

## **Beschluss der Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschland**

*(Sitzung vom 15.09.2021)*

### ***Beurteilung von Messenger- und anderen Social Media-Diensten***

Die Konferenz der Diözesandatenschutzbeauftragten beschließt, die Kriterienliste aus dem Beschluss vom 26. Juli 2018 wie folgt zu aktualisieren:

## **Kriterien zur Beurteilung von Messenger- und anderen Social Media-Diensten**

### **Vorbemerkung**

Die katholischen Datenschutzaufsichten haben nachfolgend die aus ihrer Sicht relevanten Kriterien für die Bewertung und die Auswahl eines geeigneten Messenger-Produktes unter Datenschutz-Gesichtspunkten zusammengestellt. Neben diesen können aber auch andere Kriterien eine Rolle spielen, deren Erfüllung für die legale Verbreitung im kirchlichen Raum förderlich ist.

### **Kriterien, die ein Dienst aus Sicht des Datenschutzes erfüllen muss**

**Serverstandort:** Wo verarbeitet der Dienst-Anbieter die Nutzerdaten? Hält der Provider die Drittlandbestimmungen ein, d.h. keine Datenspeicherung außerhalb der EU bzw. nur in Ländern, deren Datenschutzniveau durch die EU anerkannt ist?

Aus §§ 39-41 KDG ergibt sich, dass eine Verarbeitung personenbezogener Daten nur dann in einem Drittland, also außerhalb der EU, stattfinden darf, wenn besondere Bedingungen erfüllt sind. Das können ein Angemessenheitsbeschluss der Europäischen Kommission, geeignete Garantien (§ 40 KDG) oder eine explizite Einwilligung der betroffenen Person (§ 41 Abs. 1 KDG) sein.

Der Verantwortliche muss sich also überzeugen, dass die Rechtmäßigkeit der Verarbeitung durch Vorliegen mindestens einer dieser Bedingungen gegeben ist.

Die Überprüfung der Rechtmäßigkeit der Verarbeitung in einem Drittland führt dabei in jedem Fall zu einem deutlich größeren Aufwand bei der Einrichtung des Verfahrens im Vergleich zu einem Betrieb in einem EU-Mitgliedsland. Schon aus diesem Grund sowie

wegen des permanenten Risikos, dass die Rechtmäßigkeit durch Änderung z.B. der Gesetzeslage im Drittland oder Änderung der Anerkennungssituation entfällt, raten wir grundsätzlich von der dauerhaften Verarbeitung in einem Drittland ab, selbst wenn formal die Rechtmäßigkeit der Verarbeitung zum aktuellen Zeitpunkt gegeben wäre.

- **Sicherer Datentransport:** Werden die Inhalte der Kommunikation Ende-zu-Ende verschlüsselt, also z.B. auch bei der Zwischenpufferung auf dem Server des Providers?

Nach § 26 KDG hat der Verarbeiter geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko für die Rechte und Freiheiten der Betroffenen angemessenes Schutzniveau zu gewährleisten. Als geeignete Maßnahme wird unter anderem die Verschlüsselung personenbezogener Daten ausdrücklich genannt. Auch in § 6 Abs. 1 lit. b KDG-DVO wird Verschlüsselung als geeignete Maßnahme zum Schutz personenbezogener Daten bei deren Übertragung aufgeführt und in § 12 Abs. 2 lit e KDG-DVO für Daten der DSK II explizit gefordert. § 27 KDG fordert überdies, die Sicherheitsoptionen so zu gestalten, dass bereits durch die Voreinstellung das angemessene Schutzniveau gewahrt wird. Verschlüsselung darf deshalb nicht „optional zuschaltbar“ sein, sondern sollte per Default vorgegeben werden. Die Sicherheit der Daten sollte auch nicht nur auf dem Transport, also auf dem Weg vom Endgerät des Senders über den zentralen Server bis zum Endgerät des Empfängers gewährleistet werden, sondern auch, wenn die Daten auf dem Endgerät angekommen sind, durch eine sichere Datenhaltung in der Applikation, die die Daten z.B. gegen ungewolltes Ausspähen durch andere Applikationen auf dem gleichen Endgerät schützt. Dem aktuellen Stand der Technik (im Jahr 2020 ) entsprechen Transport- und Inhaltsverschlüsselungen nach den Standards TLS mindestens in der Version 1.2 idealerweise mit Perfect Forward Secrecy<sup>1</sup> oder AES 128 und größer, idealerweise mit der Betriebsart GCM bzw. bei der Verwendung von EC-Verfahren eine Schlüssellänge von mindestens 250 Bit<sup>2</sup>.

Falls vorhanden, sollten Zertifizierungen des Produktes oder des Anbieters durch unabhängige Institutionen in die Bewertung einfließen.

- **Datenminimierung:** Werden höchstens Metadaten der Verbindung über das Verbindungsende hinaus gespeichert und auch diese so bald wie möglich gelöscht?

Eine Beschränkung auf das für den Zweck der Verarbeitung notwendige Maß an personenbezogenen Daten wird in § 7 Abs.1 lit c) KDG gefordert. Die Beschränkung gilt für die Menge und den Zeitraum der Verarbeitung und Speicherung. Deshalb ist zu fordern, dass alle personenbezogenen Daten, also Inhalte und Verbindungsdaten der Kommunikation, sobald wie möglich gelöscht werden. Eine Speicherung von Inhalten der Kommunikation auf dem zentralen Server ist - genau wie ein Mitlesen durch den Serviceprovider - nicht akzeptabel.

Eine extreme Datenminimierung zusammen mit einer starken Ende-zu-Ende-Verschlüsselung führt dazu, dass der Provider selbst unter Zwang (z.B. durch staatliche

---

<sup>1</sup> Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie TR-02102-2 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 2 – Verwendung von Transport Layer Security (TLS), Version: 2021-01, Seite 7 ff, Kapitel 3.3

<sup>2</sup> Bundesamt für Sicherheit in der Informationstechnik, BSI – Technische Richtlinie, Kryptographische Verfahren: Empfehlungen und Schlüssellängen (BSI TR-02102-1), Version: 2021-01, Seite 28, Tabelle 3.1

Behörden) technisch nicht in der Lage ist, Daten herauszugeben. Ebenso laufen illegale Angriffe auf die zentralen Server ins Leere.

- **Respektierung der Rechte Dritter:** Werden nur die Kontaktdaten der an der Kommunikation Beteiligten verwendet und behält der Anwender die Kontrolle über die auf seinem Gerät hinterlegten personenbezogenen Daten Dritter, wird also z.B. das komplette Telefonbuch an den Provider übermittelt und die Verantwortung für die Information der Betroffenen auf den Anwender abgewälzt?

Personenbezogene Daten müssen rechtmäßig und für den Betroffenen in nachvollziehbarer Weise verarbeitet werden. (§ 7 Abs. 1 KDG). Der Betroffene hat nach den §§ 14 und 15 KDG umfassende Rechte auf Information über den Umfang und die Art der Verarbeitung seiner Daten. Dagegen verstößt regelmäßig die Ausspähung von Adressen und Kontaktdaten des Telefonbuches durch allzu neugierige Applikationen. Manche Anbieter versuchen über die AGB, die Verantwortung für die Einholung einer Einwilligung der Dritten in die Weitergabe ihrer Daten dem Nutzer aufzubürden, was dieser in der Praxis aber nie leisten kann.

## Weitere Kriterien

Zu dem erweiterten Kriterienkreis gehören zum einen die Kosten: Der Entscheider sollte prüfen, ob die Nutzung des Produktes idealerweise für den privaten Nutzer kostenfrei und für die nicht-private Nutzung, also z.B. durch eine kirchliche Einrichtung, relativ erschwinglich ist.

Bei einer Beurteilung einer Messenger-Lösung ist ferner die Verfügbarkeit des Quellcodes (Open Source) zu berücksichtigen und ggf. positiv zu bewerten. Der Quellcode erlaubt es unabhängigen Experten, einerseits die Korrektheit von Herstellerangaben zu verifizieren und eröffnet diesen andererseits die Möglichkeit, Schwachstellen im Programmcode zu identifizieren.

Darüber hinaus sind die Bedingungen der Lizenzvergabe zu prüfen, die meistens in den AGB geregelt werden. Manche Anbieter untersagen die nicht-private Nutzung, andere untersagen lediglich die kommerzielle Anwendung. Während das Produkt im ersten Fall auch durch ehrenamtliche Non-Profit-Organisationen nicht genutzt werden darf, können diese im zweiten Fall – abhängig von den Formulierungen der AGB – doch von einer bestimmungsgemäßen Nutzung ausgehen. Nicht-privaten Nutzern wird manchmal eine spezielle „Business-Lösung“ angeboten, die aber oft mit höheren Lizenzkosten verbunden ist als die Privat-Anwendung. Einige Anbieter fordern ein Mindestalter der Nutzer von 16 oder sogar 18 Jahren, andere Anbieter stellen ihr Produkt nur für Nutzer mit Wohnsitz in bestimmten Staaten zur Verfügung.

Jeder Entscheider muss sich also ausführlich und umfassend über die Lizenzbedingungen der Produkte informieren.

15.09.2021