Memorandum

an: Felix Kuna, Myosotis GmbH
von: Dr. Lukas Mezger, UNVERZAGT VON HAVE Rechtsanwälte
Datum: 19. Juni 2019
Betreff: DSGVO-Compliance der Server-Infastruktur von „myo“

I. Sachverhalt

Die Myosotis GmbH bietet eine mobile App namens „myo“ an, über die Angehörige von Pflegeheim-Bewohnern mit ebendiesen in Kontakt bleiben können. Dazu werden von den Bewohnern oder von ihren Pflegenden Neuigkeiten aus dem Pflegeheim-Alltag oder sonstige persönliche Nachrichten einschließlich Fotos, Videos und Sprachnachrichten mit den Angehörigen ausgetauscht. Dies setzt eine vorherige Registrierung der teilnehmenden Bewohnern und ihrer Angehörigen voraus. Jede Pflegeheim-Betreibergesellschaft betreibt dabei eine eigene Myo-Instanz, für die die Myosotis GmbH als Dienstleisterin auftritt.

In technischer Hinsicht ist „myo“ so ausgestaltet, dass die Kommunikation über die App von Endgerät zu Endgerät über eine Cloud-Infrastruktur abgewickelt wird. Dabei nutzt die Myosotis GmbH den Cloud-Dienst der Amazon Web Services EMEA S.à r.l. („AWS EMEA“) mit Sitz in Luxemburg. Konkret werden dabei ausschließlich die AWS-Server in Frankfurt am Main genutzt. Es findet zu keinem Zeitpunkt eine Übertragung von personenbezogenen Daten von „myo“-Endgeräten in Deutschland ins Ausland statt. Stattdessen werden die Daten wie beschrieben ausschließlich über die in Frankfurt befindlichen AWS-Server übertragen.

Die Myosotis GmbH hat mit der Amazon Web Services EMEA S.à r.l. einen entsprechenden Dienstleistungsvertrag abgeschlossen, der eine Auftragsverarbeitungsvereinbarung (AVV) nach Art. 28 DSGVO enthält, welche den Umfang der vorzunehmenden Cloud-Datenverarbeitung in Frankfurt am Main festhält und die von der Amazon Web Services EMEA S.à r.l. umzusetzenden technischen und organisatorischen Maßnahmen (TOM) vorschreibt.

Zwischen der Myosotis GmbH und den Betreibergesellschaften der einzelnen Pflegeheime besteht ebenfalls ein Dienstleistungsverhältnis, der zugrundeliegende Vertrag enthält ebenfalls eine Auftragsverarbeitungsvereinbarung.

II. datenschutzrechtliche Einordnung

Gegenüber den Betroffenen, also den Pflegenden und den Bewohnern sowie gegenüber den Angehörigen tritt die Betreibergesellschaft des jeweiligen Pflegeheims als Verantwortlicher nach Art. 4 Nr. 7 DSGVO auf. Demgegenüber ist die Myosotis GmbH Auftragsverarbeiterin nach Art. 4 Nr. 8, 28 DSGVO. Die Amazon Web Services EMEA S.à r.l. ist demgegenüber ein Unter-Auftragsverarbeiter oder auch „weiterer Auftragsverarbeiter“ nach Art. 28 Abs. 2 S. 1 DSGVO.

Für den Einsatz von Unter-Auftragsverarbeiter stellt Art. 28 Abs. 2 DSGVO besondere Voraussetzungen auf:

- Der Verantwortliche muss den Einsatz von Unter-Auftragsverarbeitern *vorher schriftlich* genehmigen.
- Hat der Verantwortliche den Einsatz von Unter-Auftragsverarbeitern dabei *allgemein* genehmigt, muss der Auftragsverarbeiter die Hinzuziehung oder die Ersetzung eines Unter-Auftragsverarbeiters vorab ankündigen und den Verantwortlichen die Möglichkeit zum Widerspruch einräumen.
- Zwischen dem Auftragsverarbeiter und dem Unter-Auftragsverarbeiter muss eine Unter-Auftragsverarbeitungsvereinbarung abgeschlossen werden, die die Anforderungen des Art. 28 Abs. 4 DSGVO erfüllt.
- Diese Unter-Auftragsverarbeitungsvereinbarung muss in Bezug auf die darin festgelegten Pflichten des Unter-Auftragsverarbeiters den Pflichten des Auftragsverarbeiters gegenüber dem Verantwortlichen entsprechen.
- Dies gilt insbesondere in Bezug auf die einzuhaltenden technischen und organisatorischen Maßnahmen, Art. 28 Abs. 4 S. 1 a.E. DSGVO.
- Besondere Anforderungen gelten schließlich für die Übertragung personenbezogener Daten in ein Land außerhalb des europäischen Wirtschaftsraums, Abs. 28 Abs. 3 lit. a) DSGVO.

Zu untersuchen war daher, ob die eben genannten Voraussetzungen erfüllt sind. Dies war – ausgehend von einem damals leicht unterschiedlichen Sachverhalt – bereits Gegenstand meiner datenschutzrechtlichen Prüfung vom 4. Februar 2019 für die ePrivacy GmbH im Rahmen der ePrivacyseal-Zertifizierung.

Dabei ergibt sich das folgende Bild:

- Es besteht eine Auftragsverarbeitungsvereinbarung zwischen der Myosotis GmbH und ihren Auftraggeberinnen als Verantwortliche, die den Vorgaben des Art. 28 DSGVO entspricht.
- Diese Auftragsverarbeitung enthält in Abschnitt 4.1 eine allgemeine Genehmigung zum Einsatz von Unter-Auftragsverarbeiter gemäß Art. 28 Abs. 2 S. 1 DSGVO.
- Auch die Unter-Auftragsverarbeitungsvereinbarung zwischen der Myosotis GmbH und der Amazon Web Services EMEA S.à r.l. erfüllt die Anforderungen des Art. 28 DSGVO, insbesondere die besonderen Voraussetzungen an die Verpflichtungen des Unter-Auftragsverarbeiters nach Art. 28 Abs. 4 DSGVO.
- Die Myosotis GmbH informiert ihre Auftraggeberinnen in Anhang 3 des Dienstleistungsvertrags gemäß Art. 28 Abs. 2 S. 2 über den beabsichtigten Einsatz der Amazon Web Services EMEA S.à r.l. als Unter-Auftragsverarbeiterin.

Fraglich ist schließlich, ob die besonderen Voraussetzungen der Art. 44 ff. DSGVO für eine Datenverarbeitung in einem so genannten Drittland, das heißt in einen Staat außerhalb des europäischen Wirtschaftsraums Anwendung finden. Hierbei ist aber wie bereits erwähnt zu beachten, dass keine Vertragsbeziehung zur Amazon Web Services, *Inc.* in den Vereinigten Staaten besteht, sondern eben zur europäischen AWS-Tochtergesellschaft mit Sitz in Luxemburg. Darüber hinaus hat die Myosotis GmbH mit der Amazon Web Services EMEA S.à r.l. konkret vereinbart, dass ausschließlich die Cloud-Infrastruktur in Frankfurt genutzt wird, so dass innerhalb der datenschutzrechtlichen Verantwortlichkeit der Betreibergesell-

schaften keine Datenverarbeitung außerhalb Deutschlands erfolgt. Die besonderen Voraussetzungen der Art. 44 ff. DSGVO sind damit *nicht* einschlägig.

III. Ergebnis

Zusammengefasst erfüllt die Server-Infrastruktur von „myo“ die Vorgaben der Datenschutzgrundverordnung. Es ist zu empfehlen, die getroffenen technischen und organisatorischen Maßnahmen zur Datensicherheit vor dem Hintergrund der Natur der verarbeiteten Daten periodisch (zum Beispiel halbjährlich) intern zu überprüfen, insbesondere was zum Beispiel die verwendeten Verschlüsselungsalgorithmen angeht.