ITDSC UG
Data-Security-Consulting
www.itdsc.de

Informationen zum Thema Datenschutz

Liebe Leserin, lieber Leser,

Viele glauben inzwischen wären alle Fragen zu Datenübermittlungen in die USA geklärt, weiterer Aufwand zur Prüfung sei nicht mehr erforderlich. Das stimmt aber so nicht. Lesen Sie, was bisher wirklich in Richtung Datenschutzabkommen mit den USA passiert ist.

Aber auch die Aufsichtsbehörden unternehmen gegenwärtig besondere Anstrengungen, zum Beispiel bei Prüfungen zur Auftragsverarbeitung.

Lernen Sie die Hintergründe kennen, die zeigen, warum die Aufwände für den Datenschutz gerechtfertigt sind.

Ich wünsche Ihnen viel Spass beim Lesen.

Detlef Riese
Datenschutzbeauftragter

Der Weg zum Privacy Shield II

Datenübermittlungen in die USA sind für viele Unternehmen wichtiger denn je. Tragfähige Rechtsgrundlagen hierfür fehlen jedoch zum Teil. Gerade Praktiker warten deshalb dringend auf den „Privacy Shield II“. Lesen Sie, was es damit auf sich hat und wann dieser „Schild“ verfügbar sein könnte.

Angemessenheitsbeschluss heißt das Zauberwort

Die USA sind in der Sprache der Datenschutz-Grundverordnung (DSGVO) ein Drittland, also ein Land außerhalb des Geltungsbereichs der DSGVO. Datenübermittlungen dorthin sind zulässig, wenn die Europäische Kommission beschlossen hat, dass dort ein angemessenes Schutzniveau herrscht. Sobald ein solcher Beschluss vorliegt, bedürfen Datenübermittlungen keiner besonderen Genehmigung durch die Aufsichtsbehörden. So regelt es Art. 45 Abs. 1 DSGVO.

Mit dem Privacy Shield I war etwa vier Jahre lang alles gut

Eine solchen Beschluss der Europäischen Kommission gab es tatsächlich schon einmal. Er betraf den „Privacy Shield I“. Dabei handelte es sich um Datenschutzvorkehrungen, die zwischen der EU und den USA für Datenübermittlungen in die USA vereinbart worden waren. Mitte Juli 2016 fasste die Europäische Kommission auf ihrer Basis einen Angemessenheitsbeschluss. Er hielt fast auf den Tag genau vier Jahre. Am 16. Juli 2020 erklärte der Europäische Gerichtshof (EuGH) den Beschluss allerdings für nichtig. Das geschah durch das Urteil „Schrems II“.

Seit 2020 bemüht man sich um einen Privacy Shield II

Seither herrscht eine gewisse rechtliche Konfusion. Natürlich gibt es durchaus noch einige andere Rechtsgrundlagen für Datenübermittlungen in die USA, etwa eine Einwilligung des Betroffenen. Sie verursachen aber viel Aufwand und sind für eine Übermittlung von Daten vieler Personen praktisch fast nicht zu handhaben. Deshalb haben die USA und die EU nach der Entscheidung „Schrems II“ sofort damit begonnen, den für nichtig erklärten „Privacy Shield I“ durch einen „Privacy Shield II“ zu ersetzen. Diese Bemühungen sind jetzt in ein entscheidendes Stadium getreten.

Dem EuGH missfielen am Privacy Shield I zwei zentrale Punkte

Den EuGH störten am „Privacy Shield I“ vor allem zwei Dinge:

- Zum einen monierte er, dass die US-Geheimdienste nach dem Recht der USA in keiner Weise an den Grundsatz der Verhältnismäßigkeit gebunden sind, wenn sie personenbezogene Daten erheben.
- Zum anderen rügte er, dass Nicht-US-Bürger gemäß dem Recht der USA keinerlei Rechtsschutz gegen derartige Datenerhebungen hätten.

US-Präsident Biden hat mit einer Executive Order reagiert

Die USA haben sich vom Prinzip her bereit erklärt, diese beiden Schwachstellen zu beheben. Das ist nach dem Recht der USA allerdings gar nicht so einfach. Beschritten wurde der Weg, dass US-Präsident Biden am

07.10.2022 eine sogenannte „Executive Order“ erlassen hat. Dabei handelt es sich um eine verbindliche Anweisung des Präsidenten an alle US-Bundesbehörden. Damit gilt sie auch für alle US-Geheimdienste. Denn Geheimdienste gibt es in den USA nur auf Bundesebene.

Die Executive Order legt den Geheimdiensten gewisse Fesseln an

Bisher konnten die US-Geheimdienste selbst entscheiden, welche Maßnahmen zur Beschaffung und Auswertung von Daten sie für erforderlich hielten. Künftig müssen sie jedes Jahr im Voraus eine Art Rahmenplan erstellen. Er bedarf der Billigung durch den jeweiligen US-Präsidenten. Veröffentlicht wird er jedoch selbstverständlich nicht. Zugleich hat die Executive Order eine Institution eingerichtet, die sie als „Data Protection Review Court“ bezeichnet. Dieses „Gericht“ soll auch Nicht-US-Bürgern Rechtsschutz gewähren.

Jetzt ist die Europäische Kommission am Zug

Nun liegt der Ball, bildlich gesprochen, bei der Europäischen Kommission. Sie muss sich darüber einig werden, ob die getroffenen Maßnahmen der USA ausreichen, um einen Angemessenheitsbeschluss erlassen zu können. Erst wenn das geschehen ist, hat die Praxis wieder eine Rechtsgrundlage, die in ihrer Wirkung dem früheren Privacy Shield I entspricht. Die Diskussion darüber, ob ein solcher Angemessenheitsbeschluss möglich ist, läuft im Augenblick. Einbezogen sind dabei intern auch die Aufsichtsbehörden der EU-Mitgliedstaaten. Belastbare Ergebnisse sind noch nicht bekannt.

Möglicherweise gibt es im April 2023 den Durchbruch

Selbstverständlich gibt es Stimmen, die den jetzt gewählten Lösungsansatz kritisieren. Mit an der Spitze steht dabei Herr Schrems, Rechtsanwalt in Österreich, nach dem gleich zwei EuGH-Urteile benannt sind. In Brüssel ist zu hören, dass man sich bis etwa April 2023 einen Angemessenheitsbeschluss zutraut. Die Praktiker in den Unternehmen wären mit Sicherheit begeistert, wenn dies gelingen würde.

Auftragsverarbeitung im Fokus der Datenschutz-Aufsicht

Kommen externe Dienstleister ins Spiel, kann eine Auftragsverarbeitung vorliegen. Lesen Sie, warum dieses Thema gerade jetzt besonders aktuell ist.

Ausgangspunkt sind Webhosting-Verträge

Ohne Internetseite kommt heute kein Unternehmen mehr aus. Zahlreiche Unternehmen haben außerdem einen Online-Shop. Gerade während Corona haben sich Online-Shops vielfach als unentbehrlich erwiesen. Um Webseiten und Online-Shops professionell betreiben zu können, wird in aller Regel ein externer Dienstleister eingeschaltet, also ein Webhoster. Er arbeitet auf der Basis eines Webhosting-Vertrags.

Webhosting ist Auftragsverarbeitung

Dass Webhosting eine Auftragsverarbeitung im Sinn der DSGVO darstellt, ist allgemeine Meinung. Denn der Auftraggeber macht dem Webbrowser genaue Vorgaben dafür, wie seine Internetseite oder sein Online-Shop betrieben werden sollen. In der Sprache des Datenschutzrechts handelt es sich dabei um Weisungen des Auftraggebers an den Auftragsverarbeiter.

Die Aufsichtsbehörden sind vielfach unzufrieden

Die Datenschutz-Aufsichtsbehörden haben prinzipiell nichts gegen Auftragsverarbeitung. Allerdings rügen sie häufig, dass aus ihrer Sicht in den Verträgen über die Auftragsverarbeitung wichtige Details fehlen. Außerdem beanstanden sie immer wieder, dass zwar von der Papierform her alles korrekt wirkt, es aber an einer ausreichenden praktischen Umsetzung der vertraglichen Regelungen fehlt.

Sie führen deshalb eine gemeinsame Prüfaktion durch

Ob die Kritik der Aufsichtsbehörden immer wirklich berechtigt ist, kann dahinstehen. Viel entscheidender ist, dass gleich sechs Aufsichtsbehörden vereinbart haben, das Thema „Auftragsverarbeitung beim Webhosting“ gemeinsam aufzugreifen. Dabei handelt es sich um die Aufsichtsbehörden von Bayern, Berlin, Niedersachsen, Rheinland-Pfalz, Sachsen und Sachsen-Anhalt. Seit Mitte 2022 führen sie eine sogenannte koordinierte Prüfung durch. Dies bedeutet, dass sie eine gemeinsame Checkliste entwickelt haben. Auf ihrer Basis treten sie an Unternehmen heran und stellen eingehende Fragen.

Unternehmen dürfen Anfragen nicht ignorieren

Die beteiligten Aufsichtsbehörden schreiben eine große Zahl von Unternehmen an und fordern sie auf, zunächst einen umfassenden Fragebogen auszufüllen. Dies löst beträchtlichen Aufwand aus. Viele Fragen lassen sich nicht sorgfältig beantworten, ohne vorher die Abläufe im Unternehmen umfassend durchzugehen. Dies berührt dann oft auch Abteilungen, die beispielsweise mit dem Online-Shop an sich unmittelbar nichts zu tun haben. Es geht aber nicht anders. Denn ein Unternehmen, das Fragen unvollständig oder sogar falsch beantwortet, riskiert eine Geldbuße.

Die Prüfaktion hat so etwas wie Fernwirkungen

Jedem Fachmann ist klar: Falls die Prüfaktion zum Webhosting aus der Sicht der Aufsichtsbehörden relevante Erkenntnisse bringt, werden ähnliche Prüfaktionen folgen. Dabei wird es jeweils um unterschiedliche Formen der Auftragsverarbeitung gehen. Das ist der Grund dafür, warum das Thema Auftragsverarbeitung insgesamt momentan einige Wellen schlägt.

Ohne Vertrag ist Auftragsverarbeitung nicht erlaubt

Gar nicht selten kommt es vor, dass eine Auftragsverarbeitung vorliegt und auch ein zuverlässiger Auftragsverarbeiter als Dienstleister tätig ist. Einen schriftlichen Vertrag gibt es allerdings nicht. Man meint vielmehr, entsprechende Auftragsscheine und Abrechnungen würden ausreichen. Das sieht die DSGVO allerdings anders:

1. Sie legt fest, dass ein ausdrücklicher Vertrag nötig ist.
2. Sie macht genaue Vorgaben zu seinem Inhalt.
3. Sie fordert einen dokumentierten Vertragstext (schriftlich oder elektronisch).

Das Thema „Unterauftrag“ verlangt besondere Aufmerksamkeit

Beim Thema „Unterauftrag“ ist die DSGVO ebenso klar und eindeutig. Sie legt fest, dass ein Auftragsverarbeiter nur dann einen weiteren Auftragsverarbeiter einschalten darf, wenn der Auftraggeber dies schriftlich genehmigt hat. Hier geht es also nicht ohne Schriftform. Manchmal liegt ein Vertrag vor, der Unteraufträge nicht vorsieht. Dann entsteht aber trotzdem kurzfristig der Bedarf, einen Unterauftragnehmer einzuschalten. Der Vertrag muss deshalb nicht unbedingt geändert werden. Nötig ist dann aber jedenfalls eine schriftliche Erlaubnis.

Bitte bleiben Sie geduldig

Nachfragen zum Thema Auftragsverarbeitung können durchaus nerven, vor allem wenn gerade viel los ist. Angesichts der Aktionen der Aufsichtsbehörden haben sie allerdings gute Gründe. Deshalb kooperieren Sie bitte.

Impressum

Detlef Riese (ITDSC UG)
Datenschutzbeauftragter
Anschrift:
ITDSC UG • Bethanienstrasse 8 • 03172 Guben
Telefon: 03561 5595574 • E-Mail: d.riese@itdsc.de