

# WhatsApp als Sicherheitsrisiko

## Datenschutz beim beruflichen Smartphone-Einsatz

**Etwa 700 Millionen Kurznachrichten verschicken die Deutschen allein per Whatsapp und SMS pro Tag – zunehmend auch im Firmeninteresse. Doch der berufliche Einsatz von Messengerdiensten gerät ins Visier von Datenschützern. Einige Unternehmen haben den Einsatz von WhatsApp bereits verboten.**



Redaktion

Stand: 18.7.2018

Lesezeit: 04:00 min



Nun gut, praktisch ist es wirklich: Mit ein paar Klicks per WhatsApp beim Kollegen nachzufragen oder in der Betriebsratsgruppe schnell etwas zu klären. Rund 40 Millionen Deutsche nutzen WhatsApp, 70 % davon sogar täglich. Das ist das Ergebnis einer YouGov-Studie aus dem vergangenen Jahr.

Trotzdem ist die berufliche Nutzung bedenklich, warnen Datenschützer – insbesondere angesichts der aktuell verschärften europäischen Regelungen zum Datenschutz. Einige Firmen haben reagiert und den Messenger auf den Dienst-Handys abgeschaltet; so etwa die Deutsche Bank und der Autozulieferer Continental.

Aber worin liegt eigentlich das Problem?

## **Umweg über Kalifornien**

WhatsApp gehört seit einigen Jahren zu Facebook, ein Unternehmen, das nicht gerade für seinen verantwortungsvollen Umgang mit Daten bekannt ist.

Da der Unternehmenssitz von WhatsApp in den USA liegt, weiß niemand in Deutschland genau, welche Daten erhoben und für welche Zwecke sie verwendet werden. Sei es das Foto von der Betriebsversammlung oder der Austausch in der „BR-Gruppe“: Jeglicher Datentransfer bei WhatsApp nimmt grundsätzlich einen Umweg über das kalifornische Unternehmen.

Inzwischen hat das Unternehmen einen Sitz in Irland. „Deine WhatsApp Dienste werden von WhatsApp Ireland Limited bereitgestellt“, heißt es. Ist damit eine Verbesserung des Datenschutzes zu erwarten? Zumindest ist Irland kein unsicheres Drittland im Sinne des Datenschutzes. Die Nutzung und der Transfer der Daten ist trotzdem ungewiss. Allerdings ist der neue zuständige Firmensitz eine Reaktion auf die europäischen Regelungen zum Datenschutz.

## **Immer wieder Sicherheitslücken**

Ende 2017 wurde bekannt, dass ein Zugriff auf personenbezogene Daten von WhatsApp-Nutzern möglich ist. 2018 folgte die Info, dass bei Gruppenchats neue Teilnehmer auch ohne die eigentlich erforderliche Einladung hinzugefügt werden können. Solche „Maulwürfe“ können Chatinhalte verfolgen. Dies sind nur zwei Beispiele die verdeutlichen, dass es immer wieder Sicherheitslücken beim Messenger gibt. Und das ist natürlich problematisch, wenn es um den Austausch vertraulicher Informationen geht.

## **Griff ins Telefonbuch**

Und nicht nur das, auch die Kontakte werden von WhatsApp abgegriffen. Denn das Unternehmen greift auf das Adressbuch des Smartphones zu, alle Telefonnummern werden an die Server von WhatsApp übertragen. WhatsApp formuliert es so: „WhatsApp verwendet die Telefonnummern aus dem Adressbuch deines Telefons und erkennt schnell und einfach, welcher deiner Kontakte ebenfalls WhatsApp benutzt.“ Der US-Konzern erhält damit auch Telefonnummern von Kontakten, die den Messenger nicht nutzen – ohne deren Wissen und ohne deren Einverständnis.

Seit Neuestem besteht zumindest für Android-Geräte die Möglichkeit, die Synchronisationsfunktion auszuschalten. Welche Kontaktdaten übermittelt und verwendet werden? All das ist unklar. Eine Datenübermittlung der Kontaktdaten findet übrigens auch bei der Verwendung von WhatsApp Business statt. Die App bietet ein paar zusätzliche Funktionen für Unternehmen, ist aber keine Verbesserung aus datenschutzrechtlicher Sicht.

## **Geheimnisse?**

WhatsApp bietet zahlreiche Möglichkeiten des Austauschs, wie etwa die Versendung von Bildern, Videos und Textnachrichten. Die eigentlichen Inhalte der Unterhaltungen bleiben dabei nach Angaben des Messengers geheim und werden lediglich verschlüsselt versendet.

Aber wer kann da sicher sein? Und was ist, wenn das Telefon verloren geht oder der Junior zuhause es in die Hände bekommt? Ein Messenger ist definitiv kein Ort für vertrauliche Informationen. Außerdem werden alle

Nachrichten, die nicht sofort zugestellt werden können, auf den Servern von WhatsApp bis zu 30 Tage gespeichert.

### **Leistungs- und Verhaltenskontrolle möglich**

Ein weiterer Gesichtspunkt sollte bei der Verwendung von WhatsApp nicht vergessen werden: die Statusanzeige. Mit dieser kann stets überprüft werden, wer wann online war. Selbst bei Deaktivierung der Statusfunktion wird immer noch angezeigt, wer gerade online ist. Zudem lässt sich überprüfen, wann eine bestimmte Nachricht gesendet wurde. Dies öffnet Tür und Tor zur Leistungs- und Verhaltenskontrolle von Arbeitnehmern.

### **Verstöße gegen die DSGVO**

WhatsApp verstößt gleich in mehreren Punkten gegen die DSGVO.

So ist die Weitergabe von Kontakten im Telefonbuch (Kundendaten) ein solcher Verstoß. Denn das Unternehmen, deren Arbeitnehmer WhatsApp nutzen, ist für die Verarbeitung der personenbezogenen Daten verantwortlich. Und von einer Einwilligung kann man nicht ausgehen.

Versendet man Bilder, handelt es sich um eine Datenübertragung an Whatsapp, für die es ebenfalls keine Einwilligung gibt.

Auch der Dokumentationspflicht des Unternehmens wird nicht nachgekommen: Im Verarbeitungsverzeichnis müssen alle Vorgänge dokumentiert sein, in denen personenbezogene Daten verarbeitet werden.

### **Fazit**

Seit fast zwei Monaten ist die europäische Datenschutz-Grundverordnung DSGVO nun in Kraft. Und noch sind viele Detailfragen nicht geklärt. Von einer „Abmahnwelle“ kann bislang nicht gesprochen werden. Trotzdem ist der Einsatz von WhatsApp mit einigen Bedenken verbunden.

Betriebsräte sollten dies mit in die Waagschale werfen, wenn es um WhatsApp im Unternehmen geht. Denn nicht immer ist der bequeme Kommunikationsweg der richtige.



## **Rechtssicher durch den Datenschutz**

Bei uns bekommen Interessenvertreter das entscheidende Know-how für den Datenschutz – inklusive praktischer Handlungshilfe, die in den untenstehenden, ausgewählten Seminaren verteilt wird. Gleich informieren unter:

## [www.ifb.de/datenschutz](http://www.ifb.de/datenschutz)

- **Sie haben schon Vorkenntnisse beim Thema Datenschutz?**

Dann ist unser Seminar „Datenschutzrecht 2018: Doppelter Handlungsbedarf für den BR“ das Richtige für Sie! ([www.ifb.de/23](http://www.ifb.de/23))

- **Ohne Vorkenntnisse empfehlen wir das Seminar**

„Der gläserner Mitarbeiter Teil I: Grundlagenwissen für mehr Sicherheit im Datenschutz“ ([www.ifb.de/68](http://www.ifb.de/68))

---

### **Kontakt zur Redaktion**

Haben Sie Fragen oder Anregungen? Wenden Sie sich gerne direkt an unsere Redaktion. Wir freuen uns über konstruktives Feedback!

[redaktion-dbr@ifb.de](mailto:redaktion-dbr@ifb.de)

**Institut zur Fortbildung von Betriebsräten GmbH & Co. KG    © 2025**