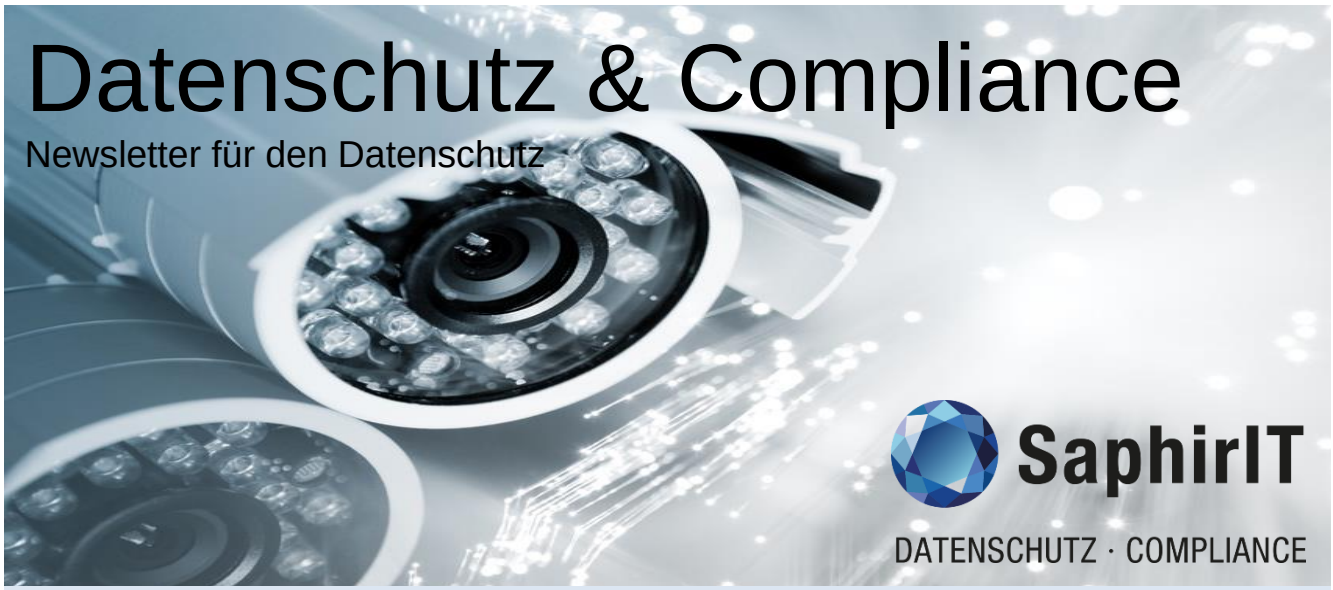

Ausgabe Juli 2020 | Seite 169 - 175

INHALT

Sehr geehrte Damen und Herren,

hiermit übersenden wir Ihnen unseren Newsletter Juli 2020.

Viel Spaß bei der Lektüre. Bei Fragen oder Anmerkungen sprechen Sie uns gerne an.

Mit freundlichen Grüßen
Ihre SaphirIT GmbH

Aus für das Privacy Shield – Ist eine datenschutzkonforme Datenübertragung in die USA noch möglich?

Mit Urteil vom 16.07.2020 hat der Europäische Gerichtshof (EuGH) im Verfahren zwischen der irischen Datenschutzaufsichtsbehörde, dem Juristen Max Schrems und Facebook ein Urteil gesprochen.

Das Urteil hat erhebliche Auswirkungen auf den Datentransfer in die USA und andere Drittländer.

Das bislang geltende EU-US Privacy Shield (Nachfolger des bereits für ungültig erklärten Safe Harbor Abkommens), wurde vom EuGH

gekippt. Auch trifft der EuGH Aussagen zu den sog. Standardvertragsklauseln und trifft Aussagen wann und wie diese rechtskonform verwendet werden können.

Ein Datentransfer in Drittländer (Länder außerhalb der EU) war schon in der Vergangenheit rechtlich nicht unproblematisch.

Die Datenschutzgrundverordnung (DSGVO) schreibt für eine rechtmäßige Datenübermittlung in Drittländer zusätzliche Voraussetzungen vor, um das Niveau des europäischen Datenschutzes zu gewährleisten.

Die relevantesten Garantien zur Herstellung eines „angemessenen Datenschutzniveaus“ (Art. 44ff DSGVO) sind derzeit Standardvertragsklauseln (SCCs), Binding Corporate Rules (BCRs) und das EU-US Privacy Shield.

Standardvertragsklauseln (SCCs)

SCCs sind spezielle, von der EU-Kommission zur Verfügung gestellte, „Musterverträge“ die zwischen dem datenexportierendem Unternehmen und dem datenimportierendem Unternehmen geschlossen werden können. Die Vorlagen der EU-Kommission müssen im Wesentlichen übernommen werden, um so ein angemessenes Datenschutzniveau zu gewährleisten. Die Verträge sind meist viele hunderte Seiten lang und enthalten viele Vorgaben die erfüllt werden müssen, damit ein rechtmäßiger Datentransfer stattfinden kann.

Binding Corporate Rules (BCRs)

Bei BCRs handelt es sich dagegen nicht um von der EU-Kommission vorgegebene Verträge, sondern um individuell zwischen den Unternehmen getroffene Regelungen, die ein entsprechendes Genehmigungsverfahren durchlaufen müssen. Dies ist meist mit einem erheblichen Zeitaufwand verbunden und auch diese Regelungen müssen viele spezielle Voraussetzungen zum Schutze personenbezogener Daten enthalten.

EU-US Privacy Shield

Die SCCs und BCRs gelten für alle Drittländer. Beim EU-US Privacy Shield handelt es sich dagegen um eine konkrete Absprache zwischen den USA und der EU. Das EU-US Privacy Shield enthielt einige Zugeständnisse auf Seiten der USA worauf die EU im Gegenzug einen eingeschränkten Angemessenheitsbeschluss erließ. Unternehmen, die sich den Regelungen des Privacy Shields unterworfen hatten, konnten eine Datenübertragung bis zum jetzt ergangenen Urteil auf das Privacy Shield stützen, auch wenn die Rechtmäßigkeit einer Datenübertragung auf dieser Grundlage nie unumstritten war.

Bereits in unserem Newsletter vom Juni 2018 hatten wir die Rechtmäßigkeit des Privacy Shields stark bezweifelt (abrufbar unter: https://www.saphirit.de/uploads/tx_hklistpdfs/Newsletter_Juni_2018.pdf).

Ausgangspunkt der ganzen Diskussion ist einmal mehr der Datentransfer von Facebook zwischen den USA und Europa. Nachdem das Safe Harbor Abkommen (Vorgänger des EU-US Privacy Shields) bereits vor einigen Jahren vom EuGH gekippt wurde, war Facebook der Auffassung, sie hätten ohnehin auch

Standardvertragsklauseln unterschrieben, sodass das Urteil für sie nicht von Relevanz gewesen wäre.

Der Kläger Max Schrems stellte seine Beschwerde daraufhin um und machte nunmehr Mängel in den Standardvertragsklauseln geltend. Ein angemessenes Datenschutzniveau bestehe nicht.

Facebook äußerte sich dahingehend, dass sich schon aus den Regelungen des EU-US-Privacy Shields ergebe, dass ein Konflikt zwischen den Überwachungsgesetzen der USA und den europäischen Grundrechten nicht bestehe.

Der irische High Court legte dem EuGH schließlich einige Fragen zur Klärung vor. Unter anderem sollte über die Rechtmäßigkeit von Standardvertragsklauseln und der allgemeinen Auswirkungen der US-amerikanischen Überwachungsgesetze auf das Datenschutzniveau entschieden werden.

Der EU-Generalanwalt kam in seinen Schlussanträgen im Wesentlichen zu dem Ergebnis, dass keine grundsätzlichen Bedenken gegen die Verwendung von Standardvertragsklauseln bestünden. Auch schlug er dem EuGH vor, dass die Frage nach der Wirksamkeit des EU-US-Privacy Shields in dem betreffenden Verfahren nicht entschieden werde müsse.

Häufig schließt sich der EuGH den Schlussanträgen des Generalanwalts an bzw. folgt diesen in weiten Teilen. Nicht so in diesem Fall.

Das Urteil des EuGHs

Der EuGH stellt in wenigen Sätzen die Unwirksamkeit des EU-US Privacy Shields fest. Der Angemessenheitsbeschluss sei „ungültig“.

Daneben stellt er fest, dass es keine Anhaltspunkte für eine grundsätzliche Unwirksamkeit der Standardvertragsklauseln gebe. Es habe sich „nichts ergeben, was seine Gültigkeit berühren könnte“.

Dennoch stellt der EuGH weiter fest, dass beim Abschluss von Standardvertragsklauseln im Einzelfall geprüft werden müsse, ob die nationale Gesetzgebung eine angemessene Sicherheit im Hinblick auf die abgeschlossenen Standardvertragsklauseln biete.

Auswirkungen für Unternehmen

Relevanz hat das Urteil für alle Unternehmen, die Daten speziell in die USA, aber auch in andere Drittländer übermitteln. Sowohl Unternehmen, die ihre Datenübertragung auf das Privacy Shield gestützt haben, als auch Unternehmen, die Standardvertragsklauseln geschlossen haben müssen ihre Datenübermittlung neu bewerten.

Jedwede Datenübermittlung auf Grundlage des EU-US Privacy Shields ist ab sofort rechtswidrig. Beim Einsatz von Standardvertragsklauseln müssten Unternehmen nach dem Urteil in jedem Einzelfall prüfen, ob ein Adressat im Drittland anhand der örtlichen Gegebenheiten überhaupt in der Lage ist die Pflichten aus den SCCs einzuhalten.

Bestehende SCCs sind an die neue Rechtsgrundlage anzupassen!

Für Unternehmen bedeutet der Beschluss absolute Rechtsunsicherheit. Es ist fraglich inwieweit aufgrund der erweiterten Vorgaben zur Überprüfung von SCCs eine Datenübertragung aufgrund von SCCs überhaupt noch möglich ist. Es besteht derzeit ein erhöhtes Risiko, dass die Datenübertragung in Drittländer auf einer nicht gesicherten Rechtsgrundlage beruht.

Zu prüfen ist im Einzelfall, ob eine Rechtmäßigkeit der Datenübertragung auf die Auffangvorschrift des Art. 49 DSGVO gestützt werden kann.

Ob und inwiefern Aufsichtsbehörden diesbezüglich jetzt schon tätig werden ist noch nicht abzusehen. Zeitnah wird dies aber der Fall sein. Dann kann bei einer Datenübertragung in die USA, ohne ausreichenden Schutz, ein hohes Bußgeld verhängt werden. Möglicherweise gibt es aber auch noch ein Moratorium, wie es dies nach dem Safe Harbor Urteil gab.

Unternehmen sollten diesbezüglich prüfen, ob und inwieweit ein mögliches Bußgeld von der D&O Versicherung abgedeckt wäre, oder ob ggf. zusätzliche Maßnahmen ergriffen werden müssen.

Insbesondere Unternehmen, die ihre Datenübertragung in die USA ausschließlich auf das EU-US Privacy Shield gestützt haben, sollten mit den Datenempfängern kurzfristig Standardvertragsklauseln schließen, um eine Datenübertragung zumindest nicht auf einen gekippten Angemessenheitsbeschluss zu stützen.

Mittelfristig sollte sich dann Gedanken gemacht werden, inwieweit es vielleicht sinnvoll ist „Binding Corporate Rules“ abzuschließen, um trotz des hohen Zeit- und Kostenaufwands einen bestmöglich gesicherten Datentransfer zu ermöglichen.

Es wird sich zeigen wie die europäischen und auch die deutschen Aufsichtsbehörden sich zu dieser Problematik positionieren werden und wie sie sich äußern, welche Maßnahmen zu treffen sein werden.

Aufsichtsbehörde hält Microsoft Teams für rechtswidrig

Bereits in unserer Spezialausgabe Mai 2020 (abrufbar unter: https://www.saphirit.de/newsletter-flyer.html) sind wir auf die momentan aus datenschutzrechtlicher Sicht rechtskonformen bzw. rechtswidrigen Videokonferenzprogramme eingegangen.

Bereits dort hatten wir geschildert, dass eine Verwendung von Microsoft Teams nur auf Grundlage des umstrittenen EU-US Privacy Shields möglich sei. Dies hat sich mit dem oben dargestellten Urteil des Europäischen Gerichtshofs (EuGH) geändert. Da das Privacy Shield für ungültig erklärt wurde, ist eine Nut-

zung von Videokonferenzsystemen wie Microsoft Teams noch problematischer geworden.

Die Berliner Aufsichtsbehörde hat sich in einer Stellungnahme vor Ergehen des Urteils durch den EuGH bereits kritisch mit der Verwendung von Videokonferenztools auseinandergesetzt.

Nach ihrer Ansicht ist nicht nur die Nutzung von Microsoft Teams, Skype (for Business), GoTo-Meeting, sondern ebenso die Nutzung von WebEx, GoogleMeet oder Zoom nicht datenschutzkonform.

Eine Rechtskonformität könne ausschließlich bei europäisch angebotenen Lösungen angenommen werden.

Die Stellungnahme können Sie unter:

https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BlnBDI-Hinweise_Berliner_Verantwortliche_zu_Anbietern_Videokonferenz-Dienste.pdf

abrufen.

Kritikpunkte der Aufsichtsbehörde an der Datenverarbeitung von Microsoft Teams sind unter anderem:

- Microsoft behalte sich in ihrer Auftragsverarbeitungsvereinbarung vor Auftragsdaten zu eigenen Zwecken zu verarbeiten;
- Auch erfülle die verwendete Auftragsverarbeitungsvereinbarung nicht die gesetzlichen Mindestanforderungen des Art. 28 Datenschutzgrundverordnung (DSGVO);
- Des Weiteren rügt die Aufsichtsbehörde, Microsoft habe ihre Auftragsverarbeitungsvereinbarung ohne Mitteilung der Betroffenen nachträglich, ohne dass Einholen einer Einwilligung geändert.

Einordnung der Kritik

Bei der Kritik handelt es sich erst einmal um die einzelne Meinung einer einzigen Aufsichtsbehörde. Höchstrichterliche Rechtsprechung gibt es zu der aufgeworfenen Kritik noch nicht.

Insbesondere im Hinblick auf das gerade ergangene Urteil des EuGHs sollte jedoch von einer Verwendung von Microsoft Teams bis auf Weiteres abgesehen werden.

Europäische Anbieter zu verwenden erscheint im Moment die datenschutzrechtlich sauberste Lösung zu sein.

Es bleibt aber, wie in vielen Sachen, auch hier abzuwarten wie sich die Lage entwickelt und wie sich auch andere Aufsichtsbehörden hierzu positionieren.

Bundesverfassungsgericht zum Zugriff auf Handydaten bei Ermittlungen

Das Bundesverfassungsgericht hat mehrere Regelungen zur sog. Bestandsdatenauskunft für rechtswidrig erklärt.

Die bisherigen Regelungen stellten einen Verstoß gegen das Grundrecht auf informationelle Selbstbestimmung dar und verletzten das Telekommunikationsgeheimnis. Dies sei unverhältnismäßig.

Bis Ende 2021 müssen das Telekommunikationsgesetz sowie andere hiervon betroffene Regelungen überarbeitet werden.

Die Richter stellten fest, dass eine Auskunft über Bestandsdaten (u.a. Name, Geburtsdatum, etc.) grundsätzlich zulässig sei. Diese läuft meist automatisch über die Bundesnetzagentur ab. Aber auch bei Providern, Krankenhäusern oder Hotels werden Daten erfragt (sog. manuelle Bestandsdatenauskunft).

Beispielsweise können Sicherheitsbehörden so bei einem Telekommunikationsunternehmen Informationen darüber bekommen, wer Inhaber eines bestimmten Telefonanschlusses ist.

Voraussetzung zur Abfrage von Bestandsdaten sei, so das Bundesverfassungsgericht, das Vorliegen einer konkreten Gefahr und eines Anfangsverdachtes.

Zudem gelte für IP-Adressen, die Rückschlüsse auf die Internetnutzung geben, ein besonderer Schutz.

Bis zur Gesetzesänderung spätestens Ende 2021 bleiben die bisherigen Regelungen aber bestehen.

1,2 Millionen Euro Bußgeld wegen Werbung ohne Einwilligung

Mit Bescheid vom 25.05.2020 hat der Landesbeauftragte für den Datenschutz und die Informationssicherheit Baden-Württemberg (LfDI) gegen die AOK Baden-Württemberg ein Bußgeld in Höhe von 1.240.000,00 EUR verhängt.

Die AOK habe zwischen 2015 und 2019 personenbezogene Daten von mehr als 500 Gewinnspielteilnehmern verwendet, ohne dass eine wirksame Einwilligung der Betroffenen vorgelegen habe. Die Kontaktdaten der Gewinnspielteilnehmern sowie deren Krankenkassenzugehörigkeit sollten im weiteren Verlauf für die Mitgliederwerbung verwendet werden.

Grundsätzlich ist es möglich die personenbezogenen Daten aus einem Gewinnspiel für Werbung zu nutzen. Dies erfordert aber die vorherige Einwilligung der Betroffenen.
Unternehmen müssen das Vorliegen einer solchen Einwilligung notfalls auch nachweisen

können. Zudem sind Einwilligungen nicht wirksam, wenn diese an eine bestimmte Bedingung gekoppelt sind. Die Gewinnspielteilnahme hätte beispielsweise nicht an die Einwilligung zur Datenverarbeitung für Werbezwecke geknüpft werden dürfen.

Das Bußgeld erging aber nicht aufgrund eines Verstoßes gegen das Kopplungsverbot. Vielmehr bemängelte das LfDI, dass die Einwilligungen formal nicht richtig erteilt worden waren.

In mehreren Fällen habe zwar eine Unterschrift der Betroffenen vorgelegen, es habe jedoch das Kreuz bei der Einwilligungserklärung von dem Betroffenen in der Checkbox gefehlt. Folge war, dass die Einwilligung missverständlich und nicht ausreichend war.

Eine wirksame Einwilligung kann nur dann angenommen werden, wenn diese unmissverständlich ist, sowie, für einen eindeutigen Zweck und freiwillig erteilt wurde.

Der AOK hätte bei einer genaueren Überprüfung der Dateien für Werbezwecke auffallen müssen, dass bei einigen Betroffenen das Häkchen gefehlt habe.

Eine Verarbeitung dieser Daten zu Werbezwecken hätte daher nicht erfolgen dürfen.

Im Falle der AOK waren es 500 Einwilligungen, die letztlich das Bußgeld in Höhe von gut 1,2 Millionen Euro ausmachten, und dies, obwohl die AOK konstruktiv mit der Aufsichtsbehörde zusammenarbeitete.

Den entscheidenden Hinweis, der letztlich das Bußgeld nach sich zog, kam übrigens von intern.

Dieser Fall zeigt einmal mehr wie wichtig es ist in jeder Hinsicht auf rechtmäßig eingeholte und nachweisbare Einwilligungen zu achten. Auch sollten die im Unternehmen vorhandenen technischen und organisatorischen Maßnahmen derart gestaltet sein, dass ein Fehler beim Einholen der Einwilligungen rechtzeitig bemerkt wird, um wie in diesem Fall einem sehr hohen Bußgeld aus dem Weg zu gehen.

Sollten Sie Hilfe bei der Erstellung entsprechend rechtmäßiger Einwilligungserklärungen benötigen oder haben Sie Fragen zu anderen datenschutzrechtlichen Angelegenheiten, dann sprechen Sie uns gerne an.

SaphirIT GmbH
Sutthauser Straße 285
49080 Osnabrück
Geschäftsführer
Amtsgericht Osnabrück

www.saphirit.de
USt-ID-Nr. DE268765300
Frank W. Stroot
HRB 20385

Oldenburgische Landesbank AG
IBAN DE29 2802 0050 5042 8200 00
BIC OLBODEH2XXX

Telefon 0541/60079296
Telefax 0541/60079297
datenschutz@saphirit.de