SPECTARIS
Deutscher Industrieverband für Optik,
Photonik, Analysen- und Medizintechnik

VDMA
Arbeitsgemeinschaft
Medizintechnik

Positionspapier zur Nutzung von US-Cloud-Anbietern und Umsetzung des Schrems II-Urteils

August 2021

Ansprechpartner

SPECTARIS – Deutscher Industrieverband für Optik, Photonik, Analysen- und Medizintechnik e. V.

Felix Dotzauer
Referent Regulatory Affairs

dotzauer@spectaris.de
www.spectaris.de

VDMA – Arbeitsgemeinschaft Medizintechnik

Diethelm Carius
Referent AG Medizintechnik

d.carius@vdw.de
medtec.vdma.org

Schrems II-Urteil: Ein Jahr Rechtsunsicherheit für Unternehmen

Durch die anhaltende Pandemie und den damit einhergehenden Digitalisierungsschub hat Cloud-Computing für Unternehmen an zusätzlicher Relevanz gewonnen. Die Nutzung von Cloud-Services – überwiegend aus den USA – stellt für viele Unternehmen eine essentielle Funktionsgrundlage dar. Seit knapp einem Jahr stehen Unternehmen in und aus Europa jedoch vor einem Dilemma der Rechtsunsicherheit bei der Verarbeitung personenbezogener Daten: Denn mit dem Schrems II-Urteil vom 16. Juli 2020 erklärte der Europäische Gerichtshof (EuGH) das EU-US Privacy Shield für unrechtmäßig. Gleichzeitig sind viele Unternehmen – mangels europäischer Alternativen und nur schwer realisierbaren Umstellungsaufwänden – auf internationalen Datentransfer und die Nutzung von Cloud-Lösungen aus den USA und weiteren Drittstaaten angewiesen. Für deutsche Unternehmen besteht im europäischen Vergleich eine besondere Unsicherheit, da Datenschutzanforderungen je nach Bundesland unterschiedlich ausfallen und die Anforderungen der Datenschutz-Grundverordnung (DSGVO) je nach Regulierungsbehörde auch auf nationaler Ebene unterschiedlich ausgelegt werden können. Dies wird vor allem für Unternehmen im Gesundheitswesen deutlich. Vor dem Hintergrund der besonderen Relevanz von Cloud-Computing für Unternehmen, allen voran aus der Medizin- und Labortechnik, verweist dieses Positionspapier auf die aktuelle Problemlage im Hinblick auf Schrems II sowie auf die Notwendigkeit langfristiger politischer Lösungen auf nationaler und internationaler Ebene, um drohende negative Effekte auf die Wettbewerbs- und Handlungsfähigkeit deutscher Unternehmen zu vermeiden.

Rechtsunsicherheit für Unternehmen in Europa

Aufgrund des EuGH-Urteils stehen europäische Unternehmen, die auf die Software und Online-Services US-amerikanischer Anbieter angewiesen sind, vor großen Herausforderungen. Gemäß der DSGVO bietet sich den Unternehmen zwar die Möglichkeit der Einzelfallprüfung und sogenannter Standardvertragsklauseln zur konformen Absicherung internationaler Datentransfers, durch die Entscheidung des EuGH werden solche Handlungsoptionen jedoch hinterfragt und stellen somit keine Garantie mehr für Unternehmen dar. Zu dieser allgemein vorherrschenden Verunsicherung gesellt sich zudem der enorme Arbeitsaufwand bei vertraglichen Einzelfallregelungen, den kleine und mittlere Unternehmen nicht stemmen können. Die kürzlich von der EU-Kommission aktualisierten Standardvertragsklauseln[1] sind zu begrüßen, lösen jedoch nicht die Problematik der aufwändigen, ergebnisoffenen und somit unsicheren Einzelfallprüfungen – speziell im Hinblick auf die USA.

Darüber hinaus mangelt es an Alternativen zu Anbietern aus den USA und weiteren Drittstaaten. Europäische Lösungen, die über die reine Datenspeicherung oder die Bereitstellung von Infrastructure-as-a-Service (IaaS) hinausgehen, sind in dem erforderlichen Umfang von deutschen oder europäischen Anbietern aktuell schwer realisierbar. Eine eigene europäische Cloud-Infrastruktur à la GAIA-X stellt einen vielversprechenden und unterstützenswerten Lösungsansatz für Unternehmen in Europa dar, der sich allerdings in der Aufbauphase befindet und somit keine kurz- oder mittelfristige Entlastung schafft. Darüber hinaus besteht hier ebenfalls Konfliktpotential, da US-amerikanische Technologiekonzerne nun ebenfalls in den Entwicklungsprozess eingebunden sind.

1 Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates (Text von Bedeutung für den EWR); https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=de

Fragmentierte Datenschutzanforderungen auf Länderebene – die besondere Rechtsunsicherheit für Unternehmen in Deutschland

Die Rechtslage für Unternehmen in und aus Deutschland ist zurzeit komplexer als in anderen EU-Mitgliedstaaten – dies liegt an dem föderalen System der Datenschutzaufsicht, das europaweit einzigartig ist. Unternehmen müssen sich stets an den Vorgaben ihrer jeweiligen Landesdatenschutzbehörden orientieren, die DSGVO-Anforderungen jedoch unterschiedlich auslegen können – die fehlende Harmonisierung von Datenschutzvorgaben auf nationaler Ebene steht somit konträr zum Harmonisierungsansatz der DSGVO und führt zu einer besonderen Komplexität besonders für Unternehmen in Deutschland, die Standorte in mehreren Bundesländern unterhalten. Die Auslegung der DSGVO im Hinblick auf Schrems II kann somit zu zusätzlicher Komplexität führen. Datenschutzbehörden der Länder sind augenscheinlich um eine harmonisierte Auslegung bemüht, wie am Beispiel des kürzlich veröffentlichten Fragebogens zur DSGVO-Einhaltung bei Unternehmen deutlich wird. Gleichwohl wird auch hier eine Fragmentierung deutlich, da sich nach aktuellem Stand nur 9 aus 16 Bundesländern daran beteiligen. Dementsprechend wäre eine gänzlich harmonisierte und flächendeckend gleiche Herangehensweise der Datenschutzbehörden wünschenswert, um mehr Rechtssicherheit und Handlungsfähigkeit für Unternehmen zu ermöglichen.

Rechtsunsicherheit für deutsche Unternehmen im Gesundheitswesen

Darüber hinaus besteht für Unternehmen aus dem Gesundheitswesen eine besondere Planungsunsicherheit, da bei der Frage der Nutzung von US-Cloud-Anbietern unterschiedliche Anforderungsniveaus zwischen den nationalen Regulierungsbehörden aus dem Gesundheitswesen auf der einen und Datenschutzbehörden auf der anderen Seite erkennbar sind. Diese Divergenz, die in zusätzlicher sektorspezifischer Rechtsunsicherheit resultiert, wird bei der Regulierung von digitalen Gesundheitsanwendungen (DiGA) exemplarisch deutlich.

……

DiGA: Rechtsunsicherheit durch abweichende Anforderungen

Dem Datenschutzniveau liegt gemäß § 4 der DiGAV die DSGVO zugrunde, weshalb hier nun durch die Aushebelung des EU-US-Privacy Shields dieselbe Problematik bei der Nutzung von US-Cloud-Anbietern besteht. Das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) äußerte sich dazu im Januar 2021: Die Verarbeitung von personenbezogenen Daten außerhalb der EU auf der Grundlage von Schutzklauseln sei für DiGAs nicht zulässig. Jedoch sei es möglich, US-Dienstleister mit EU-Niederlassung zu nutzen, sofern der Anbieter dem DiGA-Hersteller zusichere, dass weder Datentransfer noch Datenverarbeitung in den USA stattfindet. Zudem müssten, so das BfArM, personenbezogene Daten der Nutzer verschlüsselt und von den Herstellern innerhalb der EU verwaltet und gespeichert werden.[2]

Dennoch ist diese Positionierung keineswegs verbindlich, da abweichende Einschätzungen der zuständigen und federführenden Datenschutzbehörden zu veränderten Anforderungen führen könnten. Tatsächlich zeichnet sich eine wesentlich striktere Auslegung der DSGVO-Anforderungen bei digitalen Gesundheitsanwendungen durch die Datenschutzbehörden in Deutschland ab. Laut des aktuellen Tätigkeitsberichts des Bundesbeauftragten für den Datenschutz und die Informationssicherheit wurden gegenüber dem Bundesgesundheitsministerium grundsätzliche Bedenken bezüglich des Datensicherheitsniveaus geäußert, die bislang nicht berücksichtigt worden seien.[3]

---

2 Informationen zur Zulässigkeit der Datenverarbeitung außerhalb Deutschlands im Zusammenhang mit dem Prüfverfahren des BfArM gemäß § 139e Fünftes Buch Sozialgesetzbuch (SGB V), 28. Januar 2021; https://www.bfarm.de/SharedDocs/Downloads/DE/Medizinprodukte/Datenverarbeitung_au%C3%9Ferhalb_Deutschlands_FAQ.pdf

3 Tätigkeitsbericht 2020: 29. Tätigkeitsbericht für den Datenschutz und die Informationsfreiheit; https://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/29TB_20.html?nn=5217212

Die erkennbaren möglichen Auslegungsunterschiede erzeugen somit zusätzliche Rechtsunsicherheit in diesem Sektor. Während die im Fall DiGA grundsätzliche Nutzung von US-Cloud-Services unter bestimmten Voraussetzungen eingeräumt wird und zu begrüßen ist, stellt dies nur eine Einschätzung unter Vorbehalt dar, auf die sich Unternehmen nicht stützen können. Nur eine enge Abstimmung der Gesundheits- und Datenschutzbehörden kann hier zu einer tatsächlich rechtssicheren Situation führen.

Zusammenfassung

Somit ergibt sich bei der Nutzung von US-Cloud-Anbietern im Hinblick auf personenbezogene Daten in der aktuellen Situation eine zwei- oder gar dreistufige Problemlage:

- Erstens besteht durch die Rechtsprechung des EuGH akute Rechtsunsicherheit auf EU-Ebene für Unternehmen, die auf internationalen Datenaustausch angewiesen sind. Standardvertragsklauseln schaffen hier keine garantierte Abhilfe, da vor allem KMU nicht die Ressourcen für Einzelfallprüfungen besitzen und es an alternativen europäischen Lösungswegen mangelt.
- Zweitens besteht nun für deutsche Unternehmen eine besondere Komplexität, die sich durch Schrems II verstärken kann: Denn durch die jeweils eigenständig agierenden Datenschutzbehörden auf Länderebene ergibt sich aufgrund der unterschiedlichen Auslegung von DSGVO-Anforderungen eine zusätzliche Fragmentierung. Leidtragende sind schlussendlich die Unternehmen in Deutschland, die zumeist in mehreren Bundesländern agieren und nun größerer Unsicherheit als zuvor ausgesetzt sind. Insbesondere im europäischen Vergleich besteht die Gefahr, dass deutsche Hersteller vermehrt von fehlender Rechts- und Planungssicherheit betroffen sein werden, was letztlich ein zunehmendes Innovationshemmnis darstellt. Denn in anderen EU-Mitgliedstaaten, wie z.B. Frankreich, herrschen oft zentralisierte und somit harmonisierte Auslegungen von Datenschutz- und DSGVO-Anforderungen, was die Arbeit von Unternehmen erleichtert und gleichzeitig zu mehr Rechts- und Planungssicherheit führt. Letztlich läuft die derzeitige Entwicklung entgegen dem aktuellen und notwendigen Digitalisierungstrend in Deutschland. Die langfristige Konsequenz dieser andauernden Entwicklung wären massive Wettbewerbsnachteile für deutsche Unternehmen - nicht nur aus einer globalen Perspektive, sondern auch im Vergleich zu anderen EU-Mitgliedstaaten.
- Drittens besteht eine sektorspezifische Rechtsunsicherheit für Unternehmen aus dem Gesundheitswesen: Das Beispiel DiGA illustriert die bestehenden Auslegungsunterschiede zwischen den gesundheitspolitischen Akteuren und den Datenschutzbehörden bei der Nutzung von US-Cloud-Anbietern. Zu begrüßen ist die grundsätzliche Möglichkeit der Nutzung von US-Cloud-Services (am Beispiel der DiGA) unter bestimmten Voraussetzungen, die in Aussicht gestellt wird. Eine Festlegung der Anforderungen steht jedoch noch aus, weshalb von behördlicher Seite weiterhin eine Einigung und Festlegung erforderlich ist, um mehr Planungssicherheit für Unternehmen aus dem Gesundheitssektor zu ermöglichen.

Forderungen/Lösungsansätze:

Die Sicherheit von personenbezogenen Daten stellt ein hohes Gut für unsere Mitgliedsunternehmen dar. Ebenso wie z.B. die Patientensicherheit bei der Anwendung von medizintechnischen Geräten muss und soll die Sicherheit von personenbezogenen Daten auf dem bestmöglichen Niveau sichergestellt werden. Voraussetzung dafür sind jedoch realisierbare Lösungen der Politik und ein insgesamt einheitlicher Rechtsrahmen zur Nutzung von Cloud-Anbietern aus den USA und weiterer Drittstaaten, um den essentiellen internationalen Datentransfer und die Funktionsfähigkeit der Wirtschaft in Deutschland und Europa aufrechtzuerhalten. Die hier vorgestellten Lösungsansätze könnten zu mehr Planungssicherheit, zu einer

Entlastung der Unternehmen und letztlich zur langfristigen Erhaltung der Wettbewerbsfähigkeit deutscher Unternehmen beitragen:

- Auf europäischer Ebene muss sich die Bundesregierung für **politische Lösungen in der Form von Angemessenheitsbeschlüssen** zwischen der EU und den USA sowie weiteren Drittstaaten einsetzen. Nur über diesen Weg können der essentielle internationale Datenverkehr sowie die Funktionsfähigkeit von Unternehmen eine langfristig rechtssichere Grundlage erhalten.
- **Überführung der jeweiligen Datenschutzanforderungen und DSGVO-Auslegungen auf Länderebene in gemeinsame harmonisierte Vorgaben auf nationaler Ebene:** Dies würde für weitaus mehr Rechtssicherheit und Handlungsfähigkeit für Unternehmen in Deutschland sorgen, auch um ein innereuropäisches Auseinanderdriften und Wettbewerbsnachteile für die deutsche Wirtschaft zu verhindern. Es gilt zu vermeiden, dass Deutschland im Vergleich zu den anderen Mitgliedstaaten – gleich zu Beginn der von der EU-Kommission ausgerufenen „digital decade" – ins wettbewerbstechnische Hintertreffen gerät.
- Gleichzeitig empfiehlt sich auch eine verstärkte Kooperation auf europäischer Ebene zwischen den Mitgliedstaaten (und Datenschutzbehörden), um **zusätzliche Harmonisierung der DSGVO-Auslegung innerhalb der Europäischen Union** zu erzielen – ganz im Sinne des Harmonisierungsgedankens.
- Die in Art. 46, 47 DSGVO vorgesehenen **Standardvertragsklauseln zur Datenübermittlung in Drittländer müssen eine valide Option für Unternehmen darstellen**. Zudem sollten mögliche Sanktionsmaßnahmen bis zur abschließenden Klärung der Rechtslage und -auslegung ausgesetzt werden.
- Im deutschen Gesundheitswesen speziell muss in Bezug auf Schrems II und die Nutzung von US-amerikanischen Cloud-Services eine **eindeutige und einheitliche Rechtslage bezüglich der Verarbeitung und Übersendung personenbezogener Daten** geschaffen werden. Die Überwindung von deutlichen Differenzen auf regulatorischer Seite kann nur durch eine intensivierte Zusammenarbeit von Gesundheits- und Datenschutzbehörden unter dem Ziel gemeinsamer und harmonisierter DSGVO-Anforderungen erfolgen.