Datentransferabkommen zwischen EU und USA

Warum Pflegeeinrichtungen davon betroffen sind und warum sie Maßnahmen ergreifen müssen.

Foto: AdobeStock/Artcuboy

Von Thomas Althammer

Gelingt der EU und den USA endlich ein Abkommen, das personenbezogene Daten von EU-Bürger:innen in den USA ähnlich weitgehend vor staatlichen Zugriffen schützt, wie in der EU? Das lässt sich bezweifeln.

Zwar hat die EU-Kommission einen neuen Datenschutzrahmen gesteckt und möchte damit Zugriffe von US-Nachrichtendiensten auf „ein notwendiges und verhältnismäßiges Maß“ beschränken, damit US-Unternehmen, die sich dem „Data Privacy Framework“ anschließen, personenbezogene Daten ohne zusätzliche Datenschutzgarantien übermitteln können. Doch was ‚notwendig‘ und ‚verhältnismäßig‘ bedeuten, wird sich erst noch erweisen müssen. Die Datenschutzorganisation Noyb des österreichischen Juristen von Max Schrems hat bereits die dritte Runde vor dem Europäischen Gerichtshof (EuGH) angekündigt. Ausgang offen. Aber was bedeutet das alles für Pflegeeinrichtungen und warum sind sie davon betroffen?

Die Digitalisierung des Gesundheitssektors und der Pflege ist nicht aufzuhalten – schon heute setzen viele Organisationen nicht mehr auf rein lokale IT-Systeme, sondern nutzen cloudbasierte Werkzeuge wie beispielsweise Microsoft 365. Das bedeutet, dass Daten nicht mehr in einem geschlossenen System auf einem organisationseigenen Server gespeichert werden, sondern in Rechenzentren bei Plattformanbietern. Unternehmen und Organisationen sind dabei in der Regel auf die großen Softwareanbieter wie Microsoft, Apple, Google, Amazon AWS angewiesen, also auf Tech-Giganten, die in den USA oder Asien zu Hause sind und viele der Daten auch dort speichern und verarbeiten.

„Bei Verstößen haftet am Ende meist derjenige, der die kritischen Daten in der Cloud gespeichert hat.“

Thomas Althammer

Hier beginnen die Schwierigkeiten mit dem Schutz der Daten: Zum einen gelten außerhalb der EU andere Datenschutzgesetze, zum anderen werden gerade kostenlose Dienste dadurch finanziert, dass unsere personenbezogenen Daten zu Profilbildung oder Werbezwecken ausgewertet werden.

Alle Organisationen, die internationale Dienste nutzen, und sei es nur Smartphones als Dienstgeräte, müssen deshalb bezüglich des neue Data Privacy Frameworks jetzt die Datenschutzdokumentation anpassen.

Pflichten beim Cloud-Computing: Anschaffen, bezahlen & betreiben reicht nicht!

Einrichtungen müssen den beauftragten Dienstleister hinsichtlich der notwendigen technisch-organisatorischen Maßnahmen regelmäßig überprüfen. Die Datenübermittlung in das Ausland ist getrennt zu bewerten. Unabhängige Sicherheitszertifizierungen und Nachweise, z.B. gemäß ISO 27001, können als Nachweise gelebter IT-Sicherheit verwendet werden und so den Aufwand für individuelle Kontrollen reduzieren.

Der Auftraggeber ist verpflichtet, eine schutzbedarfsorientierte Risikoanalyse bezüglich der konkreten Verarbeitung von personenbezogenen Daten in der Cloud durchzuführen. Viele Einrichtungen in der Pflege verarbeiten regelmäßig besonders schützenswerte Daten und müssen bei der Migration in die Cloud zusätzliche Maßnahmen ergreifen, um den europäischen Standard des Datenschutzes für die von ihnen betreuten Klientinnen und Klienten zu gewährleisten.

Auch wenn Daten in deutschen Rechenzentren beziehungsweise innerhalb der EU gespeichert werden können – US-amerikanische Unternehmen müssen gegebenenfalls US-Behörden aufgrund des CLOUD Acts Zugriff auf diese Daten gewähren. Im Jahr 2020 kippte der Europäische Gerichtshof (EuGH) das EU-US Privacy Shield. Da aufgrund dessen die Gültigkeit der EU-Standardvertragsklauseln ohne weiterer technischer und organisatorischer (Schutz-)Maßnahmen mit US-amerikanischen Unternehmen infrage gestellt wurde, bedarf es einer neuen Vereinbarung zwischen der EU und den USA, die nun zwar vorliegt, aber auch schon wieder angezweifelt wird.

Was bedeutet das für Pflegeeinrichtungen, die Microsoft, Apple & Co einsetzen?

Vor Inbetriebnahme von Produkten von Microsoft, META, Apple & Co müssen die Einrichtungen und Organisationen eigentlich eine Datenschutzfolgenabschätzung durchführen und genau prüfen, welche Daten erhoben werden, was in der Verarbeitung mit ihnen passiert und wo sie gespeichert werden (insbesondere persönliche und Gesundheitsdaten). Außerdem muss das Risiko bewertet werden, dass mit dieser Datenverarbeitung entsteht. In der Regel ist dieses Risiko nicht akzeptabel (zumindest, wenn man den Aufsichtsbehörden folgt). Pflegeeinrichtungen als Auftraggeber sind verpflichtet zu überlegen, welche Zusatzmaßnahmen sie als Einrichtung treffen können (über den Abschluss der Verträge hinaus), um das Risiko so weit zu minimieren, dass es akzeptabel wird und Vertraulichkeit, Verfügbarkeit und Integrität der eigenen Informationen und personenbezogenen Daten gewährleistet sind. Erst wenn sie das gemacht und die Maßnahmen umgesetzt haben, können sie die Dienste nutzen – eigentlich. Wer das nicht tut, bewegt sich per se auf dünnem Eis. Denn bei Verstößen haftet am Ende meist derjenige, der die kritischen Daten in der Cloud gespeichert hat.

Ist der Einsatz von Microsoft 365 datenschutzkonform möglich?

Es gibt technische und organisatorische Möglichkeiten, die einzelnen Verarbeitungsvorgänge auf das Nötigste zu begrenzen. Hier einige Beispiele:

- Option „Telemetrie- und Diagnosedaten an Microsoft senden“ auf das Nötigste beschränken.
- So weit wie möglich lokal installierte Versionen der Microsoft-Software nutzen.
- SharePoint Online/OneDrive nur nach intensiver Auseinandersetzung mit den datenschutzrechtlichen Vorgaben nutzen. Besonders schützenswerte Daten gesondert behandeln.

Zu jedem Zeitpunkt bleibt die Pflicht des Verantwortlichen bestehen, für eine rechtmäßige Verarbeitung von personenbezogenen Daten in Microsoft 365 oder anderen Cloud-Angeboten Sorge zu tragen. Meist ist die Erstellung einer Datenschutz-Folgenabschätzung unumgänglich. Es ist also an der Zeit, die eigenen Dienste hinsichtlich des neuen Abkommens der EU mit den USA zu überprüfen und anzupassen.

Der Autor ist Geschäftsführer der Althammer & Kill GmbH & Co. KG, althammer-kill.de

CHECKLISTE FÜR PFLEGEEINRICHTUNGEN:

Datenschutzfolgenabschätzung (DSFA):
- Prüfen, welche Daten von Microsoft, META, Apple & Co erfasst werden.
- Die Verarbeitung, Speicherung und Sicherheitsmaßnahmen untersuchen.

Risikobewertung:
- Das entstehende Risiko bei der Datenverarbeitung bewerten.
- Persönliche und Gesundheitsdaten besonders berücksichtigen.

Zusatzmaßnahmen ergreifen:
- Welche Schutzmaßnahmen über Vertragsabschlüsse hinaus können ergriffen werden?
- Ziel: Minimierung des akzeptablen Risikos.

Maßnahmen umsetzen:
- Die ausgewählten Schutzmaßnahmen effektiv implementieren.
- Vertraulichkeit, Verfügbarkeit und Integrität der Daten gewährleisten

Haftungsvermeidung:
- Darauf achten, dass die getroffenen Maßnahmen den rechtlichen Anforderungen entsprechen.
- Rechtliche Konsequenzen bei Verstößen gegen Datenschutzbestimmungen vermeiden.