BRANDI
RECHTSANWÄLTE

MESSENGER-DIENSTE IM UNTERNEHMEN

Informationen zum Datenschutz I Mai 2024

English version

Einleitung

Die Nutzung von Messenger-Diensten ist aus dem Unternehmensalltag kaum noch wegzudenken. Dies betrifft zum einen die unternehmensinterne Kommunikation sowie zum anderen auch die Kommunikation mit Kunden. Vorteile aus Unternehmenssicht sind vor allem die leichtere Erreichbarkeit von Mitarbeitern ohne festen PC-Arbeitsplatz sowie die persönlichere Kommunikation mit Kunden und die zielgruppengerechte Erreichbarkeit. Problematisch ist demgegenüber häufig, dass die Messenger-Dienste umfassend auf die auf den Mobilgeräten der Nutzer gespeicherten Daten sowie Metadaten zugreifen und diese auswerten.

Kommen WhatsApp & Co. im Unternehmen zum Einsatz, gilt es deshalb, die insoweit bestehenden datenschutzrechtlichen Anforderungen einzuhalten.

WhatsApp (for Business)

Bei der Nutzung von WhatsApp besteht insbesondere die Problematik, dass der Nutzer der App im Rahmen der Installation regelmäßig die Berechtigung erteilt, die Kontaktdaten des eingesetzten Mobilgeräts auszulesen und die im Adressbuch gespeicherten personenbezogenen Daten, also vor allem Namen und Telefonnummern, in regelmäßigen Abständen an einen Server von WhatsApp (Meta) zu übertragen. Durch die Nutzung des Messenger-Dienstes initiiert der Nutzer eine wiederkehrende Übermittlung von personenbezogenen Daten in die USA. Sind in dem Adressbuch des Nutzers auch dienstliche Kontaktdaten hinterlegt, ist in aller Regel das Unternehmen für die Verarbeitung dieser personenbezogenen Kontaktdaten und die im Zuge der WhatsApp-Nutzung erfolgende Drittstaatenübermittlung verantwortlich.

Zumindest die Datenübermittlung in die USA ist zum jetzigen Zeitpunkt einigermaßen zu rechtfertigen, da sich sowohl WhatApp als auch der Meta-Konzern unter dem EU-US Data Privacy Framework zertifiziert haben und sich die mit der Nutzung des Messenger-Dienstes verbundene Drittstaatenübermittlung in die USA insoweit auf den für zertifizierte Unternehmen geltenden Angemessenheitsbeschluss der Europäischen Kommission stützen lässt.

Die Zertifizierung unter dem Data Privacy Framework rechtfertigt aber nicht das Auslesen und das Übermitteln der Kontaktdaten. Hierfür dürfte es an einer Rechtsgrundlage für die in Rede stehende Datenverarbeitung fehlen. Möglich ist allerdings ein Einsatz von WhatsApp auf freiwilliger Basis nach vorheriger Abstimmung zwischen den Kommunikationspartnern. Haben alle im Adressbuch gespeicherten Kontakte der Nutzung zugestimmt, können die im Zusammenhang mit dem Einsatz des Messenger-Dienstes erfolgenden Datenverarbeitungsprozesse auf die Rechtsgrundlage der Einwilligung gem. Art. 6 Abs. 1 S. 1 lit. a) gestützt werden. Kann eine Zustimmung aller Kontakte hingegen nicht sichergestellt werden, sollte der Einsatz des Adressbuchs auf dem eingesetzten Mobilgerät grundsätzlich unterbunden bzw. die Synchronisation des Adressbuchs auf dem Mobilgerät deaktiviert werden, um eine rechtswidrige Datenverarbeitung zu verhindern. Dabei ist darauf zu achten, dass die Einstellung von Beginn an und dauerhaft für WhatsApp vorgenommen wird. Alternativ besteht auch die Möglichkeit, WhatsApp den Zugriff auf das Adressbuch zu verweigern, indem das Adressbuch in einen isolierten Bereich des Mobilgeräts, eine sogenannte „Sandbox“, ausgegliedert wird. Hierdurch kann allerdings nicht verhindert werden, dass WhatsApp im Zuge der Nutzung des Dienstes Metadaten erfasst und diese auswertet.

Soll WhatsApp als Kommunikationskanal gegenüber Kunden verwendet werden, ist darauf zu achten, dass der Kunde der Nutzung vorab zugestimmt hat. Die Nutzung von WhatsApp sollte insoweit immer erst nach Absprache im Einzelfall erfolgen, idealerweise dann, wenn die Initiative vom Kunden bzw. Kommunikationspartner ausgeht. Unternehmen müssen zudem Ihren datenschutzrechtlichen Informationspflichten nachkommen und Kunden transparent über den Einsatz des Messengers sowie die damit einhergehenden Datenverarbeitungsprozesse informieren. Gleiches gilt letztlich für die unternehmensinterne Kommunikation über WhatsApp. Außerdem sollte trotz der Ende-zu-Ende-Verschlüsselung grundsätzlich darauf geachtet werden, dass im Rahmen der WhatsApp-Nutzung nicht unbedarft personenbezogene Daten bzw. sensible Inhalte ausgetauscht und offengelegt werden.

Die Ausführungen gelten entsprechend für andere Messenger-Dienste, soweit mit deren Nutzung ebenfalls eine Datenübermittlung an externe Unternehmen verbunden ist und sich insoweit ähnliche datenschutzrechtliche Probleme stellen.

Sonderfall: Microsoft Teams Chat

Die Chat-Funktion von Microsoft Teams wird noch überwiegend in der Desktop-Anwendung benutzt, jedoch findet auch hier vermehrt ein Rückgriff auf die mobile Teams-Version für Smartphones statt. Die Nutzung betrifft überwiegend die unternehmensinterne und ver-

einzelt auch die Kommunikation mit Außenstehenden. Der Microsoft Teams Chat ist kein klassischer Messengerdienst, jedoch wird er oftmals zur Kommunikation genutzt, weshalb auch hierbei einige datenschutzrechtliche Besonderheiten zu beachten sind.

Sowohl die Inhalte der Chats als auch die Daten über die Nutzenden, also zum Beispiel der Nutzername, die E-Mail-Adresse oder das Profilbild, werden von Microsoft Teams auf Servern in den USA gespeichert. Es gilt also wieder das oben aufgeworfene Problem der Drittstaatenübermittlung zu beachten. Microsoft hat sich aber auch unter dem EU-US Data Privacy Framework zertifiziert. Dadurch ist eine rechtmäßige Übertragung der Daten aufgrund des Angemessenheitsbeschlusses möglich.

Findet die Nutzung von Microsoft Teams und der Chatfunktion zur Begründung oder Durchführung von Verträgen statt, dann ist Art. 6 Abs. 1 lit. b) DSGVO als Rechtsgrundlage einschlägig. In den überwiegenden Fällen wird die Kommunikation aber unternehmensintern stattfinden und ist dann auf Art. 6 Abs. 1 lit. f) DSGVO zu stützen. Dabei besteht das Interesse des Unternehmens in der einfachen Einbidung der weiteren, oft genutzten Produkte von Microsoft und der Kommunikation zwischen den Mitarbeitenden sowohl in Dialogform als auch in der Gruppe.

Im Vorlauf zur Nutzung des Dienstes sind die Mitarbeitenden unbedingt auf die Bedingungen der Nutzung und die Übermittlung in die USA hinzuweisen.

Threema

Aus datenschutzrechtlicher Sicht vorzugswürdig ist etwa der Dienst Threema. Positiv fällt insoweit zunächst auf, dass der Dienst auch ohne die Angabe einer Telefonnummer oder E-Mail-Adresse und auch ohne die Angabe des eigenen Namens genutzt werden kann, da die einzelnen Nutzer über eine zufällig generierte ID identifiziert werden.

Die Kontaktlisten der Nutzer werden unmittelbar auf den Geräten der Nutzer verwaltet. Im Rahmen des Kontaktabgleichs werden die Adressbucheinträge lediglich in anonymisierter Form und nur, wenn der Nutzer dies ausdrücklich wünscht, an die Server des Messenger-Dienstes in der Schweiz übermittelt und im Anschluss an den Abgleich wieder von den Servern gelöscht. Nachrichten und Medien, wie Bilder, Videos oder Dateien, werden ebenfalls nicht dauerhaft auf den Servern des Unternehmens gespeichert, sondern von diesen gelöscht, sobald sie an den Empfänger übermittelt wurden. Die Generierung der Schlüssel erfolgt bei der Anmeldung dezentral auf den Nutzergeräten, sodass die privaten Schlüssel den Messenger-Dienst nicht bekannt sind und Nachrichten nicht entschlüsselt werden können. Threema sagt außerdem zu, keine Auswertungen personenbezogener Daten vorzunehmen oder Metadaten oder Logdateien darüber, wer wann mit wem kommuniziert hat, zu speichern.

Der Dienst bietet sich angesichts der weniger starken allgemeinen Verbreitung wohl vor allem für die unternehmensinterne Kommunikation an. Die Business-Version Threema Work („SaaS"-Lösung) bietet insoweit auch verschiedene Konfigurationsmöglichkeiten etwa in dem Bereich Administration und Nutzerverwaltung. So kann beispielsweise ausgeschiedenen Mitarbeitern der Zugang zur App zentral entzogen werden. Threema bietet Unternehmen zudem den Abschluss einer Vereinbarung zur Auftragsverarbeitung an. Darüber hinaus stellt Threema Unternehmen auch eine „On-Premise"-Lösung mit unabhängiger Chat-Umgebung und selbstgehostetem Administrationsportal zur Verfügung. Entsprechende Lösungen sind aber auch zur externen Kommunikation geeignet.

Der Nachteil von Threema ist vor allem die vergleichsweise geringe Verbereitung, weil die verschiedenen Messenger-Dienste untereinander inkompatibel sind.

Fazit

Sollen Messenger-Dienste im Unternehmen eingesetzt werden, ist auf eine datenschutzkonforme Umsetzung zu achten. Insbesondere bedürfen die in diesem Zusammenhang erfolgenden Datenverarbeitungsprozesse einer belastbaren Rechtsgrundlage. Abhängig vom jeweiligen Anbieter muss partiell auch auf die Rechtmäßigkeit der Datenübertragung in Drittstaaten geachtet werden. Welche konkreten Erfordernisse sich darüber hinaus im Rahmen der Nutzung ergeben, hängt dabei von der konkreten Ausgestaltung – den Kommunikationspartnern, eingesetzten Geräten und zu übermittelnden Inhalten – ab. Es empfiehlt sich insoweit eine einzelfallbezogene Betrachtung der jeweiligen Gegebenheiten.

Christina Prowald

Kontakt:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Christina Prowald
Wissenschaftliche Mitarbeiterin

T +49 521 96535 - 980
F +49 521 96535 - 113
M christina.prowald@brandi.net