DER DATENSCHUTZBEAUFTRAGTE
FÜR KIRCHE UND DIAKONIE

Datenschutzaufsichtsbehörde gemäß Kapitel 6 DSG-EKD für:

Ev.-Luth. Landeskirche Sachsens
Evangelische Landeskirche Anhalts
Diakonisches Werk der Ev.-Luth. Landeskirche Sachsens e.V.
Diakonisches Werk Evangelischer Kirchen in Mitteldeutschland e.V.

Der Datenschutzbeauftragte für Kirche und Diakonie
Reichenbrander Str. 4 ▪ 09117 Chemnitz

Datenschutzbeauftragter
Herr Pierre Große

Reichenbrander Str. 4
09117 Chemnitz

Tel.: 0351 4692-460
Fax: 0351 4692-469

Datenschutzbeauftragter@evlks.de

An die Verantwortlichen und Beauftragten in den Kirchen, kirchlichen Einrichtungen, Träger und Einrichtungen der Diakonischen Werke in der Ev.-Luth. Landeskirche Sachsen, in der Evangelischen Landeskirche Anhalt, im Diakonischen Werk der Ev.-Luth. Landeskirche Sachsens e.V. und im Diakonischen Werk Evangelischer Kirchen in Mitteldeutschland e.V.

Position des Datenschutzbeauftragten für Kirche und Diakonie zur Frage des Einsatzes von Microsoft Office 365

Datum:
Chemnitz, 16.07.2019

Der Datenschutzbeauftragte für Kirche und Diakonie, zuständige Aufsichtsbehörde für den Datenschutz gemäß Kapitel 6 des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD) stellt mit der heutigen Veröffentlichung seine derzeitige Position zu Fragen des Einsatzes von Office 365 dar.

Der Themenkomplex beschäftigt unsere Behörde seit ihrer Einrichtung und war zuletzt Gegenstand der Gespräche auf der Konferenz der kirchlichen Datenschutzbeauftragten im April dieses Jahres. Im Ergebnis wurde die Entschließung zur Nutzung von Microsoft Cloud-Diensten veröffentlicht. Die folgenden Ausführungen dienen für den Zuständigkeitsbereich unserer Behörde der Konkretisierung.

Mit dieser Position werden auch Fragen beantwortet, die unsere Behörde aufgrund der Stellungnahme des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zum Einsatz von Office 365 an Schulen erreicht haben: Der Hessische Beauftragte schreibt dort: „Der Einsatz von Microsoft Office 365 an Schulen ist datenschutzrechtlich unzulässig, soweit Schulen personenbezogene Daten in der europäischen Cloud speichern."

Der dazu angeführte Grund ist, dass nach jahrelanger Diskussion weiterhin die Frage bestehe, „ob die Schule als öffentliche Einrichtung personenbezogene Daten (von Kindern) in einer (europäischen) Cloud speichern kann, die z. B. einem möglichen Zugriff US-amerikanischer Behörden ausgesetzt ist." Für diese Begründung wird auf die „besondere Verantwortung hinsichtlich der Zulässigkeit und Nachvollziehbarkeit der Verarbeitung personenbezogener Daten" durch öffentliche Einrichtungen hingewiesen. Ergänzend und als weiter bestehendes Problem wird die Fülle von Telemetriedaten erwähnt, die durch das Betriebssystem Windows 10 als auch Office 365 an den Hersteller Microsoft übermittelt werden.

Der Datenschutzbeauftragte für Kirche und Diakonie erkennt die vom Hessischen Beauftragten in seiner Stellungnahme benannten und bereits länger bekannten Aspekte und offenen Fragen als solche an, schließt sich jedoch seiner Entscheidung, die Verwendung von Office 365 in Schulen als unzulässig einzuordnen für seinen Zuständigkeitsbereich nicht an.

Die angeführten Gründe stellen nach Einschätzung des Datenschutzbeauftragten für Kirche und Diakonie keine neue Lage dar, welche eine solche Entscheidung rechtfertigen und weil sich das Thema gerade nicht allein auf Schulen beschränkt bzw. jede Antwort neue Fragen für die Geltung

außerhalb des Bereiches Schule aufwerfen, antwortet dieses Positionspapier auch in dem Sinne allgemein, dass die getroffenen Aussagen umfassend verstanden werden sollen.

Die eingangs zitierte Feststellung, dass die Datenverarbeitung mit Office 365 (durch Schulen) unzulässig sei, weil „die Sicherheit und Nachvollziehbarkeit der Datenverarbeitungsprozesse nicht gewährleistet sind“, steht nach unserer Einschätzung in keinem sachlichen Zusammenhang mit dem angeführten Grund möglicher Zugriffe US-amerikanischer Behörden auf die in einer europäischen Cloud gespeicherten Daten.

Der Datenschutzbeauftragte für Kirche und Diakonie sieht sich durch die Positionierung des Europäischen Datenschutzausschusses zu den Auswirkungen des U.S. CLOUD Acts vom 10.07.2019, in seiner Einschätzung bestätigt, dass es weiterhin die erste Verantwortung der politischen Ebene ist, die Durchsetzung der vom Ausschuss formulierten Position zu erreichen, dass: „für eine rechtmäßige Übermittlung von Daten, die nach dem U.S. CLOUD Act ersucht werden, grundsätzlich ein datenschutzkonformes internationales Abkommen erforderlich ist.“ Dem Sinn nach ergibt sich daraus, dass insofern jedes nicht abgestimmte, einseitige Vorgehen nach dem U.S. CLOUD Act als Rechtsbruch und Angriff auf die Souveränität jedes Staates angesehen wird.

Die Position des Datenschutzbeauftragten für Kirche und Diakonie ist, dass allein die Möglichkeit des unautorisierten Datenzugriffs noch kein ausreichendes Indiz für die datenschutzrechtliche Unzulässigkeit einer Verarbeitung personenbezogener Daten darstellen kann. Andernfalls würde praktisch jede Datenverarbeitung unzulässig werden.

Für eine Speicherung von personenbezogenen Daten in europäischen Cloud-Umgebungen auf der Grundlage des DSG-EKD werden keine besonderen Hinderungsgründe gesehen. Unabdingbar bleibt die Nachweispflicht der Verantwortlichen, ausschließlich zuverlässige Cloud-Anbieter zu beauftragen, die ihrerseits die datenschutzkonforme Verarbeitung im Auftrag nachweisen können. Zu diesen Nachweisen gehören mindestens die Zertifizierung der Rechenzentren, für die Kriterien nach DIN EN 50600 oder vergleichbar und für die vom Cloud-Anbieter einzuhaltenden Regeln der Verarbeitung von personenbezogenen Daten in einer Cloud nach ISO/IEC 27018 oder vergleichbar.

Im Hinblick auf die Gewährleistung der Sicherheit und Nachvollziehbarkeit der Datenverarbeitungsprozesse teilen wir die Einschätzung des Hessischen Beauftragten zur Problematik der nicht vollständigen Transparenz der Telemetriedaten, sehen hier jedoch einen vorläufig ausreichenden Grad an erzielten Fortschritten vor allem auch begründet in der Bereitschaft von Microsoft zur Information und Zusammenarbeit sowie in der konkreten Maßnahmenumsetzung. So hat der Hersteller die Ende 2018 zugesagten Verbesserungen der Transparenz bei den Telemetriedaten mit der Office 365 Version 1903 begonnen umzusetzen.

Hinsichtlich der Telemetriedaten, die vom Betriebssystem Windows 10 übermittelt werden, setzen wir darüber hinaus auf weitere Erkenntnisse und Umsetzungsempfehlungen für die Praxis durch die beim Bundesamt für Sicherheit in der Informationstechnik tätige Projektgruppe zur Analyse der Telemetriekomponenten in Windows 10. Nach unserem Kenntnisstand stellt Microsoft mit den Professional- und Enterprise Versionen allen Unternehmenskunden technische Möglichkeiten zur Verfügung, um den Umfang an übermittelten Telemetriedaten zu reduzieren. Hier erwarten wir von Microsoft, weitere Anstrengungen zu unternehmen, um vollständige Transparenz herzustellen.

Der Druck auf Hersteller wie Microsoft durch öffentlichkeitswirksame behördliche Stellungnahmen zur Einhaltung des Datenschutzes bewirkt gleichzeitig Verunsicherung bei vielen Verantwortlichen auch in Einrichtungen der Kirche und Diakonie, welche gleichwertig zur DS-GVO ausschließlich dem Datenschutzrecht der evangelischen Kirche in Deutschland, dem DSG-EKD unterliegen.

Die Verunsicherung steigt, wenn bedacht wird, dass hier nur ein bekannter Hersteller und eine Produktfamilie im Fokus stehen, während die zitierten „alternativen“ Cloud-Lösungen nicht selten ungeprüft mit dem „Speicherort Deutschland“ werben.

In der Stellungnahme des Hessischen Beauftragten für den Datenschutz und die Informationsfreiheit vermissen wir die Abwägung der Verhältnismäßigkeit unter Berücksichtigung des mit Office 365 bereits heute erreichbaren Datenschutzniveaus nach dem Stand der Technik.

Der Satz in der Pressemitteilung unter Punkt 4: „Bis zu diesem Zeitpunkt kann sich Schule aber anderer Instrumente wie z. B. On-Premises Lizenzen auf lokalen Systemen bedienen." suggeriert, dass die On-Premise-Option an sich schon eine datenschutzkonforme Verarbeitung ermöglicht, was nach unserer Ansicht nicht der Fall ist. Auch beim Einsatz von Office „on premise" würde der Datenschutzbeauftragte für Kirche und Diakonie im Falle eines Audits u. a. prüfen, ob technisch-organisatorische Maßnahmen wie „Informationsschutz" und „Schutz vor Datenverlust" wirksam etabliert sind und ob Mitarbeitende wirksam auf den datenschutzgerechten Umgang mit den Anwendungen geschult sind.

Der Datenschutzbeauftragte für Kirche und Diakonie sieht den Einsatz von Microsoft Office 365 unter Bedingungen als möglich an. Zu den Bedingungen gehört die Durchführung einer Datenschutzfolgenabschätzung, wie es die Beauftragten für den Datenschutz in der EKD, zu den auch unsere Behörde gehört, in der Entschließung vom 4. April 2019 dargelegt haben. Nach unserer Einschätzung kann sich ein mögliches hohes Risiko vor allem aus der Art und Weise des praktischen Einsatzes der Software ergeben, während technische Aspekte durch den Hersteller fortlaufend umfänglich dokumentiert und Umsetzungshilfen für die technische Herstellung eines angemessenen Schutzniveaus verfügbar gemacht werden müssen.

Weitere Bedingungen für den Einsatz von Office 365 sind die Sicherstellung einer fachkundigen, datenschutzkonformen Administration der Office 365- und Betriebssystemumgebung einschließlich der regelmäßigen Auswertung und Dokumentation von Sicherheitsanalysen zur Erkennung von möglichen Schwachstellen und der Umsetzung ausgewählter Maßnahmen zur laufenden Verbesserung. Diese Aussage wiederholt nur, was bereits jetzt als Standard für den Betrieb jeglicher informationstechnischer Infrastruktur vorausgesetzt und durch die IT-Sicherheitsverordnung der EKD gesetzlich geregelt ist.

In der Verantwortung des Verantwortlichen liegt es auch, alle vom Hersteller oder auch von Drittanbietern verfügbaren technischen Optionen auszuwählen, die eine sichere und datenschutzkonforme Gesamtumgebung schaffen, soweit das geforderte Datenschutzniveau nicht allein durch organisatorische Maßnahmen gewährleistet werden kann. Dazu gehört beispielsweise zur Sicherstellung der Auskunftsfähigkeit bei Auskunftsersuchen Betroffener ein vollständiges und regelmäßiges Backup aller Office 365 Inhalte unter Anwendbarkeit der innerbetrieblich festgelegten und datenschutzkonformen Zugriffsberechtigungen. Das Hinzuziehen nachgewiesen fachkundiger Dienstleister wird erwartet, wenn in Einrichtungen und bei Trägern von Kirche und Diakonie keine eigene Expertise durch entsprechende Zertifizierungen und laufende Fortbildungen der mit IT-Themen betrauten handelnden Personen nachgewiesen werden kann.

Der Datenschutzbeauftragte für Kirche und Diakonie
Pierre Große

Autor: Erik Kahnt

Referent beim Datenschutzbeauftragten für Kirche und Diakonie, Unabhängige Aufsichtsbehörde gemäß Kapitel 6 des Kirchengesetzes über den Datenschutz (DSG-EKD)