Katholisches Datenschutzzentrum Frankfurt/M.

Datenschutzrechtliche Bewertung eines Einsatzes von Office 365 auf der Plattform der Microsoft Cloud

Vorbemerkung:

Das Katholische Datenschutzzentrum Frankfurt/M. (KDSZ-FFM) hat sich bereits von Juli 2017 bis Februar 2018 mit der Frage befasst, ob die als „Microsoft Cloud Deutschland“ beworbene Cloud-Lösung der Microsoft Deutschland, die zusammen mit der T-Systems als Datentreuhänder und völlig getrennt vom restlichen globalen Microsoft-Netz erbracht wurde unter Datenschutzaspekten zulässig betrieben werden kann. Eine europäische oder weltweite Cloud-Lösung des Unternehmens wurde damals nicht betrachtet und nicht bewertet.
Inzwischen hat Microsoft am 31.08.2018 das Angebot der „Deutschland Cloud“ zum Jahresende 2018 – zumindest für Neukunden – abgekündigt. Stattdessen sollen die deutschen Rechenzentren in Berlin und Frankfurt als neue „Rechenzentrumsregion Deutschland“ in das globale Microsoft-Netz integriert werden. Die Moderation durch einen Daten-Treuhänder wird komplett entfallen. Microsoft sichert die umfassende Befolgung der DSGVO zu, macht aber über die konkrete Umsetzung keine weiteren Angaben.

Wenige Monate zuvor wurde mit Unterzeichnung am 28. März 2018 der US-amerikanische „*CLOUD-Act*“ (Clarifying Lawful Overseas Use of Data-Act) verabschiedet. Dieses Gesetz verpflichtet US-Unternehmen, amerikanischen Sicherheitsbehörden Zugriff auch auf Nutzerdaten zu ermöglichen, die außerhalb der USA gespeichert sind. Hintergrund der umstrittenen Gesetzgebung in den USA war ein jahrelanger Streit über den Zugriff auf Daten, die US-Firmen auf Servern im Ausland gespeichert haben. Der US-Supreme Court sollte eigentlich in diesem Jahr ein Urteil fällen, ob Microsoft E-Mails von einem in Irland stehenden Server herausgeben muss. Doch nach der Verabschiedung des *CLOUD-Acts* erklärte das oberste US-Gericht den Fall für erledigt. Damit ist Microsoft definitiv dazu verpflichtet, US-Behörden auf Anforderung Beweismaterial von europäischen Servern zur Verfügung zu stellen. Damit werden normalerweise übliche Verfahren in internationalen Rechtsstreitigkeiten und Strafverfolgungen, nämlich die Anwendung von Rechtshilfeabkommen (Mutual Legal Assistance Treaty) unter Beteiligung der heimischen Behörden, umgangen. Dies wäre ein bußgeldbewehrter Verstoß gegen Artikel 48 DSGVO.

Durch die neuen Rahmenbedingungen wird die datenschutzrechtliche Betrachtung von Office 365-Projekten nicht einfacher. Auf den ersten Blick sind die Datenschutzrisiken in Office 365-Projekten durch den Verzicht auf den Treuhänder, die Integration der Microsoft-Rechenzentren in das globale Netzwerk sowie die drohende Anwendung des *CLOUD-Acts* deutlich größer geworden. Jeder Verantwortliche, der Microsoft mit der Auftragsverarbeitung seiner Daten z.B. im Rahmen einer Office 365-Anwendung beauftragt, muss sich dieser Risiken bewusst sein und entsprechende Maßnahmen treffen.

Durch den Auftraggeber zu beachtende / zu regelnde Aspekte:

Bei Office 365 von Microsoft handelt es sich um einen Cloud-Dienst, konkret in Form eines SaaS (Software-as-a-Service). Zwischen dem Kunden und Microsoft ist daher regelmäßig ein Auftragsverarbeitungsvertrag gem. § 29 KDG bzw. Art. 28 DSGVO abzuschließen. Microsoft hat sich nach den Regeln des „EU/U.S.PrivacyShields“ selbst auditiert und in die *Privacy-Shield-Liste* eintragen lassen. Damit ist die erste Hürde, nach der eine Auftragsverarbeitung im außereuropäischen Ausland nur nach Nachweis eines angemessenen Datenschutzniveaus erlaubt ist, zunächst genommen, zumindest so lange, wie das Konstrukt des *Privacy-Shield-Abkommens* von der europäischen Datenschutzrechtsprechung akzeptiert wird.

Unseres Wissens stellt Microsoft einen Vertragsentwurf zu Verfügung und wird i.d.R. im Vertrag zusichern, die Bestimmungen der europäischen Datenschutznormen einzuhalten. Es sind jedoch Zweifel erlaubt, was eine solche Zusicherung wert ist, wenn Microsoft gemäß des *CLOUD-Acts* gezwungen werden kann, entgegen den Bestimmungen des Auftragsverarbeitungsvertrages Daten gegenüber Dritten (den US-Behörden) offenzulegen.

Demnach bestehen zwei hauptsächliche Risiken, deren Eintritt zum Entfall der Rechtsgrundlage einer Auftragsverarbeitung durch Microsoft führen:

- die eventuell gerichtlich festgestellte Unwirksamkeit des *Privacy-Shield-Abkommens*
- die Erzwingung einer Offenlegung von Daten aufgrund des *CLOUD-Acts* durch US-amerikanische Behörden.

Dazu kommen die üblichen Risiken, die immer mit der Auswahl und Beauftragung eines externen Dienstleisters verbunden sind: ungeplanter, plötzlicher Ausfall des Dienstleisters durch Insolvenz oder mangelndes Interesse des Dienstleisters an der Weiterführung der Geschäftsbeziehung, ungeplante Erhöhung der Kosten durch Ausnutzen einer Monopolstellung, Abfluss von unternehmenskritischem Know-how.

Der Verantwortliche ist nach § 26 KDG verpflichtet, technische und organisatorische Maßnahmen zu treffen, die die Sicherheit der Datenverarbeitung gewährleisten. Zu den Schutzzielen gehören u.a. die Vertraulichkeit und die Verfügbarkeit der Daten. Identifizierte Risiken sind zu berücksichtigen und zusammen mit der Wirksamkeit der getroffenen Maßnahmen kontinuierlich zu beobachten.

Exit-Strategie:

Aufgrund der hohen Wahrscheinlichkeit des Eintritts eines der o.a. Risiken ist es aus Sicht des KDSZ-FFM, für den Fall der erzwungenen Vertragsbeendigung eine realistische Exit-Strategie vorzuhalten, die es erlaubt, die an Microsoft ausgelagerten Dienste innerhalb der meistens 90-tägigen Kündigungsfrist ins eigene Haus oder zu anderen, datenschutzkonform arbeitenden Dienstleistern zu übertragen.

Eine Exit-Strategie umfasst mindestens die folgenden Elemente:

- Auswahl eines Ersatz-Dienstleisters (ggf. Insourcing), der ggf. vertraglich zu einer Stand-By-Bereitschaft im erforderlichen Umfang verpflichtet wird
- Erstellung von Beschaffungsplänen für alle notwendigen Beschaffungen, die mit einem Dienstleisterwechsel oder einem Insourcing verbunden sind, einschließlich evtl. Infrastrukturmaßnahmen

- Hochrechnung von Laufzeiten für die Rückübertragung der Daten auf Basis der aktuellen und der prognostizierten Datenmengen
- Überprüfung der Machbarkeit und der Laufzeit einer Datenrückübertragung anhand von Stichproben
- Vorbereitung von Benutzeranleitungen für die Datenrückübertragung sowie geänderten Prozessbeschreibungen für den Betrieb nach der Umstellung

Die Exit-Strategie ist während der gesamten Laufzeit der Dienstleistung aktuell zu halten, an organisatorische und technische Änderungen anzupassen und ihre Wirksamkeit zu überprüfen (z.B. die Zeit, die für eine Rückladung großer Mengen von Daten (Postfächer) aus der Microsoft-Cloud benötigt wird oder auch die Lieferzeit für evtl. neu zu beschaffende Hardware im eigenen Haus).

Customer Lockbox:

Um Transparenz über die Zugriffe auf personenbezogene Daten sicherzustellen, die im Wartungsfall von Beschäftigten von Microsoft und der von diesem Unternehmen eingesetzten Unterauftragnehmer vorgenommen werden, die in einem Drittland außerhalb der EU ansässig sind, für das kein Angemessenheitsbeschluss der Europäischen Kommission i. S. v. § 40 KDG vorliegt, und Zugriffsbegehren bei besonderen Risikokonstellationen ablehnen zu können, ist die Funktion „Customer Lockbox“ zu aktivieren. Hiervon kann nur dann abgesehen werden, wenn die Datenverarbeitung keine Risiken für die Rechte und Freiheiten der betroffenen Personen birgt. Der Einsatz der Funktion bewirkt, dass zuständige Mitarbeiter des Auftragnehmers vor jedem Supportfall mit Zugriff auf Kundendaten eine explizite Einwilligung des Auftraggebers einholen müssen. Die sachkundige Beantwortung dieser Anfragen und die Erteilung der Einwilligung sind sicherzustellen.

Berechtigungskonzept:

Die Cloud-Angebote von Microsoft bieten detaillierte Möglichkeiten, Zugriffsrechte der Mitarbeiter der eigenen Institution zu verwalten. Die Cloud-Berechtigungen müssen im Rollen- und Rechtekonzept der Institution festgelegt werden.
Um eventuelle unberechtigte Datenzugriffe sowohl durch Mitarbeiter des Kunden als auch durch Supportmitarbeiter von Microsoft zumindest nachträglich erkennen zu können, sind die für die jeweiligen Produkte vorgesehenen Protokollierungsfunktionen zu aktivieren und die Protokolle regelmäßig zumindest stichprobenartig unter Beteiligung des behördlichen bzw. betrieblichen Datenschutzbeauftragten zu prüfen.

Mehr-Faktor-Authentifizierung:

Sobald personenbezogene Daten mit den Cloud-Angeboten verarbeitet werden sollen, ist Mehr-Faktor-Authentifizierung einzusetzen, wobei einer der Faktoren der Nachweis des Besitzes z. B. eines Endgerätes oder Sicherheitstokens sein muss. Der zum Nachweis des Besitzes eingesetzte Faktor darf durch die Nutzer nicht kopiert werden können. (Die Anfertigung von Sicherheitskopien im Rahmen des Notfallmanagements ist zulässig.) Microsoft bietet mehrere Mehr-Faktor-Authentifizierungsverfahren

an. Ein weltweit möglicher Zugriff der Nutzer auf personenbezogene Daten, welche allein durch ein Passwort geschützt sind, ist nicht zulässig.

Datenklassifizierung:

Sollten Daten der Kategorien gemäß § 4 Abs. 2 KDG verarbeitet werden, so sind die von Microsoft angebotenen Verfahren zur Klassifizierung von Daten entsprechend ihres Schutzbedarfes zu nutzen. In Grenzen kann die Klassifizierung auch automatisiert erfolgen.

Verschlüsselung der Daten:

Soweit Daten gemäß § 4 Abs. 2 KDG nicht umfänglich, aber mehr als gelegentlich verarbeitet werden sollen, sind weitere Schutzmaßnahmen zu treffen, die gewährleisten, dass diese Daten verschlüsselt in der Cloud gespeichert werden, wobei die Hoheit über die Schlüssel bei dem Auftraggeber liegen muss. Aufgrund der damit einhergehenden hohen Risiken (vgl. § 35 Abs.4 KDG) ist eine umfangreiche Verarbeitung von Daten der o. g. Kategorien der Microsoft Cloud voraussichtlich nicht zulässig. Als Alternative bietet sich dann nur der Einsatz äquivalenter Microsoft-Produkte in einer privaten Cloud an.

Fazit

Eine datenschutz-konforme Nutzung der Microsoft-Cloud-Angebote ist nach Auffassung des KDSZ-FFM aktuell zwar möglich, die Verantwortlichen tragen jedoch ein hohes Risiko, dass die Konformität zu KDG und DSGVO kurzfristig entfallen kann. Das wiederum führt dazu, dass der Verantwortliche jederzeit bereit und in der Lage sein muss, die Dienstleistung schnellstmöglich zu beenden und seinen Rechenbetrieb trotzdem fortzuführen.
Das Risiko besteht zwar grundsätzlich bei jeder Auftragsverarbeitung, ist aber im Fall von Office 365 besonders hoch einzustufen, da der Geschäftsbetrieb i.d.R. ohne Office-Anwendungen kaum fortgesetzt werden kann und der Standort des Dienstleisters in den USA ein besonders hohes Risiko der Nichtvereinbarkeit mit Datenschutzregeln mit sich bringt.
Der Mehraufwand einer deshalb unverzichtbaren Exit-Strategie muss von Anfang an in die Projekte und den laufenden Aufwand eingerechnet werden.
Weitere Maßnahmen zur Erhöhung der Datensicherheit und des Datenschutzes, besonders im Zusammenhang mit der Bearbeitung von Servicefällen (Tickets), sind dringend empfohlen.