Dr. Martin Bahr

Die praktischen Konsequenzen des Wegfalls des EU-Privacy-Shields

Der EuGH hat gesprochen: **Eine Datenverarbeitung in den USA ist verboten!**[1]
Die Entscheidung des Gerichts hat Datenschützer in letzter Konsequenz nicht wirklich überrascht, denn bereits das Vorgängerabkommen, nämlich Safe Harbour, wurde vor einigen Jahren als rechtswidrig eingestuft. Was aber die meisten überraschte, war der konsequente Ausspruch des Gerichts. Denn die Robenträger machten klar, dass die neue Rechtslage ab sofort gilt und es keinerlei Übergangszeiträume gibt.
Der Artikel gibt Ihnen anhand einer konkreten Checkliste eine praktische Hilfestellung bei Umsetzung der notwendigen Anpassungen.

DER AUTOR

Die **Kanzlei Dr. Bahr** (*http://www.Dr-Bahr.com*) ist auf den Bereich des Rechts der Neuen Medien und den gewerblichen Rechtsschutz (Marken-, Urheber- und Wettbewerbsrecht) spezialisiert. Unter *Suchmaschinen-und-Recht.de* betreibt sie seit 2005 ein eigenes Themenportal zur rechtlichen Dimension von Suchmaschinen.

A. Die Entscheidung

Vermutlich haben Sie bereits an anderer Stelle, zum Beispiel im Internet, über die Entscheidung des Europäischen Gerichtshofs (EuGH) irgendetwas einmal gelesen. Daher wollen wir das Urteil nur noch einmal sehr kurz zusammenfassen.

Die DSGVO bestimmt, dass eine Datenverarbeitung außerhalb der Europäischen Union nur dann erlaubt ist, wenn in dem betreffenden Land auch eine ausreichende Datensicherheit gewährleistet ist.

In der betreffenden Entscheidung ging es um die Datenverarbeitung durch Facebook, das in den USA sitzt. Der EuGH entschied nun, dass eine solche Datenverarbeitung in den USA grundsätzlich nicht möglich ist, da durch die umfangreichen Zugriffsmöglichkeiten der amerikanischen Behörden der Datenschutz für Europäer nicht mehr gewährleistet ist. Dabei differenzierte das Gericht zwischen zwei Arten: dem sogenannten EU-Privacy-Shield und den sogenannten EU-Standardvertragsklauseln.

Das EU-Privacy-Shield stuften die Richter als rechtswidrig und somit nichtig ein. Bei den EU- Standardvertragsklauseln hingegen räumten die Robenträger die Möglichkeit ein, dass eine Datenverarbeitung noch erlaubt sei, wenn die Datensicherheit gegeben sei. Die Richter ließen dabei offen, wie denn nun ein Anbieter diese Sicherheit gewährleisten kann.

Foto: AndreyPopov / gettyimages.de

[1] EuGH, Urt. v. 16.07.2020 – Az.: C -311/18.
[2] FAQ des Europäischen Datenausschusses: *https://bit.ly/2Rrdt51*.
Stellungnahme der deutschen Datenschutzkonferenz: *https://bit.ly/2GThhdg*.

B. Die praktischen Konsequenzen

Auch wenn die Entscheidung erst wenige Wochen alt ist, hat sie inzwischen sowohl in der Offline- als auch in der Online-Welt für viel Furore und Aufsehen gesorgt. Und dies ist auch kein Wunder, weil der Richterspruch nichts anderes bedeutet, als dass jede Datenverarbeitung außerhalb der EU mit drei Fragezeichen zu versehen ist. Dies gilt insbesondere für die USA, wo aktuell faktisch keine hinreichend sichere Datenverarbeitung möglich ist.

1. Reichweite der Entscheidung:

Die Entscheidung betrifft zwar formal nur die Datenverarbeitung in den USA, kann aber auf jede Datenverarbeitung außerhalb der Europäischen Union verallgemeinert werden. Die Grundsätze, die die Richter hier aufgestellt haben, müssen somit immer von Ihnen beachtet werden, wenn Sie eine Verarbeitung außerhalb von Europa durchführen. Sowohl die europäischen als auch die deutschen Datenschutzbehörden haben bereits erste Stellungnahmen veröffentlicht.[2]

Teilweise wird auch die Ansicht vertreten, dass das Urteil des EuGH gar nicht so schlimm sei, weil er doch nur das EU-Shield für unwirksam erachtet habe, bei den Standardvertragsklauseln jedoch dies gerade nicht getan habe.

Um es deutlich zu sagen: Eine solche Interpretation ist inhaltlich grundlegend falsch. Sowohl die europäischen als auch die deutschen Datenschutzbehörden haben inzwischen klargemacht, dass ein Rückgriff auf andere Möglichkeiten faktisch ausgeschlossen ist. Bei allen Alternativen (z. B. Einwilligung oder Standardvertragsklauseln) tritt nämlich die gleiche Problematik auf, die zur Unwirksamkeit des EU-Privacy-Shields geführt hat.

So hat bereits der Landesbeauftragte von Baden-Württemberg dazu Stellung genommen:[3]

> „Eine Übermittlung auf Grundlage von Standardvertragsklauseln ist zwar denkbar, wird die Anforderungen, die der EuGH an ein wirksames Schutzniveau gestellt hat, jedoch nur in seltenen Fällen erfüllen:
> Der Verantwortliche muss hier zusätzliche Garantien bieten, die einen Zugriff durch die US-amerikanischen Geheimdienste effektiv verhindern und so die Rechte der betroffenen Personen schützen; dies wäre in folgenden Fällen denkbar:
> » Verschlüsselung, bei der nur der Datenexporteur den Schlüssel hat und die auch von US-Diensten nicht gebrochen werden kann
> » Anonymisierung oder Pseudonymisierung, bei der nur der Datenexporteur die Zuordnung vornehmen kann“

Baden-Württemberg bietet – bislang als einziges Bundesland – eine praxisbezogene Orientierungshilfe nach Wegfall des EU-Privacy-Shields an.

2. Nicht betroffene Länder:

Zu bestimmten Nicht-EU-Ländern hat Europa einen sogenannten Angemessenheitsbeschluss getroffen, sodass gesetzlich angenommen wird, dass in diesen Ländern die ausreichende Datensicherheit gewährleistet ist. Zu diesen Ländern gehören aktuell: Andorra, Argentinien, Färöer-Inseln, Guernsey, Israel, Isle of Man, Jersey, Japan, Kanada, Neuseeland, Schweiz und Uruguay.[5]

Liegt Ihr Datenverarbeiter in einem dieser genannten Länder, müssen Sie sich keine weiteren Sorgen hinsichtlich der Datensicherheit machen, sondern können sich locker zurücklehnen.

C. Wie soll ich mich nun am besten verhalten?

1. Don´t Panic!

Es ist auf keinen Fall angebracht, in Hektik zu verfallen, sondern bleiben Sie ruhig und gelassen. Nehmen Sie nicht vorschnell Handlungen vor, sondern bewerten Sie die aktuelle Lage ruhig und mit Augenmaß.

Auch hier gilt der alte Spruch: DON‘T PANIC!

2. Überprüfung der eigenen Datenverarbeitung

Überprüfen Sie zunächst, in welchem Umfang in Ihrem Unternehmen überhaupt eine Datenverarbeitung im EU-Ausland gegeben ist. Stellen Sie noch einmal kritisch alle Verarbeitungsvorgänge auf den Prüfstand.

Beachten Sie dabei insbesondere auch, ob und inwieweit von Ihnen beauftragte Dritte (z. B. Ihr Webhoster oder Ihre E-Mail-Agentur) auf ausländische Anbieter zurückgreifen. In der Praxis wird dieser Punkt sehr häufig übersehen und es findet nur eine Prüfung bei Ihnen selbst statt. Sobald Sie jedoch Ressourcen von Dritten einsetzen, sind Sie dafür verantwortlich, dass auch diese Dritten rechtskonform handeln.

3. Existieren Alternativen?

Sollten Sie nach Ihrem Check zu dem Ergebnis kommen, dass bei Ihnen eine Datenverarbeitung im EU-Ausland stattfindet, analysieren Sie, ob es eine angemessene und praktikable Alternative gibt, bei der eine Verarbeitung innerhalb der EU erfolgt.

Ja, ich weiß, was Sie jetzt sagen werden: In sehr vielen Fällen gibt es keine adäquate Lösung, sondern man ist auf den amerikanischen Anbieter angewiesen. Das ist uns auch klar.
In der anwaltlichen Praxis kommt es jedoch nicht selten vor, dass hier Mandanten vorschnell die Flinte ins Korn

[3] Nachzulesen unter *https://bit.ly/2ZUnOLJ*.
[4] Die Orientierungshilfe gibt es hier: *https://bit.ly/32sVK3B*.
[5] Die jeweils aktuelle Liste findet sich unter *https://bit.ly/3keTbIv*.
[6] Siehe dazu die Pressemitteilung: *https://bit.ly/35E6jTA*.

schmeißen und behaupten, es existierten keine vergleichbaren Dienstleister.

Überdenken Sie daher bitte noch einmal ganz genau, ob Sie tatsächlich auf den jeweiligen Dienstleister angewiesen sind. Benutzen Sie beispielsweise nur alle drei Jahre ein Feature, dass es nur bei diesem Anbieter gibt, dürften Sie in der Praxis in aller Regel verschmerzen können, wenn Sie wechseln.

4. Was ist, wenn keine Alternativen existieren?

Sollten Sie bei der Überprüfung letzten Endes zu dem Ergebnis kommen, dass ein bestimmter US-Dienstleister für Sie unverzichtbar ist, empfehlen wir Folgendes:

Seien Sie sich bewusst, dass Sie datenschutzrechtlich angreifbar sind. Gefahr droht sowohl aus Richtung der Aufsichtsbehörden als auch aus Sicht einzelner User bzw. Mitbewerber. Dies gilt insbesondere dann, wenn Sie eine exponierte Webseite oder einen umstrittenen Dienst betreiben. So haben beispielsweise die deutschen Datenschutzbehörden im August 2020 bereits angekündigt, bundesweit eine Kontrolle von Tracking-Technologien auf Webseiten durchzuführen.[6]

Überprüfen Sie daher noch einmal, ob das von Ihnen eingegangene Risiko in einem angemessenen (wirtschaftlichen) Verhältnis zu dem Mehrgewinn steht, den Sie durch den Einsatz dieser spezifischen Tools erreichen.

In jedem Fall ist es notwendig, dass Sie umfangreich dokumentieren, warum Sie speziell auf diese Software angewiesen sind und welche Maßnahmen (z. B. Anonymisierung oder Verschlüsselung) Sie unternommen haben, um sich so weit wie möglich rechtskonform zu verhalten.

Der Datenschutzbeauftragte von Baden-Württemberg hat dies anschaulich in seiner Orientierungshilfe wie folgt formuliert:[7]

> „Wenn Sie uns nicht davon überzeugen können, dass der von Ihnen genutzte Dienstleister/Vertragspartner mit Transferproblematik kurz- und mittelfristig unersetzlich ist durch einen zumutbaren Dienstleister/Vertragspartner ohne Transferproblematik, dann wird der Datentransfer […]untersagt werden.
>
> Uns ist bewusst, dass mit dem Urteil des EuGH u. U. extreme Belastungen für einzelne Unternehmen einhergehen können. Der LfDI wird sein weiteres Vorgehen am Grundsatz der Verhältnismäßigkeit ausrichten. Wir werden die Entwicklung weiter beobachten und unsere Positionen dementsprechend laufend überprüfen und fortentwickeln."

Es ist daher dringend anzuraten, dass Sie alle Ihre Überlegungen schriftlich in einer Pro-und-Contra-Liste festhalten, die Sie im Zweifelsfall der Behörde vorlegen können.

Bitte beachten Sie auch, dass nicht jede Landesdatenschutzbehörde so verständig wie die aus Baden-Württemberg ist. Die Berliner Datenschutzbeauftragte beispielsweise hat unmissverständlich zum Ausdruck gebracht, dass Unternehmen umgehend zwingend auf EU-Anbieter wechseln müssen, andernfalls dürften Bußgelder und Schadensersatzforderungen drohen.[8]

Bereits heute ist absehbar, dass sich das Rechtsgefälle in den einzelnen Bundesländern bzw. EU-Ländern durch diese aktuelle Entwicklung noch verstärken wird. ¶

CHECKLISTE

Unsere praktischen Handlungsempfehlungen sind:

1. Don´t Panic!
Es ist auf keinen Fall angebracht, in Hektik zu verfallen, sondern bleiben Sie ruhig und gelassen. Nehmen Sie nicht vorschnell Handlungen vor, sondern bewerten Sie die aktuelle Lage ruhig und mit Augenmaß. Die EuGH-Entscheidung betrifft nicht nur Sie allein. Die gesamte europäische Internet-Branche steht vor diesem Scherbenhaufen.

2. Kontrollieren Sie Ihre Datenverarbeitungsvorgänge!
Überprüfen Sie Ihre sämtlichen Datenverarbeitungsvorgänge. Achten Sie dabei insbesondere darauf, dass Sie auch die Verarbeitung bei den von Ihnen beauftragten Dienstleistern miteinbeziehen.

3. Existieren Alternativen?
Überprüfen Sie noch einmal, ob Sie tatsächlich zwingend auf solche Anbieter angewiesen sind, die eine Datenverarbeitung außerhalb der EU voraussetzen. Wenn es hier für Sie angemessene und praktikable Alternativen gibt, sollten Sie dorthin wechseln.

4. Wenn keine Alternativen existieren
Seien Sie sich bewusst, dass Sie datenschutzrechtlich angreifbar sind. Überprüfen Sie, ob das von Ihnen eingegangene Risiko in einem angemessenen (wirtschaftlichen) Verhältnis zu dem erlangten Nutzen steht. Schauen Sie sich insbesondere auch die Orientierungshilfe des Datenschutzbeauftragten aus Baden-Württemberg hierzu an.
Dokumentieren Sie sämtliche Abwägungen schriftlich, sodass Sie diese jederzeit der Aufsichtsbehörde vorlegen können.

[7] *https://bit.ly/3hyjOkQ.*
[8] Pressemitteilung der Berliner Datenschutzbeauftragten: *https://bit.ly/2GV3iDO.*