FLEXPERTO

WhatsApp Business API in der Flexperto Communication Cloud

IT-Security und Datenschutz

Januar 2020

Hinweis: Flexperto ist kein offizieller Partner von WhatsApp

Inhalte

1. Einführung und Status Quo

WhatsApp ist mit mehr als 1,5 Milliarden Nutzern weltweit der populärste Messenger. Laut einer Bitkom Umfrage nutzen 81% aller Deutschen den Dienst[1] und eine weitere Umfrage YouGov fand heraus, dass jeder Fünfte findet, dass Kontakt über WhatsApp mit Unternehmen längst überfällig ist und Alltag sein sollte.[2]
Bisherige Lösungen für die Kommunikation über WhatsApp waren:

WhatsApp „Consumer“

Unternehmen nutzen die Consumer Version von WhatsApp auf den Smartphones der Mitarbeiter oder als gemeinsam genutztes Smartphone innerhalb einer Abteilung für den Kundenkontakt. Durch die Synchronisation der Daten des Telefonbuchs sowie fehlende Funktionen für ordnungsgemäßen Datenschutz ist ein großflächiger, planbarer Einsatz nicht möglich.

WhatsApp „Hack“

Aufgrund der hohen Nachfrage haben sich jedoch einige Unternehmen etabliert, die WhatsApp „Consumer“ mit einigen Enterprise Funktionen angereichert haben. Hierzu zählen insbesondere der Newsletterversand und die Einbindung in Customer Support Systeme. Diese Tools basieren jedoch nicht auf der offiziellen WhatsApp Business API, sondern basieren auf „Reverse-Engineering“ der WhatsApp „Consumer“ Lösung um damit die Grenzen der Applikation zu umgehen und weitere Funktionalitäten hinzuzufügen.

WhatsApp selbst erlaubt die Nutzung derartiger Software nicht offiziell: „Die Verwendung der offiziellen WhatsApp Business API oder anderer offizieller WhatsApp-Tools ist obligatorisch. Jegliche Missachtung dieser Verpflichtung stellt eine Verletzung unserer Richtlinien dar.“[3]

Es bleibt Unternehmen also selbst überlassen, ob sie seine WhatsApp Strategie auf technisch und rechtlich nicht 100% stabilen Lösungen aufbauen möchten.

1 https://www.bitkom.org/Presse/Presseinformation/Neun-von-zehn-Internetnutzern-verwenden-Messenger.html
2 https://yougov.de/news/2017/08/04/uber-whatsapp-mit-kunden-kommunizieren/
3 https://developers.facebook.com/docs/whatsapp/overview

WhatsApp hat zwei Business Lösungen für die gewerbliche Nutzung auf den Markt gebracht:

1. WhatsApp Business
   WhatsApp Business ist eine aktuell auf Android verfügbare Applikation für kleine Unternehmen, die es ermöglicht über eine von WhatsApp entwickelte und leicht angepasste App mit Kunden über WhatsApp zu sprechen.

2. WhatsApp Business API
   WhatsApp Business API ermöglicht es mittleren und großen Unternehmen, eine WhatsApp Instanz selbst zu hosten und mittels technischer Schnittstelle über WhatsApp mit Kunden zu kommunizieren. Dabei kommen Unternehmen in den Genuss der kompletten Datenhoheit.

Im Nachfolgenden beschäftigt sich dieses Whitepaper ausschließlich mit der WhatsApp Business API und deren Nutzung innerhalb der Flexperto Communication Cloud.

2. Grundlegende Informationen zu WhatsApp Business API

WhatsApp Business API ist eine WhatsApp Lösung für mittlere und große Unternehmen. Um Ende-zu-Ende Verschlüsselung zu gewährleisten, müssen Unternehmen eine eigene WhatsApp Instanz hosten. Ferner ist WhatsApp Business API ausschließlich eine programmatische Schnittstelle und besitzt kein Frontend (GUI - Grafische Benutzeroberfläche).

Bei der Entwicklung der WhatsApp Business Solution wurden zunächst Anwendungsfälle im Bereich Benachrichtigungen (zu Bestellungen, Lieferungen, Terminerinnerungen) und Support (Call-Center) priorisiert. WhatsApp Business unterstützt noch keine Anwendungsfälle mit reinen Marketingzwecken wie beispielsweise den Versand von Newslettern.

3. Einbindung in die Flexperto Communication Cloud

Flexperto ermöglicht es Unternehmen innerhalb der Flexperto Communication Cloud mit Kunden über WhatsApp zu kommunizieren. Hierbei greift Flexperto

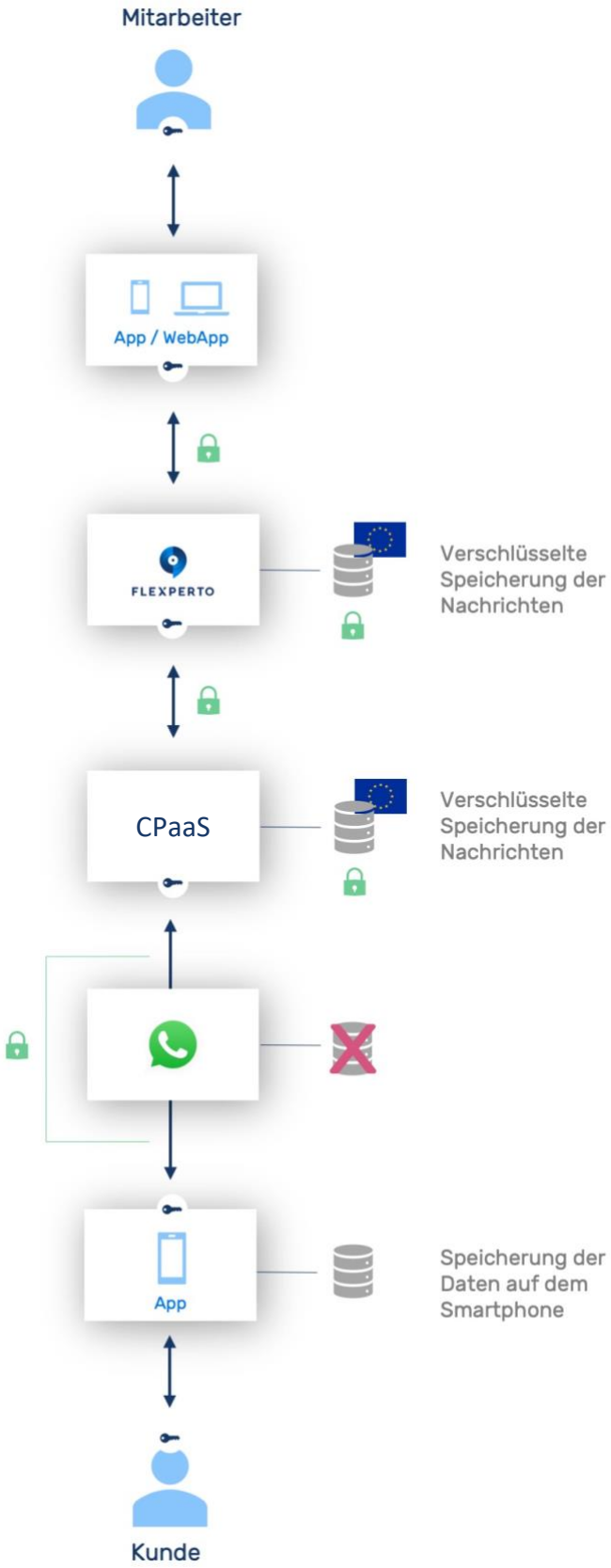
auf die offizielle WhatsApp Business API zu. Flexperto bietet eine vollständige Nutzeroberfläche für den Einsatz von WhatsApp Business API im Bereich Vertrieb und Service und nutzt die Möglichkeiten der API um Funktionen zu entwickeln, die eine datenschutzkonforme Nutzung gewährleisten. Hierzu zählen Insbesondere das Einwilligungsmanagement (Opt-In), Opt-Out, sowie Datenlöschung und Hosting der Nachrichtendaten in Europa.

Die Funktionalität des Versands von Nachrichten über den WhatsApp Kanal ist bei Flexperto im Rahmen des Produkts „Omni-Channel Messaging“ eingebunden. Hierbei ermöglicht es Flexperto auch über andere Messaging Kanäle wie Facebook Messenger, Telegram, SMS, Apple Business Chat, etc. zu kommunizieren.

4. Technische Umsetzung

Wie zuvor erwähnt, bietet Flexperto Schnittstellen zu mehreren Messengern, darunter auch WhatsApp Business API. Um die Funktionalität und Verfügbarkeit auf einem Service Level anbieten zu können, wie es für den skalierbaren Einsatz in großen Unternehmen notwendig ist, arbeitet Flexperto mit mehreren führenden Unternehmen zusammen, die sich ausschließlich darauf konzentrieren, sämtliche Änderungen der Schnittstellen zu berücksichtigen und das Hosting in skalierbaren Cloud Architekturen zur Verfügung stellen.

Diese Dienstleister sind beispielsweise Smooch Technologies, Twilio, Messagebird, 360dialog (Messagepipe), Vonage etc. und sind offizielle Partner von WhatsApp. Flexperto kann je nach Situation, Kommunikationskanal und inviduellen Anforderungen unterschiedliche Dienstleister einbinden. Die flexible technische Schnittstelle macht dies möglich. Im Nachfolgenden werden diese Anbieter auch „Communication Platform as a Service Anbieter“ (CPaaS-Anbieter) genannt. Folgende Grafik erläutert den Datenfluss zwischen Flexperto, CPaaS-Anbieter und Messaging Anbietern:


Mitarbeiter
App / WebApp
FLEXPERTO
Verschlüsselte Speicherung der Nachrichten
CPaaS
Verschlüsselte Speicherung der Nachrichten
App
Speicherung der Daten auf dem Smartphone
Kunde

5. Datenschutzrechtliche Betrachtung

5.1. Vertragsverhältnis mit Flexperto und CPaaS-Anbieter

Zwischen Ihrem und Flexperto wird eine Auftragsverarbeitung geschlossen. Der CPaaS-Anbieter wiederum ist Subdienstleister von Flexperto und damit innerhalb derselben Vertragskette der Auftragsverarbeitung. Sämtliche Auftragsverarbeitungen werden gemäß den europäischen Richtlinien ausgestaltet (Standardvertragsklauseln). Eine Verarbeitung der Daten, insbesondere die Nachrichten erfolgt ausschließlich in zertifizierten Rechenzentren innerhalb der Europäischen Union.

Die Nachrichten werden auf der mandantengetrennten Datenbank innerhalb Flexperto und des CPaaS-Anbieters gespeichert. Zwischen dem CPaaS Anbieter und dem Empfänger (Kunde) sind Nachrichten Ende-zu-Ende verschlüsselt. Aufgrund der durchgehenden Vertragskette zur Auftragsverarbeitung ist Ihr Unternehmen jedoch rechtlich gesehen über die gesamte Datenverarbeitungskette im vollständigen Besitz der Daten und Verantwortlicher.

WhatsApp selbst erhält ausschließlich Telefonnummern und Metadaten. Nachrichtendaten erhält WhatsApp nur verschlüsselt und speichert diese nur solange auf Servern zwischen, bis die Nachricht zugestellt wurde. Die Verschlüsselung basiert dabei auf dem Signal Protokoll: ein quelloffenes Protokoll von Open Whisper Systems, welches heute als Verschlüsselungsstandard bei Messengern gilt. Das Protokoll gilt nach wie vor als sehr sicher.

5.2. Vertragsverhältnis mit WhatsApp

Bei WhatsApp könnte argumentiert werden, es handele sich nicht um einen Auftragsverarbeiter, der personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet, da die Leistung in der Erbringung von Telekommunikation liegt. Insoweit könnten Messaging-Dienste mit E-Mail-Übertragungsdiensten gleichzusetzen sein (vgl. zu letzterem BT-Drs. 16/3078, S. 13 und 15; vgl. zum Thema auch DAV, Stellungnahme des Deutschen Anwaltvereins durch den Ausschuss Informationsrecht zur Anwendung des TKG auf neue Kommunikationsplattformen). In Deutschland unterfallen Messaging-Dienste demnach dem bereichsspezifischen Datenschutz des Telekommunikationsgesetzes.

Diese Auffassung wird nach unserer Lesart durch die Aufsichtsbehörden gestützt: Die Landesdatenschutzbehörde Bayern (nicht-öffentlicher Bereich) geht beispielsweise davon aus, dass TK-Dienstleistungen keine Auftragsverarbeitung darstellen: (https://www.lda.bayern.de/media/FAQ_Abgrenzung_Auftragsverarbeitung.pdf).

Ungeachtet dessen geht WhatsApp selbst davon aus, dass es im Verhältnis zu Unternehmen Auftragsverarbeiter ist. In den WhatsApp Business Nutzungsbedingungen (https://www.whatsapp.com/legal/business-terms/) regelt WhatsApp in Ziff. 7, dass es in Bezug auf Kundendaten bei Kunden aus der EU Auftragsverarbeiter ist. Ein Vertrag zur Auftragsverarbeitung wird in das Vertragsverhältnis in Form der WhatsApp Business Datenverarbeitungsbedingungen einbezogen (https://www.whatsapp.com/legal/business-data-processing-terms/). Der Auftragsverarbeitungsvertrag greift die Mindestinhalte aus Art. 28 DSGVO auf. Im Übrigen fungiert die WhatsApp Ireland Limited für Kunden aus Europa als Vertragspartner. Auf Grund von Datentransfers an die WhatsApp Inc. weisen die Datenverarbeitungsbedingungen auf dessen Privacy Shield-Zertifizierung hin. Außerdem verweist WhatsApp darauf, dass für den Abschluss der Auftragsverarbeitung die Standardvertragsklauseln gelten. Somit ist ein elektronischer Abschluss der Standardvertragsklauseln gegeben.

Sehr wichtig bei der Betrachtung der Auftragsverarbeitung ist der Fakt, dass der Anwendungsbereich des Vertrages relativ gering ist:

Es werden ausschließlich Telefonnummern und Metadaten (z.B. Zeitpunkt der Kommunikation) verarbeitet, da sämtliche Inhalte Ende-zu-Ende verschlüsselt werden und diese somit nicht in den Umfang der verarbeiteten Daten einfließen.

Vorstehende Datenkategorien könnten nach näherer Betrachtung auch aus der Auftragsverarbeitung fallen, da WhatsApp auch als Verantwortlicher gegenüber dem Kunden agiert. Bereits in dieser Vertragsbeziehung stimmt der Kunde als Betroffener gegenüber WhatsApp als Verantwortlicher der umfassenden Verarbeitung folgender Datenkategorien zu:

- Account-Informationen (Mobilfunknummer)
- Nachrichten

- Nutzungs- und Loginformationen
- Geräte- und Verbindungsdaten
- Standort-Informationen

Auch klärt WhatsApp bereits über die Datenverarbeitung durch Ihr Unterhmen auf:

„Unternehmen, mit denen du unter Nutzung von WhatsApp interagierst, stellen uns Informationen über ihre Interaktionen mit dir zur Verfügung. Ein Unternehmen auf WhatsApp kann auch ein anderes Unternehmen einsetzen, das dem ersten Unternehmen dann in dessen Auftrag beim Speichern, Lesen und Beantworten deiner Nachrichten hilft und es unterstützt. Bitte beachte, dass wenn Unternehmen Dienste Dritter nutzen, deren eigene Bedingungen und Datenschutzrichtlinien in Bezug auf deine Nutzung solcher Dienste sowie hinsichtlich der Verwendung deiner Informationen durch sie auf solchen Diensten gelten."

Die Nachrichten liegen zum einen auf dem Smartphone der Nutzer (in diesem Szenario nur der Kunde) sowie auf der vom Unternehmen kontrollierten und gehosteten WhatsApp Instanz. WhatsApp hat auf diese Daten keinen Zugriff, womit sich ergibt, dass die Nachrichtendaten kein Bestandteil der Auftragsverarbeitung sind. Für die Verarbeitung von Telefonnummern ist WhatsApp selbst auch Verantwortlicher gegenüber den Nutzern, denn die Nutzer haben WhatsApp bereits erlaubt, ihre Telefonnummer zu verarbeiten.

Abschließend lässt sich die Vertragssituation wie folgt beurteilen:

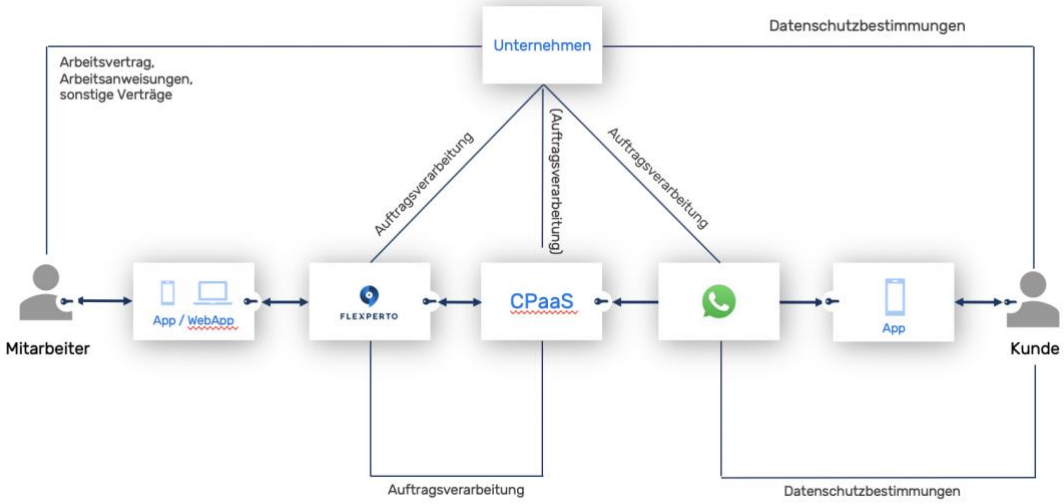
- Flexperto ist der primäre Vertragspartner Ihres Unternehmens und es besteht eine Auftragsverarbeitung.

- Flexperto nutzt CPaaS-Anbieter, um eine skalierbare Infrastruktur für das Hosting der WhatsApp Instanzen bereitzustellen und sämtliche Updates der API zu managen. Der CPaaS-Anbieter ist daher ein Subunternehmer von Flexperto und ist integriert in die Vertragskette zwischen dem Unternehmen und Flexperto.

- Alle Nachrichtendaten werden innerhalb der Europäischen Union unter voller Kontrolle Ihres Unternehmens verarbeitet.

- Ihr Unternehmen stimmt der Business Nutzungsbedingung von WhatsApp zu und schließt damit eine Auftragsverarbeitung mit WhatsApp ab - unter Bezugnahme der Standardvertragsklauseln und hilfsweise unter Verweis auf das PrivacyShield von WhatsApp. Die verarbeiteten Datenkategorien, die diesem Vertrag zugrunde liegen, beschränken sich auf Metadaten und bei enger Auslegung auf die Telefonnummer des Kunden (obwohl WhatsApp diese Nummer von Seiten Ihres Kunden bereits verarbeitet).

5.3. Visualisierung der Vertragsverhältnisse



5.4. Keine Übertragung von Kontakten im Telefonbuch

Bisher wurde die WhatsApp Lösung deshalb kritisiert, da WhatsApp zum Zeitpunkt der Installation der App das komplette Adressbuch an WhatsApp überträgt und dabei massenweise personenbezogene Daten von Betroffenen in die USA übermittelt werden, ohne dass diese explizit hierzu eingewilligt hätten.

Mit WhatsApp Business API innerhalb der Flexperto Communication Cloud wird WhatsApp nicht mehr direkt auf den Smartphones installiert. Daher hat WhatsApp auch keinen Zugriff mehr auf das Adressbuch.

Auch die Die Landesbeauftragte für Datenschutz im Saarland
und Informationsfreiheit kommt im Hinblick auf den virtualisierten Betrieb der WhatsApp Instanz und der nicht vorhandenen Übertragung zu einer positiven Einschätzung dieses Sachverhalts:

https://www.datenschutz.saarland.de/fileadmin/user_upload/uds/PM/2020/PM_WhatsApp.pdf

5.5. Einwilligung

Im Rahmen der DSGVO bedarf es bei der Nutzung von Messengern zum Zwecke der Kundenkommunikation, wie bei allen anderen Verarbeitungen von personenbezogenen Daten, einer Rechtsgrundlage. Die bevorzugte Grundlage wäre die “Einwilligung des Betroffenen” (Art. 6 Abs.1a DSGVO), die Alternative ggf. “Berechtigtes Interesse”, d.h. Im Fall dass die Interessen des werbenden Unternehmens im Einzelfall diejenigen des Betroffenen überwiegen (Art 6 Abs.1f DSGVO). Die DSGVO erkennt bspw. Direktwerbung ausdrücklich als berechtigtes Interesse eines Unternehmens an, sodass man bei einer Abwägung der Interessen durchaus zu Gunsten des Unternehmens bewerten könnte und damit die Kommunikation per WhatsApp auch ohne explizite Einwilligung legal wäre.

Flexperto unterstützt jedoch die Einholung einer Einwilligung vor Beginn der Kommunikation über WhatsApp.

Zunächst kann ein Kunde seine Einwilligung über einen anderen Kanal geben: bspw. Website, Telefon, E-Mail. Das Unternehmen versendet dann eine

Nachricht an den Kunden, welches ihn auffordert, der Verarbeitung mit einem „Ja“ zu bestätigen. Dieses Verfahren wäre analog dem im Rahmen der E-Mail-Kommunikation verwendeten Double-Opt-In Verfahren. Diese Einwilligung kann durch den vollständigen Zugriff auch außerhalb der WhatsApp Umgebung für die spätere Beweislage gespeichert werden.

5.6. Informationspflichten

Analog der initialen Nachricht hinsichtlich des zweiten „Opt-Ins“ kann ferner eine standardisierte, automatisierte Nachricht erfolgen, die den Kunden hinsichtlich der Datenschutzerklärung informiert. Dahingehend kann den Informationspflichten ebenfalls dokumentiert nachgegangen werden.

5.7. Löschpflichten

Unternehmen müssen personenbezogene Daten dann löschen, wenn sie für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind.

Da alle Daten zentral lagern, und nicht auf den Smartphones der Mitarbeiter, können die Daten zentral gelöscht werden. Außerdem erlaubt die Programmierschnittstelle ein automatisiertes Löschen von Daten basierend auf zu definierenden Kriterien.

6. Sonstige rechtliche Hinweise

6.1. Gewerbliche Nutzung

Mit den Business Lösungen gibt WhatsApp einen eindeutigen rechtlichen Rahmen für die gewerbliche Nutzung. WhatsApp hat die AGB für Kunden an den entsprechenden Stellen ergänzt. Auch existieren für Unternehmen nun dedizierte Business Nutzungsbedingungen:
https://www.whatsapp.com/legal/business-terms/
Andere Lösungen, die nicht auf den offiziellen WhatsApp Business Angeboten basieren, sind explizit verboten und Stellen laut Aussage von WhatsApp einen Verstoß gegen die Nutzungsbedingungen von WhatsApp dar.

6.2. Aufzeichnungsanforderungen und Aufbewahrungspflichten

Die Nutzung von WhatsApp „Consumer“ erfordert ein manuelles Aufzeichnen über dezentral verteilte Datenbanken (die Smartphones aller Mitarbeiter). Dies erfolgt mit WhatsApp Business API nun zentral, denn Unternehmen haben einen zentralen Zugriff auf sämtliche Nachrichtendaten und können diese automatisiert und programmatisch auf andere Systeme übertragen, kategorisieren und dokumentieren. Damit kann eine skalierbare und tragfähige Lösung für sämtliche sich ergebende Dokumentationspflichten geschaffen werden. WhatsApp Business API kann somit als zentrales Kommunikationstool in sämtlichen Customer Touchpoints eingesetzt werden.

7. Frequently Asked Questions

Gibt es eine offizielle Bestätigung von WhatsApp über die Ende-zu-Ende Verschlüsselung?

Auf der Seite https://developers.facebook.com/docs/whatsapp/faq geht Facebook hierauf konkret ein:

Wird über die WhatsApp Business API eine durchgängige Verschlüsselung aufrechterhalten?

Ja. Die Nachricht wird zwischen dem WhatsApp Business API-Client und dem Endnutzer durchgängig verschlüsselt. Wenn du bei Aufrufen an den WhatsApp Business API-Client HTTPS verwendest, werden diese Daten darüber hinaus mit SSL verschlüsselt (vom deinem Backend-Client zum WhatsApp Business API-Client).

Weiterhin erläutert Facebook, dass man aufgrund der Aufrechterhaltung der Ende-zu-Ende Verschlüsselung sich explizit gegen eine zentrale API und Datenbank entschieden hat und die WhatsApp Business API in einem technisch erheblich umständlicheren Verfahren anbietet:

Warum muss ich den WhatsApp Business API-Client mit einer Datenbank hosten? Warum kann ich nicht einfach eine API aufrufen?

WhatsApp und seine Nutzer wissen die durchgängige Verschlüsselung zu schätzen. Alle Nachrichten auf WhatsApp werden in hohem Maße verschlüsselt. Jede Nachricht wird mit Absender- und Empfängerschlüsseln verschlüsselt, die bei jedem Senden einer Nachricht weitergegeben werden. WhatsApp kann diese Nachrichten nicht lesen, da es nicht über die entsprechenden Schlüssel zur Entschlüsselung der Nachrichten verfügt. Die Schlüssel werden vom Nutzer auf dem Mobilgerät und vom Unternehmen in der Datenbank gespeichert. Aus diesem Grund ist der WhatsApp Business API-Client eine gehostete Lösung, für die eine Datenbank erforderlich ist. Durch den Einsatz einer API zur Weiterleitung von Nachrichten würde die durchgängige Verschlüsselung unterbrochen, was der Philosophie von WhatsApp widerspricht.

Weitere Informationen findest du unter WhatsApp Sicherheit. Dort kannst du außerdem auf das Whitepaper mit einem Überblick über Verschlüsselung bei WhatsApp zugreifen.

Gibt es offizielle Gutachten zur WhatsApp Business API

Eine offizielle Stellungnahme zum Einsatz von WhatsApp Business API hat kürzlich die Landesbeauftragte für Datenschutz im Saarland veröffentlicht. Diese können sie hier abrufen:

https://www.datenschutz.saarland.de/fileadmin/user_upload/uds/PM/2020/PM_WhatsApp.pdf

Bisher konzentriert sich die weit verbreitete Kritik auf den Übertrag von Adressbuchdaten. Diese ist im Rahmen der Nutzung der WhatsApp Business API von Seiten Ihres Unternehmens ausgeschlossen. Auf Seiten der Kunden, ist die Übertragung, sofern nicht explizit vom Kunden bei Installation verneint, weiterhin intakt.

Kann ich besonders Schützenswerte Daten wie Gesundheitsdaten über WhatsApp Business API versenden?

Bei der Verarbeitung besonderer Kategorien personenbezogener Daten nach Art. 9 DSGVO sind folgende Dinge zu beachten:

Prinzipiell ist die Verarbeitung verboten, es sei denn

a. es tritt eine der in Art. 9 Abs. 2 DSGVO genannten Ausnahmen in Kraft
b. Die Übermittlung der Daten erfolgt durch den Betroffenen selbst, so dass insofern keine Rechtsgrundlage erforderlich ist.

Bei vorstehender Ziffer a. ist dies in konkreten Fall meist eine ausdrückliche Einwilligung des Kunden (Betroffener) an Ihr Unternehmen (Verantwortlicher).

Allerdings ist die besondere Schutzbedürftigkeit der Gesundheitsdaten Art. 25 Abs. 1 DSGVO zu berücksichtigen. An die technischen und organisatorischen Maßnahmen des in dieses Verfahren eingebundenen Instant-Messenger-Services sind entsprechend höhere Anforderungen zu stellen.

Aufgrund der verwendeten Verschlüsselung der Inhalte, zwischen den WhatsApp Client's auch Ende-zu-Ende kann von besonderen Maßnahmen des Schutzes der Inhalte der Kommunikation ausgegangen werden.

Wir haben in einem separaten Whitepaper die Verarbeitung von Gesundheitsdaten unter Verweis auf eines von der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) herausgegeben Whitepapers den Sachverhalt detailliert analysiert.