Nutzung von Microsoft Cloud-Diensten

Die Konferenz der Beauftragten für den Datenschutz in der EKD hat am 4. April 2019 einstimmig die folgende Entschließung verabschiedet, nach der eine Verwendung von Microsoft Cloud-Diensten unter bestimmten Voraussetzungen datenschutzkonform erscheint:

- *Es wird von Microsoft eine wirksame Zusatzvereinbarung nach § 30 Abs. 5 DSG-EKD angeboten.*
- *Eine Verschlüsselung der Daten ohne Zugang von Microsoft ist möglich (HYOK = Hold your own Key).*
- *Die Übersendung von Telemetriedaten kann durch entsprechende Einstellungen unterbunden werden.*

Vor diesem Hintergrund geben wir nunmehr folgende Empfehlungen und Hinweise zur Nutzung von Microsoft Cloud-Diensten.

Empfehlungen und Hinweise zur ersten Voraussetzung der Entschließung

In den letzten Monaten wurden mit Microsoft ausführliche Verhandlungen über eine wirksame Zusatzvereinbarung geführt. Auf der Grundlage des erreichten Verhandlungsstandes wurde mit einer Landeskirche nunmehr eine Zusatzvereinbarung gem. § 30 Abs. 5 DSG-EKD geschlossen, die als Muster dienen kann. Wir fügen diese Zusatzvereinbarung in anonymisierter Form bei (**s. Anlage**).

Problematisch bleibt an dieser Zusatzvereinbarung die Mehrdeutigkeit. Microsoft war in den geführten Verhandlungen nicht zu eindeutigeren Formulierungen bereit. Wir empfehlen daher dringend in einem Begleitschreiben zur Unterzeichnung der Zusatzvereinbarung die rechtskonforme Auslegung wie folgt festzustellen.

> Zum 2. Absatz der Zusatzvereinbarung:
> Dieser Absatz stellt fest, dass die rechtsgeschäftliche Vereinbarung der Unterwerfung unter die kirchliche Datenschutzaufsicht die gesetzliche Zuständigkeit der staatlichen Datenschutzaufsicht nicht berührt.
>
> Zu Ziffer 1 Satz 2 der Zusatzvereinbarung:
> Diese Regelung könnte als eine Präzisierung der Unterwerfung unter die kirchliche Datenschutzaufsicht nach Satz 1 missverstanden werden. Allerdings bezieht sich Satz 2 auf die Anlage 4 der OST. Dort sind aber gerade keine Regelungen zur Ausübung der Datenschutzkontrolle durch die Datenschutzaufsicht enthalten. Somit kommt eine Auslegung von Satz 2 im vorgenannten Sinne als Präzisierung oder Einschränkung der allgemeinen Aufsichtsbefugnisse nicht in Betracht. Vielmehr handelt es sich bei Satz 2 um

eine zusätzliche Regelung zur allgemeinen Unterwerfung unter die kirchliche Datenschutzaufsicht und es bleibt bei den Kontrollrechten durch die kirchliche Datenschutzaufsicht. Auch im staatlichen Aufsichtsbereich gibt es die vertraglichen Regelungen nach Anlage 4 der OST neben den aufsichtlichen Befugnissen.

Nur wenn die Zusatzvereinbarung in dieser Weise ausgelegt wird, ist sie datenschutzrechtskonform.

Abschließend noch ein Hinweis zu Ziffer 1 Satz 3 der Zusatzvereinbarung: Microsoft besteht auf einer Vergütung und beziffert diese bis heute nicht. Dadurch werden unwägbare Risiken auf den Auftraggeber verlagert, der insbesondere im Falle einer Anweisung durch die Aufsichtsbehörde diese Vergütung tragen muss.

Empfehlungen und Hinweise zur zweiten Voraussetzung der Entschließung

Erforderlich ist, dass eine Ende-zu-Ende-Verschlüsselung aller in die Cloud synchronisierten Daten erfolgt. Das schließt insbesondere E-Mails, Aufgaben und den Kalender in Outlook sowie Dokumente in OneDrive for Business mit ein. Wir empfehlen, dass eine Volltextsuche der verschlüsselten Daten Bestandteil einer solchen Lösung ist. Dabei muss der Schlüssel zum Ver- und Entschlüsseln der Daten immer beim Benutzer selbst liegen. Das bedeutet, dass kein Dritter (z. B. Microsoft) die Daten in der Cloud entschlüsseln und somit einsehen kann.

Empfehlungen und Hinweise zur dritten Voraussetzung der Entschließung

In der Enterprise-Version von Office 365 bietet Microsoft die Möglichkeit, Telemetriedaten abzuschalten. Von dieser Möglichkeit muss Gebrauch gemacht werden.

Hinweis: Grundsätzlich sollte jegliche eingesetzte Software in der Business bzw. Enterprise Edition lizensiert werden.

Wenn Sie bei Ihrer Planung und bei der Einführung von Microsoft Cloud-Diensten diese Empfehlungen und Hinweise beachten, ist der Einsatz nach dem EKD-Datenschutzgesetz zulässig. Bitte beachten Sie, dass die Datenschutzaufsichtsbehörden in der EKD mit ihrer Entschließung davon ausgehen, dass vor Einführung entsprechender Systeme eine Datenschutz-Folgenabschätzung nach § 34 Abs. 1 DSG-EKD durchzuführen ist.