how to

DIE CLEVERE LÖSUNG FÜR EINE SICHERE KONTAKTVERWALTUNG

INHALT

VORWORT: Geschäftskontakte auf dem Firmenhandy sicher verwalten // 04

RECHTLICHE GRUNDLAGEN: Datenverarbeitung nach DSGVO // 06

DATENSCHUTZRISIKO: Ungewollter Datenabfluss bei Kontaktsynchronisation // 09

Synchronisation mit Messenger-Diensten // 11

Persönliche Profile in Mietautos und Carsharing // 12

WIE KÖNNEN DATENSCHUTZVERSTÖSSE VERHINDERT WERDEN? // 13

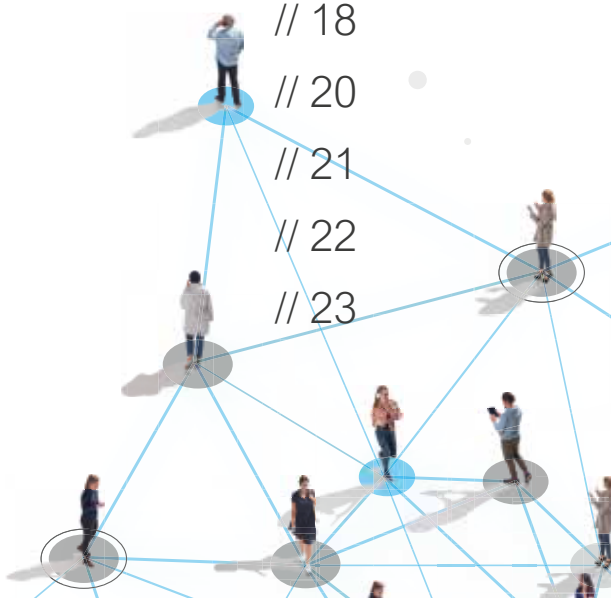
BEST PRACTICE FÜR DATENSCHUTZ: Die Secure Contacts App – DSGVO-konform, praktisch und einfach // 18

Datenschutz & Usability vereint in einer App // 20

Alle Features auf einem Blick // 21

Die App im Vergleich // 22

FAZIT: Kontakte effizient schützen und DSGVO-Schutzziele erfüllen // 23



ABSTRACT

Geschäftskontakte auf dem Firmenhandy sicher verwalten

Die Arbeitswelt der Zukunft ist digital und flexibel. Das Smartphone, als Sinnbild des mobilen Arbeitens, ist daraus nicht mehr wegzudenken. Deshalb bieten immer mehr Unternehmen ihren Mitarbeitenden Szenarien, die auch eine private Nutzung von dienstlichen Geräten ermöglichen. Ob BYOD oder COPE: Was für User Vorteile bringt, birgt für Unternehmen auf datenschutzrechtlicher Seite jedoch erhebliche Risiken.

Diese treten vor allem dann auf, wenn die Anwender*innen Social-Media- und Messenger-Dienste aus dem Consumer-Umfeld auf den Geräten verwenden oder sie mit Infotainment-Systemen in Mietwägen oder Carsharing koppeln. Hier können die auf dem Smartphone gespeicherten Daten durch Dritte abgegriffen werden, was einen
erheblichen Verstoß gegen Datenschutz-Richtlinien darstellt.

Denn was vielen nicht bewusst ist: Geschäftsdaten dürfen datenschutzbedingt nur nach einer vorherigen Zustimmung des Kontakts an Dritte übertragen werden. Wie gelingt es Unternehmen also Datenschutz-Vorgaben einzuhalten, ohne die Produktivität der Mitarbeitenden einzuschränken?

Erfahren Sie, welche Richtlinien zu beachten sind, wo Risiken drohen und wie Sie Datenschutzverstöße vorbeugen können.

VORWORT

VORWORT

Geschäftskontakte auf dem Firmenhandy sicher verwalten
von RA Wilfried Reiners, PRW Rechtsanwälte

Angesichts der zunehmenden Relevanz des Datenschutzes und der Datensicherheit, nicht sollten sondern müssen Organisationen sicherstellen, dass die Nutzung von Firmenhandys in einem rechtskonformen Rahmen stattfindet. Die Datenschutzgrundverordnung (DSGVO) legt fest, unter welchen Bedingungen personenbezogene Daten verarbeitet werden dürfen. Kommen mobile Geräte sowohl beruflich als auch privat zum Einsatz, müssen die darauf gespeicherten Daten und übertragene Informationen ebenfalls gemäß DSGVO geschützt werden. Hier gibt es jedoch immer wieder Anwendungsfälle, die unzureichende Sicherheit bieten.

Um mögliche und vermutlich hohe Bußgelder zu vermeiden, sind Unternehmen deshalb gut beraten, besondere Vorkehrungen zu treffen. Denn werden sensible Daten, wie die persönlichen Kontaktdaten von Kunden oder Geschäftspartnern, ohne Zustimmung der betroffenen Personen bei der Synchronisation des Smartphone-Adressbuchs an Dritte übertragen, ist der Sanktionskatalog der DSGVO eröffnet. Wir haben selbst die Secure Contacts App getestet und werden die App in der gesamten PRW Group einsetzen. Hier wird mit wenig Aufwand sehr viel Positives erreicht.“

RECHTLICHE GRUNDLAGEN

RECHTLICHE GRUNDLAGEN

Die Verarbeitung personenbezogener Daten nach DSGVO

Mit Inkrafttreten der Datenschutzgrundverordnung (DSGVO) hat die EU die Regelungen zur Verarbeitung personenbezogener Daten vereinheitlicht. Die Verordnung schützt die Grundrechte und -freiheiten natürlicher Personen und stärkt deren Recht auf Datenschutz.

Hohe Bußgelder für Verstöße

Jedoch nicht in allen Unternehmen herrscht ausreichendes Bewusstsein darüber, wie weit der Schutz geht und welche Pflichten bestehen. Derweil können Datenschutzverstöße Unternehmen teuer zu stehen kommen. Gehen personenbezogene Daten verloren oder gelangen ohne Erlaubnis in die Hände Dritter, werden sie in die Haftung gezogen. Die Strafen sind empfindlich: Bis zu 20 Millionen Euro oder vier Prozent des globalen Umsatzes – je nachdem, welcher Betrag höher ausfällt – können fällig werden. Wichtig ist deshalb, Schwachstellen zu identifizieren und Pflichtverletzungen zu vermeiden.

DEFINITION

Was versteht der Gesetzgeber unter personenbezogenen Daten?

Personenbezogene Daten sind Informationen, die eindeutig einer Person zugeordnet werden können und damit Rückschlüsse auf sie zulassen. Beispiele hierfür sind Name, Adresse, Geburtsdatum, Telefonnummer, E-Mail-Adresse, Kreditkartennummer oder IP-Adressen.

Wann dürfen personenbezogene Daten verarbeitet werden?

Unter die Verarbeitung personenbezogener Daten fallen sowohl das Erheben, Nutzen, Verändern, Übermitteln und Speichern als auch deren Löschung. Diese Aktivitäten dürfen nur dann durchgeführt werden, wenn es ein Gesetz erlaubt oder die betroffene Person dazu eingewilligt hat. Das heißt: Grundsätzlich ist alles verboten, was nicht ausdrücklich erlaubt ist. Dies nennt man in der Fachsprache Verbot mit Erlaubnisvorbehalt.

Die Einwilligung Betroffener muss freiwillig und informiert erfolgen. Neben der Einholung der Zustimmung sind Verantwortliche verpflichtet, über den möglichen Widerruf unmissverständlich in Kenntnis zu setzen.

Von Gesetzeswegen ist die Verarbeitung personenbezogener Daten dann erlaubt, wenn vertragliche Verpflichtungen wie zum Beispiel Lieferbeziehungen zwischen den Parteien bestehen.

Was beinhaltet die Auftragsverarbeitung?

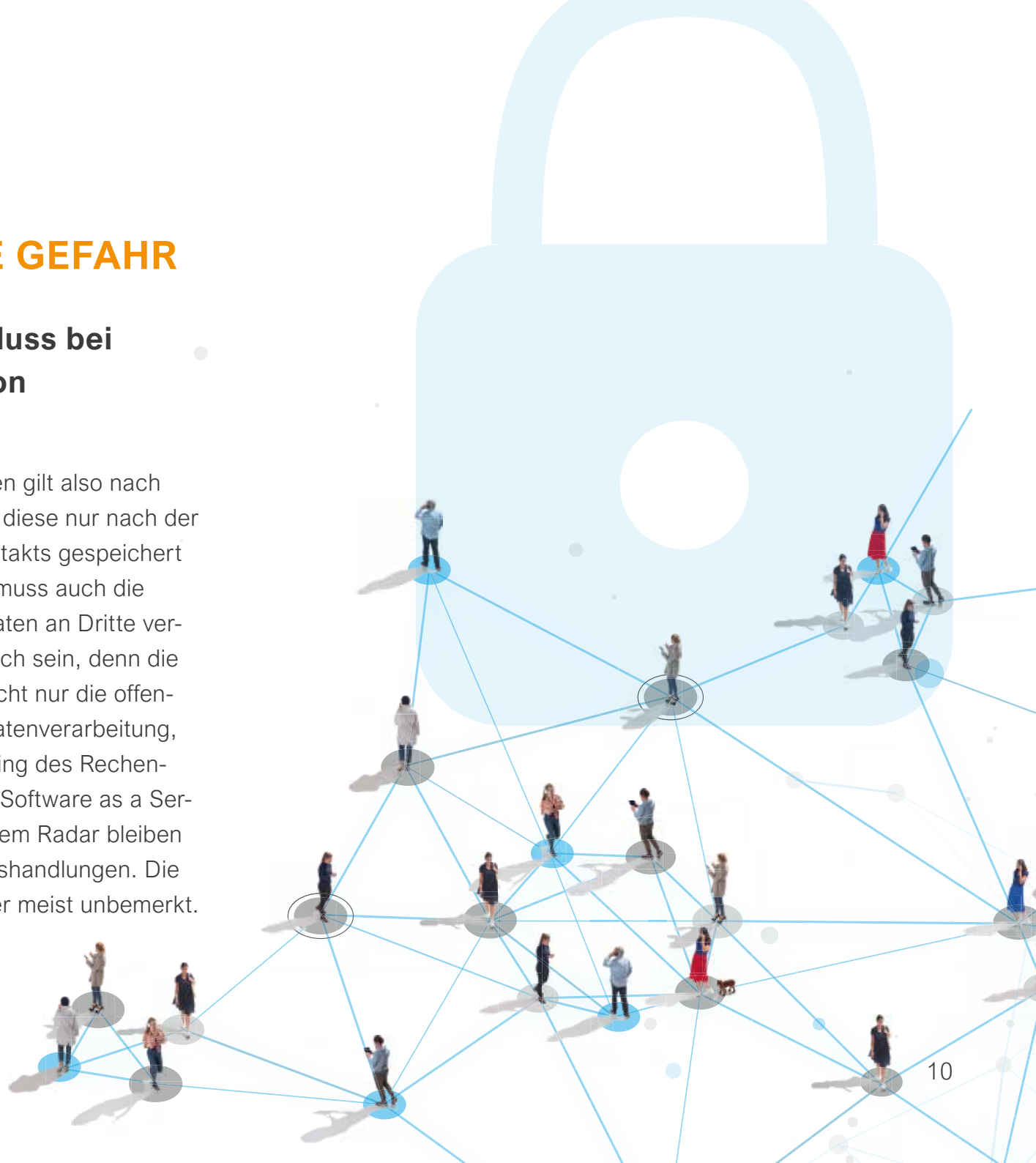
Im Zuge einer Auftragsverarbeitung, erfolgt die Verarbeitung personenbezogener Daten durch Dritte, wie zum Beispiel durch externe Dienstleister. Liegt ein Auftragsverarbeitungsverhältnis vor, ist auch ein entsprechender Vertrag zu erstellen. Zudem treffen den Auftraggeber Kontroll- und Dokumentationspflichten, beispielsweise hinsichtlich der Einhaltung der technisch-organisatorischen Maßnahmen durch den Auftragnehmer.

DATENSCHUTZRISIKO

UNTERSCHÄTZTE GEFAHR

Ungewollter Datenabfluss bei Kontaktsynchronisation

Bei Geschäfts- bzw. Kundendaten gilt also nach DSGVO die klare Vorgabe, dass diese nur nach der vorherigen Zustimmung des Kontakts gespeichert werden dürfen. Darüber hinaus muss auch die automatische Weitergabe der Daten an Dritte verhindert werden. Das kann tückisch sein, denn die Auftragsverarbeitung umfasst nicht nur die offensichtlichen Fälle der externen Datenverarbeitung, wie zum Beispiel beim Outsourcing des Rechenzentrums oder der Nutzung von Software as a Service und Cloud-DienstenUnter dem Radar bleiben zum Standard gewordene Alltagshandlungen. Die Datenverarbeitung geschieht hier meist unbemerkt.



Automatische Synchronisation von Kontaktdaten durch Messenger-Dienste

Laut dem Mobile-Work-Index nutzen 38 Prozent der Arbeitnehmer*innen Messenger-Dienste auf ihrem Firmenhandy. Das Problem bei WhatsApp & Co.: Die Anwendungen verschaffen sich automatisch Zugriff auf alle gespeicherten Kontaktdaten aus dem Adressbuch und speichern sie zum Datenabgleich auf eigenen Servern in der Cloud.
Was für die User praktisch ist, da sie die Daten nicht noch einmal händisch in der App einspeichern müssen, versetzt Datenschutzbeauftragte in Alarmbereitschaft. Denn hier fehlt es zum einen an der Möglichkeit einen Auftragsverarbeitungsvertrag abzuschließen, zum anderen ist es im geschäftlichen Alltag praktisch unmöglich von sämtlichen geschäftlichen Kontakten eine entsprechende schriftliche Einwilligung zu holen. Noch komplizierter wird es, wenn nicht alle Kontakte ihre Zustimmung erteilen. Konsequenterweise dürfte der Messenger-Dienst entweder generell nicht installiert oder es müsste für alle Kontakte, die ihre Zustimmung nicht erteilt haben, ein Smartphone ohne WhatsApp betrieben werden

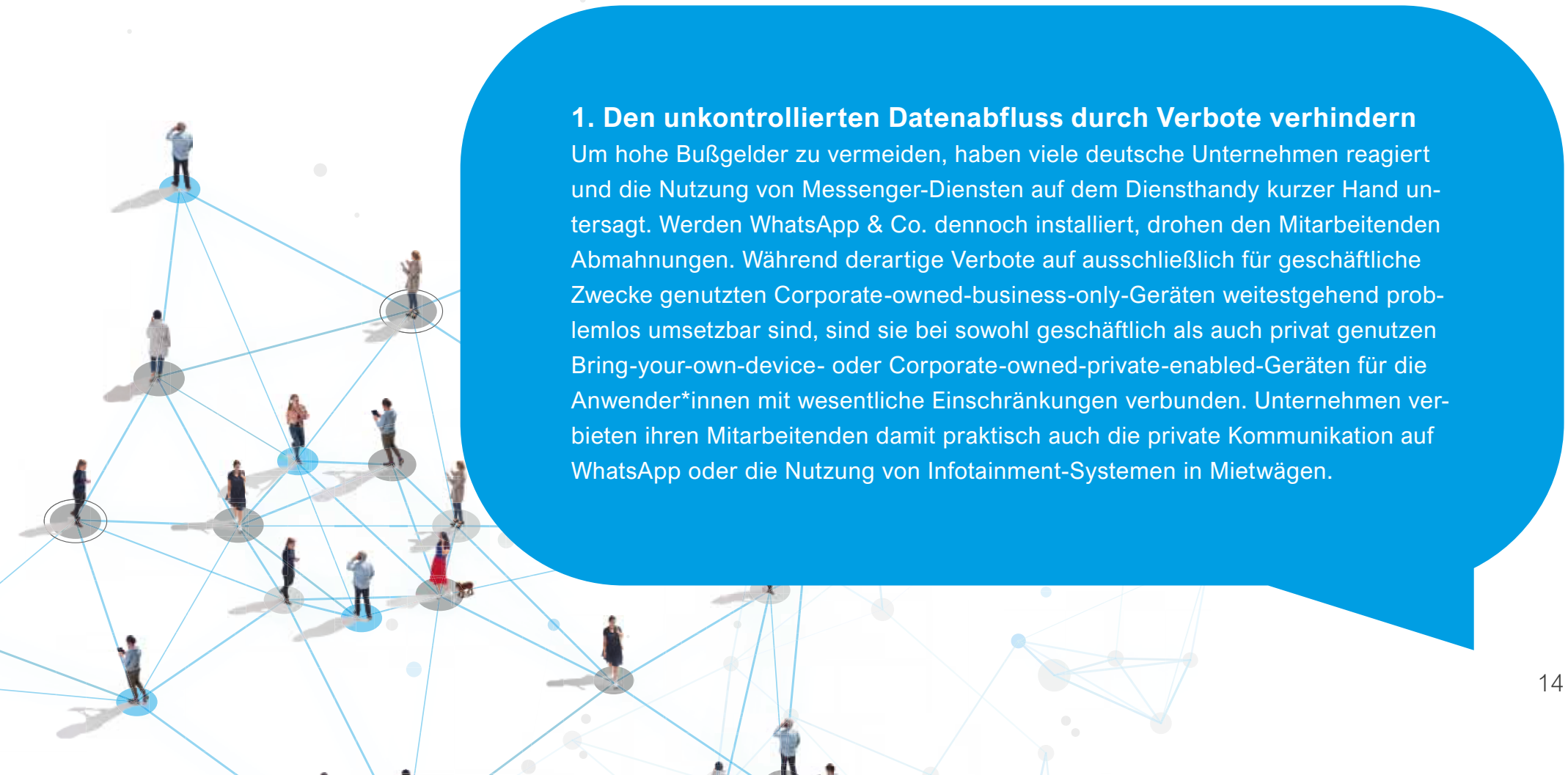
Persönliche Profile in Mietautos und Carsharing

Mietautos und Carsharing erfreuen sich ebenfalls immer größerer Beliebtheit. Neben Navigation und Radio wird hier meist auch die Koppelung des Smartphones mit dem Infotainment-System angeboten. Während die Möglichkeit Anrufe und Nachrichten während der Fahrt zu empfangen, gern genutzt wird, geht damit jedoch ein erhebliches Datenrisiko einher.
Im Zuge der automatischen Synchronisation mit dem Adressbuch des Smartphones werden die Kontakte im System des Fahrzeugs gespeichert. Der Datenverlust nach einer Synchronisation lässt sich nur verhindern, indem das System nach der Fahrt manuell auf Werkeinstellung zurückgesetzt wird, sagen Automobilhersteller. Laut eines Berichts des ADACs kann eine solche Rücksetzung jedoch von Automodell zu Automodell grundlegend verschieden sein und bisweilen ein erhebliches Unterfangen bedeuten. Ein Aufwand, den viele Nutzer nicht betreiben, sofern überhaupt das Bewusstsein für die Problematik vorhanden ist. Darüber hinaus berichtet der ADAC, dass zwar vier von fünf Autovermieter persönliche Daten von Fahrzeugnutzern nach der Fahrt löschen, dies allerding nur teilweise nach jeder Rückgabe geschieht. Auf diese Weise bleibt jedoch eine Vielzahl schützenswerter Daten völlig offen für andere Mieter oder Automobil-Verleiher in den zurückgegebenen Wägen.

WIE KÖNNEN DATEN-SCHUTZVERSTÖSSE VERHINDERT WERDEN?

Die Nutzung von Messenger-Diensten auf dem Firmenhandy oder die Koppelung mit Infotainment-Systemen in Mietwägen ist aus datenschutzrechtlicher Sicht kaum möglich. Sind Verbote also die einzige Möglichkeit Datenschutz-Richtlinien einzuhalten?

Wir haben vier Lösungsansätze unter die Lupe genommen:



1. Den unkontrollierten Datenabfluss durch Verbote verhindern

Um hohe Bußgelder zu vermeiden, haben viele deutsche Unternehmen reagiert und die Nutzung von Messenger-Diensten auf dem Diensthandy kurzer Hand untersagt. Werden WhatsApp & Co. dennoch installiert, drohen den Mitarbeitenden Abmahnungen. Während derartige Verbote auf ausschließlich für geschäftliche Zwecke genutzten Corporate-owned-business-only-Geräten weitestgehend problemlos umsetzbar sind, sind sie bei sowohl geschäftlich als auch privat genutzen Bring-your-own-device- oder Corporate-owned-private-enabled-Geräten für die Anwender*innen mit wesentliche Einschränkungen verbunden. Unternehmen verbieten ihren Mitarbeitenden damit praktisch auch die private Kommunikation auf WhatsApp oder die Nutzung von Infotainment-Systemen in Mietwägen.

2. Die Nutzung von Messenger & Co. mit Compliance-Richtlinien einschränken

Um keine Verbote aussprechen zu müssen, versuchen andere Unternehmen die Nutzung von Messenger-Diensten mit Compliance-Richtlinien zu regulieren. Dabei werden jedoch oft nur Teilaspekte des Datenschutzes erfasst, während andere Bereiche davon völlig unberührt bleiben. Mitarbeitende werden beispielsweise angehalten Messenger-Dienste nicht für berufliche Zwecke zu nutzen. Wer darauf trotz aller Richtlinien nicht verzichten wollte, soll zumindest eine ausreichende Dokumentation sicherstellen. Hiervon völlig unberührt bleiben jedoch Verstöße gegen Datenschutzrichtlinien, die bereits bei Installation der Anwendungen, durch die automatische Weitergabe von Kontaktdaten an Unternehmen wie Meta, begangen werden. Diese können ebenfalls behördlich abgemahnt werden.

3. Auf das Abspeichern von Kontaktdaten im Firmenhandy verzichten

Nun lässt sich weder ein Verbot von WhatsApp für alle geschäftlich genutzten Smartphones sinnvoll umsetzen, noch können interne Nutzungsrichtlinien jeden rechtlichen Verstoß beseitigen. Was übrig bleibt, wäre eine Regelung, mit der die Speicherung von geschäftlichen Kontakten im Adressbuch des Firmenhandys nur mit zuvor abgeschlossenem Auftragsverarbeitungsvertrag erlaubt ist oder ein komplettes Speicherverbot für geschäftliche Daten. Dies geht jedoch für die Mitarbeitenden mit einer enormen Verringerung der Usability einher, denn bei eingehenden Anrufen von Geschäftspartnern oder Kunden, kann der Anrufer nicht mehr namentlich identifiziert werden. Auch für ausgehende Anrufe muss zunächst die Nummer aus dem CRM oder dem Outlook-Adressbuch herausgesucht werden. Dies kostet nicht nur Zeit, sondern auch Nerven.

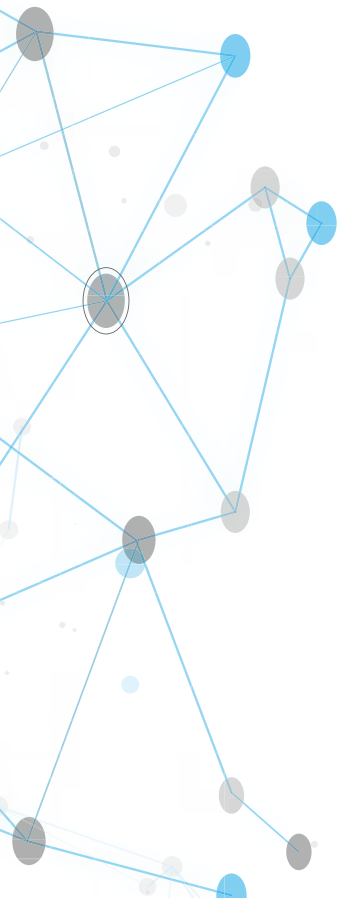
4. Mit einer sicheren Zusatzapp den ungewollten Datenabfluss verhindern

Um Datenschutzverstöße effektiv zu verhindern, müssen dienstliche von privaten Daten auf mobilen Endgeräten getrennt werden. Hierfür kann eine Zusatzapp eingesetzt werden. Das ist eine mobile Anwendung, die einen geschützten Bereich (Container) auf dem mobilen Endgerät abtrennt. Für Anwender*innen bedeutet das, dass sie auf dem Smartphone nur innerhalb einer geschützten und verschlüsselten Umgebung auf geschäftliche Daten zugreifen können. Datenschutzrechtlich kritische Anwendungen wie WhatsApp erhalten dabei keinen Zugriff auf geschäftliche Kontakte.

BEST PRACTICE FÜR DATENSCHUTZ

BEST PRACTICE FÜR DATENSCHUTZ

Die Secure Contacts App – DSGVO-konform, praktisch und einfach



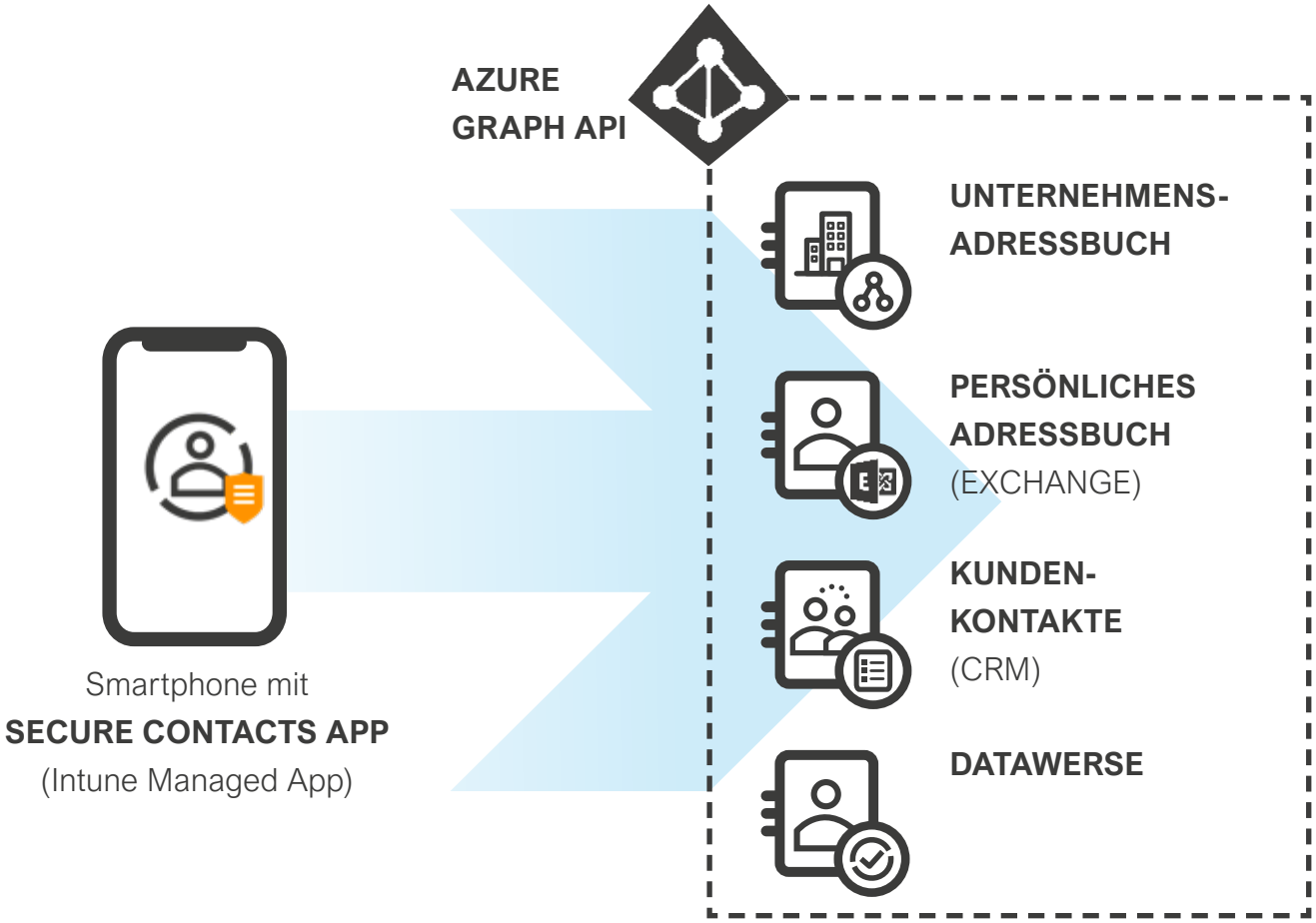
Die Secure Contacts App ermöglicht die durchgängig datenschutzkonforme Nutzung von Geschäftskontakten auf dem Smartphone. Durch die vollständige Integration mit Microsoft Intune werden Kontaktdaten geschützt und die Synchronisation mit Apps von Drittanbietern wie WhatsApp, Google, etc. verhindert. Die Nutzer müssen keinen einzigen Kontakt auf ihrem eigenen Gerät speichern und pflegen. Dies ist nicht nur praktisch für die Mitarbeitenden, sondern birgt einen entscheidenden Vorteil: Wo keine Datenspeicherung, da kein Schaden.

Wertvolle Daten gezielt schützen

Alle Geschäftsdaten aus dem Firmenadressbuch, dem persönlichen Outlook-Adressbuch und Kundendaten aus beliebigen CRM-Systemen oder anderen Quellen werden in der App zusammengeführt und zentral verwaltet. Die App fungiert dabei als geschützter und verschlüsselter Container, der einen unkontrollierten Datenabfluss verhindert. Auch eine Synchronisation mit Mietwägen und Carsharing wird unterbunden. Einmal im System haben alle Firmenmitglieder Zugriff auf die für sie berechtigten Kontakte. Dank der automatisierten Datenpflege entfällt das händische Einspeichern neuer Kontakte, Doppelkontakte werden konsolidiert und die Daten durchgängig aktualisiert.

Im Adressbuch des Smartphones können alle Kontakte gespeichert werden, die rein privat genutzt werden. Diese unterliegen dem Privileg persönlicher und familiärer Tätigkeiten und sind nicht DSGVO-relevant. Somit ist die Installation und private Nutzung von WhatsApp auf dem Firmenhandy ohne Compliance-Risiken möglich.

SICHERHEIT DUCH MICROSOFT AZURE & INTUNE



- **VOLLSTÄNDIGE INTEGRATION** in Microsoft Intune
- **ZUGRIFFS-BERECHTIGUNGEN** Zentral und individuell verwaltbar
- **PASSWORTLOSE NUTZUNG** durch Single-Sign-On
- **SERVERLESS**

ALLE FEATURES AUF EINEN BLICK

Datenschutz & Usability

Daten-Integration mit einmaligem Login, alle Kontakte aus dem Unternehmensadressbuch, persönlichem Outlook-Adressbuch und CRM automatisiert synchronisieren

Anrufererkennung aus allen synchronisierten Quellen und Anzeige des Unternehmensnamen

Anonyme Anrufe können direkt aus der App getätigt werden, ohne dass die eigene Rufnummer mitgesendet wird

Integration von MS Teams
Anzeige des Teams Status, Starten von MS Teams(Video-)Calls und Chats

Schnellsuche von Kontakten aus allen verknüpften Datenquellen

Digitale Visitenkarte für effizientes und nachhaltiges Networking

Urlaubsfunktion die nur Anrufe favorisierter Kontakte zulässt

Die App im Vergleich: Die wichtigsten Punkte auf einen Blick

USABILITY		Secure Contacts App	iPhone Kontakte App	MS Outlook App for iOS	MS Teams App for iOS
Ausgehende anrufe: Telefonie	Kontakte aus dem Outlook-Adressbuch	✓	✓	✓	✓
	Kontakte aus dem Unternehmens-adressbuch (Global Adress-List)	✓	✗	✓	✓
	Kontakte aus weiteren Quellen wie CRM-System	✓	✗	✗	✗
Anrufer-erkennung eingehender anrufe	Kontakte aus dem Outlook-Adressbuch	✓	✓	–	–
	Kontakte aus dem Unternehmens-adressbuch (Global Adress-List)	✓	✗	✗	–
	Kontakte aus weiteren Quellen wie CRM-System	✓	✗	✗	✗
Microsoft Teams Statusanzeige	Anzeige des Microsoft Teams Status für Kontakte aus dem Unternehmensadressbuch	✓	✗	✗	✓
DATENSCHUTZ- & INFORMATIONSSICHERHEIT					
DSGVO konform	DSGVO konforme Ablage der daten	✓	✗	✓	✓
	Verhinderung des unkontrollierten Abflusses von Kontaktdaten durch Apps mit zugriff auf das Gerätetelefonbuch (wie z.B. WhatsApp)	✓	✗	✓	✓
VERWALTUNG					
Zentrale Verwaltung der App (via Microsoft Intune)	Geräte-basierte Konfiguration	✗	✓	✗	✗
	App-basierte Konfiguration • App Schutzrichtlinien • App Einstellungen	✓	✗	✓	✓
	Globale filterregeln für kontakte	✓	✗	✗	✗

FAZIT

Kontakte effizient schützen und DSGVO-Schutzziele erfüllen

Geschäftskontakte auf dem Firmenhandy sind meist Standard – aber gefährlich. Unternehmen sollten sich dieser Gefahr bewusst sein und sind selbst in der Pflicht aktiv zu werden, um sich vor Strafzahlungen durch Datenschutzverstöße zu schützen.
Testen Sie deshalb die Secure Contacts App und fordern Sie die kostenfreie Testlizenz mit vollem Funktionsumfang direkt bei uns an. Überzeugen Sie sich selbst von den vielen Vorteilen für Ihren Arbeitsalltag. Sie bezahlen nur, wenn Sie nach Ablauf der Testlizenz tatsächlich überzeugt sind.
Unsere Kunden sind bereits begeistert:

„Die integrierte Anruferkennung der Secure Contacts App von Provectus sowie die sichere Bereitstellung von unterschiedlichen Kontaktquellen ist für uns als Kunde ein signifikanter Benefit – eine tolle Lösung mit viel Potential."

TOBIAS JAKOB, DIRECTOR INFRASTRUCTURE BEI HOME SHOPPING EUROPE GMBH

JETZT KONTAKT AUFNEHMEN!

Sie wollen Ihre Geschäftskontakte schützen und dabei die Arbeit Ihrer Mitarbeitenden nicht beeinträchtigen? Lassen Sie uns über ihr Projekt sprechen!

Ihr Ansprechpartner:
Alexandros Garoufis
Mail: alexandros@provectus.de
Tel.: +49 (0) 89 710 409 20