Baden-Württemberg
DER LANDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ UND DIE INFORMATIONSFREIHEIT

LfDI Baden-Württemberg · Postfach 10 29 32 · 70025 Stuttgart

Datum 4. März 2020
Name [redacted]
Durchwahl 0711/615541[redacted]
Aktenzeichen P 6200/282
(Bitte bei Antwort angeben)

Per E-Mail:

Ministerium für Kultus, Jugend und Sport
Baden-Württemberg
[redacted]

poststelle@km.kv.bwl.de

nachrichtlich:

[redacted]

Verzeichnis der Verarbeitungstätigkeiten und Vereinbarung zur Auftragsdatenverarbeitung zu Threema
Unsere Besprechung vom 04.12.2019 und E-Mail von [redacted] vom 04.12.2019

Sehr [redacted]

vielen Dank für die Zusendung des Verzeichnisses der Verarbeitungstätigkeiten und der Vereinbarung zur Auftragsdatenverarbeitung im Auftrag zu Threema. Wie zwischen Herrn Föll und Herrn Dr. Brink besprochen, beraten wir Sie gerne schon im Vorfeld bei den datenschutzrechtlichen Aspekten der verschiedenen Komponenten der digitalen Bildungsplattform. In diesem Zusammenhang haben wir im Folgenden einige Fragen bzw. Anregungen zu den beiden genannten Dokumenten.

Verzeichnis der Verarbeitungstätigkeiten

zu A Hauptblatt

Als Verantwortlicher wird die Threema GmbH, Pfäffikon angegeben. Sollte dies tatsächlich der Fall sein, würden personenbezogene Daten bei der Verwendung der App von der Schule an Threema übermittelt. Hierzu ist eine Rechtsgrundlage erforderlich.

In den Einzelblättern B bis E wird unter „Rechtmäßigkeit der Verarbeitung" „Einwilligung" als Rechtsgrundlage genannt. Wir möchten hierzu auf Erwägungsgrund 43 der Datenschutzgrundverordnung (DS-GVO, abrufbar unter https://www.baden-wuerttemberg.datenschutz.de/ds-gvo/) hinweisen, da nur dann davon ausgegangen werden kann, dass eine Einwilligung freiwillig gegeben wurde, wenn eine echte und freie Wahl möglich ist. In Fällen, wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht, insbesondere wenn es sich bei dem Verantwortlichen um eine Behörde handelt, kann eine Einwilligung keine gültige Rechtsgrundlage liefern. So muss hier ein alternativer Informationsweg für die betroffenen Personen möglich sein, d.h. es darf auch keine indirekte Verpflichtung zur Verwendung des Messengers bestehen, damit Personen nicht benachteiligt werden, wenn sie nicht einwilligen.

Unabhängig hiervon widerspricht die Angabe des Verantwortlichen im Verzeichnis der Verarbeitungstätigkeiten (Verantwortlicher: Threema GmbH, Pfäffikon) der Vereinbarung zur Auftragsverarbeitung, da hier das Kultusministerium als Verantwortlicher und die Threema GmbH, Pfäffikon als Auftragnehmer genannt sind.

Die Frage der datenschutzrechtlichen Verantwortlichkeit muss geklärt werden (Threema GmbH, Kultusministerium oder Schule bzw. gemeinsame Verantwortung nach Artikel 26 DS-GVO, gegebenenfalls inwieweit).

Das Beiblatt zu den technisch-organisatorischen Maßnahmen lag leider nicht bei.

zu B Einzelblatt (Nutzerverwaltung und App-Konfiguration)

1. Unter „Rechtmäßigkeit der Verarbeitung" wird als Rechtsgrundlage eine Einwilligung genannt (diese ist in Artikel 6 Absatz 1 Buchstabe a DS-GVO geregelt). Allerdings wird in der linken Spalte die Erfüllung eines Vertrages als Rechtsgrundlage („*Art. 6 Abs. 1 lib b*") angegeben. Dies widerspricht sich.
2. Unter „Kategorien betroffener Personen" wird ein Administrator erwähnt. An welcher Stelle ist dieser angesiedelt (Kultusministerium oder an den einzelnen Schulen)?
3. Wer ist „externer Nutzer" bzw. wer ist nutzungsberechtigt?

4. Unter „Kategorien personenbezogener Daten“ werden individuelle Zugangsdaten erwähnt. Wie erhält ein Nutzer diese Daten?
5. Warum ist ein Zeitstempel der letzten App-Aktivität erforderlich?
6. Wessen Kreditkartendaten werden hier wozu verwendet?
7. Welche der hier optional angegebenen Kategorien personenbezogener Daten werden in welcher Form tatsächlich verwendet?
8. Threema ist zumindest als Auftragsverarbeiter Empfänger der Daten (vgl. Artikel 4 Nummer 9 DS-GVO). Da der Sitz und die Datenverarbeitung von Threema in der Schweiz liegen, befindet sich der Empfänger nach der DS-GVO in einem Drittland. Die Datenübermittlung ist jedoch nicht zu beanstanden, da es für die Schweiz einen Angemessenheitsbeschluss gibt. Dies sollte jedoch hier entsprechend vermerkt werden.
9. Welche „verschiedenen“ „Fristen für die Löschung verschiedener Datenkategorien“ sind hier gemeint?

<u>zu C Einzelblatt (Übertragung von Kurznachrichten und Medien)</u>

1. Unter „Kategorien personenbezogener Daten“ wird erwähnt: „wenn dies der Kunde explizit so einstellt und wünscht“. Welche Wahl hat hier das Kultusministerium als Kunde getroffen?
2. Warum und auf welcher Rechtsgrundlage benötigt die Geschäftsleitung der Threema GmbH die [redacted] und/oder [redacted] oder die [redacted]?
3. Es wird erwähnt, dass Daten nur „einwegverschlüsselt“ verarbeitet werden. Wir vermuten hier einen sog. Hash. Wir weisen darauf hin, dass auch ein Hash von personenbezogenen Daten weiterhin als personenbezogenes Datum anzusehen ist (vgl. VGH München, Beschluss vom 26.09.2018 – 5 CS 18.1157). Dies muss bei der Bewertung der Risiken berücksichtigt werden.

<u>zu D Einzelblatt (Verarbeitung und Speicherung eingehender und ausgehender Nachrichten, zentrale Gruppen- und Empfängerverwaltung)</u>

1. Unter „Kategorien personenbezogener Daten“ werden optionale Kategorien erwähnt. Welche werden hier wie verwendet?
2. Wessen Kreditkartendaten werden hier wozu verwendet?
3. Werden Chatverläufe auf dem Server gespeichert?

zu E Einzelblatt (Threema Gateway Messaging API)

1. Wird der Nachrichteninhalt als Klartext („Basic-Option") oder unter Ende-zu-Ende-Verschlüsselung (End-to-End Option") weitergeleitet?
2. Unter „Kategorien personenbezogener Daten" werden optionale Kategorien erwähnt. Welche werden hier wie verwendet?
3. Wessen Kreditkartendaten werden hier wozu verwendet?

Vereinbarung zur Auftragsverarbeitung

Wie unter Verzeichnis der Verarbeitungstätigkeiten, A Hauptblatt bereits angesprochen muss geklärt werden, wer verantwortliche Stelle ist.

zu 3. Art und Umfang der verarbeitenden Daten

Ausgehend davon, dass keine besonderen Datenkategorien im Sinne von Artikel 9 Absatz 1 oder Artikel 10 DS-GVO verarbeitet werden dürfen, möchten wir Sie darauf hinweisen, dass dann u.a. keine Gesundheitsdaten (z.B. Krankmeldungen), Gewerkschaftsdaten (Mitgliedschaft einer Lehrkraft in der Gewerkschaft) oder religiöse Überzeugungen (z.B. Entschuldigungen wegen religiöser Feste) per Threema übermittelt werden dürfen. Evtl. ist bereits die Tatsache, dass ein SBBZ besucht oder beratend tätig ist, ein Gesundheitsdatum.
Sollte die Übermittlung von solchen Daten untersagt sein, sind die Nutzer durch geeignete Maßnahmen darüber zu informieren. Wir halten es für sehr unwahrscheinlich, dass Nutzer auf die Übermittlung solcher Daten verzichten. Deswegen sollte dieser Punkt überarbeitet und, sofern nötig, die technisch-organisatorischen Maßnahmen angepasst werden.

Der gesamte Abschnitt 3 enthält keine Angaben zu IP-Adressen und wie damit umgegangen wird, obwohl es sich bei IP-Adressen um personenbezogene Daten handelt (vgl. Urteil des Europäischen Gerichtshofs in der Rechtssache C-582/14 vom 19. Oktober 2016, berichtigt durch Beschluss vom 6. Dezember 2016). Daher ist nicht geklärt, wie Threema mit diesen umgeht und sie verarbeitet.

A) Bestandsdaten

1. Es ist uns nicht ersichtlich, warum die Threema-ID und ein lokal generierter öffentlicher Schlüssel keine personenbezogenen Daten darstellen sollen. Über beide Daten kann eindeutig auf ein Endgerät und dessen Besitzer geschlossen werden. Abweichend von der Angabe hier, wird die Threema-ID im Verzeichnis von Verarbeitungstätigkeiten als personenbezogenes Datum beschrieben, der Schlüssel nicht erwähnt.

2. Welche optional durch den Verantwortlichen oder dessen Nutzer erfassten personenbezogenen Daten sind real vorgesehen?
3. Was ist unter „Vorbelegte Einträge auf der Kontaktliste" zu verstehen?
4. Wie oben unter C Einzelblatt beschrieben, weisen wir darauf hin, dass gehashte Daten weiterhin personenbezogene Daten sind.

B) Nachrichteninhalte

Die Angabe, es werde ein „hochsicheres" Verfahren zur Ende-zu-Ende-Verschlüsselung genutzt, ist nicht ausreichend (siehe auch *„zu 5. Technische und organisatorische Maßnahmen"* unten).

zu 4. Dauer der Datenspeicherung

Welche Daten fallen unter „Auftragsdaten" und werden erst nach zehn Jahren gelöscht?

zu 5. Technische und organisatorische Maßnahmen

Es fehlen Angaben zu Verschlüsselungsalgorithmen, Schlüssel-Längen sowie verwendeten Cipher-Suiten.

zu 6. Rechte und Pflichten des Auftragnehmers

In Punkt 6.7 wird ein Zutrittsrecht für den Auftraggeber zu den Räumlichkeiten des Auftragnehmers vorgesehen. Ohne ein Recht auf Prüfung (v.a. technische Prüfung und Einsicht in Unterlagen, Quellcodes und Konfigurationen) ist dies nur beschränkt hilfreich. Es ist zu klären und zu spezifizieren, welche weiteren Rechte als das Betreten der Räumlichkeiten der Auftraggeber hat.

zu 7. Rechte und Pflichten des Verantwortlichen

zu 1.

Es ist zu klären, wer Verantwortlicher ist (siehe oben).

zu 3.

1. Wie werden die Sicherheit und der Datenschutz auf den (privaten) Endgeräten sichergestellt?
2. Warum wird hier explizit in Bezug auf die Endgeräte und den Transportweg „Verschlüsselung" erwähnt? Liefert die App eine Verschlüsselung sowohl auf dem Endgerät als auch auf dem Transportweg?
3. Welche Sicherheitsmaßnahmen bietet die App zur Sicherheit der Daten auf den Endgeräten?

zu 12. Schlussbestimmungen

1. Wie weit gilt die Europäische Datenschutzgrundverordnung, wenn Schweizer Recht gilt?

Abhängig von den Antworten auf obige Fragen, können sich evtl. weitere ergeben.

Gerne können Sie sich bei Fragen zu diesem Schreiben oder zu datenschutzrechtlichen Sachverhalten der digitalen Bildungsplattform an uns wenden. Wir beraten Sie hierzu gerne.

Mit freundlichen Grüßen

[redacted]