Datenschutz newsbox

Ausgabe 08 2020

DATAKONTEXT

Editorial:

Nun ist es schon über einen Monat her, dass der EuGH mit seinem Urteil vom 16. Juli 2020 (Rechtssache C311/18) den Beschluss 2016/1250 der Europäischen Kommission zur Übermittlung personenbezogener Daten in die USA (Privacy Shield) für unwirksam erklärt und zugleich festgestellt hat, dass die Entscheidung 2010/87/EG der Kommission über Standardvertragsklauseln (Standard Contractual Clauses - SCC) grundsätzlich weiterhin gültig ist.

Was das in Konsequenz bedeutet, hat der DSK in seiner Pressemitteilung kurz und knapp erläutert: „Die Übermittlung personenbezogener Daten in die USA auf der Grundlage des Privacy Shield ist unzulässig und muss unverzüglich eingestellt werden."

Spannende Frage: Wie viele Unternehmen, die Übermittlungen in die USA auf Grundlage von Privacy Shield durchführten, haben diese Übermittlungen von einem auf den anderen Tag kappen können?

Die zweite Feststellung des DSK zum Urteil des EuGH ist ebenfalls knapp: „Für eine Übermittlung personenbezogener Daten in die USA und andere Drittländer können die bestehenden Standardvertragsklauseln der Europäischen Kommission zwar grundsätzlich weiter genutzt werden." Nicht nur Juristen dürften den Begriff „grundsätzlich" in Verbindung mit „zwar" als Trigger für „Vorsicht! Da kommt noch was! Genau lesen" empfinden. In der Tat kommt dann noch etwas. Und zwar folgendes: „Der EuGH betonte jedoch die Verantwortung des Verantwortlichen und des Empfängers, zu bewerten, ob die Rechte der betroffenen Personen im Drittland ein gleichwertiges Schutzniveau wie in der Union genießen. Nur dann kann entschieden werden, ob die Garantien aus den Standardvertragsklauseln in der Praxis verwirklicht werden können."

Was das aber nun genau bedeutet, und ob es ein Rettungsring für Verantwortliche ist, oder eher etwas woran sich Verantwortliche lieber in ihrer Not nicht klammern sollten, scheint so unklar zu sein, dass die Bedeutung dieses Satzes sogar von Experten in Seminaren diskutiert werden muss, denn eine weitere Aussage des DSK ist wiederum wieder sehr deutlich und klar: „Verantwortliche, die weiterhin personenbezogene Daten in die USA oder andere Drittländer übermitteln möchten, müssen unverzüglich überprüfen, ob sie dies unter den genannten Bedingungen tun können. Der EuGH hat keine Übergangs- bzw. Schonfrist eingeräumt."

Damit dürfte die Situation wohl wie folgt zusammenzufassen sein: „So wie es aktuell gemacht wird, geht es nicht. Vielleicht aber anders? Fest steht jedoch: Es besteht akuter Handlungsbedarf".

Ihr Levent Ferik

DATAKONTEXT

Impressum

DATAKONTEXT GmbH
Augustinusstraße 9d
50226 Frechen

Tel.: 02234/98 94 9-30
Fax: 02234/98 94 9-32
fachverlag@datakontext.com
www.datakontext.com

Geschäftsführer:
Dr. Karl Ulrich/Hans-Günter Böse
Handelsregister
Amtsgericht Köln HRB 82299

Datenschutz und Polizeigesetz NRW

Die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW) informiert über die rechtlichen Voraussetzungen für das Speichern und Löschen von personenbezogenen Daten durch die Polizei. Nach eigenen Angaben ist der LDI NRW weder möglich, noch ist sie befugt, die Datenlöschungen selbst vorzunehmen. Verantwortliche im datenschutzrechtlichen Sinne seien vielmehr die Polizeibehörden, die die Daten erheben, speichern und verarbeiten.
In der Ausarbeitung der LDi NRW finden Interessierte Hinweise zum Auskunftsrecht betroffener Personen. Der Beitrag beschränkt sich auf Datenverarbeitungen nach dem Polizeigesetz NRW (PolG NRW), das heißt, solche zum Zwecke der Gefahrenabwehr (sogenannte präventive Tätigkeit). Vor dem Hintergrund, dass Datenverarbeitungen der Polizei zu Zwecken der Strafverfolgung (sogenannte repressive Tätigkeit) sich nach den Vorschriften der Strafprozessordnung richten, bleiben diese in der Darstellung der LDI NRW außen vor.

Die Ausarbeitung beschäftigt sich mit folgenden Fragen:

- Auf welcher Rechtsgrundlage darf die Polizei personenbezogene Daten speichern?
- Wie lange darf die Polizei personenbezogene Daten speichern?
- Wann muss die Polizei die Daten löschen?
- Darf die Polizei Daten einer Person zu einem abgeschlossenen Strafverfahren weiterhin speichern, wenn keine Verurteilung erfolgt ist?
- Wie kann ich erfahren, welche Daten die Polizei über mich gespeichert hat?

Die Ausarbeitung wird durch ein zum Download zur Verfügung gestelltes Musterschreiben für die Geltendmachung von Auskunfts- und gegebenenfalls Löschungsansprüchen von Betroffenen abgerundet.

Quelle: Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen

Der Privacy-Shield soll „nachgebessert“ werden

Nach Angaben der EU-Kommission haben das US-Handelsministerium und die Kommission mit Gesprächen begonnen, um auszuloten, wie der EU-US-Privacy Shield gestärkt werden könnte, um den Anforderungen zu genügen, die mit dem Urteil des EuGH vom 16.07.2020 im Fall Schrems II einhergingen. In diesem Urteil wurde erklärt, dass der Privacy Shield nicht mehr herangezogen werden kann, um personenbezogene Daten aus der Europäischen Union in die Vereinigten Staaten zu übermitteln.

Die Europäische Union und die Vereinigten Staaten erkennen die große Bedeutung des Datenschutzes und die Bedeutung des grenzüberschreitenden Datentransfers für ihre Bürger an, so die EU-Kommission in ihrer Pressemitteilung. Weitere Details zu inhaltlichen Änderungen oder einen zeitlichen Rahmen gab die EU-Kommission noch nicht bekannt.

Quelle: Europäische Kommission

Broschüre zum Kita-Datenschutz

Das Thema des Rechts am eigenen Bild und die Frage, ob und was sich nach Geltung der DS-GVO in diesem Bereich geändert hat, ist auch zwei Jahre nach Wirksamwerden der DS-GVO ein Dauerbrenner. Da sich diese Fragen nicht nur den Unternehmen und deren Datenschutzbeauftragten stellen, sondern auch in KiTas, Schulen, Vereinen und auch bei der privaten Nutzung von Social Media, ist sowohl das Interesse als auch die Unsicherheit bei dem Thema nach wie vor groß.
Die Senatsverwaltung für Bildung, Jugend und Familie sowie die Berliner Beauftragte für Datenschutz fokussieren sich in der neu überarbeiteten Broschüre: „Datenschutz bei Bild-, Ton- und Videoaufnahmen. Was ist in der Kindertageseinrichtung zu beachten?“, auf den Teilbereich der Kindertageseinrichtungen und möchten mit der Broschüre umfassend über die aktuellen rechtlichen Vorgaben informieren. Zu diesem Zweck wurde diese bereits an alle rund 2.700 Berliner Kitas versandt und ist als PDF kostenlos abrufbar.

Auf 44 Seiten werden unter anderem, im Zusammenhang mit Bild-, Ton- und Videoaufnahmen in Kitas, Themen wie die datenschutzrechtliche Einordnung (Rechtsgrundlagen und Grundsätze), Datenschutz bei Aufnahmen von Kindern (Einwilligungserklärung, Aufnahmen bei Veranstaltungen und im pädagogischen Alltag, wissenschaftliche Projekte, Veröffentlichung durch Externe), Datenschutz von Mitarbeiterinnen und Mitarbeitern (Erforderlichkeit für das Arbeitsverhältnis, Abhängigkeitsverhältnis vom Arbeitgeber) und Medienkompetenz im pädagogischen Alltag behandelt.

Die Broschüre kann unter folgendem Link heruntergeladen werden:
www.berlin.de/sen/jugend/familie-und-kinder/kindertagesbetreuung/qualitaet/datenschutz_in_kitas_2020.pdf

Berufsgeheimnisträger und unverschlüsselter E-Mail-Versand

Die Frage, ob Anwältinnen und Anwälte unverschlüsselt per E-Mail mit Mandanten kommunizieren dürfen, ohne gegen die Pflicht zur Verschwiegenheit zu verstoßen, war in jüngster Vergangenheit öfter ein Streitpunkt. Datenschutz-Aufsichtsbehörden betrachteten die Fragestellung noch genereller und stellten diese Frage für jegliche Berufsgeheimnisträger, so bspw. auch für Ärzte (Tätigkeitsbericht 2017/18 – Bayerisches Landesamt für Datenschutzaufsicht, S. 94, Ziffer 16.7).

In § 2 der Berufsordnung der Rechtsanwälte existiert seit Anfang 2020 eine neue Regelung zur Verschwiegenheit hinsichtlich der Frage, wann Anwältinnen und Anwälte bei Risiken für die Vertraulichkeit von der Zustimmung ihrer Mandanten ausgehen dürfen und wann es erforderlich ist, dem Mandanten einen Warnhinweis diesbezüglich zu geben.

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz gibt in einer aktuellen Pressemitteilung weitere hilfreiche Hinweise zu der Thematik.
Der LfDI Rheinland-Pfalz weist darauf hin, dass die Anforderungen des Art. 32 DS-GVO insbesondere auch für andere Berufsgeheimnisträger wie bspw. Steuerberater, Ärzte, Psychotherapeuten, Apotheker, Mitarbeiter staatlich anerkannter Beratungsstellen, Sozialarbeiter sowie Mitarbeiter privater Kranken-, Unfall- oder Lebensversicherungen gelten und führt diesbezüglich aus, dass für die Datenverarbeitung Verantwortliche geeignete technische und organisatorische Maßnahmen zu ergreifen haben, um ein angemessenes Schutzniveau der E-Mail-Kommunikation zu gewährleisten.

Nach Art. 5 Abs. 1 lit. f DS-GVO müssten Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet. Hierzu gehöre etwa der Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder Schädigung durch geeignete technische und organisatorische Maßnahmen. In der Konsequenz müssen Berufsgeheimnisträger daher E-Mail-Kommunikation, die personenbezogene Daten enthält, dem Stand der Technik entsprechend datensicher organisieren, um sich keines Verstoßes gegen die genannten Normen vorwerfen lassen zu müssen.
Grundsätzlich sollten E-Mails mit personenbezogenen Daten, sofern diese nicht pseudonymisiert werden, mindestens mit einer „Transportverschlüsselung“ versendet werden. Bei besonders sensiblen Daten sollte eine „Inhaltsverschlüsselung“ das Mittel der Wahl darstellen“, so der LfDI Rheinland-Pfalz.

Ein Unterschreiten der genannten Sicherheitsanforderungen sei datenschutzrechtlich hinnehmbar, sofern eine freiwillige und informierte Einwilligung der betroffenen Person in eine unverschlüsselte E-Mail-Kommunikation vorliege. Dies bedeute unter anderem, dass der Berufsgeheimnisträger eine Verschlüsselung der E-Mail-Kommunikation angeboten haben müsse. Maßstab für die Anforderungen an eine derartige Einwilligung sei Art. 7 DS-GVO. Der Berufsgeheimnisträger habe hiernach nachzuweisen, dass die betroffene Person, in Kenntnis aller Risiken durch entsprechende Aufklärung, ihr Einverständnis erteilt habe, unverschlüsselt zu kommunizieren.

Von einer informierten Einwilligung sei nicht auszugehen, wenn die betroffene Person, etwa ein Mandant, die unverschlüsselte E-Mail-Kommunikation begonnen habe.

BSI veröffentlicht Handlungshilfe für ersetzendes Scannen

Das sogenannte ersetzende Scannen beschreibt einen Prozess, in dessen Verlauf ein Dokument unter Beachtung strenger Vorschriften in eine digitale Form umgewandelt und die Papierform im Anschluss vernichtet werden darf. Der Prozess stellt dabei sicher, dass das Dokument danach in der digitalen Form die gleichen Eigenschaften wie das Original behält und eine entsprechende rechtliche Gültigkeit aufweist.

Bei Überlegungen, die die digitale Aktenführung betreffen, steht bei den Unternehmen auch die Rechtssicherheit im Fokus. Unsicherheiten bestehen darüber, wie Papierakten in ein digitales Archiv überführt werden können, ohne Aufbewahrungspflichten zu verletzen oder den Beweiswert des originalen Dokuments zu verlieren.
In diesem Zusammenhang spielt das vom Bundesamt für Sicherheit in der Informationstechnik erlassene Richtlinie TR-03138 eine wichtige Rolle.

Seit 2013 schafft die TR 03138 (TR-RESISCAN) Rechtssicherheit für papierlose Archive. Um die Implementierung der Technischen Richtlinie zu erleichtern, hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) Ende Juli eine zusammenfassende Handlungshilfe veröffentlicht.
Das Dokument beschreibt den Aufbau und die Kernanforderungen der TR-RESISCAN. Ergänzende Vorgehensmodelle, Regelungsbedarfe und Praxisbeispiele verdeutlichen, wie Prozesse für das ersetzende Scannen sicher gestaltet und umgesetzt werden können. Zur Zielgruppe gehören Verwaltung, Justiz, Wirtschaft und Gesundheitswesen gleichermaßen.

Zielsetzung der TR-RESISCAN ist die Steigerung der Rechtssicherung im Bereich des ersetzenden Scannens. Die Richtlinie hat also einen empfehlenden Charakter. Sie soll Anwendern aus Verwaltung, Justiz, Wirtschaft und Gesundheitswesen einen praxisorientierten Handlungsleitfaden zur sicheren Gestaltung ihrer Prozesse für das ersetzende Scannen bieten. Kein Bestandteil der TR-RESISCAN ist die Regelung der Zulässigkeit des ersetzenden Scannens. Dies ist von jedem Anwender in seinem Anwendungs- und Verantwortungsbereich auf Grundlage der entsprechenden Rechtsvorschriften zu prüfen. Die TR-RESISCAN definiert die Anforderung an Prozesse. Sie definiert nicht, welche Soft- oder Hardware genutzt werden soll.

Quelle: Bundesamt für Sicherheit in der Informationstechnik

EuGH erklärt EU-US-Privacy Shield für ungültig

Der Europäische Gerichtshof (EuGH) hat mit seinem Urteil vom 16.07.2020 das sogenannte Privacy Shield, das den Datenaustausch zwischen der EU und den USA regelt, für ungültig erklärt. Außerdem hat er entschieden, dass der Datenaustausch mit Nicht-EU-Ländern auf Basis der sogenannten Standardvertragsklauseln zwar rechtens ist, aber im Einzelfall geprüft werden muss.

Die Gesellschaft für Datenschutz und Datensicherheit äußert sich zu dem Urteil und seinen Folgen für die Verantwortlichen wie folgt:

Mit Urteil vom 16.07.2020 (Az: C-311/18 – Volltextveröffentlichung hier) hat sich der Europäische Gerichtshof mit der Zulässigkeit der EU-Standardvertragsklauseln in der Variante „Controller-to-Processor" (2010/87/EU) sowie des Angemessenheitsbeschluss der EU-Kommission zum EU-US Privacy Shields (Durchführungsbeschluss (EU) 2016/1250) befasst.

Was hat der EuGH entschieden?

Der EuGH hatte sich anhand der Vorlagefragen des irischen High Courts insbesondere mit der Frage zu befassen, inwieweit die Garantien für den Export personenbezogener Daten in ein Drittland in Gestalt des EU-US Privacy Shields und der EU-Standardvertragsklauseln als ausreichende Schutzmechanismen anzusehen sein, um ein im wesentlichen gleichwertiges Datenschutzniveau hinsichtlich dem gesetzlichen Schutz der Rechte und Freiheiten von Betroffenen in der Europäischen Union herzustellen.

EU-US Privacy Shield

Das Gericht hat das EU-US Privacy Shield als Nachfolgeregelung für das Safe Harbor Abkommen **für ungültig erklärt**. Der Grund hierfür sind mögliche Zugriffe auf personenbezogene Daten von EU-Bürgern durch US-amerikanische Sicherheitsbehörden aufgrund vorrangiger Erfordernisse der nationalen Sicherheit, des öffentlichen Interesses oder zur Durchführung von Gesetzen, was nicht in Einklang mit den Grundrechten der EU-Bürger zu bringen sei. Zusätzlich seien die Überwachungsprogramme durch US-Sicherheitsbehörden als unverhältnismäßig einzustufen. EU-Bürgern stünden im Übrigen keine ausreichenden Rechtsschutzmöglichkeiten vor den US-Gerichten zur Verfügung, um Rechtsverletzungen überprüfen zu lassen. Auch die im Privacy Shield eingerichtete Ombudsperson könne keine ausreichenden Überwachungskompetenzen gegenüber den US-Geheimdiensten ausüben, um möglichen Rechtsverletzungen entgegenzuwirken.

EU-Standardvertragsklauseln

Die EU-Standardvertragsklauseln hingegen **bleiben nach der Entscheidung des EuGH gültig**. Zwar bestünde auch hier das Risiko für Betroffene, dass öffentliche Stellen Rechte und Freiheiten durch einen Zugriff auf personenbezogene Daten verletzen, **allerdings wären die in den Standardvertragsklausen vorgesehenen Schutzmechanismen grundsätzlich erweiterbar**. Dies sei der fundamentale Unterschied zu einer Angemessenheitsentscheidung wie dem EU-US Privacy Shield, in dem rechtsverbindlich untersucht würde, ob die bestehenden Gesetze u.a. hinsichtlich der Zugriffe von Behörden aus Gründen eines nationalen Sicherheitsinteresses mit Blick auf die EU-Gesetzgebung als angemessen zu erachten seien. Bei den Standardvertragsklauseln erfolge eine solche rechtsverbindliche Prüfung nicht, da die Klauseln nicht sämtliche Garantien für ein angemessenes Schutzniveau in einem Drittland beinhalteten.

Die Rolle des Verantwortlichen und des Auftragsverarbeiters

Der EuGH erinnert daran, dass es die Pflicht des Verantwortlichen (und ggf. des Auftragsverarbeiters) sei, beim Fehlen einer Angemessenheitsentscheidung der Kommission **ausreichende Schutzmechanismen zugunsten von Betroffenen für den Datenexport zu implementieren.** Daher müssten – je nach Situation im Drittland – ggf. **zusätzliche Garantien** mittels der Möglichkeit der Erweiterung der Standardvertragsklauseln über geschäftsbezogene Klauseln geschaffen werden. Verantwortliche seien daher in der Pflicht, die jeweilige Situation im Drittland **über eine Einzelfallprüfung** zu evaluieren.

Die Rolle der Aufsichtsbehörden

Ergeben sich Hinweise für den Datenexporteur, so aufgrund einer Information des Datenimporteurs, dass die vereinbarten Standardvertragsklauseln aufgrund der Gesetze im Drittland nicht eingehalten werden können, hat er hierüber seine zuständige Aufsichtsbehörde zu informieren. Dieser wiederum stünden über die Standardvertragsklauseln Auditrechte beim Datenimporteur oder dessen Unterauftragnehmer zu. Die Behörden seien hierbei in der Pflicht, einen Datentransfer auszusetzen, wenn die Zusicherungen der Standardvertragsklauseln im Drittland nicht eingehalten werden könnten. (Fortsetzung nächste Seite.)

EuGH erklärt EU-US-Privacy Shield für ungültig (Fortsetzung)

Fazit

Verantwortliche oder Auftragsverarbeiter können ab dem 16.07.2020 keine personenbezogenen Daten mehr auf Basis des EU-US Privacy Shields an Empfänger in den Vereinigten Staaten übermitteln. Bei den EU-Standardvertragsklauseln werden Verantwortliche durch den EuGH in die Pflicht genommen, für jeden Datenexport in ein Drittland zu untersuchen, ob der Empfänger die Zusicherungen der Vertragsklauseln einhalten kann oder ob lokale Gesetze ihm dies verbieten. Ergeben sich Hinweise, dass die EU-Standardvertragsklauseln nicht mehr eingehalten werden können, ist – neben dem Aussetzen des Exports – die Aufsichtsbehörde zu informieren, die wiederum ihrerseits eine diesbezügliche Prüfung anstrebt und ein Aussetzen ihrerseits verlangen kann.

Der EuGH wählt in seinem Urteil eine formale Herangehensweise an die EU-Standardvertragsklauseln, das die ohnehin bestehenden Pflichten für Exporteure und Importeure nochmals beleuchtet. Unklar bleibt für Verantwortliche, welche Hinweise im Drittland den Export personenbezogener Daten als unzulässig erscheinen lassen bzw. welche technisch-organisatorischen Maßnahmen ergänzend zu treffen sind.

Die GDD fordert:

- Sanktionsmaßnahmen von **EU-Aufsichtsbehörden** bezüglich der Datenexporte in Drittländer, insbesondere die USA, sind vorerst auszusetzen. Datenverarbeiter müssen die Möglichkeit erhalten, ihre Datenflüsse in Drittländer nach dem Urteil des EuGH evaluieren können.
- Seitens des **Europäischen Datenschutzausschusses** sind Hinweise zu erarbeiten, nach welchen Kriterien Datenexporte auf Basis der EU-Standardvertragsklauseln in ein Drittland auszusetzen sind. Hier wären beispielsweise Black- oder Whitelists für Länder oder bestimmte Sektoren denkbar. Alleingänge nationaler Aufsichtsbehörden wären nicht zielführend.
- Verhandlungen zwischen der Europäischen Kommission und den Vereinigten Staaten für Änderungen des EU-US Privacy Shields sind zeitnah aufzunehmen. Insbesondere die Datenzugriffe von Behörden aus Sicherheitsinteressen müssen einer effektiven und verbindlichen Kontrolle unterliegen und sich am Verhältnismäßigkeitsgrundsatz orientieren. Rechtsschutzmöglichkeiten für EU-Bürger sind stärker zu berücksichtigen.

Nach dem Ende des Privacy-Shields: GDD gibt Handlungsempfehlungen

Der EuGH hat das EU-Privacy Shield mit seinem Urteil vom 16.07.2020 (Az: C-311/18) für ungültig erklärt und an die Pflichten für Datenexporteure und Datenimporteure bei Anwendung der EU-Standardvertragsklauseln, insbesondere hinsichtlich einer rechtskonformen Datenübermittlung, erinnert. Datenexportierende verantwortliche Stellen mit Sitz in der Europäischen Union oder in Ländern des Europäischen Wirtschaftsraums stehen nun vor der Herausforderung, wie personenbezogene Daten weiterhin rechtskonform in Drittländer übermittelt werden können. Die GDD möchte Handlungsempfehlungen bezüglich des Endes des Privacy-Shields geben, um Verantwortliche und deren Datenschutzbeauftragte bei der Umsetzung zu unterstützen.

Dabei erstrecken sich die Empfehlungen auch darauf, ob und wie der Einsatz der sog. EU-Standardvertragsklauseln aussehen kann sowie eine Beschäftigung mit der Frage, wie die sog. Angemessenheitsbeschlüsse der EU-Kommission bzgl. der jeweiligen Drittländer zu bewerten sind.

Die Ausarbeitung der GDD beschäftigt sich ebenso mit dem Instrument der „anderen Garantien (Art. 46 DS-GVO) bzw. Ausnahmen für bestimmte Fälle (Art. 49 DS-GVO)“

>> Zu den Handlungsempfehlungen der Gesellschaft für Datenschutz und Datensicherheit (GDD e.V.)

>> https://www.gdd.de/aktuelles/startseite/handlungsempfehlung-gdd-eugh-eu-us-privacy-shield-SCC

Einigung in Sicht? EU-Ratspräsidentschaft legt Diskussionspapier zur ePrivacy-Verordnung vor

Seit Jahren wird in Brüssel heiß über die ePrivacy-Verordnung gestritten. Dabei geht es um den Schutz personenbezogener Daten bei elektronischer Kommunikation. Ursprünglich sollte diese bereits im Jahr 2018 in Kraft treten.
Nun – zwei Jahre später – scheint eine tragfähige Lösung immer noch nur schwer vorstellbar. Noch immer wurde kein geeigneter Kompromiss zwischen Datenschutz und den wirtschaftlichen Interessen gefunden.
Dieser Streit bedeutet allerdings auch, dass auf bestimmten Gebieten rechtliche Unklarheiten und Regelungslücken entstehen oder fortbestehen. Die deutsche Ratspräsidentschaft hat sich deshalb zum Ziel gesetzt, eine Einigung der Mitgliedsstaaten herbeizuführen.
Deutschland hat die EU-Ratspräsidentschaft seit dem 1. Juli 2020 inne. Bereits am 6. Juli 2020 wurde dann ein Ratspapier zur ePrivacy-VO als weitere Diskussionsgrundlage vorgelegt. Damit sollen möglichst erfolgreiche Verhandlungen mit dem Europäischen Parlament ermöglicht werden. Das Papier setzt bei den entgegenstehenden Meinungen an: Einmal soll es bei der ePrivacy-Verordnung darum gehen, unter Einhaltung der Grundrechte, die private elektronische Kommunikation zu schützen. Außerdem zielt sie auf Erhalt und Fortschritt innovativer digitaler Geschäftsmodelle ab.
Als besonders umstritten gelten die Regelungen zur Verarbeitung von Daten elektronischer Kommunikation (Art. 6-6d) und zum Schutz der Endgeräteinformation (Art. 8). Vor allem bezüglich dieser Regelungen befindet sich nun die deutsche Ratspräsidentschaft in Rücksprache mit den weiteren 26 Mitgliedsstaaten. In diesen Diskussionen sollen tragfähige Kompromisse und ein gemeinsamer Entwurf für eine ePrivacy-Verordnung entstehen.

Einigung in Sicht?
Mehr dazu auf DataAgenda

EDSA beantwortet häufige Fragen zu Schrems II

Der Europäische Gerichtshof (EuGH) hat mit seinem Urteil vom 16.07.2020 das sogenannte Privacy Shield, das den Datenaustausch zwischen der EU und den USA regelt, für ungültig erklärt. Außerdem hat er entschieden, dass der Datenaustausch mit Nicht-EU-Ländern auf Basis der sogenannten Standardvertragsklauseln zwar rechtens ist, aber im Einzelfall geprüft werden muss.

Die nach diesem Urteil entstandene Unsicherheit versucht der Europäische Datenschutzausschuss (EDSA) mit einer FAQ mildern. Am 23.07.2020 hat der EDSA auf Antworten zu den wichtigsten Fragen bzgl. der Konsequenzen aus dem Schrems-II-Urteil des Europäischen Gerichtshofs zum Datentransfer in Länder außerhalb der EU geeinigt.

Eine der häufigsten Fragen der betroffenen Unternehmen dürfte gewesen sein, ob es eine „Gnadenfrist" für Datenverarbeitungen auf Grundlage des vom Europäischen Gerichtshof für ungültig erklärten „Privacy Shield" geben wird. Sofern Unternehmen diese Hoffnung tatsächlich gehabt haben sollten, wird diese in den FAQ zunichtegemacht: Die Umstellung muss ohne Verzögerung begonnen werden.

Eine andere Frage, die den Unternehmen unter den Nägeln brannte und sich aufdrängte, war, die Frage zur Zukunft der sog. EU-Standardvertragsklauseln. Auch hierzu geben das FAQ der EDSA zumindest erste Hinweise:

Die Datenübermittlung in die USA und sonstige Drittstaaten außerhalb der Europäischen Union auf der Grundlage von Standardvertragsklauseln bleiben unter bestimmten Voraussetzungen möglich. Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz erläutert dies in einer eigenen Bewertung der FAQ des EDSA wie folgt:
„Die Standardvertragsklauseln müssen ggf. durch weitere Vereinbarungen oder Elemente ergänzt werden, um sicherzustellen, dass bei der Datenübermittlung in den Drittstaat das angemessene Schutzniveau erhalten ist. Für Datenübermittlungen in die USA bedeutet dies, dass erhebliche Anstrengungen der Verantwortlichen erforderlich sind, die vermutlich nur in seltenen Fällen als ausreichend angesehen werden können. Dies ist aber eine Frage des Einzelfalles. Zugleich müssen die Verantwortlichen ihre Datenübermittlungen in andere Drittstaaten, z.B. Indien, China oder Russland daraufhin prüfen, ob sie dem Datenschutzniveau entsprechen, das die Datenschutz-Grundverordnung verlangt. Dies war vorher schon so und ist nunmehr erst recht dringend erforderlich, hier werden einschlägige Nachprüfungen angeraten."

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) weist auf folgenden wichtigen Umstand in Bezug auf die FAQ des EDSA hin: Die FAQ seien als „lebendes Dokument" zu verstehen. Der EDSA kläre mit der FAQ entscheidende Fragen, die sich nach dem Urteil stellen. Das Dokument sei aber nicht abschließend.