Herausforderungen der Digitalisierung – April 2021

// (US-)Dienstleister-Management

Lesezeit: 3 Minuten

Europäisches Datenschutzrecht stuft Länder außerhalb des EWR als unsicher ein. Personenbezogene Daten dürfen in diesen Ländern nur verarbeitet werden, wenn angemessene Garantien bestehen und sichergestellt ist, dass die personenbezogenen Daten dort sicher sind. Das betrifft viele US-Dienstleister, deren Dienste ganz selbstverständlicher Bestandteil der IT-Infrastruktur vieler Unternehmen sind, wie AWS, Microsoft, Mailchimp, Cisco und viele mehr. Den Einsatz dieser Dienste datenschutzkonform zu gestalten ist schwer. Verstöße sollen nun verstärkt ermittelt und sanktioniert werden. Lesen Sie, was Sie tun können, um Ihr Unternehmen darauf vorzubereiten.

Hintergrund

Mit der sogenannten Schrems II-Entscheidung (C-311/18) hat der EuGH das Privacy Shield Abkommen gekippt und damit ist eine wichtige Möglichkeit zur datenschutzkonformen Einbindung von US-Dienstleistern entfallen. Zudem hat der EuGH in Frage gestellt, ob personenbezogene Daten überhaupt noch in die USA übermittelt und von US-Dienstleistern verarbeitet werden dürfen. Hintergrund sind potentiell weitreichende Möglichkeiten von US-Behörden zum Zugriff auf diese personenbezogenen Daten. Im Ergebnis bleibt in Europa nur noch die Möglichkeit,

- sogenannte EU-Standardvertragsklauseln abzuschließen und
- zusätzliche technische- und organisatorische Garantien zu schaffen, die einen Zugriff von US-Behörden auf personenbezogene Daten möglichst ausschließen.

Deutsche Aufsichtsbehörden planen nun koordinierte Maßnahmen, um das zu überprüfen. Dafür wurden nach Auskunft des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (Professor Caspar) 5 Fragenkataloge entwickelt, die systematisch von den deutschen Aufsichtsbehörden an Unternehmen versandt werden sollen und von diesen zu beantworten sind. Die Fragenkataloge umfassen

- Tracking-Tools
- Mailhoster
- konzerninternen Datenverkehr
- zwei weitere Fragebögen

Die Aufsichtsbehörden gehen davon aus, dass es in diesen Bereichen möglich sei, auf US-Dienstleister zu verzichten. Darauf soll dann hingewirkt werden. Im Zweifel auch mit den Mitteln des Verwaltungszwangs. Bußgelder stehen aber offenbar (noch) nicht im Fokus.

Wie kann ich das Risiko meines Unternehmens verringern?

Deutsche Unternehmen sind gut beraten, zu prüfen, ob sie US-Dienstleister einsetzen und angemessene Maßnahmen dafür getroffen haben. Mit folgender Checkliste können Sie Ihre Risiken identifizieren und gezielt verringern.

/ **Werden US-Dienstleister eingesetzt?**

Machen Sie eine Risikoinventur und prüfen Sie, welche US-Dienstleister Sie einsetzen. Wichtig: auch wenn eine Verarbeitung durch den US-Dienstleister im EWR erfolgt, zum Beispiel das Hosting in einem europäischen Rechenzentrum, kann es zu relevanten Datenübermittlungen in die USA kommen.

/ **Kann auf den Einsatz der US-Dienstleister verzichtet werden?**

Die effizienteste Maßnahme zur Risikoverringerung ist es, auf den Einsatz von US- und anderen Drittstaaten-Dienstleistern zu verzichten. Prüfen Sie sorgfältig, ob es gleichwertige Alternativangebote von Dienstleistern im EWR gibt. Diese sollten Sie bevorzugen.

/ **Bestehen vertragliche Grundlagen für die Einbindung von US-Dienstleistern?**

Die Einbindung von US-Dienstleistern sollte nur auf der Basis angemessener (vertraglicher) Grundlagen geschehen. Das sind insbesondere die sogenannten EU-Standardvertragsklauseln. Bei der Beauftragung konzerninterner Dienstleister können zudem Binding Corporate Rules diese Funktion übernehmen. Prüfen Sie unbedingt, ob entsprechende Vereinbarungen bestehen.

/ **Bestehen zusätzliche technische- und organisatorische Garantien (sogenannte Supplementary Measures)?**

Über das Bestehen einer vertraglichen Grundlage hinaus müssen zusätzliche Garantien geschaffen werden, mit denen der Zugriff von US-Behörden auf personenbezogene Daten effektiv verhindert werden. Mit vertraglichen Zusicherungen allein können diese Garantien nicht geschaffen werden. Das gilt auch für sogenannte „Warrant Canaries“, mit denen sich Dienstleister zur Offenlegung von Behördenanfragen verpflichten. Vermeintlich sichere Garantien sind im Ergebnis wohl nur technische Maßnahmen wie Anonymisierung, Pseudonymisierung und Verschlüsselung, die das Auslesen der Information verhindern. Ob der konkrete Dienst mit diesen technischen Maßnahmen noch genutzt werden kann, muss individuell geprüft werden.

// Kanzlei

Digitalisierung ist eine Herausforderung für kleine und große Unternehmen. Wir sind überzeugt, dass eine flexible und spezialisierte Einheit wie **PLANIT** // LEGAL am besten in der Lage ist, den Bedürfnissen nationaler und internationaler Mandanten gerecht zu werden.

PLANIT // LEGAL bietet umfassende Beratung im deutschen und europäischen **IT- und Datenschutzrecht**, sowohl in der Rolle des **externen Datenschutzbeauftragten,** des **EU Vertreters, anwaltlichen Beraters** und in unterstützender Funktion für Rechts-, Datenschutz- und Compliance-Abteilungen.

Wir beraten Sie zu Softwarelizenzen, IT-Vergaben, E-Commerce-Recht, IT- und Datenschutz-Compliance sowie Datenschutz- und IT-Due-Diligence. Gemeinsam mit Ihnen entwickeln wir Lösungen, die für Ihr Unternehmen passen. Dabei gestalten wir IT- und Datenschutzverträge, unterstützen bei IT-Projekten und vertreten Ihre Interessen und Rechte in gerichtlichen oder aufsichtsbehördlichen Auseinandersetzungen.

Die Anwälte von **PLANIT** // LEGAL verfügen über **langjährige Beratungserfahrung** aus IT- und Datenschutzabteilungen internationaler Großkanzleien, im IT- und Datenschutzrecht spezialisierten kleineren Einheiten, ihrer Tätigkeit für Datenschutz-Aufsichtsbehörden und als betriebliche Datenschutzbeauftragte.

PLANIT // LEGAL hat ein **starkes Netzwerk** und arbeitet bei Bedarf eng mit Kollegen aus anderen Jurisdiktionen oder mit anderen Spezialisierungen zusammen.

Kontakt
PLANIT // LEGAL
Jungfernstieg 1
20095 Hamburg
mail@planit.legal
040 609 44 190