seitige Studie „Cloud for the German Market – Are we getting there? A Rough Line Legal Comparison“ veröffentlicht. Untersucht wurde das Angebot namhafter internationaler Anbieter, die ihre Cloud Services auch auf dem deutschen Markt anbieten. Untersucht wurde das Angebot von Amazon Web Services, HP, IBM, Microsoft, Oracle, Salesfroce und SAP.

Es wurden folgende Geschäftsvereinbarungen analysiert:

• Amazon Web Services: “AWS Customer Agreement” (as of 15 March 2012), governed by the laws of the State of Washington, and “AWS Service Terms” (as of 26 September 2012), http://aws.amazon.com/de/agreement/

• HP: “Customer Agreement” for HP Cloud Services (as of 3 July 2012), governed by the laws of the State of New York , https://www.hpcloud.com/customer_agreement

• IBM: “Smart Cloud Vereinbarung” (as of 31 August 2012), governed by German law, http://www-05.ibm.com/services/europe/de/cloud-development/contracts/Z125-8499-12_SmartCloud_Agreement_International_31Aug2012_%28sign%29_de.pdf

• Microsoft: “Online-Abonnement-Vertrag” and “Nutzungsrechte für Onlinedienste” (as of October 2012), governed by Irish law, http://www.microsoft.com/global/en-us/office365/RenderingAssets/mosa/MOSA2011Agr-EMEA-GER.htm and ttp://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=31

• Oracle: “RightNow Master Cloud Services Agreement” (as of 13 April 2012), governed by German law, http://www.oracle.com/us/corporate/contracts/rightnow-csa-germany-1715203.pdf

• Salesforce: “Rahmen Abonnementvertrag” (as of 15 September 2009), governed by German law, http://www.salesforce.com/de/company/updated_privacy.jsp (neu seit 25.9.2010)

• SAP: “General Terms and Conditions for SAP Cloud Services” (as of August 2012, updated as of January 2013), governed by German law, http://www.sap.com/corporate-en/our-company/agreements/western-europe/agreements.epx?SearchText=&SortBy=&SortOrder=ASC&Filter1=DE&Filter2=&Filter3=AGMT011&Filter4=TYP0083&page=1&pageSize=20

Trotz Bemühungen der Cloud Sercices Anbieter, den Anforderungen des deutschen Rechts nachzukommen, zählt das Fazit der Studie gewichtige Bedenken und Mängel auf:

- Die Lizenzbedingungen sind teilweise nicht sehr ausführlich.
- Die Haftungs- und Gewährleistungsbestimmungen sind überwiegend inkompatibel mit AGB-Rechtsnormen (BGB).
- Konformität mit AGB-Rechtsnormen (BGB) stellt eine Herausforderung für die Geschäftsmodelle dar.
- Die Datenschutz-Dokumentation ist deutlich unterentwickelt.
- Die Bedingungen zur Vertragsbeendigung sind rückständig und aus der Sicht des Anwenders Besorgnis erregend .
- Die Allgemeinen Geschäftsbedingen sind zu verbessern - die Entwicklung bewährter Methoden ist im Fluss.

Hinsichtlich der Anforderungen des BDSG, insbesondere durch den § 11, Auftragsdatenverarbeitung und § 9, Technisch-organisatorische Maßnahme, werden schwere Versäumnisse attestiert.

Quelle:

http://www.twobirds.com/English/News/Documents/CloudGermanMarket_03.2013_001032-05.pdf

Weitere Empfehlungen zum Thema Cloud Computing:

- BMWI Cloud Computing – Leitfaden für mittelständische Unternehmen
- BSI Sicherheitsempfehlungen für Cloud Computing Anbieter
- Stellungnahme des Deutschen Anwaltvereins zum Cloud Computing

Bestellung von Datenschutzbeauftragten für Arztpraxen

Anwendbar für den Arzt bzw. die Arztpraxis ist das Bundesdatenschutzgesetz (BDSG). § 4 BDSG beschreibt den Grundsatz der Zulässigkeit der Datenerhebung, Verarbeitung und Nutzung. Diese sind nur zulässig, soweit das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Für den Arzt sind des Weiteren die Regelungen des Dritten Abschnitts des BDSG relevant. Dieser regelt u. a. das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke.

Nach § 4 f BDSG sind auch nicht-öffentliche Stellen, die Patientendaten automatisiert verarbeiten, verpflichtet, einen betrieblichen Datenschutzbeauftragten zu bestellen. Nach § 4 f BDSG besteht diese Verpflichtung immer dann, wenn mehr als neun Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Bei der Ermittlung der Anzahl der Personen sind die Mitarbeiter(innen) zu berücksichtigen, die nicht nur gelegentlich mit der Datenverarbeitung beschäftigt sind; dies sind typischerweise die Mitarbeiter(innen), die z. B. mit der Datenerfassung (Empfang) oder Datenverarbeitung (Abrechnung) befasst sind. Erfasst werden auch angestellte Ärzte, Auszubildende sowie sonstige freie Mitarbeiter, aber nicht der Praxisinhaber selbst. Ständig beschäftigt ist eine Person, wenn sie für diese Aufgabe, die nicht ihre Hauptaufgabe zu sein braucht, auf unbestimmte, zumindest aber längere Zeit vorgesehen ist und sie entsprechend wahrnimmt.

§ 4 f Abs. 2 BDSG legt die qualitativen Anforderungen an betriebliche Datenschutzbeauftragte fest. Zum betrieblichen Datenschutzbeauftragten kann nur bestellt werden, wer die zur Erfüllung der Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. Das Maß der erforderlichen Fachkunde bestimmt sich nach dem Umfang der Datenverarbeitung und dem Schutzbedarf der personenbezogenen Daten. Zur erforderlichen Fachkunde gehören neben guten Kenntnissen über die technischen Gegebenheiten auch gute Kenntnisse über die rechtlichen Regelungen, insbesondere über die ärztliche Schweigepflicht. Auch ein Mitarbeiter der Arztpraxis, der über entsprechende Kenntnisse verfügt, kann zum betrieblichen Datenschutzbeauftragten bestellt werden. Die Fachkenntnisse können auch über Schulungen, die beispielsweise von den Ärztekammern und Kassenärztlichen Vereinigungen angeboten werden, erworben werden.

Da das BDSG in § 4 f Abs. 2 Satz 3 nunmehr ausdrücklich auch den externen Datenschutzbeauftragten vorsieht, kann mit der Wahrnehmung der Funktion des betrieblichen Datenschutzbeauftragten in Arztpraxen auch ein Externer beauftragt werden. Diesem steht ebenso wie dem Arzt ein Zeugnisverweigerungsrecht zu. Im Übrigen wird ihm gem. § 203 Abs. 2 a StGB eine strafbewehrte Schweigepflicht auferlegt.

Quelle: http://www.bundesaerztekammer.de/downloads/Empfehlung_Schweigepflicht_Datenschutz.pdf

Risiken von Fernwartungssoftware – Schutz der Betriebsangehörigen

Unter Fernwartung versteht man den Fernzugriff mittels einer Fernwartungssoftware (auch "Remote-Software" genannt) auf Systeme, wie PCs, Server oder Industrieanlagen, zu Wartungs- und Reparaturzwecken. Eine Fernwartungssoftware ermöglicht, auf andere PCs zuzugreifen, Daten zu übertragen oder gemeinsam an Projekten zu arbeiten.

Ein missbräuchlicher Einsatz der Fernwartungssoftware, etwa zur Ausforschung der PCs von Beschäftigten, ist aus technischer Sicht grundsätzlich möglich. So können z.B. Tastaturanschläge und Mausbewegungen nahezu in Echtzeit übertragen werden. Auch können Support-Techniker die Bildschirmansicht eines fremden PCs auf dem eigenen Bildschirm wiedergeben. Fernwartungssoftware darf nur unter den jeweils geltenden materiell-rechtlichen Voraussetzungen und technisch-organisatorischen Bedingungen verwendet werden, die einen Missbrauch soweit wie möglich ausschließen. Maßnahmen zur technischen Absicherung von Fernwartung werden vom Bundesamt für Sicherheit in der Informationstechnik empfohlen (abrufbar unter www.bsi.de). Sie eröffnen einen Weg zur datenschutzgerechten Ausgestaltung derartiger Zugänge.

Zudem sind in § 9 Satz 1 Bundesdatenschutzgesetz sowie dessen Anlage 1 Anforderungen festgelegt, die auch bei einer datenschutzgerechten Gestaltung von Wartungsprozessen zu berücksichtigen sind. Dazu gehört insbesondere, dass nur autorisierte Personen Zugang zu den Anlagen haben, mit denen personenbezogene Daten verarbeitet oder genutzt werden, der Zugriff Unbefugter ausgeschlossen sowie zu gewährleisten ist, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.

Fazit: Es wird dringend empfohlen gemeinsam mit dem Betriebsrat für die erforderliche Transparenz zu sorgen.

Quelle: Tätigkeitsbericht des Landesbeauftragten für Datenschutz und Informationsfreiheit NRW, 2011/2012