

UNVERZAGT

RECHTSANWÄLTE

UNVERZAGT Rechtsanwälte
HEIMHUDER STRASSE 71 20148 HAMBURG

Myosotis GmbH
Herrn Felix Kuna

Swinemünder Str. 110
10435 Berlin

per E-Mail: felix@myo.de

ANSPRECHPARTNER: Dr. Lukas Mezger
DURCHWAHL: +49.40.41 40 00-34
FAX DIREKT: +49.40.41 40 00-42
E-MAIL: mezger@unverzagt.law

UNSER ZEICHEN: E-1199-18/E/LM

DATUM: 15.01.2021

Datentransfers in die USA nach *Schrems II* hier: Nutzung von Cloud-Diensten der AWS Europe S.à r.l.

Sehr geehrter Herr Kuna,

wie besprochen habe ich mir die Frage der Nutzung von Cloud-Diensten der AWS Europe S.à r.l. vor dem Hintergrund der Rechtsprechung des europäischen Gerichtshofs in Sachen *Schrems II* aus datenschutzrechtlicher Sicht angesehen.

Anbei finden Sie ein kurzes Memorandum zu dieser Fragestellung. Zusammengefasst erfüllt die genutzte Server-Infrastruktur die Vorgaben der Datenschutzgrundverordnung nach *Schrems II*.

Mit freundlichen Grüßen



Dr. Lukas Mezger
Rechtsanwalt

HAMBURG

ALEXANDER UNVERZAGT
DR. FRANK EICKMEIER
DR. ANDREAS PENSE, M.S.J. (Paris)
DR. GERO BRUGMANN, LL.M. (UNSW)
CLAUDIA GIPS*
DR. SEBASTIAN RENGSHAUSEN**
INA-MARA HELBIG, LL.M.**
MICHAEL PHILIPPI
DR. ULRICH BÖRGER
DR. MINA KIANFAR
DR. ANDREA M. PARTIKEL
VANESSA PIETRAS, LL.M.
DR. LUKAS MEZGER
SIGRID COBET-NÜSE
DR. MARIAN KLINGEBIEL
PHILIPP SCHIFFMANN
JONATHAN SCHÄFER

*Fachwältin für Urheber- und Medienrecht
**Fachanwälte für Gewerblichen Rechtsschutz

HEIMHUDER STRASSE 71
20148 HAMBURG

TELEFON +49 (0) 40 41 40 00-0
TELEFAX +49 (0) 40 41 40 00-40
hamburg@unverzagt.law

BERLIN

KAI MAY

MONBIJOUPLATZ 2
10178 BERLIN

TELEFON +49 (0)30 28 87 63-33
TELEFAX +49 (0)30 28 87 63-44
berlin@unverzagt.law

DIRK FELDMANN
(of Counsel, Partner bis 2019)
KURT-MICHAEL LOITZ (of Counsel)

www.unverzagt.law

DEUTSCHE BANK

IBAN DE49 2007 0024 0656 2110 00
BIC/SWIFT DEUTDE33HAN

HASPA

IBAN DE28 2005 0550 1282 1318 51
BIC/SWIFT HASPDE33HAN

ANDERKONTO DEUTSCHE BANK

IBAN DE52 2007 0024 0807 7620 00
BIC/SWIFT DEUTDE33HAN

Partnerschaftsgesellschaft mbB
Partnerschaftsregister des AG Hamburg PR 746

Memorandum

an: Felix Kuna, Myosotis GmbH
von: Dr. Lukas Mezger, UNVERZAGT Rechtsanwälte
Datum: 15. Januar 2021
Betreff: Nutzung von Cloud-Diensten der AWS Europe S.à r.l. nach *Schrems II*

I. Sachverhalt

Die Myosotis GmbH bietet eine mobile App namens „myo“ an, über die Angehörige von in Pflege befindlichen Personen mit ebendiesen in Kontakt bleiben können. Dazu werden von den Patienten/Bewohnern oder von ihren Pflegenden Neuigkeiten aus dem Alltag der Einrichtung oder sonstige persönliche Nachrichten einschließlich Fotos, Videos und Sprachnachrichten mit den Angehörigen ausgetauscht. Dies setzt eine vorherige Registrierung der teilnehmenden Patienten/Bewohner und ihrer Angehörigen voraus. Jede 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 Einrichtungen besteht ebenfalls ein Dienstleistungsverhältnis, der zugrundeliegende Vertrag enthält ebenfalls eine Auftragsverarbeitungsvereinbarung.

II. Datenschutzrechtliche Einordnung

Gegenüber den Betroffenen, also den Pflegenden und den Patienten/Bewohnern sowie gegenüber den Angehörigen tritt die Betreibergesellschaft der jeweiligen Einrichtung als Verant-

wortlicher 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-Auftragsverarbeitern 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, Art. 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 Anforderungen 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 Betreibergesellschaften keine Datenverarbeitung außerhalb Deutschlands erfolgt. Die besonderen Anforderungen der Art. 44 ff. DSGVO sind damit *nicht* einschlägig.

Nicht unerwähnt bleiben soll hier, dass es durchaus Überlegungen gibt, den Datenschutz über den hier beschriebenen, von der DSGVO vorgegebenen Rahmen hinaus weiter zu denken, zum Beispiel weil US-Behörden die AWS-Muttergesellschaft AWS Inc. theoretisch auffordern könnten, ihre europäische Tochtergesellschaft AWS EMEA zur (rechtswidrigen) Weitergabe von Daten europäischer Nutzer entgegen der Vorgaben der DSGVO zu bewegen.¹

Im Ergebnis bleibt es jedoch auf der Grundlage des geltenden Rechts beim bisher Gesagten. Dies bestätigt auch eine aktuelle Entscheidung des obersten französischen Verwaltungsgerichts aus dem Oktober 2020, die einen mit der hier untersuchten Konstellation beinahe identischen Sachverhalt betraf: Der Conseil d'État erklärte im so genannten „Health Data Hub“-Beschluss die Verarbeitung von Gesundheitsdaten französischer Bürger innerhalb der EU durch die irische Tochtergesellschaft des amerikanischen Unternehmens Microsoft für zulässig.²

¹ *Die Landesbeauftragte für den Datenschutz Niedersachsen*, „Der CLOUD Act– Zugriff von US-Behörden auf Daten in der EU“, in: 25. Tätigkeitsbericht 2019, S. 26 ff.; *Gausling*, „Offenlegung von Daten auf Basis des CLOUD Act, CLOUD Act und DS-GVO im Spannungsverhältnis“ MMR 2018, 578 ff.; s.a. *Punke*, „Cloud Act: Alles nur halb so schlimm...“, eGovernment Computing, 4.6.2019.

² *Conseil d'État*, Beschluss v. 13.10.2020, Az. 444937 – *Health Data Hub*.

Zum Hintergrund: Die Plattform „Health Data Hub“ ist eine Einrichtung der französischen Regierung, die den Austausch von Gesundheitsdaten zu Forschungszwecken erleichtern soll. Insbesondere werden derzeit Daten im Zusammenhang mit der COVID-19-Pandemie verarbeitet. Das Hosting der Daten und die Nutzung der für ihre Verarbeitung erforderlichen Software erfolgt durch die Microsoft Ireland Operation Limited (im Folgenden „Microsoft Ireland“), einer irischen Tochtergesellschaft des US-amerikanischen Microsoft-Konzerns.

Mehrere Kläger befürchteten nun, dass auf diesem Wege eine Übermittlung personenbezogener Daten in die USA erfolge, wo laut dem Urteil des Europäischen Gerichtshofs in Sachen „Schrems II“ zumindest im Regelfall kein angemessenes Datenschutzniveau im Sinne der DSGVO gewährleistet ist.³

Der Conseil d'État hat in seinem Beschluss zunächst auf die zu Grunde liegende Auftragsverarbeitungsvereinbarung von Microsoft Ireland verwiesen und festgestellt, dass im Rahmen dieser Auftragsverarbeitung *keine* Übermittlung von personenbezogenen Daten in die USA stattfindet. Der genannte Vertrag sieht nämlich vor, dass Microsoft Ireland keine Gesundheitsdaten in Länder außerhalb der EU übermittelt oder dort verarbeitet.

Außerdem liege auch *keine* Unzulässigkeit der Datenübermittlung nach den Grundsätzen des „Schrems II“-Urteils des EuGH vor. Gegenstand dieses Urteils waren wie erwähnt die Anforderungen für eine zulässige Übermittlung personenbezogener Daten in die USA. Im Fall des „Health Data Hubs“ erfolgt jedoch wie dargestellt eine Verarbeitung personenbezogener Daten (nur) in Europa, konkret durch die europäische Tochtergesellschaft eines amerikanischen Unternehmens als Auftragsverarbeiter. Anders ausgedrückt: Die Schrems-II-Entscheidung findet *keine* Anwendung auf Datenverarbeitungsvorgänge, bei denen die Daten von einem Auftragsverarbeiter mit Sitz in der Europäischen Union verarbeitet werden.

Auf eine allenfalls hypothetische, zukünftige Übertragung in die USA komme es *nicht* an. Zwar könne nicht ganz ausgeschlossen werden, dass amerikanische Behörden Einfluss auf den Microsoft-Konzern und dieser wiederum auf seine europäischen Tochtergesellschaften nehmen. Allerdings bestehe dieses Risiko nur in dem Fall, dass Microsoft Ireland nicht in der Lage ist, sich einer entsprechenden Weisung zu widersetzen. Zudem seien die bei Microsoft Ireland gespeicherten Daten verschlüsselt.

³ EuGH, Urt. v. 16.7.2020, Az. C-311/18 – *Schrems II*.

III. Ergebnis

Zusammengefasst erfüllt die Server-Infrastruktur von „myo“ die Vorgaben der Datenschutzgrundverordnung.