RoCas GbR.
Guido Rochow & Astrid Casteel
Hotline: +49 (2163) 8998088
Fax: +49 (2163) 8998087
Web: www.rocas-heilpraxis.de
Mail: heilpraxis@rocas.de

Die wichtigsten Maßnahmen:

- Überprüfung Software
- Überprüfung Cloud-Dienste
- ADV Verträge abschließen
- Datenschutzerklärungen prüfen
- Daten verschlüsseln

Privacy Shield gekippt

Was bedeutet das für eine Heilpraxis?

Kaum jemand weiß was der „Privacy Shield“ ist und was es bedeutet, dass dieser „gekippt“, also für ungültig erklärt wurde, auch wenn es für einen Inhaber einer Praxis erhebliche Folgen haben kann. Deswegen möchten wir etwas genauer darauf eingehen und erklären, wie man trotz der Verarbeitung sensibler Patientendaten, die laut DSGVO Art. 9 unter besonderem Schutz stehen, die Datenverarbeitung innerhalb einer Praxis rechtskonform organisieren kann.

Guido Rochow
Chefentwickler der
RoCas Heilpraxis

Was ist das „Schrems II“-Urteil?

Das nach dem österreichischen Juristen, Autor und Datenschutzaktivisten Max Schrems benannte „Schrems II“-Urteil (Az.: C-311/18) wurde am 16. Juli 2020 gesprochen und führte dazu, dass der Privacy Shield (laut Durchführungsbeschluss (EU) 2016/1250 der Kommission vom 12. Juli 2016 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des vom EU-US-Datenschutzschild) mit sofortiger Wirkung gekippt wurde und für den Datentransfer in die USA andere Garantien bedürfen, vor allem nach Art. 44 ff. DSGVO (hiermit sind vor allem die sog. Standard-Vertragsklauseln gemeint).

Schrems hatte zuvor mit seiner Datenschutzorganisation „Nyob“ auch den Vorgänger des Privacy Shields, den sog. „Safe Harbour“ zu Fall gebracht.

Worum geht es denn beim Privacy Shield?

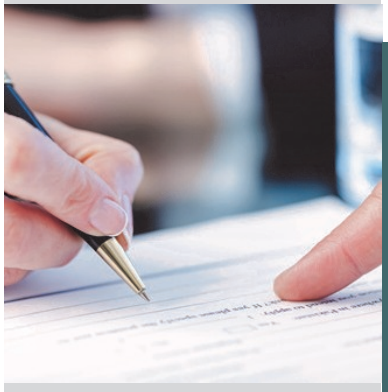
Der Privacy Shield war dem Safe Harbour ähnlich und es ging um ein Datenschutzabkommen zwischen den USA und der EU. Hiermit sollte also geregelt werden, wie die Daten europäischer Bürger, in den USA geschützt werden sollten. Beide Abkommen wurden jedoch mittlerweile für unzulässig erklärt, weil Amerikanische Cloud-Dienste und weitere Dienstleister im Bereich der Datenverarbeitung unter die FISA (Foreign Intelligence Surveillance Act) Regelung fallen und somit amerikanische Geheimdienste das Recht haben, auf diese Daten zuzugreifen. Dieser Zugriff ist nicht mit europäischem Recht vereinbar, zumal hier, nach US-Recht, auch nicht von Belang ist, ob der Server eines amerikanischen Unternehmens in der EU steht. Es reicht, wenn die Server von einem amerikanischen Unternehmen betrieben werden.

Was heißt das nun für einen Praxisinhaber?

Im Grunde genommen, dass jeder Softwareeinsatz und jede Datenverarbeitung dahingehend geprüft werden muss, ob personenbezogene Daten in den USA verarbeitet oder dorthin übermittelt werden. Das beginnt beim Virenscanner, der ggf. Dateien auf den eigenen Server überträgt um diese zu scannen, wenn Dokumente in der Cloud abgeglichen werden, oder Clouddienste für das Backup des Praxisrechners verwendet werden, aber auch Terminverwaltungssoftware eines US-Herstellers genutzt wird. Ebenso gilt dies z.B. für Cloudversionen von Office-Produkten, usw.. Jedwede Anwendung, die mit personenbezogenen Daten in Kontakt kommt, sollte überprüft werden. Das ist auch nicht nur für Praxisinhaber so, aber hier muss man ganz speziell betonen, dass Sie mit sehr sensiblen Patientendaten umgehen.
Auch Ihr Mailprovider sollte unbedingt aus Europa sein und hier sollte ebenso ein Auftragsdatenverarbeitungsvertrag vorliegen. Zudem können Rechnungen mit Leistungsziffern und Diagnosen nicht unverschlüsselt per Mail gesendet werden, selbst wenn Ihr Anbieter innerhalb der EU agiert.
Leider hat sich die Ende-zu–Ende Verschlüsselung bei Mails noch nicht durchgesetzt, deshalb haben wir in der Heilpraxis ein individuelles Patientenpasswort hinterlegt, mit dem solche Dokumente geschützt werden können.

RoCas Heilpraxis

RoCas GbR.
Guido Rochow & Astrid Casteel
Hotline: +49 (2163) 8998088
Fax: +49 (2163) 8998087
Web: www.rocas-heilpraxis.de
Mail: heilpraxis@rocas.de



Wie bekomme ich heraus, welche Dienste und Software ich nutzen kann?

Schauen Sie sich an, wo das Unternehmen, das den Dienst oder die Software anbietet, sitzt und werfen Sie einen Blick in dessen Datenschutzerklärung. Da Sie mit derartigen Unternehmen einen Auftragsdatenverarbeitungsvertrag schließen müssen und dies ein Grundprinzip der DSGVO ist, werden Sie spätestens hier fündig. Ein Unternehmen, welches Ihre Daten DSGVO konform verarbeitet, wird sicherlich auch auf Nachfrage darüber Auskunft geben.
Bedenken Sie bei dem Neukauf von Software, bzw. bei neuen Vertragsabschlüssen auch daran, dass die Beziehungen zu Großbritannien auch noch nicht abschließend geklärt sind. Dies ist ein großer Unsicherheitsfaktor, den man jetzt schon mitbedenken sollte.
Selbst die derzeit noch gültigen Standardvertragsklauseln stehen in der Kritik, weil eine endgültige Lösung der Einsichtnahme US-amerikanischer Geheimdienste noch nicht in Sicht ist.

Gibt es sichere Anbieter außerhalb der EU?

Sichere Drittländer derzeit :

- Andorra
- Argentinien
- Kanada
- Faroer Inseln
- Guernsey
- Israel
- Isle of Man
- Japan
- Jersey
- Neuseeland
- Schweiz
- Großbrittanien (mit Einschränkungen)
- Uruguay
- Südkorea

Diese Liste wird ständig aktualisiert und überarbeitet und ist auf der Homepage der Europäischen Kommission (https://ec.europa.eu) unter dem Stichwort „Adequacy decisions“ einsehbar.

Generell sollte jedoch vor der Übertragung von Daten in ein sicheres Drittland geprüft werden, ob die Voraussetzung für eine rechtmäßige Datenübermittlung vorliegt und die eigene Datenschutzerklärung dementsprechend angepasst werden. Außerdem muss auch hier natürlich sichergestellt werden, dass der erwogene Anbieter die notwendigen Schutzmaßnahmen für sensible Daten (Patientendaten, Art.9) bereitstellen und aufrecht erhalten kann. Letztendlich sind Sie für die Einhaltung der DSGVO verantwortlich.

Was raten Sie?

Nun, wer uns kennt, kennt unsere Haltung zur Cloud. Diese halten wir für medizinische Daten für nicht geeignet, da auch Verschlüsselung kein Allheilmittel ist und immer wieder gezeigt wurde, dass auch dies irgendwann überwunden werden kann (gängige Lehrmeinung z.B. der TU Darmstadt). Bei solch schützenswerten Daten bevorzugen wir lokal installierte Programme und lokale Datenhaltung. Bei Mailprovidern und ähnlichen Diensten gibt es ganz sicher auch gute Anbieter aus Deutschland, bzw. aus der EU. Damit entgeht man von vornherein dieser Problematik. Virenscanner und Backupsoftware, die nach diesen Kriterien geeignet sind, haben wir ebenso im Sortiment und unterstützen unsere Kunden auch mit weiteren Hilfestellungen innerhalb unserer Software um möglichst gut und bequem die DSGVO umsetzen zu können.

Alle Aspekte die sich nun aus dem Urteil ergeben, können wir in diesem kurzen Text nicht erläutern.
Wir möchten darauf Hinweisen, dass dieser Artikel keinesfalls eine Rechts– oder Datenschutzberatung darstellt, oder ersetzt. Unter anderem beratend tätig sind die zuständigen Datenschutzbehörden Ihres Bundeslandes.

Unter EU-Privacy Shield gibt es hierüber auch einen ausführlichen Artikel auf Wikipedia, wie auch zu Max Schrems und seiner Datenschutzorganisation Nyob. Des weiteren sind sämtliche Artikel der DSGVO mit einschlägigen Suchmaschinen übersichtlich im Internet zu finden.
Wir unterstützen unsere Kunden bestmöglich innerhalb unserer Software, wie auch mit weiteren Produkten bei der Einhaltung der DSGVO. Bei technischen Fragen können Sie sich gerne an unseren Service wenden (heilpraxis@rocas.de)

Bildquellen:
Pixabay, Billionphotos, RoCas GbR.