MYRA

EXPERTENINTERVIEW

Datenschutzaufsicht geht gegen US-Cloud-Nutzung vor

MYRA
Neue digitale Sicherheit

Datenschutzaufsicht macht Ernst: Behörden gehen gegen unzulässigen Einsatz von US-Cloud-Dienstleistern vor

Zahlreiche deutsche Unternehmen bekommen derzeit Post von der Datenschutzaufsicht mit der Aufforderung, sich für den Einsatz eines US-amerikanischen Cloud-Dienstleisters zu rechtfertigen. Betroffene Firmen müssen darlegen, wie sie einen DSGVO-konformen Datentransfer in Drittländer wie die USA sicherstellen.

Spätestens seit dem Wegfall des Privacy-Shield-Abkommens durch das EuGH-Urteil zu „Schrems II" ist der DSGVO-konforme Einsatz von US-Cloud-Unternehmen in der Praxis nahezu unmöglich. US-Gesetze wie der Cloud Act, der Behörden in den USA unbeschränkten Zugriff auf die von US-Unternehmen verarbeiteten Daten gibt, sind nicht mit der DSGVO vereinbar. Wer jedoch keinen rechtskonformen Transfer sensibler Daten in die USA gewährleisten kann, muss die Datenübermittlung unverzüglich beenden oder letztlich sogar den Dienstleister wechseln.

Sebastian Hoegl, Senior Manager und Leiter des Bereichs IT- und Datenschutzrecht bei der KPMG Law Rechtsanwaltsgesellschaft GmbH, hat regelmäßig mit solchen Fällen zu tun. Im Interview gibt er Unternehmen Tipps, wie sie am besten reagieren.

Sebastian Hoegl
Rechtsanwalt und Fachanwalt für IT-Recht bei KPMG Law

Sebastian Hoegl ist als Rechtsanwalt und Fachanwalt für Informationstechnologierecht bei der KPMG Law Rechtsanwaltsgesellschaft GmbH verantwortlich für den Bereich Datenschutzrecht und IT-Recht, in dem derzeit mehr als 15 Rechtsanwälte und Rechtsanwältinnen tätig sind. Sein besonderer Tätigkeitsschwerpunkt liegt in der Beratung der öffentlichen Hand sowie der umfassenden Beratung von daten- und technologiegetriebenen Unternehmen. Sebastian Hoegl hat in Freiburg, Köln und Wellington (Neuseeland) studiert und ist seit 2011 als Rechtsanwalt zugelassen.

> ***„Der EuGH hat die klare Erwartung an die Aufsichtsbehörden formuliert, unzulässige Datenübermittlungen auszusetzen oder zu verbieten."***

Im April haben die Datenschutzbehörden angekündigt, ihre Ermittlungen zu Datenschutzvestößen durch US-Cloud-Nutzung zu intensivieren. Wie sieht die Situation ein halbes Jahr später aus – haben die Behörden ihre Ankündigung wahr gemacht?
Sebastian Hoegl: Der EuGH hat in seinem Urteil in der Rechtssache „Schrems II" die klare Erwartung an die Aufsichtsbehörden formuliert, unzulässige Datenübermittlungen auszusetzen oder zu verbieten. Diese Erwartung nehmen die Aufsichtsbehörden sehr ernst. Die Aufsichtsbehörden mehrerer Bundesländer, darunter Berlin, Brandenburg, Bayern, Niedersachsen, Baden-Württemberg, Bremen, Hamburg, Rheinland-Pfalz und Saarland, führen derzeit eine sogenannte „Koordinierte Prüfung internationaler Datentransfers" durch. In diesem Rahmen schreiben die Aufsichtsbehörden ausgewählte Unternehmen an und fordern sie in einem ersten Schritt zum Ausfüllen eines Fragenkatalogs zu den Themen „Bewerberportale", „Konzerninterner Datenverkehr", „Mailhoster", „Tracking" oder „Webhoster" auf. Die Behörden entscheiden selbst, worauf sie hierbei den Fokus legen. Zudem wird deutlich, dass das Augenmerk der Aufsichtsbehörden auch bei den regulären Prüfungen immer mehr auf dem Drittlandsdatentransfer liegt.

Ist Deutschland ein Einzelfall oder greift die Datenschutzaufsicht auch in anderen Ländern durch?
Hoegl: Die deutschen Aufsichtsbehörden vertreten grundsätzlich eine strenge Linie in Bezug auf Drittlandsdatentransfers und deren Überprüfung. Aber auch in anderen Ländern treiben die Aufsichtsbehörden die Kontrolle internationaler Datentransfers voran. Die Aufsichtsbehörden in Dänemark und Finnland haben beispielsweise angekündigt, die Übermittlung personenbezogener Daten in Drittländer durch eine Reihe von Unternehmen und Behörden intensiver zu überwachen und bereits Informationen zu den auf Grundlage der

„Schrems II"-Entscheidung ergriffenen Maßnahmen von diesen angefordert. Auch die Aufsichtsbehörden in Schweden haben bereits Untersuchungen gegen Unternehmen eingeleitet. Und die Aufsicht in Portugal hat einer staatlichen Behörde die Nutzung von Cloudflare aufgrund eines vermeintlich fehlenden angemessenen Schutzniveaus untersagt.

Welche Branchen sind besonders betroffen?
Hoegl: Bislang wurden keine Informationen dazu veröffentlicht, welche Brachen im Zusammenhang mit der länderübergreifenden Kontrolle der Datenübermittlungen besonders im Fokus stehen. Prinzipiell kann jedes Unternehmen aus jeder Branche Adressat einer solchen Prüfung werden. Allerdings reagieren die Aufsichtsbehörden immer noch vorrangig auf Beschwerden und Eingaben von Betroffenen. Daher kann man sagen, dass vor allem Branchen mit intensivem Kontakt zu Verbrauchern besonders „prüfungsgefährdet" sind.

> ***„Es gibt kaum praktisch umsetzbare Maßnahmen, die den Aufsichtsbehörden genügen."***

Was fordern die Datenschutzbehörden konkret von den Unternehmen hinsichtlich des Datentransfers in Drittländer wie die USA?
Hoegl: Die Fragebögen der Aufsichtsbehörden sind insgesamt sehr umfangreich und gehen in die Tiefe. Die Aufsichtsbehörden fragen neben den rein formalen Voraussetzungen (z.B. Nutzung der Standarddatenschutzklauseln) insbesondere ab, welche zusätzlichen technischen und organisatorischen Maßnahmen ergriffen werden, um ein „angemessenes Datenschutzniveau" zu gewährleisten. Und hier liegt auch das große Problem für die Unternehmen: Einerseits gibt es kaum praktisch umsetzbare Maßnahmen, die den Aufsichtsbehörden genügen. Und andererseits sind die Unternehmen hier auf ihre Dienstleister angewiesen, die Informationen oftmals nur zögerlich bereitstellen – nicht zuletzt, auch weil sie selbst wissen, dass die Maßnahmen den Behörden ohnehin nicht aureichen. Grundsätzlich wird von den Unternehmen verlangt, dass sie ihre Datenverarbeitungsvorgänge kennen, bereits neue Standarddatenschutzklauseln abgeschlossen haben oder bestehende Standardvertragsklauseln entsprechend ergänzt haben und dass sie die ensprechenden organisatorischen, vertraglichen und technischen Maßnahmen getroffen haben, um die personenbezogenen Daten bestmöglich zu schützen.

Welche Konsequenzen drohen Unternehmen, wenn sie keine DSGVO-konforme Datenübermittlung in die USA belegen können? Werden die rechtlich möglichen Geldbußen tatsächlich verhängt?
Hoegl: Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg, Stefan Brink, hat sich dahingehend ausgesprochen, dass die Prüfung zunächst dazu diene, das Gespräch mit den Unternehmen zu suchen. Man erwarte aber auch, dass die Unternehmen, die von der Drittstaatenproblematik betroffen sind, bereits ernsthaft nach tragfähigen Lösungen gesucht haben. Auch im Referat für den internationalen Datenverkehr beim Bayerischen Landesamt für Datenschutzaufsicht (BayLDA) hat man betont, dass die Entscheidung, ob es zu Geldbußen kommen wird, noch nicht feststehe, sondern vom Einzelfall abhängen wird. Entscheidend sei zunächst viel mehr, dass Unternehmen, die personenbezogene Daten in Drittländer übermitteln, ohne dabei die Anforderungen des „Schrems II"-Urteils und die Anforderungen der DSGVO umzusetzen, eine solche Übermittlung unverzüglich beenden müssen. Der Worstcase ist aber nach unserer Erfahrung gar nicht das mögliche Bußgeld. Das Bußgeld tut einmalig weh und die Verantwortlichen müssen sich ggfs. dann auch intern rechtfertigen. Viel schlimmer ist es aber, wenn die Aufsichtsbehörde eine bestimmte Verarbeitungstätigkeit bzw. die Nutzung von Tools untersagt, die unternehmenskritisch sind. Hierfür sollten Unternehmen also – gerade beim Einsatz internationaler Dienstleister – gewappnet sein und einen Plan B zumindest in der Schublade haben.

> ***„Unternehmen, die personenbezogene Daten in Drittländer übermitteln, ohne dabei die Anforderungen des ‚Schrems II'-Urteils und der DSGVO umzusetzen, müssen eine solche Übermittlung unverzüglich beenden."***

Wie viel Zeit haben betroffene Unternehmen, um auf die Forderungen der Datenschutzbehörden zu reagieren?
Hoegl: Die Frist zur Umsetzung der konkreten Forderungen der Datenschutzbehörden wird wohl je nach

Einzelfall variieren. Die Aufsichtsbehörden betonen aber auch, dass Unternehmen nun bereits ein Jahr lang Zeit hatten, um auf die Rechtslage nach dem „Schrems II"-Urteil zu reagieren. Die uns bekannten Umsetzungsfristen sind daher oftmals eher knappgehalten, gerade wenn man berücksichtigt, dass es sich oft um komplexe und kritische Verarbeitungstätigkeiten handelt.

Was raten Sie betroffenen Unternehmen, wie sie den DSGVO-Vorgaben zur Drittlandübermittlung gerecht werden?
Hoegl: Die Datenübermittlung in die USA und andere Drittländer ist unter bestimmten Voraussetzungen weiterhin möglich. Die Anforderungen sind allerdings sehr hoch. Unternehmen müssen einen bunten Strauß organisatorischer, vertraglicher und technischer Maßnahmen treffen, um den Vorgaben zur Drittlandsübermittlung gerecht zu werden. Unternehmen sollten intensiv ihren Einsatz von Dienstleistern mit Drittlandsbezug prüfen und falls erforderlich die entsprechenden Transfer Impact Assessments (= welche datenschutzrechtlichen Risiken und Konsequenzen hat der Drittlandstransfer?) durchführen. Falls möglich sollten Vereinbarungen zur ausschließlichen Datenverarbeitung in der EU getroffen werden. Zudem sollten ausreichende technische Maßnahmen ergriffen werden, wie eine weitestgehende Anonymisierung der Daten, eine ausreichende Transportverschlüsselung und die Verwendung sicherer Schlüssellängen und Chiffren gemäß der Empfehlungen des BSI.

> ***„Durch die bloße Vereinbarung der Standardvertragsklauseln kann noch kein gleichwertiges Datenschutzniveau geschaffen werden."***

Die Unternehmen sollten mit ihren Dienstleistern die neuen Standardvertragsklauseln abschließen oder bis zum Abschluss dieser eine Ergänzung der alten Standardvertragsklauseln vereinbaren, insbesondere im Hinblick auf Schadensersatzpflichten, Informationspflichten und Anfechtungspflichten. Zu beachten ist jedoch, dass durch die bloße Vereinbarung der Standardvertragsklauseln noch kein gleichwertiges Datenschutzniveau geschaffen werden kann. Die Standardvertragsklauseln können die Behörden im Empfängerland nicht binden, so dass auch bei ihrem Abschluss ein Zugriff auf die Daten und damit der Eingriff in die Rechte der Betroffenen nicht ausgeschlossen werden kann. Die Vertragsparteien müssen daher zwingend die vorstehend beschriebenen ergänzenden Maßnahmen ergreifen, um einen solchen Zugriff auszuschließen. Eine Datenübermittlung ist sonst nicht rechtssicher möglich.

Womit müssen Unternehmen bei dem Thema in Zukunft noch rechnen? Erwarten Sie intensivere Kontrollen der Datenschutzbehörden?
Hoegl: Es ist damit zu rechnen, dass die Aufsichtbehörden die Überprüfung der Drittlandsdatentransfers weiterhin ernst nehmen und die Prüfungen weiter ausdehnen. Nicht zuletzt gibt es auch eine ganze Reihe von Organisationen, die sich den Datenschutz auf die Fahne geschrieben haben und die ihrerseits die Behörden durch Beschwerden zum Handeln zwingen. Unternehmen sollten sich hierfür ausreichend vorbereiten und die weiteren Reaktionen der Aufsichtsbehörden und mögliche gerichtliche Entscheidungen genauestens beobachten.

> ***„Unternehmen sollten untersuchen, inwiefern ihre Dienstleister Überwachungsgesetzen in außereuropäischen Ländern unterliegen."***

Was empfehlen Sie Unternehmen, die noch nicht von der Datenschutzaufsicht angeschrieben wurden, aber Zweifel haben, ob sie durch den Einsatz von US-Cloud-Anbietern Datenschutzverstöße begehen?
Hoegl: Unternehmen sollten ihre Datenverarbeitungsvorgänge jetzt auf einen möglichen Drittlandsbezug hin überprüfen und sich vergewissern, dass sie die notwendigen Verträge, insbesondere Standardvertragsklauseln bzw. Standarddatenschutzklauseln abgeschlossen haben. Zudem sollten Unternehmen untersuchen, inwiefern ihre Dienstleister Überwachungsgesetzen in außereuropäischen Ländern unterliegen und welche weiteren Maßnahmen daher erforderlich sind. Aufgrund der weitreichenden technischen Fragen der Aufsichtsbehörden sollten Unternehmen kontrollieren, wo ihre Daten gespeichert werden und welche Verschlüsselung zum Einsatz kommt, einschließlich aller technischen Details wie verwendeter Protokolle, Chiffren und Schlüssellängen. Schließlich sollten Unternehmen einen „Notfallplan" für den Fall der Untersagung der Verarbeitung durch die Aufsichtsbehörden vorbereiten.