IT-Recht
als Compliance-Aufgabe

Schlaglichter auf Helsana+ (was heisst Schriftlichkeit?) und WhatsApp (im Unternehmen einsetzbar?)

Perica Grasarevic

LAUX LAWYERS AG
ZURICH | BASEL

LAUX LAWYERS AG
ZURICH | BASEL

Teil 1: Schlaglichter auf Helsana+ (was heisst Schriftlichkeit?)

Ausgangslage: Helsana+ Urteil BVGer A-3548_2018 vom 19. März 2019

- Konzerninterne Datenbeschaffung (von [Trägerin] Grundversicherung auf [Trägerin] Privatversicherung
- Beschaffung durch Helsana Zusatzversicherungen AG („Helsana“) = Übermittlung durch Grundversicherung
- Bei der Trägerin der Grundversicherung / bei den Grundversicherten
- Für App-gestütztes Bonusprogramm „Helsana+“
- Versicherter erteilt Helsana über App Zustimmung zur Einholung von Daten = Rechtswidrig

Feststellungen BVGer A-3548_2019

- Übermittlung von Daten aus Grundversicherung (Tätigkeit nach KVG) an Zusatzversicherung (Tätigkeit als „Private“) ohne **gültige** Einwilligung unzulässig.
- Einwilligung zur Datenbekanntgabe an „Dritte“ kann **nur im Einzelfall** eingeholt werden (Sonderregel in Art. 84a Abs. 5 lit. a KVG)
- Schriftlichkeitserfordernis, wobei schriftlich = Art. 14 OR.
- Datenbearbeitung zu rechtwidrigem Zweck nur dann rechtswidrige Datenbearbeitung i.S. des DSG, wenn dabei Normverstoss, der den Schutz der Persönlichkeit einer Person bezweckt. (≠ EU, welche Erhebung nur für „legitime“ Zwecke vorsieht)

Datenbekanntgaberegeln für Bundesbehörden: DSG

DSG kennt besondere Regeln. Bekanntgabe ist für Bundesbehörden nach Art. 19 Abs. 2 lit. b DSG eingeschränkt.

Art. 19 Abs. 1 lit. b DSG lautet wie folgt:

> *Art. 19 Bekanntgabe von Personendaten*
>
> *1 Bundesorgane dürfen Personendaten nur bekannt geben, wenn dafür eine **Rechtsgrundlage** im Sinne von Artikel 17 besteht oder wenn:*
>
> *a. die Daten für den Empfänger im Einzelfall **zur Erfüllung seiner gesetzlichen Aufgabe unentbehrlich** sind;*
>
> *b. die betroffene Person **im Einzelfall eingewilligt** hat;*
>
> *c ...*
>
> *[Absätze 1bis – 4]..*

Datenbekanntgaberegeln für Bundesbehörden: KVG (ebenso: AHVG, UVG, AVIG)

Art. 84a KVG, Art. 50a AHVG, Art. 97 UVG und Art. 97a AVIG lauten alle in etwa so:

Datenbekanntgabe, Absatz 4:

> *4 In den übrigen Fällen dürfen Daten in Abweichung von Artikel 33 ATSG an Dritte wie folgt bekannt gegeben werden:*
>
> *a. nicht personenbezogene Daten, sofern die Bekanntgabe einem überwiegenden Interesse entspricht;*
>
> *b. Personendaten, sofern die betroffene Person **im Einzelfall schriftlich eingewilligt** hat oder, wenn das Einholen der Einwilligung nicht möglich ist, diese nach den Umständen als im Interesse des Versicherten vorausgesetzt werden darf.*

IVG ist der einzige sozialversicherungsrechtliche Erlass, welcher keine entsprechenden Bekanntgaberegeln enthält.

Datenbekanntgaberegeln für Bundesbehörden: BVG

Art. 86a Datenbekanntgabe, Absatz 5:

5 In den übrigen Fällen dürfen Daten an Dritte wie folgt bekannt gegeben werden:

a. nicht personenbezogene Daten, sofern die Bekanntgabe einem überwiegenden Interesse entspricht;

b. Personendaten, sofern die betroffene Person ***im Einzelfall schriftlich eingewilligt*** *hat oder, wenn das Einholen der Einwilligung nicht möglich ist, diese nach den Umständen als im Interesse des Versicherten vorausgesetzt werden darf.*

Bedeutung der Datenbekanntgaberegeln

- Auf den ersten Blick: Vergleich mit Art. 19 DSG legt eine „Verstärkung“ des Datenschutzes im Sozialversicherungsbereich nahe
- Es geht jedoch um strafbewehrte Geheimhaltungspflicht (Schweigepflicht nach Art. 33 ATSG und ähnliche Normen)
- Zwei Elemente zentral für eine gültige Zustimmung: **Einzelfall** und **Schriftlichkeit**

Zweck der „Einzelfall-Anforderung“

- Identifizierung aus den Materialien nicht möglich
- Mögliche Bedeutungen:
  - Behörde soll nach Ermessen entscheiden dürfen
  - Anlasszweck soll konkret definiert sein
  - Datenbearbeitung soll nicht „ausufern“
    (sprich Limitierung nach Umfang, Häufigkeit und Einsatzzweck)
- Herleitung legt **Limitierungsfunktion** nahe

Bedeutung der „Einzelfall-Anforderung“

Datenübermittlung soll nicht „ausarten“. Einsatzzweck, Umfang der Datenlieferung und Einsatzzweck sollen definiert sein:

- BVGer, E. 4.8.4: **mehrmals jährlich in einem automatisierten Prozess** [kein] Einzelfall
- 99.093 Botschaft über die Anpassung und Harmonisierung der gesetzlichen Grundlagen für die Bearbeitung von Personendaten in den Sozialversicherungen vom 24.11.1999, 265: «Ein Einzelfall **kann auch mehrere Personen betreffen** (z. B. wenn der Zweck der Anfrage darin besteht, zu prüfen, ob ein Arbeitgeber für alle Arbeitnehmer und Arbeitnehmerinnen des Unternehmens die Sozialversicherungsbeiträge tatsächlich bezahlt hat»
- Botschaft zum DSG 2003, zu Art. 17 II b: «**Gestützt auf die vorliegende Delegationsklausel kann somit nicht eine unbestimmte Anzahl von Fällen bewilligt werden.**»

Würdigung der „Einzelfall-Anforderung“

LAUX LAWYERS AG
ZURICH | BASEL

Würdigung:

- einmaliger Zweck
- in einer bestimmten Situation
- in einer einmaligen Situation

Jedoch:

- «einmalig» (immer noch) kein besonders klarer Begriff ...

Zweck der „Schriftformregel“

- Identifizierung aus den Materialien nicht möglich
- Herleitung legt **zwei mögliche Funktionen nahe:**
  - Schutz vor Überrumpelung / Übervorteilung (Beispiel: Einwilligung in Datenbearbeitung führt zu Bonus/Malus Versicherung, die um ein Vielfaches teurer sein kann als die ursprüngliche)
  - Beweisbarkeitsregel / Dokumentationsregel / Rechtsklarheit (siehe als Beispiel für eine Norm, die ebenfalls Dokumentationszweck verfolgt: Art. 165 Abs. 1 OR für das Zessionsrecht)

Bedeutung der „Schriftformregel“

- Schriftform stellt klar, ob Versicherungsträger ihre Geheimhaltungspflicht einhalten oder nicht:
  - Bei mündlicher Zustimmung könnte Nachweis kaum erbracht werden
  - Verschwiegenheit würde aus den Angeln gehoben
  - Schutz des öffentlichen Interesses an vertrauenswürdigen Versicherungsträgern

Umgang mit Schriftformerfordernis

- Verschiedene Gestaltungsformen zur Abwicklung des Schriftformerfordernisses möglich
- Nachfolgend Skizzierung, welche Formen der Anforderung «**Zustimmung schriftlich im Einzelfall**» genügen

Beispiel zum Umgang mit Schriftformerfordernis

- **Schriftform**: Deckblattvertrag ist kurz; Einwilligung steht im Deckblattvertrag; es sind Checkboxen vorgesehen; diese sind nicht vorab ausgewählt; Einwilligungserklärung ist nicht versteckt, sondern gut sichtbar und steht gerade überhalb der Unterschriftenzeile.
- **Einzelfall**: Die Einwilligungserklärung bezeichnet ganz konkret den Einzelfall, etwa wie folgt: "Wenn Sie 65 sind, werden wir die folgenden Daten (x y z) an unsere Schwestergesellschaft ABC weiterleiten, damit diese XYZ mit diesen Angaben machen kann."

Fazit

- Datenbekanntgaberegeln finden sich nicht nur im DSG und den kantonalen Datenschutzerlassen
- Compliance mit Einzelfall- und Schriftformerfordernis ist möglich, führt aber zu einem „Bruch“ der User-Journey eines App-Nutzers

LAUX LAWYERS AG
ZURICH | BASEL

Teil 2: WhatsApp (im Unternehmen einsetzbar?)

Einordnung von WhatsApp

- WhatsApp Inc. als US-Unternehmen mit Hauptsitz in Kalifornien
- WhatsApp Inc. als Tochterunternehmen von Facebook
- WhatsApp Inc. als Schwesterunternehmen von Instagram

- WhatsApp Applikation für Private via Mobiltelefon und als Webapp
- WhatsApp Business für KMUs via Mobiltelefon und als Webbapp
- WhatsApp Business API für grössere Unternehmen über Schnittstellen mit einer eigenen Lösung oder mit Drittlösungen

Relevante Eigenschaften von WhatsApp

- Datenübermittlung an und über **US-Server**
- WhatsApp Inc. ist Swiss-US und EU-US **Privacy Shield**-zertifiziert
- Nachrichten werden bis zur erfolgreichen Übermittlung an Empfänger **auf WhatsApp Server zwischengespeichert** (kein P2P, Speicherung bis zu 30 Tage)
- Kommunikation erfolgt auf Basis einer „**Ende-zu-Ende-Verschlüsselung**“
- WhatsApp hat **Kenntnis von Metadaten** (wer kommunizierte wann mit wem auf welche Weise), bearbeitet diese für **eigene Zwecke** und gibt sie **an Dritte weiter**
- WhatsApp liest standardmässig sämtliche **Kontaktdaten aus dem Adressbuch** aus, bearbeitet diese für eigene Zwecke und gibt sie an Dritte weiter

Nutzung von WhatsApp und WhatsApp Business im Unternehmen (1/2)

LAUX LAWYERS AG
ZURICH | BASEL

- Inhaltsdaten gelten als sicher = Verschlüsselung von WhatsApp funktioniert nach heutigem Verständnis
- Schwerpunkt der datenschutzrechtlichen Problemstellung deshalb auf Metadaten und Adressbuch:
  - Übermittlung der Kontakte aus dem Adressbuch an WhatsApp
  - Übermittlung von personenbezogenen Daten in die USA
  - Die Nutzung von personenbezogenen Daten durch WhatsApp
  - Die Übermittlung von personenbezogenen Daten an andere Unternehmen des Facebook-Konzerns

Nutzung von Whatsapp und Whatsapp Business im Unternehmen (2/2)

- Übermittlung der Kontakte aus dem Adressbuch:
  - Zugriff auf Adressbuch verweigern (man kann nur noch angeschrieben werden und reagieren) oder bei allen Kontakten Einwilligung einholen (unrealistisch)
- Übermittlung von Personendaten in die USA
  - Übermittlung dank Privacy Shield-Zertifizierung Übermittlung datenschutzrechtlich möglich
- Die Nutzung von Personendaten durch Whatsapp
  - Jeder Nutzer hat den Bedingungen von Whatsapp zugestimmt, ansonsten die Nutzung nicht möglich wäre. Sprich die Zustimmung umfasst auch die Gegenseite. Es braucht keine separate Einwilligung.
- Die Übermittlung von Personendaten an andere Unternehmen des Facebook-Konzerns
  - Jeder Nutzer hat den Bedingungen von Whatsapp zugestimmt, ansonsten die Nutzung nicht möglich wäre. Sprich die Zustimmung umfasst auch die Gegenseite. Es braucht keine separate Einwilligung.

Lösung: Trennung der Kontakte auf Geschäftsmobiltelefonen (mittels Android Enterprise mit unterschiedlichen Profilen) oder „Kontakttrennung“ bei iPhone

Nutzung der WhatsApp Business API im Unternehmen

- Schnittstellenanbindung mithilfe einer eigener oder Drittlösung
- Ermöglicht Kommunikation mit Kunden, Übermittlung von beliebigen Daten und Benachrichtigungen gegen Gebühr (pro Nutzung)
- WhatsApp hat keinen Zugriff auf Inhalt der Kommunikation oder Adressbuch, jedoch auf die Meta-Daten der Kommunikation
- WhatsApp schlägt rund 50 „zertifizierte“ Service-Provider als Partner für die Nutzung der WhatsApp Business API vor

Verschiebung der datenschutzrechtlichen Fragestellung

- Möchte man keine eigene Lösung entwickeln, muss man auf Service-Provider zurückgreifen
- Kommunikation wird vom Service-Providern bearbeitet und an WhatsApp-Server übermittelt
- Service-Provider handelt als Auftragsdatenbearbeiter
- Service-Provider kann Klartext-Zugriff auf Kommunikation haben
- Service-Provider hat mit Sicherheit Klartextzugriff auf Metadaten

Inanspruchnahme von Service-Providern bei Nutzung der WhatsApp Business API

- Bei Bearbeitung von Personendaten: Art. 10a DSG beachten, Auftragsdatenbearbeitungsvertrag, keine Einwilligung der Kunden nötig
- Bei Bearbeitung von besonders schützenswerten Personendaten: Ausdrückliche Einwilligung der Kunden nötig und Anforderungen an Risikomanagement und Sicherheitsmassnahmen höher
- Bei Bearbeitung von Daten, deren unrechtmässige Übermittlung oder Offenbarung unter Strafe steht (BankG, Sozialversicherungsgesetze etc.): Einbindung des Service-Providers in die eigene Geheimsphäre, Erweiterung des eigenen Perimeters, Umsetzung der erforderlichen technischen, organisatorischen und vertraglichen Massnahmen.

Fazit

- Der professionelle Einsatz der „klassischen“ WhatsApp-Lösung und von WhatsApp Business im Unternehmen ist aus datenschutzrechtlichen Gründen nicht empfehlenswert
- Die private Nutzung der „klassischen“ WhatsApp-Lösung auf Dienstgeräten ist aus Unternehmenssicht möglich
- Die professionelle Einsatz der WhatsApp Business API ist möglich, solange (insbesondere im Umgang mit Service-Providern) die erforderlichen Massnahmen getroffen werden

Kontakt

Perica Grasarevic
Rechtsanwalt
perica.grasarevic@lauxlawyers.ch

LAUX LAWYERS AG
http://www.lauxlawyers.ch

Seegartenstrasse 2
Postfach
CH – 8024 Zurich
+41 44 880 24 24