Adressverwaltung DSGVO- und DSG-EKD-konform

Ein neuerer, grundlegenderer Text zur Verwendung von WhatsApp in Kirche findet sich unter diesem Link: http://n16.me/dkn

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 Kontaktdaten 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!
Als Kirchen auf diesen von sehr vielen Menschen genutzten Kommunikationsweg mit WhatsApp verzichten? Zeitgemäße kirchliche Arbeit 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, eine (schriftliches) Einwilligung einholen (auf Papier).[1] Leider ist einiges technisches Verständnis und Aufwand (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 und Austausch im Internet und auf Tagungen wie der „re:publica“ oder dem „barcamp Kirche online“ und Tests mit Geräten vor Ort sowie einem exemplarischen Setup, das in einem gesonderten Bericht beschrieben wurde. [2]

---

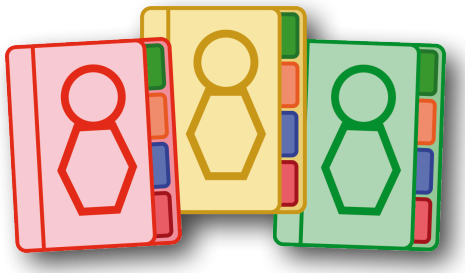
[1] Diese schriftliche Einwilligung (siehe letzte Seite) wird im weiteren Verlauf als gegeben vorausgesetzt. Link zur Vorlage: www.neumedier.de/Einwilligungsvorlage.doc

[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
- Schriftliche Einwilligung zum Speichern und ggf. Teilen (mit Messengern und Socialmedia-Diensten) der Kontaktdaten [3] (siehe letzte Seite)
- Mögliche Synchronisation der Kontaktdaten zwischen den verschiedenen Endgeräten
- Klare Trennung von Dienst und Privat
- Wahrung des Datenschutzes (vor allem Differenzierung der Kontaktdaten mit und ohne Hochladen zu WhatsApp etc.)
- Backup der Daten



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. [4] 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 wollen daher die Nutzung von WhatsApp und ähnlichen Diensten verbieten. Das aber ist einer zeitgemäßen Kommunikation abträglich und unrealistisch. Zumal es anders geht:

Gesucht wurden Apps, die nicht automatisch Daten von allen Kontakten zu WhatsApp und vergleichbaren Messengern wie auch Socialmedia-Diensten hochlädt. Das erklärte Ziel: Nur die Daten der Kontakte mit WhatsApp und CO teilen, die dem ausdrücklich zugestimmt haben. Andere Kontaktdaten vor Zugriff von Messengern schützen.

4. Die Lösung für Android

Hier bietet sich z,B, die App „WhatsBox“ [5,7] für € 5,99 an. WhatsApp läuft nach Installation von WhatsBox innerhalb dieser Container-App und teilt nur solche Kontakte mit WhatsApp, die ausdrücklich zum Teilen freigegeben wurden. Alle anderen Kontakte werden nicht mit WhatsApp geteilt.

Sicher gibt es weitere solcher Container-Apps.[6]

---

[3] Ggf mit Unterschrift der Eltern (Art. 8 DSGVO (bis 16 Jahre) und §12 DSG-EKD (vor Religionsmündigkeit))

[4] Hier bieten sich einige Wege an, z.B. Nextcloud (https://nextcloud.com), 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.neumedier.de/digitalekirche.php

[5] Dank an den Kollegen Marcus Kleinert (@marcus_kleinert) für den Hinweis auf diese App.

[6] Sachdienliche Hinweise nimmt der Verfasser immer gerne entgegen: mail@neumedier.de

5. Die Lösung für iPhone

Die Lösung für iOS findet sich in der App „SecureContact Pro“, die die unter 1. genannten Voraussetzungen erfüllt. [7] 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.

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:

1. Dienstliche Kontakte mit schriftlicher Erlaubnis WhatsApp-Nutzung: normale iOS-eigene Kontakte-App [6]
2. Private Kontakte SecureContact Pro [7]
3. Dienstliche Kontakte ohne WhatsApp-Synchronisation: SercureContact Pers [8]

So werden sowojhl dienstliche und private Kontakte von einander getrennt gespeichert als auch solche, die der Nutzung von WhatsApp zugestimmt haben. Für den gebotenen Leistungsumfang sind die aufgerufenen, jeweils pro App einmalig zu zahlenden, € 6,99 akzeptabel.

6. Fazit:

Es ist möglich, verschiedene Kontaktdaten DSGVO- und DSG-EKD-konform so zu speichern und mit Computer und iPhone synchron zu halten, dass nur die Kontaktdaten derjenigen Kontakte mit Messengern geteilt werden, die eine schriftliche Einwilligung unterschrieben haben. Die Kontaktdaten aller anderen, können datenschutzkonform ohne (automatischen) Upload gespeichert werden. Die DSGVO- und DSG-EKD-konforme Nutzung erfordert derzeit allerdings etwas Aufwand. Statt Verboten sollten Hilfsmöglichkeiten und Anleitungen zur Verfügung gestellt und verbreitet werden.

Jedes generelle Verbot von WhatsApp mit Bezug auf die DSGVO oder das DSG-EKD zeugt von Unkenntnis verfügbarer Möglichkeiten oder dem Unwillen, die in diesem Paper oder von anderen [8] an anderer Stelle vorgestellten Überlegungen zur Kenntnis zu nehmen oder nach anderen gangbaren Wegen zu suchen.

Ein generelles Verbot der dienstlichen WhatsApp-Nutzung ist nicht nötig und nicht angebracht.

Ein generelles Verbot der kirchlichen WhatsApp-Nutzung widerspricht dem kirchlichen Auftrag, dort zu den Menschen zu gehen, wo sie sind.

Ein generelles Verbot der dienstlichen WhatsApp-Nutzung sollte nicht gefordert bzw. umgehend aufgehoben werden.

Statt Verboten sollte Hilfe zur datenschutzkonformen Nutzung angeboten werden.

---

[7] Der Verfasser erhält keine Provisionen oder anderweitige Vergünstigungen von den Entwicklern der Apps, ist aber den Entwicklern von SecureContact dankbar für den schnellen und guten Support.

[8] Z.B. Ralf Peter Reimann (@ralpe) auf theonet.de: http://n16.me/theonet