Entschließung der Konferenz der Datenschutzbeauftragten in der Evangelischen Kirche in Deutschland zum Thema Cloud Computing vom 1. Juli 2015

1. Cloud Computing von personenbezogenen Daten ist möglich, wenn der kirchliche Datenschutz beachtet wird.

Auch im kirchlichen Bereich werden immer häufiger technische Lösungen in einer Cloud angestrebt. Die Cloud (zu Deutsch: Wolke) steht in der Informatik immer für eine „ferne und undurchsichtige“ Rechnerlandschaft. Unter Cloud Computing verstehen wir daher die Datenverarbeitung in solch einer Rechnerlandschaft. Diese Rechnerlandschaften werden in der Regel automatisiert bedarfsgerecht angepasst, um so größere oder auch geringere Verarbeitungskapazitäten zu erlangen. Die Spannbreite der im Rahmen des Cloud Computings angebotenen Dienstleistungen umfasst insbesondere Infrastrukturen (z.B. Rechenleistung, Speicherplatz), Plattformen und Software.

Wenn man das Thema Cloud Computing unter datenschutzrechtlichen Gesichtspunkten betrachtet, gibt es mehrere grundsätzliche Aspekte, die im kirchlichen Bereich beachtet werden müssen:

- Sofern der Cloud-Anwender eine kirchliche Stelle im Bereich verfasster Kirche oder im Bereich der Diakonie ist, kommt das Datenschutzgesetz der EKD (DSG-EKD) zur Anwendung. Das im staatlichen Bereich geltende Bundesdatenschutzgesetz gilt nicht im kirchlichen Bereich. In den meisten Landeskirchen gibt es darüber hinaus Durchführungsbestimmungen oder ergänzende Bestimmungen zum DSG-EKD. Welche weiteren kirchlichen oder sonstigen datenschutzrechtlichen Regelungen zur Anwendung kommen, muss im Einzelfall geprüft werden.
- Das Thema Cloud Computing ist unter datenschutzrechtlichen Gesichtspunkten dann relevant, wenn personenbezogene Daten in der Cloud gespeichert werden. Gemäß § 2 Absatz 1 DSG-EKD sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person.
- Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind auch in der Cloud nur zulässig, wenn das DSG-EKD oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder soweit die betroffene Person eingewilligt hat (§ 3 DSG-EKD).
- Bei Cloud Computing handelt es sich datenschutzrechtlich um eine Auftragsdatenverarbeitung (ADV) gemäß § 11 DSG-EKD. Die gesetzlichen Vorgaben zur Auftragsdatenverarbeitung sind deswegen auch beim Cloud Computing einzuhalten.
- Die besonderen Vorschriften für Daten, die dem Berufsgeheimnis nach § 203 StGB unterliegen, sind zu berücksichtigen.

2. Die kirchliche Stelle, die das Cloud Computing von personenbezogenen Daten einsetzt, schließt mit dem Cloud-Anbieter einen schriftlichen Vertrag zur Auftragsdatenverarbeitung auf der Grundlage des DSG-EKD ab.

Beim Cloud Computing von personenbezogenen Daten gelten die Bestimmungen nach § 11 DSG-EKD. Dabei muss zwischen der kirchlichen Stelle und dem Cloud-Anbieter ein schriftlicher Vertrag zur Auftragsdatenverarbeitung (ADV-Vertrag) abgeschlossen werden, der die Anforderungen aus § 11 DSG-EKD erfüllt. Insbesondere muss er Regelungen zu allen in § 11 Absatz 3 Nr. 1 bis 10 DSG-EKD genannten Punkten enthalten. Der Cloud-Anwender als Auftraggeber bleibt verantwortliche Stelle. So machen Betroffene ihre Rechte weiterhin gegenüber dem Auftraggeber geltend.

Der Cloud-Anbieter als Auftragnehmer muss sorgfältig ausgewählt werden. Wichtige Kriterien sind dabei die von ihm getroffenen technischen und organisatorischen Maßnahmen. Deshalb ist die kirchliche Stelle als Auftraggeber verpflichtet, sich vor Beginn der ADV und danach regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers zu überzeugen und dies auch zu dokumentieren. Alternativ kann der Nachweis der Umsetzung dieser Maßnahmen auch durch Vorlage eines aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudits (z.B. nach BSI-Grundschutz, TCDP) erbracht werden.

Der Cloud-Anwender muss außerdem im Vertrag sicherstellen, dass ein nicht kirchlicher Cloud-Anbieter die kirchlichen Datenschutzbestimmungen - das sind nicht nur die Bestimmungen des DSG-EKD, sondern beispielsweise auch Verordnungen der Landeskirchen oder Dienstvereinbarungen - beachtet und sich der Kontrolle kirchlicher Datenschutzbeauftragter unterwirft.

3. Cloud Computing von personenbezogenen Daten in Staaten außerhalb der Europäischen Union ist verboten.

Gemäß § 11 Absatz 2 Satz 1 DSG-EKD dürfen personenbezogene Daten nur innerhalb der Mitgliedsstaaten der Europäischen Union erhoben, verarbeitet oder genutzt werden. Ausnahmen können durch die Evangelische Kirche von Deutschland gemäß § 11 Absatz 2 Satz 2 DSG-EKD zugelassen werden, wenn die Staaten ein dem DSG-EKD angemessenes Datenschutzniveau nachgewiesen haben. Da bisher keine Ausnahmen durch die Evangelische Kirche in Deutschland definiert wurden, ist zum gegenwärtigen Zeitpunkt eine Nutzung von Cloud-Diensten für personenbezogene Daten in Staaten außerhalb der Europäischen Union verboten.

4. Cloud Computing von unverschlüsselten personenbezogenen Daten innerhalb der Mitgliedsstaaten der Europäischen Union ist zulässig, wenn der Cloud-Anbieter sicherstellen kann, dass die personenbezogenen Daten nicht an Institutionen außerhalb der Europäischen Union übermittelt werden.

Das Datenschutzniveau in Ländern außerhalb der Europäischen Union entspricht in weiten Teilen nicht den europäischen Standards. Deshalb wurde bei der Novellierung des DSG-EKD eine Bestimmung aufgenommen, die die Datenverarbeitung im Auftrag nur innerhalb der Mitgliedsstaaten der Europäischen Union erlaubt (§ 11 Absatz 2 DSG-EKD).

Vor diesem Hintergrund bieten viele ausländische, insbesondere US-amerikanische Unternehmen, für ihre Cloud-Dienste die Möglichkeit an, die Daten auf Servern in einem Mitgliedsstaat der Europäischen Union verarbeiten zu lassen. Dennoch ist die Inanspruchnahme von ausländischen Cloud-Anbietern, die ihre Daten auf Servern in einem Mitgliedsstaat der Europäischen Union verarbeiten lassen, aufgrund der momentan ungeklärten rechtlichen Situation problematisch.

Selbst wenn die Datenverarbeitung in einem Mitgliedsstaat der Europäischen Union erfolgt, ist damit noch nicht gewährleistet, dass die Daten auch dort bleiben. Insbesondere US-Unternehmen müssen ihren Sicherheitsbehörden (FBI, NSA, CIA) nach US-amerikanischem Recht (z.B. Patriot Act) auch dann Zugang zu Kundendaten gewähren, wenn diese auf Servern im Ausland gespeichert sind. Dies haben in der Vergangenheit mehrere US-Bundesgerichte bestätigt. Aufgrund dieser Situation können Unternehmen wie Microsoft, Google oder Amazon derzeit nicht ausschließen, dass US-Sicherheitsbehörden Zugriff auf die auf ihren europäischen Servern gespeicherten Kundendaten erhalten.

Darüber hinaus ist bisher ungeklärt, welche Konsequenzen es hat, dass im Rahmen der Administration der Cloud (z.B. Einspielen von Updates, Problembehebung) Personen außerhalb der Mitgliedsstaaten der Europäischen Union Zugriff auf die personenbezogene Daten des Cloud-Anwenders haben.

Gerade deswegen ist die Nutzung von Cloud-Diensten eines US-amerikanischen Unternehmens auf europäischen Servern nur dann datenschutzrechtlich vertretbar, wenn gewährleistet ist, dass

- alle personenbezogenen Daten verschlüsselt an die Server in der Cloud übertragen werden,
- dort auch nur verschlüsselt gespeichert werden,
- die Schlüssel ausschließlich beim Cloud-Anwender gespeichert werden und
- die verwendeten Schlüssel dem Stand der Technik entsprechende Sicherheit gewährleisten,

so dass weder die US-Unternehmen noch die US-Sicherheitsbehörden eine Möglichkeit zur Entschlüsselung der Daten haben.

5. Die kirchliche Stelle, die das Cloud Computing von personenbezogenen Daten einsetzt, trägt zu jeder Zeit die volle Verantwortung für die personenbezogenen Daten.

Auch wenn die kirchliche Stelle beim Cloud Computing die personenbezogenen Daten nicht selbst verarbeitet, bleibt sie die für die Einhaltung des Datenschutzes verantwortliche Stelle. Daher machen die betroffenen Personen ihre Rechte auf Auskunft, Berichtigung, Löschung oder Sperrung von Daten ihr gegenüber geltend. Auch eventuelle Schadensersatzansprüche nach § 8 DSG-EKD werden ihr gegenüber geltend gemacht.

Eine kirchliche Stelle, die Cloud Computing betreibt, ist auch dann vollumfänglich zum Schadensersatz nach § 8 DSG-EKD verpflichtet, wenn die den Schaden verursachende und nach den Vorschriften dieses Kirchengesetzes oder nach anderen kirchlichen Vorschriften über den Datenschutz unzulässige oder unrichtige automatisierte Verarbeitung personenbezogener Daten vom Cloud-Anbieter verursacht wurde. Eben deshalb ist für den Auftraggeber die sorgfältige Auswahl des Cloud-Dienstleisters und der Abschluss eines ADV-Vertrags von entscheidender Bedeutung (siehe auch Abschnitt 2): Im ADV-Vertrag muss der Cloud-Anbieter zusichern, dass er für den Fall, dass ihm die unrichtige oder unzulässige automatisierte Verarbeitung anzulasten ist, die kirchliche Stelle von Schadensersatzansprüchen freistellt.

6. Besondere Arten personenbezogener Daten müssen in der Cloud verschlüsselt abgespeichert werden.

Besondere Arten personenbezogener Daten sind nach § 2 Absatz 11 DSG-EKD „Angaben über rassische und ethnische Herkunft, politische Meinungen, religiöse und weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben. Dazu gehört nicht die Zugehörigkeit zu einer Kirche oder sonstigen Religionsgemeinschaft“.

Solche Daten unterliegen einem höheren Schutzbedarf als sonstige personenbezogene Daten und dürfen deswegen aufgrund ihrer besonderen Sensibilität nur verschlüsselt auf Cloud-Dienste übertragen und darin gespeichert werden. Dies bedeutet, dass die Daten verschlüsselt werden, bevor sie auf die Server des Cloud-Anbieters übertragen werden. Die hierfür verwendeten Schlüssel dürfen dem Cloud-Anbieter nicht bekannt sein und müssen eine dem Stand der Technik entsprechende Sicherheit gewährleisten.

Hannover, den 1. Juli 2015

Die Beauftragten für den Datenschutz in der EKD