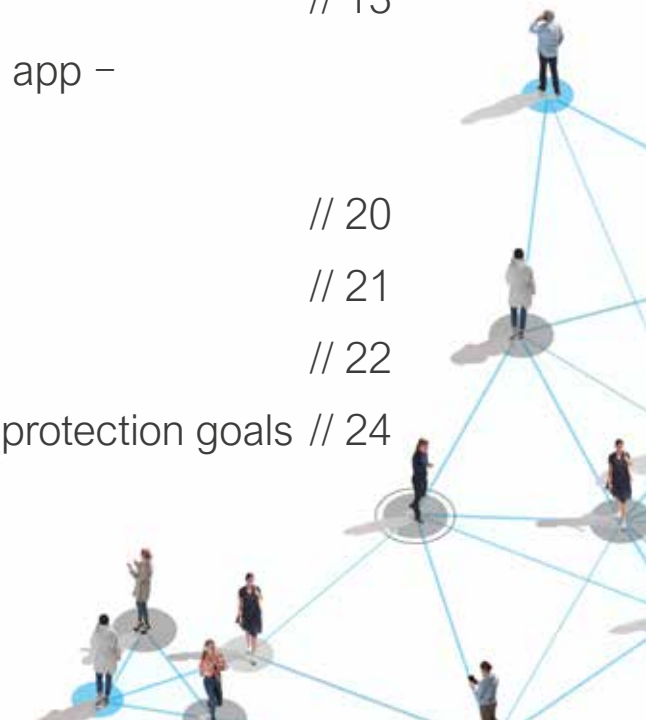
how to

THE SMART SOLUTION FOR SECURE CONTACT MANAGEMENT

INHALT



ABSTRACT

Securely manage business contacts on a company cell phone

The working world of the future is digital and flexible. The smartphone, the embodiment of mobile work, has become indispensable. That's why more and more companies are offering their employees scenarios that also allow the private use of company-owned devices. Whether BYOD or COPE: what is beneficial for users, entails considerable risks for companies in terms of data protection.

These mainly occur when users use social media and messenger services from the consumer environment on such devices or pair them to infotainment systems in rental car or car sharing services. In such cases, the data stored on the smartphone can be accessed by third parties, which represents a significant violation of data protection guidelines.

Because what many people don't realize is that, for data protection reasons, business data may only be transferred to third parties with the prior consent of the contact. So how can companies comply with data protection regulations without restricting employee productivity?

Find out which policies must be observed, where the risks lie, and how you can prevent violations of data protection law.

PREFACE

PREFACE

Securely manage business contacts on a company cell phone
by Wilfried Reiners, Attorney, PRW Rechtsanwälte

Given the increasing relevance of data protection and data security, organizations not only should, but must, ensure that the use of company cell phones takes place within a legally compliant framework. The General Data Protection Regulation (GDPR) defines the conditions under which personal data may be processed. If mobile devices are used both professionally and privately, the data stored on them and the information transmitted must also be protected as required by the GDPR. However, time and again there are applications that do not afford sufficient security.

Consequently, to avoid possible and potentially heavy fines, companies are well advised to take special precautions. After all, if sensitive data, such as the personal contact data of customers or business partners, is transferred to third parties when synchronizing the smartphone address book without the consent of the data subjects, this opens the door to the GDPR's catalog of sanctions. We have tested the Secure Contacts app ourselves and will be using the app in the entire PRW Group. This is a way to achieve a lot of positive results with very little effort. “

LEGAL BASIS

LEGAL BASIS

Processing personal data pursuant to the GDPR

Upon the General Data Protection Regulation (GDPR) entering into force, the EU standardized the regulations on the processing of personal data. The regulation protects the fundamental rights and freedoms of natural persons and underpins their right to data protection.

High fines for violations

However, not all companies are fully aware of how far protection goes and what their obligations entail. Meanwhile, data protection violations can cost companies dearly. If personal data is lost or falls into the hands of third parties without permission, they will be held liable. The penalties are severe: up to 20 million euros or four percent of global sales, whichever is higher, can be imposed. It is therefore important to identify vulnerabilities and avoid breaches of duty.

DEFINITION

How does the law define personal data?
Personal data is information that can be explicitly assigned to an individual and thus allows conclusions to be drawn about that person. Examples include name, address, date of birth, telephone number, email address, credit card number, or IP addresses.

When may personal data be processed?

The processing of personal data includes the collection, use, modification, transmission, and storage of personal data as well as its deletion. These activities may only be carried out if permitted by law or with the consent of the data subject. In other words, everything that is not expressly permitted is prohibited. In technical jargon, this is referred to as prohibition with reservation of permission.

The consent of data subjects must be voluntary and informed. In addition to obtaining consent, data controllers are required to provide unambiguous information about the option of withdrawing it. The processing of personal data is permitted by law if contractual obligations exist between the parties, such as supply relationships.

What does commissioned data processing entail?

As part of commissioned data processing, the processing of personal data is carried out by third parties, such as external service providers. If a commissioned data processing relationship exists, a contract to that effect must also be drawn up. In addition, the principal is subject to monitoring and documentation obligations, for example with regard to the contractor's compliance with technical and organizational measures.

DATA PRIVACY RISK

UNDERRATED RISK

Unintentional data loss when synchronizing contacts

In the case of business or customer data, the GDPR clearly stipulates that this data may only be stored with the prior consent of the contact. In addition, the automatic transfer of data to third parties must also be prevented. This can be tricky, because commissioned data processing not only includes the obvious cases of external data processing, such as when outsourcing the data center or using software as a service and cloud services. It's the standard everyday actions that fall under the radar. For the most part, data processing takes place unnoticed here.

Automatic synchronization of contact data by messenger services

According to the Mobile Work Index, 38 percent of employees use messenger services on their company cell phones. The problem with WhatsApp and the like is that the applications automatically gain access to all stored contact data from the address book and store it on their own servers in the cloud for data synchronization.

While this is convenient for users because they don't have to manually enter the data into the app again, this sets off alarm bells with data protection officers. For one, there is no possibility of concluding a commissioned data processing agreement, and for another, it is virtually impossible in daily business to obtain written consent from every business contact. It becomes even more complicated if not all of the contacts give their consent. Consequently, the messenger service should either generally not be installed or a smartphone without WhatsApp would have to be used for those contacts who have not given their consent.

Personal profiles in rental cars and car sharing

Rental car and car sharing services are becoming increasingly popular. In addition to a navigation system and radio, the smartphone can usually be paired with the infotainment system. While the option of getting calls and messages while driving is welcomed, it is accompanied by a significant data risk.
During automatic synchronization with the smartphone's address book, contacts are stored in the vehicle's system. The loss of data after synchronization can only be prevented by manually resetting the system to factory settings after the trip, say car manufacturers. However, according to a report by ADAC, such a reset can be radically different from one car model to the next and can sometimes be a formidable task. This is something many users don't bother to do, if they are aware of the problem at all. In addition, ADAC reports that although four out of five car rental companies delete the personal data of users after the trip, this only occurs to a limited extent after each return. This means that a large amount of sensitive data remains completely accessible to other renters or car rental companies in the returned cars.

HOW CAN DATA PRIVACY BREACHES BE PREVENTED?

From a data protection perspective, the use of messenger services on company cell phones or pairing with infotainment systems in rental cars is virtually untenable. So are bans the only way to comply with data protection guidelines?

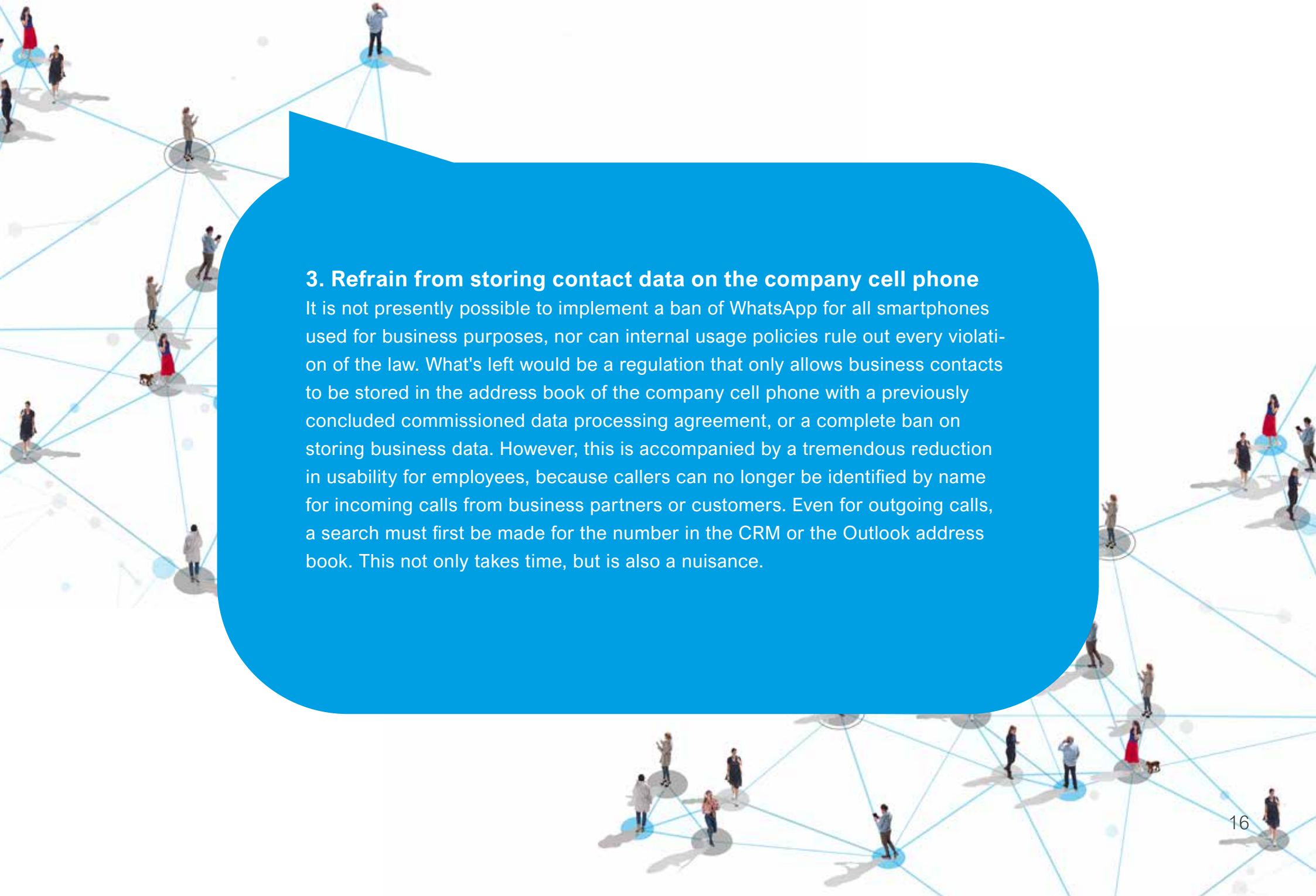
We have examined four possible solutions in detail:

1. Prevent uncontrolled data loss through bans

In order to avoid heavy fines, many German companies have reacted and summarily prohibited the use of messenger services on company cell phones. If WhatsApp and the like are nevertheless installed, employees are threatened with formal warnings. While such bans are generally easy to implement on corporate-owned business-only devices, they impose significant restrictions on users of bring your own device (BYOD) or corporate-owned personally enabled (COPE) devices used for both business and private purposes. This means that companies are effectively prohibiting their employees from communicating privately on WhatsApp or using infotainment systems in rental cars.

2. Restrict the use of messenger services and the like with compliance policies

To avoid having to issue complete bans, some companies try to regulate the use of messenger services with compliance policies. However, this often only covers specific aspects of data protection, while other areas remain completely unaddressed. For example, employees are urged not to use messenger services for professional purposes. Those who didn't want to go without them despite all the policies should at least ensure that there is adequate documentation. Completely unaffected by this, however, are violations of privacy policies that are already committed when the applications are installed, through the automatic forwarding of contact data to companies such as Meta. These can also be subject to official warnings.



3. Refrain from storing contact data on the company cell phone

It is not presently possible to implement a ban of WhatsApp for all smartphones used for business purposes, nor can internal usage policies rule out every violation of the law. What's left would be a regulation that only allows business contacts to be stored in the address book of the company cell phone with a previously concluded commissioned data processing agreement, or a complete ban on storing business data. However, this is accompanied by a tremendous reduction in usability for employees, because callers can no longer be identified by name for incoming calls from business partners or customers. Even for outgoing calls, a search must first be made for the number in the CRM or the Outlook address book. This not only takes time, but is also a nuisance.

4. Prevent unintentional data loss with an additional secure app

To effectively prevent data privacy violations, business data must be separated from private data on mobile devices. An additional app can be used for this purpose. This is a mobile application that creates a protected area (container) on the mobile device. For users this means that they can only access business data on their smartphone within a protected and encrypted environment. Applications that are critical from a data protection perspective, such as WhatsApp, are not granted access to business contacts.

BEST PRACTICE FOR DATA PROTECTION

BEST PRACTICE FOR DATA PROTECTION

The Secure Contacts app—GDPR-compliant, practical, and easy to use

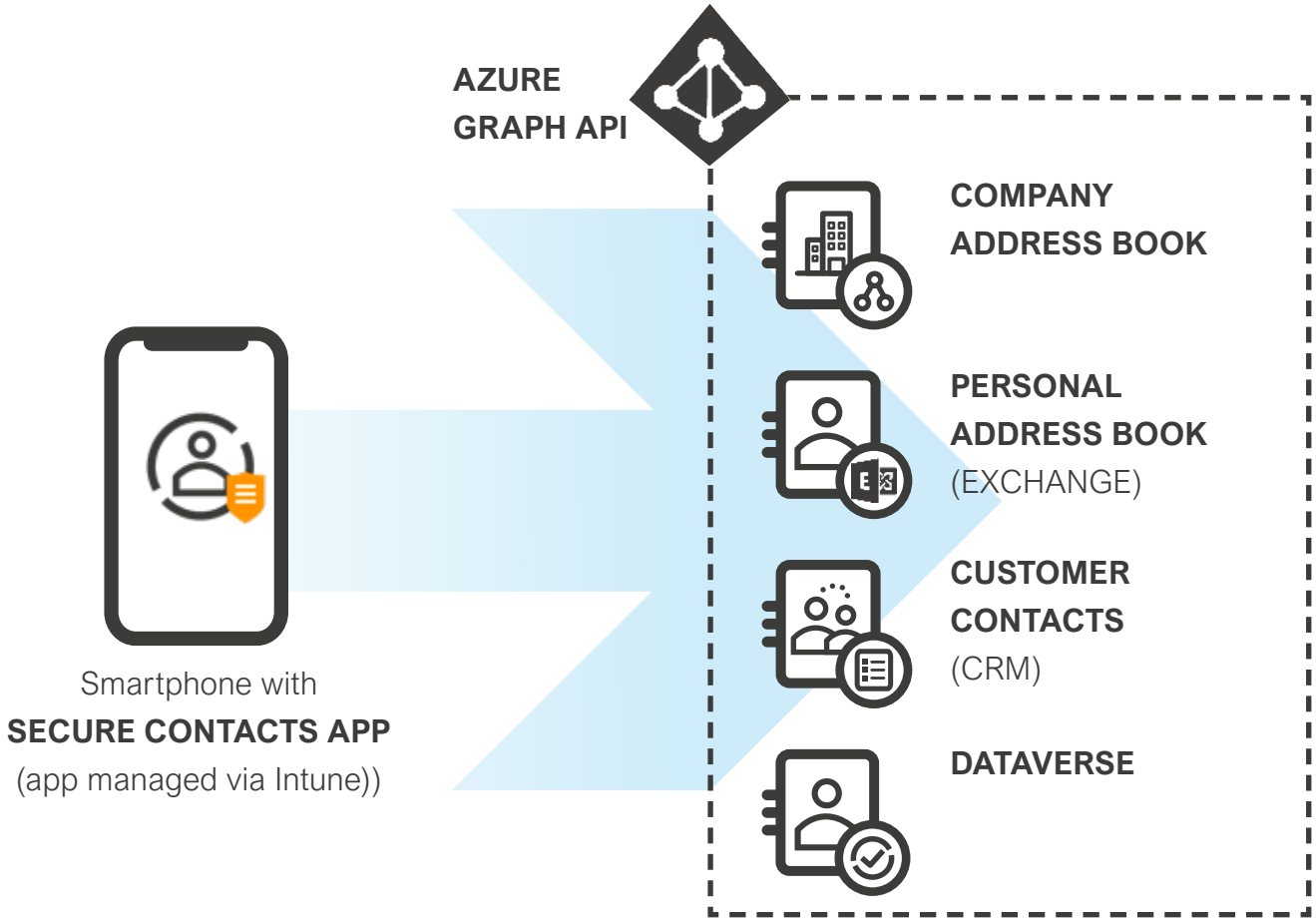
The Secure Contacts app enables end-to-end data protection-compliant use of business contacts on a smartphone. Full integration with Microsoft Intune protects contact data and prevents synchronization with third-party apps such as WhatsApp, Google, etc. Users don't have to store and maintain a single contact on their own device. This is not only convenient for employees, but also has a major benefit: harm cannot occur where no data is stored.

Protect valuable data in a targeted way

All business data from the company address book, the personal Outlook address book, and customer data from any CRM systems or other sources are pooled in the app and managed centrally. The app acts as a protected and encrypted container that prevents unintentional data loss. Synchronization with rental car and car sharing services is also prevented. Once in the system, all members of the company have access to the contacts authorized for them. Thanks to automated data maintenance, there is no need to manually enter new contacts, duplicate contacts are consolidated, and data is consistently updated.

All contacts used for private purposes only can be stored in the smartphone address book. They are subject to the privilege of personal and family activities with no relevance to the GDPR. This makes it is possible to install WhatsApp on the company cell phone and use it privately with no compliance risks.

PRIVACY & USABILITY COMBINED IN ONE APP



- **FULLY INTEGRATED** with Microsoft Intune
- **ACCESS PERMISSIONS** managed centrally and individually
- **NO PASSWORD REQUIRED** due single sign-on
- **SERVERLESS**

ALL THE FEATURES AT A GLANCE

Privacy & usability

Data integration with single login, automatically syncs all contacts from company address book, personal Outlook address book, and CRM

Caller identification from all data sources

Anonymous calls can be made directly from the app without sharing your own phone number

Integration of MS Teams

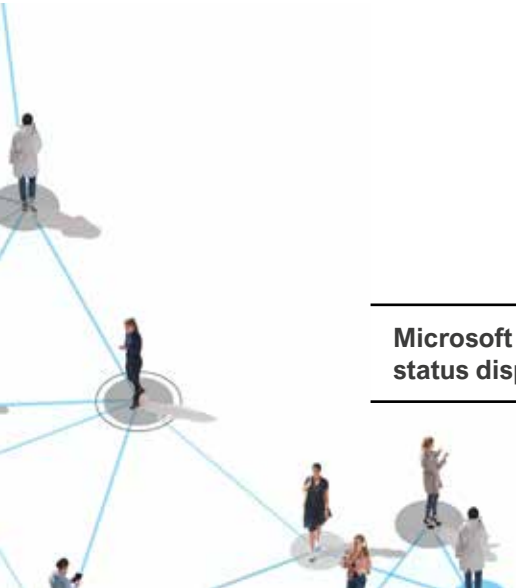
Quick search of contacts from all linked data sources

Digital business card for efficient and effective networking

Out-of-office feature that only allows calls from favorite contacts

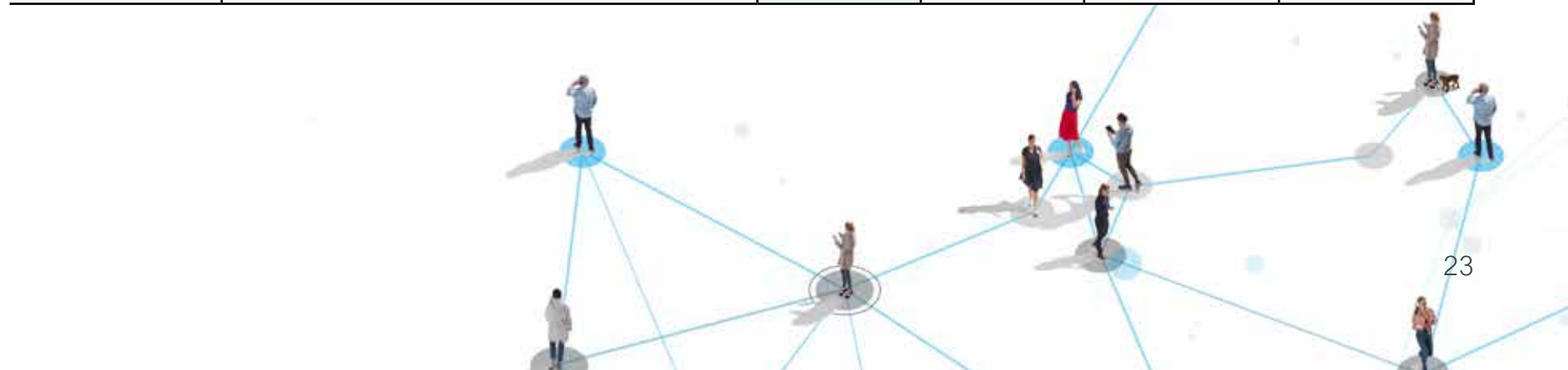
The app in comparison: the main points at a glance

		Secure Contacts app	iPhone Contacts app	Outlook app for iOS	Teams app for iOS
Usability					
Outgoing calls: Telephony	Contacts from the Outlook address book	✓	✓	✓	✓
	Contacts from the company address book (global address list)	✓		✓	✓
	Contacts from other sources, such as the CRM system	✓			
	Simple, anonymizedcalls	✓			
Caller ID for incoming calls	Contacts from the Outlook address book	✓	✓	✓ Only with syncing to local address book	✓ Teams calls only
	Contacts from the company address book (global address list)	✓			✓ Teams calls only
	Contacts from other sources, such as the CRM system	✓			
	Out-of-office and sleep mode (in development) (business calls forwarded to voicemail)	✓			
Microsoft Teams status display	Displays Microsoft Teams status for contacts from the company address book	✓			✓



The app in comparison: the main points at a glance

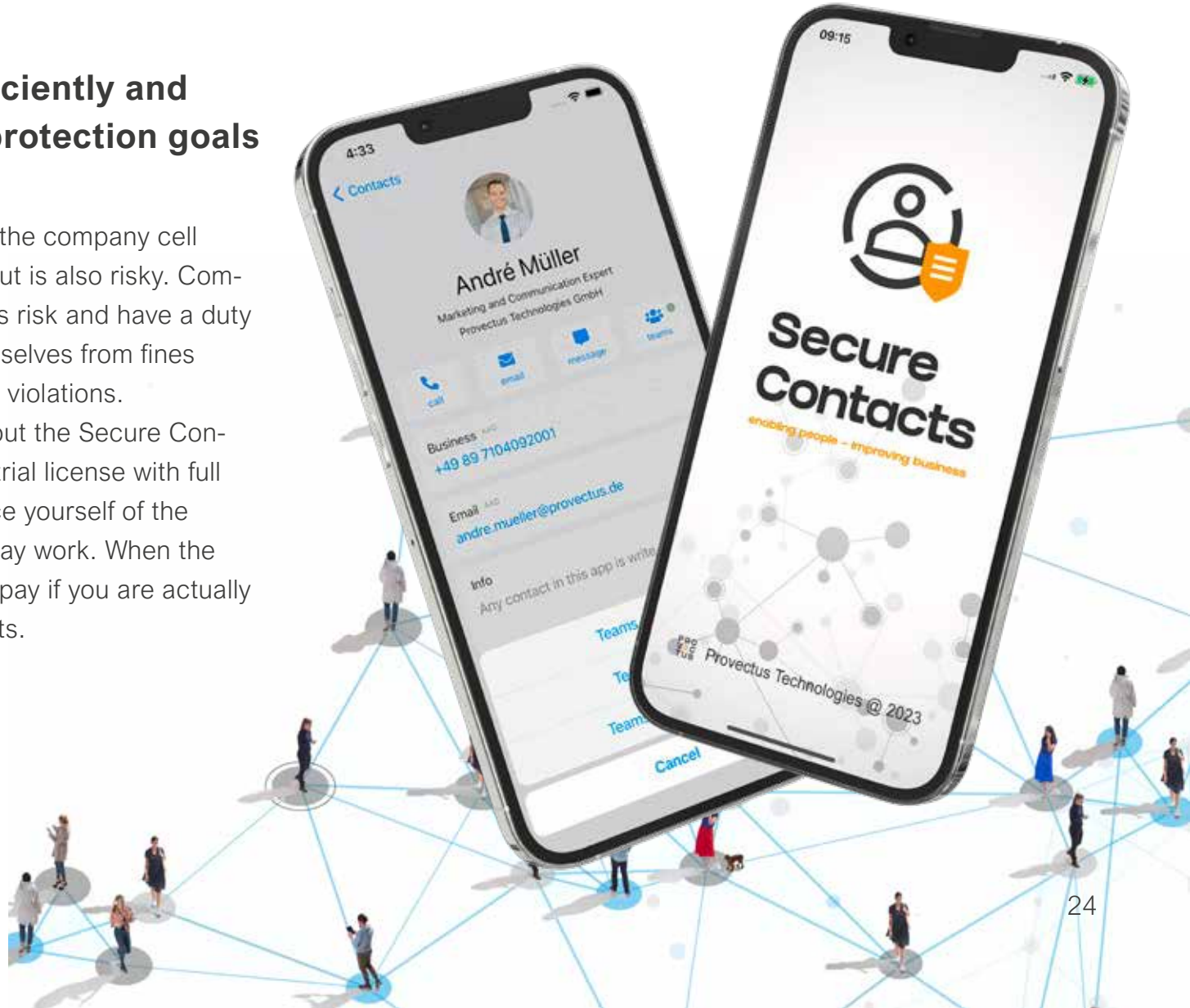
		Secure Contacts app	iPhone Contacts app	Outlook app for iOS	Teams app for iOS
Data protection and information security					
GDPR-compliant	GDPR-compliantdatastorage	✓		✓	✓
	Prevents uncontrolled outflow of contact data to apps with access to the device's phonebook (such as WhatsApp)	✓		✓	✓
App management					
Central management of the app (via Microsoft Intune)	Device-basedconfiguration		✓ Only for MDM-mgd. devices		
	App-basedconfiguration •App protectionguidelines •App settings	✓		✓	✓
	Global filter rules for contacts	✓			
	CI adjustments	✓			



CONCLUSION

Protect contacts efficiently and comply with GDPR protection goals

Having business contacts on the company cell phone is typically the norm, but is also risky. Companies should be aware of this risk and have a duty to take action to protect themselves from fines resulting from data protection violations.
So that's why you should try out the Secure Contacts app and request a free trial license with full functionality from us. Convince yourself of the many benefits for your everyday work. When the trial license expires, you only pay if you are actually convinced of the app's benefits.



„Having caller identification built into the Secure Contacts app from Provectus, as well as the secure provision of different contact sources, is a significant benefit for us as a customer! It's a great solution with lots of potential."

TOBIAS JAKOB, DIRECTOR OF INFRASTRUCTURE AT HOME SHOPPING EUROPE GMBH