

Adressverwaltung DSGVO-konform

Outlook, iCloud, GMX-Konto, Google-Account, auf der Simkarte oder ein Adressbuch ganz klassisch auf Papier...

Wo lagern die Kontaktdaten, dienstliche und privat so, dass sie immer greifbar sind aber doch Datenschutz-konform?

Ganz sicher geht das mit einem Adressbuch in Papierform.

Wirklich praktisch und zeitgemäß ist das nicht.

Also haben wohl die meisten heute die Adressen von Verwandten und Geschäftspartnern digital gespeichert.

Aber da fangen die Probleme auch gleich an:

Sind Kontaktdaten nur auf dem Computer zuhause, oder werden sie abgeglichen mit dem Smartphone?

Geht das dann über Google (bei Android) oder die iCloud (fürs iPhone), oder liegen sie im Internet beim Email-Dienstanbieter wie zum Beispiel bei GMX?

Liegen die Daten damit auf Servern in Europa oder z.B. in den USA?

Liegen alle Kontaktdaten in einer einzigen Datenbank, egal ob Privat oder Dienst, alles gut gemischt?

Wurden und werden die Daten abgefragt von Diensten wie Facebook und WhatsApp und vielen anderen Socialmedia-Diensten mehr?

Datenschutz geht anders...

Dann WhatsApp verbieten? Kommunikation einschränken?

Modernes Leben geht anders...



Früher, ohne Datenschutz-Überlegungen, war alles mal so einfach: Kontakte eingeben am Computer oder Handy und automatisch synchron halten mit iCloud oder Google. Und schon sind die Daten auf allen eigenen digitalen Geräten verfügbar, aber leider nicht nur da... Die Service-Provider kennen die Daten auch und wer die Daten auf dem Handy haben und z.B. Für WhatsApp nutzen will, muss den Konzernen Zugriff auf die Kontaktdatenbank erlauben. Das entspricht aber nicht den Datenschutz-Anforderungen. Also muss man von allen Kontakten, mit denen man auch per WhatsApp kommunizieren will, ein (schriftliches) Einverständnis einholen (auf Papier).¹ Und dann ist einiges technisches Verständnis und Aufwand leider (wieder) nötig, um dem Datenschutz und den berechtigten Interessen der Kontakte gerecht zu werden, deren Daten gespeichert werden.

Alternative: Zurück zum Papier? Oder Speicherung nur auf dem Computer und auf Papier dabei für unterwegs? Aber wie sieht es dann mit dem Erkennen der Anrufer auf dem Handy aus? Geht nicht. Das muss auch mit Datenschutz anders gehen.

Der Verfasser ist weder Jurist noch IT-Fachmann, die nachfolgenden Überlegungen sind Ergebnis intensiver Recherchen im Internet und auf Tagungen wie der re:publica und Tests mit Geräten vor Ort sowie einem exemplarischen Setup, das in einem gesonderten Bericht beschrieben wurde².

¹ Dies schriftliche Einverständnis wird im weiteren Verlauf als gegeben vorausgesetzt

² „Anforderungen für die Digitale Kirche“ auf: www.neumedier.de/digitalekirche.php

1. Voraussetzungen

Um zeitgemäß zu arbeiten und zugleich Datenschutz-konform Adressen speichern zu können bedarf es einiger Voraussetzungen:

- Digitale Verwaltung der Kontaktdaten
- Mögliche Synchronisation der Kontaktdaten zwischen den verschiedenen Endgeräten
- Klare Trennung von Dienst und Privat
- Wahrung des Datenschutzes (vor allem auch Differenzierung der Kontaktdaten mit und ohne Hochladen zu WhatsApp & Co)
- Backup der Daten
- Verzicht auf außereuropäische Server

2. CardDAV-Server

Will man die Daten nicht nur auf einem Computer speichern sondern synchron halten auf allen Endgeräten, bedarf es eines Servers. Das geht mit Office365 oder einem Exchange-Server (aber Microsoft!) oder mit einem beliebigen anderen CardDAV-Server, der aber in Europa stehen muss. Es lassen sich auch eigene CardDAV-Server installieren.³

Ausführlich zu beschreiben, wie dies geht, würde hier aber zu weit führen. Ein Beispiel ist ausführlich beschrieben im schon vorher erwähnten Text.²

Gängige Adressprogramme für Computer können mit mehreren CardDAV-Servern zugleich synchronisieren. Komplizierter wird es auf Smartphones.

3. Problem Kontaktdaten-Synchronisation auf dem Smartphone

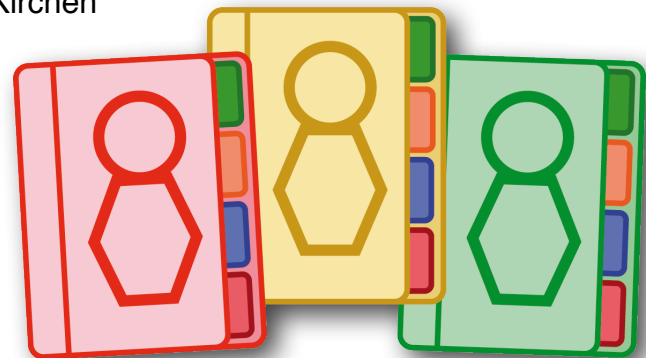
Die vorinstallierten Apps auf Android und iPhone können auch mit CardDAV synchronisieren. Auf Handys aber ergibt sich die Problematik des Abgleichs mit WhatsApp und anderen Diensten: Will man diese nutzen, verlangen sie die Einwilligung, die Kontaktdatenbank mit ihren Servern abzugleichen - und schon landen alle Kontaktdaten auf fremden (außereuropäischen) Servern.

Viele Firmen und auch die beiden großen deutschen Kirchen verbieten daher die Nutzung von WhatsApp und ähnlichen Diensten generell. Das aber ist einer zeitgemäßen Kommunikation abträglich und unrealistisch.

Zumal es anders geht:

Gesucht wurde eine App, die unabhängig der auf Android und iOS vorinstallierten Kontakte-Apps Daten von Kontakten speichert und darüber hinaus synchronisieren kann und bei der gleichzeitig

sichergestellt ist, dass die Kontaktdaten nicht (alle) zu WhatsApp und vergleichbaren Messengern wie auch Socialmedia-Diensten hochlädt. Das erklärte Ziel: Zwei (oder mehr) voneinander unabhängige Kontaktdatenbanken auf dem Smartphone zu haben, mit denen auch - wenn gewünscht - eine Synchronisation mit einem Server (und anderen Endgeräten) möglich ist. Im Android-Bereich hat der Verfasser leider noch keine App gefunden, die außerhalb der Android-Kontaktdatenbank und von ihr unabhängig speichert.⁴



³ Hier bieten sich einige Wege an, z.B.

Nextcloud (<https://nextcloud.com>) und ownCloud (<https://owncloud.org>), oder NAS-Systeme wie z.B.

Synology (<https://www.synology.com/de-de>) oder QNAP (<https://www.qnap.com/de-de/>).

Mehr dazu auch in „Anforderungen für die Digitale Kirche“ auf: www.neumедier.de/digitalekirche.php

⁴ Sachdienliche Hinweise werden gerne entgegengenommen.

4. Die Lösung für iOS: Die Apps „SecureContact Pro“

Die Lösung für iOS findet sich in der App „SecureContact Pro“, die die unter 1. genannten Voraussetzungen erfüllt.⁵ Sie liegt in zwei Versionen vor, sodass mit der iOS-eigenen Kontakte-App zusammen insgesamt drei von einander vollkommen unabhängige Kontaktdatenbanken mit dem iPhone synchronisiert werden können.

Die Einrichtung der Synchronisation mit CardDAV-Servern erfolgt problemlos, Anleitungen zur Hilfe mit verschiedenen Servern sind auf der Webseite der Entwickler zu finden.

In den Einstellungen der App findet sich unter „SecureConfiguration“ die Möglichkeit festzulegen, ob die App die in ihr gespeicherten Daten z.B. mit WhatsApp austauschen darf.

Besonders schön ist der Wahlschalter „Urlaubsmodus“, mit dessen Hilfe - wenn eingeschaltet - Anrufe von Nummern aus der entsprechenden Datenbank blockiert werden (festgelegte Favoriten werden nicht blockiert). Auch lässt sich die App mit einem gesonderten PIN-Schutz sichern.

Bei Anrufen werden die Namen der Anrufenden aus allen drei Kontakte Apps angezeigt. Einziger Nachteil ist, dass bei WhatsApp die Namen der Kontakte, die in den Apps SecureContact gespeichert sind, nicht angezeigt werden.

Folgende drei Datenbanken sind beispielsweise gesondert auf einem Handy einrichtbar:

Privathandy:

1. Private Kontakte: normale iOS-eigene Kontakte-App⁶
2. Dienstliche Kontakte mit schriftlicher Erlaubnis WhatsApp-Nutzung: SecureContact Pro⁷
3. Dienstliche Kontakte ohne WhatsApp-Synchronisation: SercureContact Pers⁸

Diensthandy:

1. Dienstliche Kontakte mit schriftlicher Erlaubnis WhatsApp-Nutzung: normale iOS-eigene Kontakte-App⁶
 2. Private Kontakte SecureContact Pro⁷
 3. Dienstliche Kontakte ohne WhatsApp-Synchronisation: SercureContact Pers⁸
- Für den gebotenen Leistungsumfang sind die aufgerufenen, jeweils pro App einmalig zu zahlenden, € 6,99 akzeptabel.



5. Fazit:

Es ist möglich, verschiedene Kontaktdaten-Gruppen DSGVO-konform in verschiedenen Datenbanken zu speichern und mit Computer und iPhone synchron zu halten. Ein generelles Verbot der dienstlichen WhatsApp-Nutzung ist daher nicht nötig und sollte aufgehoben werden. Die Datenschutzgesetze der beiden großen Kirchen (DSG-EKD und KDG) sind entsprechend zu überarbeiten.

⁵ Der Verfasser erhält keine Provisionen oder anderweitige Vergünstigungen von den Entwicklern der App, ist aber dankbar für den schnellen und guten Support derselben.

⁶ Anzeige des Namens der Kontakte bei Anrufen und in WhatsApp

⁷ Anzeige des Namens nur bei Anrufen, nicht bei WhatsApp

⁸ Anzeige des Namens bei Anrufen, WhatsApp-Upload blockiert