Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI
Bundesamt für Sozialversicherung BSV
Direktionstab DS – IT Management ITM

eGov Mitteilung Nr. 054 vom 10.03.2025

Geht an:

- Durchführungsstellen der 1. Säule/FamZ

Betreff: Neue Vorgaben zur Verwendung von Microsoft 365 (M365) bei den Durchführungsstellen der 1. Säule/FamZ (Version 1.0:2025)

Mit dem vorliegenden Schreiben präzisiert das BSV die eGov Mitteilung 053[1] bezüglich der Verwendung von M365.

Seit der Veröffentlichung der eGov Mitteilung 043[2] Anfang 2022 haben diverse Entwicklungen stattgefunden. So hat der Bundesrat mit dem Swiss-U:S. Data Privacy Framework[3] auf den 15. September 2024 eine Änderung der Datenschutzverordnung in Kraft gesetzt (Anhang[4]). Weiter wurden die Risiken des Foreign Lawful Access (Zugriff auf Daten durch ausländische Behörden, namentlich CLOUD Act) neu bewertet.

Ausgangslage und Grundsatz

Microsoft bietet mit M365 eine umfassende Office-Suite (Word, Excel, PowerPoint etc.) an, mit der die Anwender ortsunabhängig mittels verschiedenster Endgeräte arbeiten können. Die ebenfalls zur M365 gehörende Applikation «Teams» ermöglicht als Nachfolgerin von «Skype for Business» umfassende Audio- und Videokommunikation, Chat und die Verwaltung, Bearbeitung und Speicherung von Daten auf SharePoint Online. Zudem wird mit Exchange Online ein cloudbasierter E-Mail-Dienst bereitgestellt, der die Verwaltung und Speicherung von E-Mails, Kalendern und Kontakten ermöglicht.

Die Daten sämtlicher Anwendungen, einschliesslich der in Exchange Online verwalteten E-Mail-Postfächer, werden dabei verschlüsselt in einer Public-Cloud von Microsoft gespeichert.

Die Verschlüsselung der Daten erfolgt bei M365 mittels Keys von Microsoft, so dass die Firma Microsoft die gespeicherten Daten auf Anfrage von US-amerikanischen Gerichten entschlüsseln und gezwungen sein kann, die entschlüsselten Daten gegenüber US-amerikanischen Behörden offenzulegen. Dieses Problem existiert bei on-Premises Lösungen nicht, dafür besteht beim Betrieb von Systemen wie E-Mail (Exchange) unter Umständen ein erhöhtes Risiko für Cyber-Attacken und signifikante Störungen im Betriebsablauf einer Durchführungsstelle,da entsprechende Spezialisten, welche das notwendige Know-How für Wartung und Betrieb besitzen, schwierig zu akquirieren sind.

[1] eGov Mitteilung Nr 053 vom 17.12.2024
[2] eGov Mitteilung Nr. 043 vom 01.01.2022
[3] Medienmitteilung zum Swiss-U.S. Data Privacy Framework: https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-102054.html
[4] Ergänzung im Anhang 1 der DSV: https://www.fedlex.admin.ch/eli/oc/2024/435/de

Bei Public-Cloud Lösungen hingegen werden die jeweils aktuellen Versionen und Techniken verwendet und notwendige Schutzmassnahmen gegenüber Cyber-Attacken sind standardmässig implementiert. Zudem werden Betrieb sowie die Konfiguration der Systeme durch Microsoft selbst gewährleistet.

Nach Abwägung dieser Vor- und Nachteile kommt das BSV zum Schluss, dass die Durchführungsstellen der 1. Säule/FamZ M365 nutzen können. Sie sind jedoch auch weiterhin selber für den Schutz der Daten verantwortlich und müssen sicherstellen, dass die Daten zwingend nur in Rechenzentren innerhalb der Schweiz bearbeitet und gespeichert werden und dass die ISDS-Dokumentation regelmässig aktualisiert, den geltenden Datenschutzbestimmungen entspricht und geeignete technische sowie organisatorische Massnahmen zum Schutz der Daten (beispielsweise Verschlüsselung) getroffen werden. Bei höheren Anforderungen von beispielsweise besonders schützenswerten Personendaten sind eine Schutzbedarfsanalyse, eine Risikoanalyse, die Prüfung der Rechtskonformität und eine Datenschutz-Folgenabschätzung unabdingbar.

Bei der Verwendung von M365 ist bei der Einrichtung ein Tenant (Speicherplatz) in der Schweiz zwingend. Mit diesem ist die Bearbeitung von Personendaten auf verwalteten Endgeräten ohne zusätzliche Verschlüsselung möglich. Ebenfalls können Daten mit Online-Applikationen von M365 bearbeitet und online gespeichert werden. (Beispielsweise Teams, Sharepoint Online, OneDrive for Business oder Exchange Online). Falls auf diese Dienste von ausserhalb der Organisation oder über das Internet zugegriffen wird, muss eine Multi-Factor Authentication (MFA[5]) implementiert sein.

Eine Abhängigkeit von Microsoft-Cloud-Diensten sowie anderen Cloud-Diensten ist mit Risiken verbunden. Die Durchführungsstellen entwickeln eine Ausstiegsstrategie und dokumentieren Massnahmen, um im Notfall handlungsfähig zu bleiben. Details dazu finden sich in der W-ISDS[6] unter Rz 2.15.2.

Die Verwendung von Microsoft Exchange Online ist im Rahmen der oben beschriebenen Limitationen wie Analyse und Bewertung für besonders schützenswerte Personendaten möglich. Der Zugriff von ausserhalb der Organisation, respektive über das Internet muss mittels einer MFA-Lösung abgesichert sein.
Für den Versand von besonders schützenswerten Daten muss zudem zwingend eine entsprechende Verschlüsselungstechnologie nach Stand der Technik eingesetzt werden. (Beispielsweise IncaMail oder gleichwertig)
Details zu den Analysen und Bewertungen finden sich in der W-ISDS, Anhang 3 und 4.

Die Verwendung von weiteren Cloud-Diensten und -Anbietern wird in einer zukünftigen eGov-Mitteilung thematisiert werden.

Wir danken Ihnen für Ihre Kenntnisnahme und die Umsetzung in Ihrer Durchführungsstelle.

Der Bereich ITM

Für anderweitige Fragen wenden Sie sich an egov@bsv.admin.ch

[5] Microsoft MFA: https://go.microsoft.com/fwlink/?linkid=2227647&clcid=0x807&culture=de-ch&country=ch
[6] W-ISDS: https://sozialversicherungen.admin.ch/de/d/20253/download

Hintergrund CLOUD Act und FISA

Durch die beiden US-Gesetze, den CLOUD Act[7] sowie den Foreign Intelligence Surveillance Act (FISA[8]), besteht bei der Verwendung von Public Cloud Providern das Risiko einer Verletzung des schweizerischen Datenschutzes durch Firmen wie Microsoft. Aktuelles Grundproblem ist die Auftrags-Datenbearbeitung durch Firmen, welche aus Schweizer Sicht dem Schweizer Recht unterstehen, jedoch aufgrund des US-amerikanischen Cloud-Acts und FISA von US-amerikanischen Gerichten gezwungen werden können, bestimmte Daten gegenüber US-amerikanischen Behörden offen zu legen. Es ist davon auszugehen, dass ähnliche Probleme auch mit dem Recht anderer Länder bestehen (z.B. China).
Grundsätzlich erlaubt die Schweizer Gesetzgebung die Bekanntgabe von Daten im Rahmen einer Strafuntersuchung (vgl. z.B. Art. 50 Abs. 1 Bst. d AHVG). Aufgrund des Territorialprinzips gehen die verlangten Daten aber nur an eine schweizerische Untersuchungsbehörde. Will eine ausländische Untersuchungsbehörde Auskunft, muss sie die Bekanntgabe von Daten auf dem Weg der Rechtshilfe – gestützt auf entsprechende internationale Abkommen – einfordern. Die zuständige Schweizer Behörde wird dann an die Durchführungsstelle gelangen und die Herausgabe der Daten anfordern. Allerdings erst nach Prüfung des Rechtshilfebegehrens. Rechtshilfebegehren für Straftatbestände, die es nach Schweizer Recht gar nicht gibt, wird nicht stattgegeben.
Cloud-Act und FISA ermöglichen es den US-Behörden quasi in «eigenmächtige Rechtshilfe» das Territorialprinzip auszuschalten und die etablierte Form des Rechtshilfebegehrens zu umgehen.

[7] CLOUD Act: https://www.justice.gov/d9/pages/attachments/2019/04/09/cloud_act.pdf
[8] FISA: Foreign Intelligence Surveillance Act (FISA)