ALTHAMMER & KILL

Datenschutz-Seminar

Selbstständiges Wohnen gGmbH

06.10.2020

ALTHAMMER & KILL

Ihr Referent

Andreas Hellmann

Berater für Datenschutz und Informationssicherheit

ALTHAMMER & KILL

1. **Unzulässigkeit Privacy Shield – Datentransfer USA**
2. **WhatsApp**
3. **Bring your own device**
4. **Externe Dienstleister – Auftragsverarbeitung**
5. **Sprachassistenten**
6. **Störerhaftung**
7. **App Entwicklung**
8. **Fragerunde/Spezialthemen**
9. **Unterstützung durch Althammer & Kill**

Unzulässigkeit Privacy Shield – Datentransfer USA

ALTHAMMER & KILL

Worum geht es?

Der Europäische Gerichtshof (EuGH) hat mit seinem Urteil vom 16.07.2020 (Schrems II) das EU-US Privacy Shield gekippt. Das EU-US Privacy Shield ist eine informelle Absprache auf dem Gebiet des Datenschutzrechts, welche zwischen der Europäischen Union (EU) und den Vereinigten Staaten von Amerika (USA) ausgehandelt wurde. Diese Absprache regelt den Schutz personenbezogener Daten, die aus einem Mitgliedsstaat der EU in die USA übermittelt werden (Datenexport). Es ist nicht das erste Instrument dieser Art, welches von der europäischen Rechtsprechung für nichtig erklärt wurde – bereits 2015 hat der EuGH den Vorgänger des EU-US-Privacy Shield – den Safe-Harbor-Beschluss – für ungültig erklärt.

ALTHAMMER & KILL

Welche Auswirkung hat die Entscheidung?

Die Übermittlung von personenbezogenen Daten in ein Drittland oder eine internationale Organisation ist nur zulässig, wenn die Grundsätze der Art. 44 ff DSGVO eingehalten werden. Neben dem Abschluss von **Standardvertragsklauseln** galt bisher unter anderem der EU-US Privacy Shield als geeignete Rechtsgrundlage – dies ist mit dem EuGH-Urteil nun Geschichte. Unternehmen und Organisationen sind daher angehalten, ihre **Datenverarbeitung zu überprüfen**. Übermittlungen in die USA, die auf Grundlage des EU-US Privacy Shield durchgeführt werden, sind somit nicht mehr rechtmäßig.

Aktuelle Infos zum Thema:
https://www.althammer-kill.de/news/

https://www.heise.de/news/Microsoft-Office-365-Die-Gruende-fuer-das-Nein-der-Datenschuetzer-4919847.html

WhatsApp

ALTHAMMER & KILL

Worum geht es?

Fraglich ist, ob für die **Übermittlung der Telefonnummern an WhatsApp** eine Rechtsgrundlage vorliegt. Bei der Ermittlung der Rechtsgrundlage lässt sich zwischen den bereits bestehenden WhatsApp-Nutzern und Personen unterscheiden, die WhatsApp nicht nutzen. Die bestehenden Nutzer haben ihre Telefonnummer im Rahmen der Registrierung selbst an WhatsApp übertragen. Zudem ist problematisch, dass WhatsApp keine Möglichkeit vorsieht, den automatischen Upload des Adressbuches zu verhindern oder einzelne Kontakte manuell freizugeben.

WhatsApp versucht insofern durch seine Nutzungsbedingungen die Verantwortung für die rechtmäßige Verarbeitung auf den Endanwender abzuwälzen. Dem Nutzer liegen aber in der Regel keine Einwilligungen seiner Kontakte in die Datenübermittlung an WhatsApp vor.

ALTHAMMER & KILL

Handlungsempfehlung und Hinweis

Prüfen Sie kritisch, ob der Einsatz von WhatsApp im Unternehmen nicht durch andere datenschutzfreundlichere Lösungen ersetzt werden kann. Ist dies nicht der Fall, so sollten Vorkehrungen für den sicheren Einsatz getroffen werden.

Weitere problematische Themen in Bezug zu WhatsApp sind z. B. (1) dass die Ende-zu-Ende-Verschlüsselung aufgrund der amerikanischen Überwachungspraxis unglaubwürdig ist, (2) der fragwürdige Versuch der Verkettung von Benutzerkonten von WhatsApp mit Facebook, oder (3) die Einführung eines angemessenen Mindestalters (aktuell 13 Jahre – siehe WhatsApp AGB) für die Nutzung des Dienstes (mit Bedeutung für Kinder- und Jugendhilfe). Durch die DSGVO liegt das Mindestalter bei 16 Jahren, sofern es sich um eine geschäftliche Nutzung/Verarbeitung handelt.

Info zum WhatsApp Urteil (Privatbereich):
https://www.lareda.hessenrecht.hessen.de/bshe/document/LARE190000030

Bring your own device (BYOD)

ALTHAMMER & KILL

Ausgangslage

Beim Thema „bring your own device“ (BYOD) geht es darum, dass – personenbezogene – Daten aus dem Verantwortungsbereich eines Unternehmen auf privaten Endgeräten der Mitarbeitenden verarbeitet werden.

Gemäß Art. 5 DSGVO ist der Verantwortliche verpflichtet, die Sicherheit der Daten zu gewährleisten und dies nachweisen zu können.

Die Schwierigkeit dabei ist, auf einem Endgerät, über welches der Verantwortliche keine Entscheidungsgewalt hat, die Kontrolle über die Daten zu behalten, die Sicherheit der Daten überprüfen zu können und die Daten gegenüber dem privaten Bereich des Mitarbeitenden klar abzugrenzen.

ALTHAMMER & KILL

Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Da es für den Verantwortlichen nicht möglich ist, die Sicherheit der Daten auf dem privaten Gerät ausschließlich durch organisatorische Maßnahmen zu gewährleisten, liegt es nah, dass eine technische Maßnahme erforderlich ist. Eine praktikable Lösung ist der Einsatz eines Mobile Device Management Systems (MDM).

Bei der Konfiguration müssen viele Dinge beachtet werden, die sich aus der speziellen Situation ergeben. Hierzu gehören unter anderem die Nutzung der Geräte durch Familienmitglieder, eine Zugriffsbeschränkung für andere Anwendungen auf dem Gerät, Unterdrücken von Cloud-basierten Sprachassistenten in Geschäftsanwendungen, webbasierter Zugriff über separate Browser, etc.

Wenn möglich sollte eine Speicherung der Daten auf den Endgeräten vermieden werden!

ALTHAMMER & KILL

Kurzinfo zu weiteren gesetzlichen Auflagen

- Haftung bei mangelhafter Konfiguration
  Hiervon können die Daten des Unternehmens betroffen sein (Schadsoftware), aber auch private Daten des Mitarbeitenden (versehentliche vollständige Fernlöschung).
- Gewährleisten der gesetzlichen Aufbewahrungspflichten.
- Steuerrecht
  Abgrenzung betrieblicher und privater Kosten (Stichwort: geldwerter Vorteil).
- Arbeitsrecht
  Arbeitszeiten, ständige Erreichbarkeit, Überwachung im privaten Bereich
- Betriebsrat
  Betriebsvereinbarungen

Weitere Infos zum Thema:
https://www.youtube.com/watch?v=as0zwSMVkNk

ALTHAMMER & KILL

Links

- BSI IT-Grundschutz – Umsetzungshinweise zum Baustein Mobile Device Management (MDM)
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/umsetzungshinweise/SYS/Umsetzungshinweise_zum_Baustein_SYS_3_2_2_Mobile_Device_Management_(MDM).html

- BSI Hilfsmittel
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Extern/Diplomarbeiten/Berrendorf_BYOD.pdf?__blob=publicationFile&v=2

- Bitkom Leitfaden
  https://www.bitkom.org/sites/default/files/file/import/130304-LF-BYOD.pdf

Externe Dienstleister – Auftragsverarbeitung

ALTHAMMER & KILL

Grundlagen

Als erstes muss festgestellt werden, ob es sich überhaupt um eine Auftragsverarbeitung handelt, oder ob „nur“ eine Übermittlung oder eine „Funktionsübertragung“ vorliegt.

Übermittlung: Die Daten werden – meistens in nur eine Richtung – an einen anderen Verantwortlichen übermittelt, damit dieser die Daten für seine – z. B. gesetzlich vorgeschriebenen - Zwecke verarbeiten kann.
Beispiel: Finanzamt, Krankenkassen, Microsoft, Amazon, Google

Funktionsübertragung (selten): Die Daten werden zwar „im Auftrag“ aber von der anderen Verantwortlichen Stelle komplett selbstständig erhoben und verarbeitet.
Beispiel: Hausverwaltung, Hotel, Reisebüro

Auftragsverarbeitung: Die Daten werden zur weiteren Verarbeitung und - ggf. Rücklieferung eines überarbeiteten Ergebnis – an einen Auftragsverarbeiter geschickt oder dieser kann auf die Daten zugreifen (z. B. Fernwartung).
Beispiel: IT-Dienstleister, Rechenzentrum

ALTHAMMER & KILL

Hilfe zur Beurteilung

Eine Auftragsverarbeitung liegt vor, wenn der Auftragsverarbeiter die personenbezogenen Daten **weisungsgebunden** verarbeitet z. B. Service für IT, Telefonanlage, Kopierer, Webseiten, Datenträgervernichtung, Rechenzentrum.
Das bedeutet, dass der Verantwortliche z. B. bestimmen kann, wie die Daten verarbeitet werden, welche Daten verarbeitet werden und was nach dem Auftragsende mit den Daten zu tun ist.

Hinweis: Dies gilt auch, wenn bei der Dienstleistung ein Zugriff auf personenbezogene Daten (Lesen bei einer Fernwartung) nicht ausgeschlossen werden kann. Es muss also im IT-Sinn keine Verarbeitung stattfinden, aber im Datenschutz-Sinn (Art. 4 Abs. 2 DSGVO) ist dies eine Verarbeitung z. B. Speichern im Rechenzentrum.

ALTHAMMER & KILL

Hilfe zur Beurteilung

In folgenden Fällen liegt **keine Auftragsverarbeitung** vor:

- wenn der Dienstleister einer Berufsgeheimnispflicht nach § 203 StGB unterliegt
  z. B. Anwälte, Ärzte, Steuerberater (Ausnahme Lohnbuchhaltung), Versicherungen, diverse Beratungen (Familienberatung, Suchtberatung), Inkassogesellschaften (Ausnahme Debitorenmahnverfahren)
- wenn die Übermittlung der personenbezogenen Daten gesetzlich verpflichtend ist
  z. B. Finanzamt, Krankenkassen
- wenn der Dienstleister eine **weisungsfreie** Leistung anbietet (bei denen die Verarbeitung personenbezogener Daten normalerweise durch die entsprechenden Gesetze geregelt bzw. vorgeschrieben ist)
  z. B. Ticketkauf bei der Bahn, Buchung im Hotel, Buchung im Reisebüro, Firmenkonto bei der Bank, etc. Dies sind klassische Fällen einer Funktionsübertragung, da der Dienstleister nach der Übermittlung selbst für die Daten verantwortlich ist.

Sprachassistenten

ALTHAMMER & KILL

Allgemeine Informationen

1. Alexa hört ständig mit und zeichnet auch bei – unbeabsichtigter - Aktivierung durch ähnliche Worte wie „Alexa“ auf.

Hier zwar etwas ältere Meldungen, deren aufgezeigtes Risiko aber berücksichtigt werden sollte, auch wenn Amazons aktuelle Meldung lautet „Entwickelt, um Datenschutz zu gewährleisten.“

https://www.heise.de/select/ct/2019/10/1557137785871125

https://www.heise.de/newsticker/meldung/Justizministerium-warnt-vor-Zugriff-auf-Daten-von-Alexa-Co-4441123.html

https://www.amazon.de/b/?node=17084415031

ALTHAMMER & KILL

Allgemeine Informationen

2. Durch dieses Mithören und Aufzeichnen, besteht grundsätzlich die Möglichkeit, dass eine **Übermittlung personenbezogener Daten in die USA** zu Amazon stattfindet.

3. Diese personenbezogenen Daten können auch der Schweigepflicht gemäß § 203 StGB unterliegen.

4. Dies gilt nicht nur für Alexa, sondern auch für Sprachassistenten in Smartphones, Tablets oder Notebooks z. B. Apples Siri, Microsofts Cortanan oder Google Assistant („OK Google“).

ALTHAMMER & KILL

Datenschutzrechtliche Beurteilung

Im Rahmen der Hausregeln und des Betreuungsvertrages kann der Klient oder dessen gesetzlicher Betreuer selbst bestimmen, wie der privaten Bereich des Klienten gestaltet wird und welche Geräte und Technik er dort nutzt.

Zunächst müssen zwei datenschutzrechtliche Fragen geklärt werden.

1. Ist dies überhaupt ein Datenschutzthema?
2. Wer ist für die Verarbeitung verantwortlich?

Beantwortet man zunächst Frage Nr. 2 ist es einfach, sofern der Klient selbst die Alexa anschafft bzw. die Anschaffung beauftragt und sie „selbst betreibt“, und somit auch für deren Datenverarbeitung verantwortlich ist. Dies ist unabhängig davon, ob die SeWo den Klienten bei der Installation/Einrichtung unterstützt und ob die Verbindung über eine Internetleitung der SeWo aufgebaut wird (Einschränkung der Störerhaftung).

Datenschutzrechtliche Beurteilung

Dies beantwortet automatisch Frage Nr. 1, da eine Verarbeitung durch den Klienten nicht in den Anwendungsbereich Art. 2 DSGVO (siehe Abs. 2 lit. c DSGVO) fällt und die Verarbeitung somit „kein Datenschutzthema“ mehr ist.

Aus Sicht des Klienten ist somit zunächst das Wichtigste geklärt, aber wie sieht es mit dem Verantwortungsbereich der SeWo und den Daten die unter die Schweigepflicht fallen aus? Betrachtet man zunächst die Kommunikation der SeWo mit dem Klienten, könnte man Alexa – und andere Sprachassistenten - mit einer anwesenden Person vergleichen.

Vorausgesetzt der Klient ist sich bewusst, dass Alexa bzw. andere Personen zuhören, hat der Klient die Möglichkeit Alexa auszuschalten, so wie er eine anwesende Person für die Dauer des Klientengesprächs hinausbitten kann. Sofern dies nicht in den Hausregeln oder dem Betreuungsvertrag geregelt ist (siehe Empfehlung), können die Mitarbeitenden der SeWo den Klienten auf Alexa oder anwesende Personen und die Vertraulichkeit des Gespräches hinweisen, sind hierzu aber nicht zwingend verpflichtet.

ALTHAMMER & KILL

Datenschutzrechtliche Beurteilung

Sofern einzelne Mitarbeitende in Bezug auf ihre eigenen Datenschutzrechte mit einer Verarbeitung durch Alexa nicht einverstanden sind, können sie den Klienten bitten Alexa auszuschalten.

Wenn dies nicht in Hausregeln oder Betreuungsvertrag geregelt ist, können sie den Klienten aber nicht dazu auffordern!

Als für die Verarbeitung durch Alexa Verantwortlicher obliegt es dem Klienten dieses Thema mit anderen Klienten im Zimmer zu regeln.

Da dies in der Praxis wahrscheinlich schwer umsetzbar ist, empfehlen wir Ihnen Folgendes.

ALTHAMMER & KILL

Handlungsempfehlungen

Auch wenn die SeWo – abgesehen von den Mitarbeitenden - nicht dazu verpflichtet ist, sollten Sie alle Beteiligten (Klienten, gesetzliche Betreuer und Mitarbeitende) sensibilisieren.

Inwiefern Hausregeln für eine Abschaltung von Alexa und ggf. anderen Sprachassistenten für die Dauer von Klientengesprächen (auch anderer Bewohner des Zimmers) ergänzt oder erstellt werden ist Ihre Entscheidung.

Zur Absicherung und Abgrenzung können Sie auch die oben genannten Verantwortungsbereiche als Information in Hausregeln oder Betreuungsvertrag ergänzen.

Störerhaftung

ALTHAMMER & KILL

Worum geht es?

Mit der Verabschiedung des dritten Telemedienänderungsgesetz am 30. 06. 2017 bezweckte der Gesetzgeber die Rechtsunsicherheit über die Haftungslage beim Betrieb von WLANs aufzuheben. Dadurch soll die Verbreitung von offenen Netzen in Deutschland, die im Vergleich zu anderen Ländern deutlich geringer ausfällt, gefördert werden. Da nun die BGH-Entscheidung Dead Island im Juli 2018 mehr Klarheit über die entsprechenden Normen geschaffen hat, ist eine Bereitschaft zur Bereitstellung von offenem WLAN seitens Unternehmen zu erwarten.

ALTHAMMER & KILL

Störerhaftung – Abschaffung und Restrisiko

Die Störerhaftung wurde in Bezug auf Schadensersatz, Abmahnkosten und Unterlassungsansprüche abgeschafft.

Allerdings gilt die Störerhaftung nach § 7 Abs. 4 TMG für einen Anspruch auf **Sperrmaßnahmen** immer noch. Der Rechteinhaber könnte, sofern keine andere Möglichkeit zur Abhilfe besteht und die jeweilige Sperrmaßnahme zumutbar und verhältnismäßig ist, einen Anspruch auf Sperrung bestimmter Ports am konkreten WLAN-Router, auf Sperrung des Zugriffs auf bestimmte Webseiten, auf DNS-, IP- und URL-Sperren oder auf Datenmengen-begrenzungen pro Nutzer haben.

ALTHAMMER & KILL

Rechtliche Vorkehrungen

Als die effektivste rechtliche Vorkehrung kommen angepasste Nutzungsbedingungen und Datenschutzerklärungen in Betracht. Über diese kann geregelt werden, dass kein Vertragsverhältnis mit dem Nutzer begründet wird, sodass keine entsprechenden Sorgfaltspflichten bestehen. In der Datenschutzerklärung sollte offengelegt werden, welche Informationen erhoben werden und wie sie gespeichert und verarbeitet werden. Die Kenntnis darüber, dass personenbezogene Daten erhoben werden, könnte zudem einige potenzielle „Urheberrechtsverletzer“ abschrecken. Sofern der WLAN-Anbieter durch die WLAN-Nutzung ein **Nutzerprofil** der Nutzer zu erstellen beabsichtigt, müsste er nach § 100 Abs. 3 TKG diese Daten anonymisieren oder pseudonymisieren. Der WLAN-Nutzer müsste die Nutzungsbedingungen freiwillig und bewusst bestätigen und somit die datenschutzrechtliche Einwilligung nach Art. 5 Abs. 1 Nr. 1 DSGVO abgeben.

ALTHAMMER & KILL

Technische Vorkehrungen

Als technische Vorkehrungen um insbesondere Urheberrechtsverstöße zu vermeiden, eignen sich die Begrenzung des Datenvolumens pro Nutzer sowie die zeitliche Befristung der WLAN-Zugänge. Damit kann erschwert oder verhindert werden, dass große Datenmengen hoch- oder runtergeladen werden. Sofern dem WLAN-Betreiber Ports oder Webseiten bekannt sind, über die urheberechtsverletzende Handlungen begangen werden, könnte er diese schon bei der Bereitstellung sperren, sodass über die gängigsten und bekannten Wege die Möglichkeit zur Urheberrechtsverletzung minimiert wird.

Um auch datenschutzrechtlich konform zu bleiben, sollte ein stimmiges Löschungskonzept implementiert werden, nach dem wenigstens die Anmeldedaten und die zugehörigen IP-Adressen der Nutzer für eine bestimmte Zeit gespeichert werden.

App Entwicklung

ALTHAMMER & KILL

Datenschutzkonforme Gestaltung

1. Experten für Datenschutz und IT-Sicherheit rechtzeitig einbinden!
2. Datenflussdiagramm erstellen (inklusive Art der Daten, Verschlüsselungen, beteiligter Unternehmen und Speicherorten).
3. Screenshot Diagramm erstellen (jeden Screen und mögliche Verzweigungen abbilden).
4. Prüfen der Rechtsgrundlagen insbesondere in Bezug zu erforderlichen Einwilligungen.
5. Die Datenschutzerklärung auf einem der ersten Screens und den Link darauf wenn möglich immer im Footer der App anzeigen.
6. Hohes Niveau für die Absicherung der Zugänge und die Verschlüsselung von Datentransfer und Speicherorten einrichten.
7. Pentest vor dem ersten Einsatz der App durchführen.

Fragerunde / Spezialthemen

Unterstützung durch Althammer & Kill

Hinweis und Nutzungsrechte

Diese Präsentation wurde nach bestem Wissen anhand des zum Zeitpunkt der Erstellung geltenden Rechtsstandes erstellt. Es wird kein Anspruch auf Vollständigkeit und Richtigkeit erhoben.

Die Überlassung der Präsentation erfolgt nur für den internen Gebrauch des Empfängers.
Weitergabe oder Veröffentlichung sind nur mit ausdrücklicher vorheriger Zustimmung der Althammer & Kill GmbH & Co. KG erlaubt.

Wir verwenden Bilder und Grafiken von:
www.miniansichten.de, www.pixabay.de und DATAKONTEXT GmbH

Vielen Dank!

Bleiben Sie mit uns in Verbindung...

ALTHAMMER & KILL

Andreas Hellmann

Berater für Datenschutz
und Informationssicherheit

Tel. +49 211 936748-34
ah@althammer-kill.de
www.althammer-kill.de

http://xing.to/AndreasHellmann