Geschäftsstelle Dresden:
Königsbrücker Landstraße 40
01109 Dresden
Tel: 0351 8881251

Niederlassung Böblingen:
Otto-Lilienthal-Straße 36
71034 Böblingen
Tel: 07031 7145660

mail@sodalitas-gmbh.de
www.sodalitas-gmbh.de
Fax: 0351 8881252

IT-Ticker 01/2019

Der IT-Ticker 01/2019 informiert Sie über folgende Themen:

Bundestag beschließt überarbeiteten Entwurf für Geschäftsgeheimnisgesetz

Der Bundestag hat am Donnerstag, den 21. März 2019, den von der Bundesregierung vorgelegten Entwurf (BT-Drucksache 19/4724) für ein Geschäftsgeheimnisgesetz zum Schutz von geheimen Unternehmensinformationen beschlossen.

Das in Unternehmenskreisen gefürchtete Instrument des Whistleblowings wird darin erstmals gesetzlich geregelt. Ausgangspunkt für den Entwurf des neuen Gesetzes war die europäische Richtlinie 2016/943 über den Schutz von Geschäftsgeheimnissen, die Wirtschaftsspionage und Geheimnisverrat in der EU wirkungsvoll verhindern soll und deren Umsetzungsfrist für die Mitgliedstaaten bereits im Sommer 2018 abgelaufen war. Bislang war der Schutz von Geschäftsgeheimnissen uneinheitlich in verschiedenen Gesetzen verankert. Der bisherige Schutz reichte zur Umsetzung der Richtlinie jedoch nicht aus. Das neue Gesetz, soll daher den bisherigen Schutz verstärken und zentral in dem eigens dafür geschaffenen Gesetz normieren, um den unbefugten Abfluss von Informationen zu verhindern. Möglich ist künftig auch ein effektiver Schutz z.B. von Algorithmen der künstlichen Intelligenz oder von innovativen Prozessabläufen, die bisher meist bewusst aufgrund fehlender Schutzmechanismen gegen Kopien nicht im Wege z.B. von Patentanmeldungen offengelegt wurden.

Voraussetzung für einen umfassenden Schutz von Geschäftsgeheimnissen ist künftig, dass die Unternehmen angemessene Geheimhaltungsmaßnahmen getroffen haben. Beispiele für konkrete Maßnahmen, die der Gesetzgeber als angemessen einstuft, enthält das Gesetz allerdings nicht.

Praxishinweis:
Je höher der Stellenwert der jeweiligen Information für das Unternehmen ist, desto höher sind die Anforderungen an die zu treffenden Geheimhaltungsmaßnahmen. Ratsam ist daher zunächst eine abgestufte Klassifikation der bestehenden Geschäftsgeheimnisse, um im nächsten Schritt ein umfassendes Schutzkonzept zu schaffen.

Denkbare Geheimhaltungsmaßnahmen sind unter anderem: Technische Maßnahmen wie angemessene IT-Sicherheitssysteme, physische Zugangshindernisse und eine Verschlüsselung der Kommunikation zwischen den Mitwissenden, als auch organisatorische Maßnahmen wie Geheimnisschutzvereinbarungen in Arbeitsverträgen mit Mitarbeitern und in Rahmenverträgen mit Geschäftspartnern.

Wichtig ist, dass sich Unternehmen nicht mehr auf den Schutz des Geschäftsgeheimnisschutzgesetzes berufen können, sobald die geheime Information offenbart wurde und dadurch den Geheimnischarakter verloren hat.

Lara Guyot, Berlin
l.guyot@skwschwarz.de

Steuerrecht: Keine (nachträgliche) Steuerpflicht bei der Schaltung von Werbung auf Google, Facebook

Digitale Unternehmen wie Google, Ebay und Facebook können ihre Produkte grenzüberschreitend anbieten und Gewinne erzielen, ohne im betreffenden Land eine klassische Betriebsstätte zu unterhalten. Deshalb werden ihre Erträge im deutschen Steuerrecht oft nicht erfasst und sie bleiben unversteuert. Diese Steuerungerechtigkeit soll künftig möglicherweise – so zumindest der Vorschlag einiger EU-Staaten – durch eine Digitalsteuer beseitigt werden.

Die deutschen Finanzbehörden hatten darüber hinaus Anfang 2019 die Idee, Steuern (auch rückwirkend) über einen Umweg einzutreiben. Leidtragende waren insbesondere deutsche Mittelständler. Denn die Finanzbehörden argumentierten, ohne vorherige Ankündigung und rechtliche Indikation, plötzlich damit, dass das Schalten einer Online-Werbung steuerlich als Rechteüberlassung zu bewerten sei. Bei einer grenzüberschreitenden Überlassung von Rechten wird grundsätzlich die sog. Quellensteuer festgesetzt, d. h. bei einem Erwerb von Rechten aus dem Ausland hat der Zahlungspflichtige 15 % Quellensteuer einzubehalten und abzuführen und nur die verbleibenden 85 % an den Überlasser der Rechte zu leisten. Wenn also z. B. ein deutscher Unternehmer mit Google-Ads (das Unternehmen sitzt im Ausland) für das Schalten von Werbung einen Preis in Höhe von EUR 1 Mio. vereinbart, darf im Fall der Rechteüberlassung nur ein Betrag in Höhe von EUR 850.000,00 an Google gezahlt werden und ein Betrag in Höhe von EUR 150.000,00 müsste durch das deutsche Unternehmen an das Bundeszentralamt für Steuern abgeführt werden.

Für die Zukunft hätte dieses Vorgehen (zumindest sofern die vertraglichen Vereinbarungen nichts hiervon abweichendes regeln) Google, Facebook und Co. betroffen, denn die Frage, ob die Quellensteuer letztlich doch an das leistende Unternehmen auszukehren ist, ist grundsätzlich ausschließlich zwischen dem ausländischen Unternehmen und den Bundeszentralamt für Steuern zu klären. Nach Ansicht der Finanzbehörden sollte der Quellensteuerabzug aber nachträglich ab dem Jahr 2012 greifen. Als Folge dieser jüngst entwickelten und nur bedingt nachvollziehbaren Rechtsauffassung wurden auch sogleich entsprechende Steuerbescheide erlassen. Unternehmen, die in den Jahren 2012 und 2013 z. B. EUR 5 Mio. in Online-Werbung investierten, sollten nun nachträglich Steuern in Höhe von EUR 750.000,00 nachzahlen. Dies führte insbesondere bei mittelständischen Unternehmen zu einer nicht unerheblichen Anzahl einer völlig unerwarteten Insolvenzgefährdung, denn die Chance die Quellensteuer nach 7 Jahren von Google und Co. erstattet zu bekommen, ist verschwindend gering, bzw. voraussichtlich mit einem so hohen Zeit- und Kostenaufwand verbunden, dass die Insolvenz vorher eintreten würde. Zudem finden sich gerade in den Vertragswerken von Google und Co. oft Regelungen, nach denen Google stets den vollen Preis erhält und das deutsche Unternehmen eine zusätzliche Steuerlast oder Kosten selbst zu tragen hat.

Praxistipp:
Glücklicherweise ist auch die Regierung auf dieses Problem aufmerksam geworden. Mit Pressemitteilung vom 14.03.2019 hat das Bayerische Staatsministerium der Finanzen verkündet, dass auf Bund-Länder-Ebene eine Einigkeit darüber erreicht wurde, dass eine Belastung von inländischen Unternehmen mit Quellensteuer bei der Nutzung von Online-Werbung nicht in Betracht komme. Dennoch empfehlen wir auch für die Zukunft eine Prüfung und Anpassung der Verträge mit Google, Ebay, Facebook und Co., um einem möglicherweisen erneuten Ansatz der Finanzbehörden schon auf Vertragsebene begegnen zu können.

Nicole Thomann, München
n.thomann@skwschwarz.de
Heiko Wunderlich, München
h.wunderlich@skwschwarz.de

Europäischer Datenschutzausschuss informiert zu Datentransfer nach Großbritannien im Falle eines ungeordneten Brexit

In wenigen Tagen wird Großbritannien aus der EU austreten und die Wahrscheinlichkeit eines ungeordneten Brexit steigt mit jedem weiteren Tag, welcher ohne einen „Deal“ vergeht. Gerade erst ist Theresa May im Parlament mit einer Beschlussvorlage gescheitert, die sowohl ein Mandat für Nachverhandlungen am Brexit Deal als auch eine Absage an den EU-Austritt ohne Abkommen bestätigen sollte.

Unternehmen sind somit gut beraten, sich schnellstmöglich auf das Szenario eines ungeregelten Brexit vorzubereiten. In diesem Falle wird Großbritannien datenschutzrechtlich gesehen zu einem Drittland, in welches Datentransfers nur unter bestimmten Voraussetzungen möglich sind. Eine Hilfestellung, um Datentransfers zukünftig rechtmäßig durchführen zu können, bietet die „Information note on data transfers under the GDPR in the event of a no-deal Brexit“ des Europäischen Datenschutzausschusses. Danach sind im Bereich des Datenschutzes verschiedene Anpassungen vorzunehmen, um auch künftig Daten rechtmäßig nach Großbritannien übermitteln zu können. Dies gilt sowohl für Datentransfers innerhalb eines Unternehmens, im Konzern als auch an dritte Unternehmen.

1. Prüfung der betroffenen Daten und Personen

Zunächst sollte im Unternehmen geprüft werden, ob und welche Daten nach Großbritannien übermittelt werden. Dabei sind auch „exotische“ Themen, wie z.B. Reisebuchungen für Mitarbeiter, nicht zu vergessen. Da diese wichtige Vorarbeit aus unserer Erfahrung einige Zeit in Anspruch nimmt, sollten Unternehmen unverzüglich mit dieser Prüfung beginnen.

Erst wenn bekannt ist, welche Daten zu welchem Zweck nach Großbritannien übermittelt werden, können die weiteren notwendigen Maßnahmen ergriffen werden.

2. Geeignete Garantien für den Transfer

Das Problem im Hinblick auf den Austritt von Großbritannien ist die knapp verbleibende Zeit, um angemessene Maßnahmen zu ergreifen. Aus diesem Grund wird zum Beispiel ein viele Vorteile bringender Angemessenheitsbeschluss der Europäischen Kommission vor dem 30. März 2019 nicht mehr herbeizuführen sein. Auch wenn ein solcher wohl in der Zukunft ergehen wird, müssen sich Unternehmen bis zum Beschluss mit anderen Mitteln behelfen.

Diese Mittel ergeben sich aus der DSGVO direkt. Entweder ist eine der in Art. 49 DSGVO genannten Ausnahmen einschlägig oder der Empfänger gewährleistet durch geeignete Garantien ein angemessenes Datenschutzniveau. Die Ausnahmevorschriften der DSGVO sind allerdings eng auszulegen und nur in den explizit genannten Fällen einschlägig.

Konzerne, welche bereits über Binding Corporate Rules verfügen, können den Transfer nach Großbritannien innerhalb des Konzerns zukünftig einfach auf diese stützen. Um neue Binding Corporate Rules innerhalb des Konzerns zu vereinbaren, ist die verbleibende Zeit allerdings ebenfalls zu knapp.

Jedoch verbleiben weitere Möglichkeiten, Datentransfers auch kurzfristig rechtmäßig durchzuführen, sofern die Ausnahmevorschriften der DSGVO nicht greifen. Zunächst kommt der Abschluss der sogenannten Standarddatenschutzklauseln in Betracht. Dies sind von der Europäischen Kommission veröffentlichte Musterklauseln für verschiedene Szenarien (Auftragsverarbeitung oder Transfer zwischen zwei Verantwortlichen). Die Standarddatenschutzklauseln dürfen durch die Parteien allerdings nicht verändert werden. Im Falle der Änderung der Klauseln gelten diese als Individualvertrag, welcher durch die zuständige Aufsichtsbehörde zu genehmigen ist.

In Einzelfällen kann der Transfer auch auf eine Einwilligung der betroffenen Person gestützt werden. Für einen regelmäßigen Datentransfer eignet sich die Einwilligung aber sicherlich – wie auch schon bislang – nicht.

3. Weitere notwendige Anpassungen

Neben der Absicherung des eigentlichen Transfers müssen im Unternehmen weitere Punkte berücksichtigt werden, um eine Datenschutz-Compliance herzustellen:

- Anpassung der Datenschutzinformationen nach Art. 13/14 DSGVO sowie sämtlicher Dokumente, welche entsprechende Informationen enthalten
- Anpassung der betroffenen Verarbeitungsverzeichnisse
- Anpassung des Auskunftsprozesses nach Art. 15 DSGVO
- Eventuell erstmalige Durchführung einer Datenschutzfolgenabschätzung

Diese Anpassungen sollten in Abstimmung mit fachkundigen Experten durchgeführt werden, da der Drittlandtransfer besondere datenschutzrechtliche Problemstellungen birgt.

Praxistipp:
Jede verantwortliche Stelle, welche personenbezogene Daten aus einem Mitgliedstaat der EU nach Großbritannien übermittelt, muss sich spätestens jetzt auf einen ungeordneten Brexit vorbereiten, um die Einhaltung des Datenschutzrechts auch nach dem 29. März 2019 gewährleisten zu können. Dies empfiehlt auch der Landesbeauftragte für Datenschutz und die Informationsfreiheit Rheinland-Pfalz. Anderenfalls drohen Verfahren der Aufsichtsbehörden und Bußgelder.

Franziska Ladiges, Frankfurt/Main
f.ladiges@skwschwarz.de

BayLDA analysiert Websites und stellt erhebliche Defizite bei bekannten Internetdiensten in Bezug auf Cybersicherheit und Einsatz von Tracking-Tools fest

Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) hat sich am Safer Internet Day (SID) beteiligt und Websites mit großer Reichweite untersucht. Dabei wurden zum einen die Sicherheit der Nutzerkonten und zum anderen der Einsatz von Tracking-Tools untersucht. Obwohl sich einige der prominentesten Internetdienste unter den Geprüften befinden, fällt das Ergebnis aus datenschutzrechtlicher Sicht ernüchternd aus.

Im Fokus der Datenschutzprüfung stand zunächst die Sicherheit von Nutzerkonten der entsprechenden Dienste. Dabei wurde insbesondere untersucht, wie die Website-Betreiber mit den Passwörtern ihrer Nutzer umgehen. Es wurden Online-Dienste unterschiedlicher Art unter die Lupe genommen. Darunter waren Streaming- und Videoportale, E-Mail-Dienste, Elektronik-Shops, Fotoservices, Gesundheits- und Kosmetik-Websites, Möbel-Shops, Mode-Shops, Preisvergleich-Seiten und soziale Netzwerke. Es wurden insgesamt 22 Prüfpunkte hinsichtlich der Registrierung und 17 Prüfpunkte im Zusammenhang mit dem Login untersucht.

Im Ergebnis hat das BayLDA festgestellt, dass bei keinem dieser Dienste ausreichende Maßnahmen getroffen wurden, um starke Passwörter vom Nutzer zu fordern. So waren beispielsweise oft sehr schwache Passwörter wie „123456“, „Passwort“ oder sogar „0000“ möglich. Zusätzliche Sicherheitsmaßnahmen und Hilfestellungen zum Schutz des Accounts haben dabei nur wenige der Dienste angeboten. Das BayLDA hat angekündigt, die festgestellten Defizite im Nachgang im schriftlichen Verfahren oder vor Ort bei den Unternehmen zu untersuchen.

Aus datenschutzrechtlicher Sicht interessanter waren die Feststellungen im Zusammenhang mit dem Einsatz von Tracking-Tools und Cookie-Bannern. Es wurden vierzig große bayerische Anbieter im Hinblick darauf untersucht, ob die Nutzer transparent über die Einbindung von Drittanbietern, insbesondere von Tracking-Tools, auf der Website informiert werden. Unter den untersuchten Unternehmen waren Online-Shops, Medienunternehmen, Versicherungen, Banken, Sportvereine und sonstige Webseitenbetreiber (ausführliche Auflistung der geprüften Unternehmen auf Folie 21 des Ergebnispapiers). Als erstes fiel der Behörde auf, dass sämtliche Anbieter Tracking-Tools einsetzen, jedoch nur 25 Prozent der Websites die Nutzer transparent über den Einsatz von diesen Tools informieren. Bei den restlichen Anbietern wurde der Nutzer nicht oder nur unzureichend über den Einsatz der Tracking-Tools im Rahmen der Datenschutzerklärung informiert. Auch bei dem Einsatz von Cookie-Bannern sieht die Behörde erhebliches Verbesserungspotenzial. Auf zwanzig Prozent der Websites wird beispielsweise vom Nutzer gar keine Einwilligung zum Einsatz von Cookies eingeholt.

Aber auch in den Fällen, in denen eine Einwilligung eingeholt wurde, geschah dies in keinem einzigen Fall wirksam. Die Einwilligungen wurden entweder nicht vorab erteilt, sie erfolgten nicht informiert oder es hat die Freiwilligkeit gefehlt (Mängel der Einwilligungen sind auf Seite 25 des Ergebnispapiers zu finden).

Zudem hat das BayLDA festgestellt, dass von den vierzig untersuchten Websites nur bei einer die Möglichkeit bestand, die Profilbildung aufgrund eigener Einstellungen im Browser zu verhindern (Ergebnisse zur Profilbildung auf Seite 26 des Ergebnispapiers).

Der Präsident des BayLDA, Thomas Kranig, hat sich nach den ernüchternden Feststellungen geäußert:

„Das Ergebnis dieses Datenschutzchecks war deutlich schlechter als das der Cybersicherheitsprüfung: Alle begutachteten Websites begehen Datenschutzverstöße beim Einsatz der Tracking-Werkzeuge. Für die verantwortlichen Unternehmen wird unsere Prüfung ein Nachspiel haben.Wir haben uns entschlossen, diese Missstände abzustellen sowie die Einleitung von Bußgeldverfahren zu prüfen. Gerade von den großen Unternehmen erwarten wir, dass sie in der Lage sind, die rechtlichen Vorgaben einzuhalten."

Handlungsempfehlung:
Wir empfehlen dringend, die Websites auf Datenschutzkonformität – insbesondere im Hinblick auf den Einsatz von Tracking-Tools und die Einholung von Einwilligungen – zu überprüfen. Auch wenn für das BayLDA zurzeit bekannte Website-Betreiber im Fokus stehen, können sämtliche Unternehmen von einer Datenschutzprüfung getroffen werden.

Ivan Brankov, Frankfurt/Main
i.brankov@skwschwarz.de

Die Datenschutzaufsicht macht Ernst: 50 Millionen Euro Geldbuße

Am 21.01.2019 hat die französische Datenschutzaufsichtsbehörde CNIL gegen GOOGLE LLC eine Geldbuße von 50 Millionen Euro wegen Verstößen gegen die Datenschutz-Grundverordnung verhängt.

Das Bußgeldverfahren war nach mehreren Sammelbeschwerden eröffnet worden, die bei der CNIL bereits kurz nach Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) eingingen. Zunächst stellte die CNIL fest, dass GOOGLE über keine Niederlassung in der EU verfügt, die eigenständig Entscheidungen über die Datenverarbeitung treffen kann. Daher gilt das Prinzip des „one stop shop" nicht, wonach für Unternehmen mit Sitz in der EU nur die lokale Datenschutzaufsicht zuständig ist. Vielmehr ist jede Datenschutzaufsichtsbehörde in der EU berechtigt, Verstöße zu verfolgen.

Daher untersuchte die CNIL die Neueinrichtung eines GOOGLE Accounts während der Konfiguration eines Mobile Device mit dem Betriebssystem Android. Dabei wurden mehrere Verstöße festgestellt:

Zum einen würden die Anforderungen an die transparente Information des Nutzers nicht eingehalten. Wesentliche Informationen (Verarbeitungszwecke, Speicherdauern, Kategorien personenbezogener Daten für die Personalisierung von Anzeigen) sind breit über mehrere Dokumente verstreut mit Buttons und Links, die zur Anzeige weiterer Informationen genutzt werden müssen. Die relevanten Informationen wären erst nach mehreren Schritten zugänglich, teilweise erst nach fünf oder sechs Aktionen. Zudem wären die so dargestellten Informationen nicht stets klar und umfassend.

Zum anderen würde eine Einwilligung des Betroffenen nicht wirksam eingeholt. Einerseits sei der Betroffene vor seiner (unwirksamen) Einwilligungserklärung nicht ausreichend informiert. Zum anderen sei eine pauschale Einwilligung bereits als Voreinstellung ausgewählt und der Nutzer könne Einschränkungen nur über gesondert aufzurufende Menüoptionen vornehmen.

Die Entscheidung über das Bußgeld in Höhe von 50 Millionen Euro ist noch nicht rechtskräftig und kann noch angefochten werden.

Praxistipp:
Die Datenschutzaufsicht macht nun Ernst mit den Sanktionen der DSGVO. Mit dem Bußgeld von 50 Millionen Euro werden nur Verstöße bei der Ersteinrichtung von Nutzeraccounts in Android sanktioniert, nicht etwa denkbare andere Verstöße. Auch in Deutschland sind bereits über vierzig Bußgelder nach DSGVO verhängt worden und wohl über hundert weitere Bußgeldverfahren laufen. Auch aus finanziellen Gründen empfiehlt es sich, die Anforderungen der DSGVO vollständig und genau umzusetzen.

Martin Schweinoch, München
m.schweinoch@skwschwarz.de

Bestellung auf Knopfdruck? – Nicht wenn es nach der Verbraucherzentrale Nordrhein-Westfalen geht

Das Oberlandesgericht München gab mit Urteil vom 10. Januar 2019 (Az.: 29 U 1091/18) einer Klage der Verbraucherzentrale Nordrhein-Westfalen gegen die Amazon EU S.a.r.l. statt und stellte die Rechtswidrigkeit des Bestellkonzepts der sog. „Amazon Dash Buttons“ fest. Das harte Urteil gegen eine der ersten „Smart Home“-Anwendungen wird in der Tech-Branche kritisiert.

Die „Amazon Dash Buttons“ sind mit WLAN verbundene Knöpfe zum Aufkleben, mit denen Kunden Produkte des täglichen Lebens per Knopfdruck nachbestellen können. Jeder Knopf ist an ein bestimmtes Produkt wie Waschmittel, Windeln oder Kaffee gekoppelt, welches beim Einrichten des „Dash Buttons“ ausgewählt wurde. Amazon behält sich in seinen Allgemeinen Geschäftsbedingungen jedoch das Recht vor, den Preis des Produkts anzupassen oder ein Alternativprodukt liefern zu können.

Diese Klausel in den Allgemeinen Geschäftsbedingungen hielt das OLG München für unzulässig. Das Gericht kritisierte zudem weitere Punkte des Geschäftsmodells: Amazon informiere den Kunden nicht vor Abschluss der Bestellung über den Preis und die tatsächlich bestellte Ware, sondern stelle diese Informationen erst nach Vertragsschluss in der Amazon-App bereit. Auch ein Hinweis, dass beim Drücken des Knopfs eine Zahlungspflicht ausgelöst wird, fehle. Dieser Hinweis ist jedoch bei Verträgen über kostenpflichtige Leistungen mit Verbrauchern im elektronischen Geschäftsverkehr nach § 312j Abs. 3 BGB bei der Button-Lösung verpflichtend. Insgesamt befanden die Richter das Bestellkonzept als zu intransparent.

Das Urteil ist noch nicht rechtskräftig. Die Revision zum Bundesgerichtshof ließen die Münchner Richter zwar nicht zu, Amazon kündigte aber bereits an, Nichtzulassungsbeschwerde einlegen zu wollen.

Dass das OLG München in der Auseinandersetzung zwischen Verbraucherschutz und Innovation, dem „Smart Home“-Gerät eine derart deutliche Absage erteilte, wird in der innovationsaffinen Tech-Branche teils als rückschrittlich bewertet. Kritiker des Urteils argumentieren insbesondere, dass Kunden die „Dash Buttons“ bewusst und in Kenntnis des Konzepts installierten, um von einem möglichst einfachen und bequemen Einkaufserlebnis profitieren zu können. Kunden hätten außerdem die Möglichkeit, die Bestellung bei Amazon im Nachhinein zu stornieren oder zurückzusenden. Der „Dash Button“ gilt als Vorläufer von „Smart Home“-Anwendungen, für deren künftige rechtskonforme Ausgestaltung das OLG-Urteil daher durchaus beachtlich und eine schwere Hürde sein dürfte.

Corinna Sobottka, München
c.sobottka@skwschwarz.de

EU-Kommission bestätigt EU-U.S. Privacy Shield

Die Vereinigten Staaten gewährleisten auch nach Inkrafttreten der DSGVO ein angemessenes Schutzniveau für personenbezogene Daten, die aus der EU an teilnehmende Unternehmen in den USA übermittelt werden.
Die EU-Kommission hat am 19.12.2018 ihren Bericht über die zweite jährliche Überprüfung der Funktionsweise des EU-US-Datenschutzschilds veröffentlicht. Danach haben die von den US-Behörden ergriffenen Maßnahmen zur Umsetzung der Empfehlungen der Kommission aus ihrem letztjährigen Bericht das Funktionieren des Rahmens verbessert.

Die USA bieten deswegen nach wie vor ein angemessenes Schutzniveau für personenbezogene Daten, die aus der EU im Rahmen des Datenschutzschilds an teilnehmende Unternehmen in den USA übermittelt werden. Im Großen und Ganzen ist das Privacy-Shield-Abkommen nach Auffassung der EU-Kommission ein Erfolg.

Völlig frei von Kritik ist der Bericht dennoch nicht. So fordert die EU-Kommission die US-Behörden dazu auf, bis zum 28. Februar 2019 eine ständige Ombudsperson zu benennen. Diese solle gewährleisten, dass Beschwerden über den Zugriff von US-Behörden auf personenbezogene Daten überprüft und behandelt werden. Diese ständige Ombudsperson soll die im September 2018 auf Druck der EU von der USA eingesetzte Ombudsperson ersetzen.

Praxistipp:
Bis auf weiteres gilt die Feststellung eines angemessenen Datenschutzniveaus (Art. 46 DSGVO) für am Privacy Shield teilnehmende US-Unternehmen fort. Die Teilnahme am Privacy Shield bleibt also eine Option für den rechtmäßigen Datentransfer in die USA.

Dr. Daniel Meßmer, München
d.messmer@skwschwarz.de