Die Nutzung von WhatsApp und die DSGVO

Aufgeklärte WhatsApp-Nutzer wissen, dass hinter dem 2009 gegründeten Instant-Messaging-Dienst WhatsApp seit nunmehr sechs Jahren das Unternehmen Facebook Inc. steht. Doch nur wenige Nutzer wissen, dass durch diese Verbindung entsprechende Metadaten und Telefonnummern aus der WhatsApp-Nutzung an die Social Media Plattform weitergegeben werden können. Dies ist zwar offiziell nicht erlaubt, findet aber trotzdem statt. Dieser Newsletter soll den Datenschutz bei WhatsApp näher beleuchten und Alternativen für die Kommunikation innerhalb von Unternehmen aufzeigen.

1. WhatsApp: Riskante Bequemlichkeit

Die Kommunikation über WhatsApp ist unkompliziert, schnell und effizient. Das Problem bei WhatsApp ist jedoch, dass der Nutzer durch Zustimmung zu den Nutzungsbedingungen einwilligt, dass sämtliche Daten auf den Servern von WhatsApp gespeichert und gesammelt werden. Dies sind nicht nur die Daten der jeweiligen Nutzer selbst sondern auch die sogenannten Metadaten, also Informationen über die Daten selbst. Auf diesem Wege kann WhatsApp erkennen, wann über den Dienst kommuniziert wird und in diesem Zusammenhang sowohl die Geräte- als auch die Telefonnummer des jeweiligen Nutzers herausfinden. Der Inhalt der Nachricht kann zwar aufgrund der Ende-zu-Ende-Verschlüsselung nicht ausgelesen werden, aber auch hier können sowohl der Versender als auch der Empfänger der Nachrichten ebenso wie der Standort und die Uhrzeit der Nachrichten ermittelt werden. Dies alles reicht aus, um ein ausführliches Personenprofil des Nutzers zu erstellen („Profiling“ hier wäre zwingend eine Datenschutzfolgenabschätzung durchzuführen).

Der Zusammenschluss mit Facebook führte weiterhin dazu, dass verknüpfte Telefonnummern und zusätzliche Account-Informationen mit dem Messenger-Dienst ausgetauscht werden. So können beispielsweise fehlende Profilinformationen von Facebook-Profilen durch die WhatsApp-Metadaten ergänzt werden. Diese Datenweitergabe rechtfertigt WhatsApp in seinen FAQs damit, dass sie diese Auswertung vornehmen, um den Messaging-Dienst kontinuierlich zu verbessern. Nach eigenen Angaben werden also folgende Daten kontinuierlich ausgewertet:

- Telefonnummer
- Art und Häufigkeit der Nutzung
- Nutzungsinformationen
- Geräteinformationen (z.B. Modellnummer, Betriebssystemversion, Stand der WhatsApp-App)
- Datum der Registrierung
- Das Land / den Ländercode
- Netzwerkcode

Auch die Adressbuchdaten werden erhoben, wenn die NutzerInnen ausdrücklich zugestimmt haben.

Problematisch ist nun, dass die DSGVO eine Datenweitergabe nur dann erlaubt, wenn eine taugliche Rechtsgrundlage (z.B. eine Einwilligung des Nutzers) vorliegt. Auch WhatsApp muss sich an die neuen Vorgaben der DSGVO halten. Wenn jedoch zwei Unternehmen ein sogenanntes berechtigtes Interesse an einem Datenaustausch haben, kann ein solcher trotz der Vorgaben der DSGVO zulässig sein. Ein solches berechtigtes Interesse liegt beispielsweise dann vor, wenn der Datenaustausch zum Schutz der Daten selbst erforderlich ist. Hier nennt Facebook als berechtigtes Interesse, seine Nutzer vor falschen Accounts, Spam und Fake News schützen zu können. Haben Sie also den WhatsApp Nutzungsbedingungen zugestimmt, können Sie eine Datenweitergabe an Facebook nicht verhindern.

WhatsApp ist aber auch aus arbeitsrechtlicher Sicht bedenklich: Durch die „Online/Offline"-Anzeige eines Mitarbeiter-Accounts kann nicht selten auch eine Kontrolle durch den Arbeitgeber erfolgen, die eine Mitbestimmungspflicht des Betriebsrates gem. § 87 Abs. 1 Nr. 6 BetrVG begründet.

2. Alternative Messaging-Dienste

Das hier aufgezeigte Problem mit WhatsApp besteht sowohl bei der Nutzung im privaten als auch im dienstlichen Bereich. Welche Alternativen bestehen also für Unternehmen, die nicht auf die schnelle und unkomplizierte Kommunikation via Instant-Messenger verzichten wollen?

2.1 Ist WhatsApp Business die Lösung?

WhatsApp Business ist eine Variante des herkömmlichen Messaging-Dienstes WhatsApp, die sich speziell an kleinere Unternehmen richtet. Diese kostenfreie Version bietet im Unterschied zur herkömmlichen Version einige Zusatzfunktionen an. Größere Unternehmen können auch die kostenpflichtige Variante WhatsApp Business API nutzen, die sogar eine Anbindung an das eigene CRM-System zulässt. Die WhatsApp Business App unterscheidet sich dabei in der Funktionsweise nicht von der Consumer-Variante. Die App wird auf dem Smartphone installiert und synchronisiert das vorhandene Adressbuch mit den WhatsApp-Servern.

Ein scheinbarer Vorteil gegenüber der Consumer-App: Für seine Business-Produkte betrachtet sich WhatsApp als Auftragsverarbeiter nach Art. 28 DSGVO und stellt mit den Datenverarbeitungsbedingungen einen auffallend übersichtlichen Auftragsverarbeitungsvertrag bereit. Dieser „Auftragsverarbeitungsvertrag" enthält jedoch nicht einmal die Mindestangaben nach Art. 28 Abs. 3 DSGVO. So fehlen bereits Angaben zur Datenverarbeitung, zu der WhatsApp beauftragt werden soll. Auch wird nicht aufgeklärt, wie die Datenübermittlung an Facebook gerechtfertigt werden könnte. WhatsApp Business bietet derzeit folglich in keiner seiner beiden Ausprägungen eine DSGVO-konforme Kommunikationsmöglichkeit. Auch für eine dienstliche Kommunikation unter den Mitarbeitern sind die Business-Varianten genauso ungeeignet wie das klassische WhatsApp.

2.2 Threema

Eine DSGVO-konforme Alternative zu WhatsApp bietet der Schweizer Messaging-Dienst Threema. Bei Threema muss der Nutzer keine persönlichen Angaben machen, um die App überhaupt nutzen zu können. Threema vergibt eine zufällig generierte ID, unter der der Nutzer für andere angezeigt wird. Die Eingabe von personenbezogenen Daten geschieht auf eigenen Wunsch und auch nur verschlüsselt. Dies hat zur Folge, dass die Erstellung eines Personenprofils hier nicht möglich ist. Threema ist nicht kostenfrei, kann aber je nach Handy-Betriebssystem zu einem Preis von 2,99 bis 3,49 EUR erworben werden. Zudem bietet Threema eine Ende-zu-Ende-Verschlüsselung. Auch hier gibt es mit Threema Work einen Dienst, der die unternehmensinterne Kommunikation datenschutzkonform gewährleistet. Threema betreibt allerdings seine Server in der Schweiz und damit in einem Nicht-EU-Land. Aktuell gibt es einen Angemessenheitsbeschluss in dem die Europäische Kommission feststellt, dass personenbezogene Daten in dem Drittland Schweiz einen vergleichbaren adäquaten Schutz genießen.

2.3 Signal

Der Messenger-Dienst Signal kommt aus den USA und hat dort sowie in anderen Ländern seine Server. Die App verlangt zur Nutzung eine Handnummer, damit man sich anmelden kann. Auch Signal möchte auf das Adressbuch des Smartphones zugreifen. Allerdings werden hier beim Abgleich des Adressbuches – anders als bei WhatsApp – alle Kontakte anonymisiert und nach dem Abgleich wieder von den Servern gelöscht. Signal arbeitet darüber hinaus an einem Verfahren, das verhindert, dass die Betreiber der Server die übertragenen Kontaktdaten einsehen können. Der Messenger-Dienst Signal ist kostenlos. Derzeit wird allerdings keine gesonderte Version zur Unternehmenskommunikation angeboten. Eine Ende-zu-Ende-Verschlüsselung findet auch hier statt.

3. Nutzung privater Geräte im dienstlichen Bereich: Die Container Lösung

Unter einer Container-Lösung versteht man eine bestimmte Art des Mobile Device Managements (MDM). Oftmals wollen Mitarbeiter eines Unternehmens ihre eigenen mobilen Geräte nutzen, um auch unterwegs oder am Wochenende flexibel ihre Mails zu checken oder andere Arbeiten zu erledigen. Wie bringt man also „Bring Your Own Device“ mit dem Datenschutz in Einklang? Um eine ordnungsgemäße Geräteverwaltung zu gewährleisten, muss die IT-Abteilung natürlich Zugriff auf das Gerät bekommen. Hier gilt es, einheitliche Sicherheitseinstellungen und Richtlinien für Smartphones und Tablets festzulegen und Zugriffsrechte zu definieren. Daraus ergibt sich der zweite Ansatzpunkt für einen wirksamen Schutz sensibler Daten. Der private Bereich muss strikt vom dienstlichen Bereich getrennt werden. Dies kann durch die Einrichtung eines „Sicherheits-Containers“ geschehen. Komplementär zur Kontrolle der Geräte – eine Aufgabe, die das MDM-Tool übernimmt – konzentriert sich der Container-Ansatz auf die Sicherung der dienstlichen Applikation und Daten auf den

Smartphones und Tablets. Der Sicherheits-Container verpackt Unternehmensdaten, E-Mails, Kontakte, Kalender, Notizen, Aufgaben und Dokumente in einen verschlüsselten Bereich. Selbst bei Diebstahl oder Verlust des Geräts bleiben die Daten vor Missbrauch geschützt. Gleichzeitig verhindert der Sicherheits-Container, dass ein Mitarbeiter aus dem sicheren Unternehmensbereich auf eine private App zugreift. Zudem gibt es keine Copy-and-Paste-Funktion, mit der sich Firmeninformationen in den Privatbereich verschieben ließen.

Insgesamt weist die Container-Lösung also sowohl Vor- als auch Nachteile auf, wenn es um die Nutzung privater Geräte im dienstlichen Bereich geht. Dennoch ist diese Lösung auch unter Betrachtung der Nachteile, immer noch vorzugswürdiger, als eine Nutzung privater Geräte ohne jegliche Regelungen in Bezug auf den Datenschutz.

4. Fazit / Empfehlung

In vielen Unternehmen stellt sich die Frage, „ob“ ein Messenger dienstlich Verwendung findet, oftmals nicht mehr. Zu etabliert sind bereits gefundene Lösungen. Vielmehr geht es um die Frage, welcher Dienst eingesetzt wird und wie dieser eingesetzt wird. Bei der Entscheidung sind insbesondere die Sensibilität der übermittelten Daten, die Unternehmensstruktur und das Geschäftsfeld in die erforderliche Abwägung einzubeziehen.

Ein Einsatz sollte auch immer durch entsprechende Richtlinien und Dienstanweisungen dokumentiert werden, um bestehenden Risiken bestmöglich entgegenwirken zu können.

Sollten Sie darüber hinaus gehende Fragen haben, stehen wir Ihnen jederzeit gern zur Verfügung.

Ihr Team der RKM Data GmbH