Fazit

Ein datenschutzkonformer Betrieb von Microsoft 365 erscheint nur in Ausnahmefällen möglich. Selbst eine starke Einschränkung der beinhalteten Funktionen kann zwar die Verarbeitung personenbezogener Daten einschränken, diese jedoch nicht vollständig unter die Kontrolle eines Microsoft-Kunden bringen.

Eine genaue Prüfung der datenschutzrechtlichen Aspekte bei einem etwaigen Einsatz von Microsoft 365 und oftmals auch eine Datenschutzfolgenabschätzung sind unumgänglich. Kann ein datenschutzkonformer Einsatz nicht sichergestellt werden, ist davon abzusehen bzw. ist dieser zu beenden. Falls Microsoft 365 bereits eingesetzt wird, ist es daher empfehlenswert, als Verantwortlicher eine Exit-Strategie für Microsoft 365 zu entwickeln und umzusetzen.

Referenzen

Arbeitshilfe Microsoft 365 (KDSZ Frankfurt/M.):

https://www.kath-datenschutzzentrum-ffm.de/wp-content/uploads/Microsoft-365-04-2022-KDSZ-FFM.pdf

Neubewertung des LfDI Baden-Württemberg bezüglich der Datenschutzfolgenabschätzung von Microsoft Office 365:

https://fragdenstaat.de/anfrage/neubewertung-des-lfdi-bezuglich-der-dsfa-von-microsoft-office-365-1/626585/anhang/2021-04-23_Empfehlung_LfDI.pdf

Kath. Datenschutzzentrum Frankfurt/M. Diözesandatenschutzbeauftragte

für die Mittel- und Südwestdeutschen Bistümer

(Erz-)Bistümer Freiburg, Fulda, Limburg, Mainz, Rottenburg-Stuttgart, Speyer, Trier

Domplatz 3, 60311 Frankfurt a.M.
Tel.: 069 8008718-800
E-Mail: info@kdsz-ffm.de

Die weiteren Diözesandatenschutzbeauftragten der Katholischen Kirche sind:

Norddeutsche Bistümer

(Erz-)Bistümer Hamburg, Hildesheim, Osnabrück, Münster (niedersächsischer Teil)

Katholische Datenschutzaufsicht Nord
Diözesandatenschutzbeauftragter
Unser Lieben Frauen Kirchhof 20, 28195 Bremen
Tel.: 0421 330056-0
E-Mail: info@kdsa-nord.de

Ostdeutsche Bistümer und Katholischer Militärbischof

(Erz-)Bistümer Berlin, Dresden-Meißen, Erfurt, Görlitz, Magdeburg

Kirchliche Datenschutzaufsicht
Diözesandatenschutzbeauftragter
Badepark 4, 39218 Schönebeck
Tel.: 03928 7179018
E-Mail: kontakt@kdsa-ost.de

Nordrhein-Westfälische Bistümer und VDD

(Erz-)Bistümer Aachen, Essen, Köln, Münster (nordrhein-westfälischer Teil), Paderborn

Katholisches Datenschutzzentrum
Diözesan- und Verbandsdatenschutzbeauftragter
Brackeler Hellweg 144, 44309 Dortmund
Tel.: 0231 138985-0
E-Mail: info@kdsz.de

Bayerische Bistümer

(Erz-)Bistümer Augsburg, Bamberg, Eichstätt, München-Freising, Passau, Regensburg, Würzburg

Gem. Datenschutzaufsicht der bayerischen (Erz-)Dözesen
Diözesandatenschutzbeauftragter
Kapellenstraße 4, 80333 München
Tel.: 089 21371796
E-Mail: jjoachimski@eomuc.de

Kath. Datenschutzzentrum Frankfurt/M.

Hinweise zur Nutzung von Microsoft 365

Stock Rocket – stock.adobe.com

Hinweise zur Nutzung von Microsoft 365

Dieser Flyer soll Hinweise darauf geben, wo im Zusammenhang mit Microsoft 365 datenschutzrechtliche Herausforderungen liegen und ob ein Verantwortlicher, der mit Microsoft 365 arbeiten möchte, Maßnahmen ergreifen kann, durch die die erkannten Probleme gelöst werden können. Da die datenschutzrechtlichen Bedenken derzeit kaum von den möglichen Gegenmaßnahmen vollständig ausgeräumt werden, empfiehlt das Kath. Datenschutzzentrum Frankfurt/M., den Einsatz von Microsoft 365 zu vermeiden und nötigenfalls Alternativen zu prüfen.

Eine genaue Prüfung der datenschutzrechtlichen Aspekte bei einem etwaigen Einsatz von Microsoft 365 durch den Verantwortlichen und oftmals auch eine Datenschutzfolgenabschätzung ist unumgänglich. Kann ein datenschutzkonformer Einsatz nicht sichergestellt werden, ist davon abzusehen bzw. ist dieser zu beenden. Hier kann bei Bedarf aus zahlreichen alternativen Angeboten ausgewählt werden.

Datenschutzrechtliche Bedenken

Die folgende Auflistung der datenschutzrechtlichen Problempunkte bezieht sich in Teilen auch auf die Ergebnisse einer Studie des LfDI Baden-Württemberg zur Zulässigkeit von Microsoft 365 im Einsatz in Schulen. Es sind diese im Wesentlichen:

- Die unklaren Verarbeitungen personenbezogener Daten durch Microsoft. Die Unklarheiten beziehen sich sowohl auf die tatsächlich verarbeiteten Datenkategorien („Welche Daten werden verarbeitet?“), als auch auf deren Mengen und insbesondere auf die Zwecke, zu denen Microsoft die Daten der Nutzer erhebt und verarbeitet.
- Die Verarbeitung personenbezogener Daten über den zur Bereitstellung der Funktionen notwendigen Umfang hinaus.
- Die Verarbeitung personenbezogener Daten durch Microsoft und unter der Verantwortung Microsofts, die von Auftraggebern nicht verhindert werden können.
- Die umfangreichen Verarbeitungen personenbezogener Daten außerhalb von Inhaltsdaten, insbesondere durch Funktionen, die zu unzulässiger Überwachung und Bewertung von Nutzern missbraucht werden können, und dementsprechende Mängel in Bezug auf Datenschutz durch Technikgestaltung (Privacy-By-Design).
- Die hohe Komplexität bei der Konfiguration und Mängel in Bezug auf die tatsächlich von Microsoft vorgesehenen, nicht datensparsamen Voreinstellungen erschwert die datenschutzgerechte Konfiguration von Microsoft 365 (Privacy-By-Default, § 27 Abs. 2 KDG).
- Die nicht zu vermeidenden Drittlandsübermittlungen personenbezogener Daten zu Microsoft in die USA (die nach dem „Schrems II“-Urteil nicht zulässig sind), sowohl im Zuge des regulären Betriebs als auch im Rahmen von Auskünften an US-Behörden in Bezug auf innerhalb der EU vorgehaltene Daten.

Verfügbare Maßnahmen

Es gibt Maßnahmen, die die datenschutzrechtlichen Schwächen von Microsoft 365 abmildern, die aber nach dem derzeitigen Stand der Erkenntnisse nicht dazu führen, dass Microsoft 365 datenschutzkonform betrieben werden kann. Ein datenschutzkonformer Betrieb von Microsoft 365 erscheint derzeit allenfalls in Ausnahmefällen möglich.

- Grundsätzlich sollten so wenige wie möglich der verfügbaren Module der Microsoft-365-Suite erworben werden bzw. zum Einsatz kommen; z. B. sollten optionale Dienste wie „Connected Experiences“ oder „Productivity Score“ komplett deaktiviert werden.
- Um zu verhindern, dass in Dokumenten enthaltene personenbezogene Daten grundsätzlich auf Microsoft-Servern gespeichert werden, sollte die Synchronisation mit der Microsoft-365-Cloud (beispielsweise One-Drive) deaktiviert und Dokumente nur über Kanäle außerhalb von Microsoft 365 ausgetauscht werden. Dabei sind jedoch zahlreiche Funktionen für das Arbeiten im Team nicht nutzbar.
- E-Mails sollten in einer eigenen E-Mail-Infrastruktur oder bei einem europäischen Dienstleister verarbeitet werden.
- Es ist zu empfehlen, dass nur Desktop-Anwendungen zum Einsatz kommen und mobile Anwendungen gemieden werden. Letztere bergen erhöhte Risiken z. B. dadurch, dass Microsoft keine Möglichkeit zur zentralen Deaktivierung der „Connected Experiences“ in Office Online und in den Mobile Office Apps anbietet.
- Es sollten nur die notwendigen Anwendungen genutzt und weitere Anwendungen aus dem Microsoft Store gemieden werden.
- Funktionen, die Inhalte aus Dokumenten an Microsoft-Server übertragen, wie z. B. zur maschinellen Übersetzung, sollten deaktiviert werden.