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 04/2017

Der IT-Ticker 04/2017 informiert Sie über folgende Themen:

Fintech mal ganz anders - neue Regeln für den Betrieb der IT in Banken

Nicht nur Fintech-Unternehmen, auch die traditionellen Banken digitalisieren sich zunehmend. Für die Bankenaufsicht BaFin haben IT-Sicherheit und IT Governance „inzwischen den gleichen Stellenwert, wie die Ausstattung der Institute mit Kapital und Liquidität“. Sie hat daher ihre Anforderungen an den Betrieb von IT in Banken gerade komplett neu definiert.

Sie hat zum einen ihr Rundschreiben MaRisk von 2012 aktualisiert, zum anderen aber auch ein neues Rundschreiben formuliert, das die allgemeinen Anforderungen der MaRisk durch spezifische bankaufsichtliche Anforderungen an die IT (BAIT) weiter konkretisiert. Dabei sind die meisten Anforderungen sofort umzusetzen, da sie nach Meinung der BaFin ja nur die bereits bestehenden Gesetze konkretisieren. Lediglich für neu eingeführte Anforderungen der MaRisk gilt eine Umsetzungsfrist bis 31.10.2018. Die neuen Regeln führen z.B. die Funktion des IT-Sicherheitsbeauftragten in der Bank ein, der neben der Beratung der Geschäftsleitung auch eigene Rechte wahrnimmt, z.B. IT-Dienstleister zu überprüfen oder IT-Sicherheitsvorfälle zu untersuchen. Die Stelle ist intern mit eigenem Budget und Ausstattung zu besetzen, darf sich aber externe Unterstützung holen. Die Risikokultur der Banken soll gefördert werden, indem Eigenentwicklungen von Applikationen in gleicher Weise der Risikoprüfung zu unterziehen sind wie extern bezogene Software. Beim bloßen externen Bezug von Software (inkl. Wartung und Implementierung) wird nun klargestellt, dass dies keine Auslagerung ist. Allerdings stellen die BAIT auch für diesen Fremdbezug inhaltliche Anforderungen auf, die den Unterschied zur strenger regulierten Auslagerung kleiner

werden lassen. Die BaFin reagiert auf die Entwicklung in der IT-Industrie, wenn sie Cloud-Dienste und den Softwarebezug per SaaS aufgrund des Fremdbetriebs der Anwendungen als regulierte Auslagerung definiert. Für die künftig immer mehr automatisierten Prozesse der Fintechs dürfte von Bedeutung sein, dass auch die Aktionen von Maschinenusern immer auf eine konkret handelnde Person zurückzuführen sein müssen. Der voll automatisierte Prozess verlangt immer noch nach einem (automatisiert) verantwortlich zu machenden Menschen.

Praxistipp: Wer den IT-Betrieb in einer Bank verantwortet oder als Dienstleister in den Betrieb der Banken-IT involviert ist, kommt um eine detaillierte Prüfung der Auswirkungen aus MaRisk 2017 und BAIT auf seinen Service nicht herum. Die Ausschreibungen der Banken setzen dies bereits ab sofort voraus.

Dr. Matthias Orthwein, München
m.orthwein@skwschwarz.de

WLAN: Drittes Gesetz zur Änderung des Telemediengesetzes in Kraft

Schon seit geraumer Zeit versucht der deutsche Gesetzgeber die rechtlichen Grundlagen für eine Ausweitung an offenem WLAN in Deutschland zu schaffen. Am 13.10.2017 ist nun der jüngste Regelungsversuch in Kraft getreten: das Dritte Gesetz zur Änderung des Telemediengesetzes (3. TMGÄndG).

Deutschland hängt nicht nur beim Breitbandausbau hinterher. Auch bei der Anzahl frei verfügbarer WLAN-Hotspots hapert es. Seit 13.10.2017 ist nun das 3. TMGÄndG (BGBl. I S. 3530) in Kraft. Der Gesetzgeber erhofft sich, durch dieses Gesetz Rechtssicherheit für Anbieter von offenem WLAN zu schaffen und so das Angebot von offenem WLAN auszuweiten.

Das Gesetz gilt für kommerzielle wie private WLAN-Anbieter gleichermaßen. Es schließt die Störerhaftung aus, die bisher als Grundlage für Abmahnungen und Urteile gegen WLAN-Anbieter bei der Verbreitung rechtswidriger Inhalte herangezogen wurde. WLAN-Anbieter laufen damit nicht mehr Gefahr, als Störer für die durch Dritte verbreiteten rechtswidrigen Inhalte in Anspruch genommen zu werden.

Durch die Abschaffung der Störerhaftung werden die WLAN-Anbieter aber nicht völlig aus der Verantwortlichkeit für Rechtsverletzungen entlassen. Das Gesetz schafft mit § 7 Abs. 4 TMG einen neuen Anspruch für Inhaber von Rechten an geistigem Eigentum (Urheberrecht, Markenrecht, etc.). Danach können WLAN-Anbieter zur Sperrung des Zugangs zu rechtsverletzenden Inhalten verpflichtet werden. Der Anspruch steht Rechteinhabern allerdings erst offen, wenn sie die Rechtsverletzung nicht auf andere Weise beseitigen konnten. Welche Maßnahmen vorrangig in Anspruch zu nehmen sind, lässt das Gesetz jedoch offen. Aktuell tendiert die Rechtsprechung dazu, von den Rechteinhabern ein umfassendes und erfolgloses vorheriges Vorgehen gegen die Rechtsverletzer zu verlangen. Der Bundesgerichtshof hatte für Internetzugangsanbieter in seiner Goldesel-Entscheidung (I ZR 174/14) zuletzt u. a. die erfolglose Einschaltung von Privatdetekteien bei der Ermittlung der Rechtsverletzer gefordert.

Außerdem lässt das Gesetz offen, welche Sperrmaßnahmen von einem WLAN-Anbieter verlangt werden können. Es dürften aber insbesondere DNS-, IP-, URL- oder Portsperren in Betracht kommen.

Die Auswahl der konkreten Maßnahme muss dabei nach Zumutbarkeits- und Verhältnismäßigkeitsgesichtspunkten, also im Rahmen einer umfassenden Interessenabwägung, für den einzelnen WLAN-Anbieter beurteilt werden. Schon bei den Internetserviceprovidern war diese Abwägung in der Vergangenheit höchst umstritten. Insbesondere bei privaten WLAN-Anbietern ist daher noch offen, unter welchen Umständen die Sperrpflicht tatsächlich umgesetzt werden muss. Hier ist die Rechtsprechung gefordert, Leitlinien zu entwickeln.

Das Gesetz schließt zudem weitgehend die Möglichkeit für Rechteinhaber aus, WLAN-Anbieter für Kosten in Anspruch zu nehmen, die im Zusammenhang mit der Durchsetzung ihrer Rechte entstanden sind. Einzig bei einer gerichtlichen Inanspruchnahme bleibt es bei der normalen Kostenverteilung gemäß § 91 ZPO: wer den Prozess verliert zahlt die Gerichtskosten.

Fazit: Der Gesetzgeber bemüht sich, mit dem 3. TMGÄndG die notwendige Rechtssicherheit für WLAN Anbieter zu schaffen, um eine größere Abdeckung mit offenem WLAN zu gewährleisten. Aus Sicht der Praxis dürften sich die Identifizierung und Ausschöpfung der vorrangigen Maßnahmen sowie die Beurteilung der individuellen Zumutbarkeit und Verhältnismäßigkeit der Sperrmaßnahmen (noch) als große Herausforderungen erweisen.

Philipp Thomé, München
p.thome@skwschwarz.de

Wichtige Änderungen der Regelungen für Mängelkosten und Abnahmen

Kaum bemerkt ändern sich für Neugeschäft ab 01.01.2018 einige Vorschriften, auch für Mängelkosten im Kaufrecht und für die Abnahme werkvertraglicher Leistungen. Das hat erhebliche Auswirkungen für ITK-Verträge, etwa auf den Verkauf von Software und Hardware sowie insbesondere auf die Abnahmephase von Projekten.

Mängelkosten bei Kaufverträgen

In Zukunft muss ein Verkäufer nach den gesetzlichen Regelungen auch die Kosten des Ausbaus mangelhafter Leistungen und des Einbaus einer Neulieferung tragen. Solche Kosten kann der Verkäufer dann von seinem Vorverkäufer ersetzt verlangen. Das hat auch für ITK-Leistungen erhebliche Bedeutung: Bei dem Verkauf von Hardware – ob einzelne Komponenten oder ganze Systeme – und auch wenn Software gegen einmalige Vergütung zur dauerhaften Nutzung überlassen wird. In der Praxis können solche Aus- und Einbaukosten im Verhältnis zum Kaufpreis erhebliche Größenordnungen erreichen. Dann sieht das Gesetz zwar eine Begrenzungsmöglichkeit zu ersetzender Kosten auf angemessene Beträge vor. Gleichwohl bedeutet dies eine erhebliche Mehrbelastung für einen Verkäufer, zumal das Gesetz ihm kein Recht zur Selbstvornahme solcher Arbeiten einräumt.

Paradigmenwechsel für Abnahmeverlangen

Bei werkvertraglichen Leistungen muss der Auftragnehmer nach der gesetzlichen Regelung bislang eine vollständige und im Wesentlichen mangelfreie Leistung belegen, wenn er eine Abnahmeerklärung des Auftraggebers verlangen will. Das war oft nicht pragmatisch umsetzbar. Gleichwohl wird nach dem Gesetz erst mit der Abnahmeerklärung des Auftraggebers die Vergütung fällig und erst dann beginnt die Gewährleistung.

Für die Abnahme ändern sich die Rollen nun wesentlich: Zukünftig liegt eine Abnahme bereits dann vor, wenn der Auftragnehmer eine angemessene Frist zur Abnahme der fertigen Leistung setzt und der Auftraggeber innerhalb dieser Frist die Abnahme nicht unter Angabe mindestens eines Mangels verweigert. Untätigkeit des Auftraggebers führt also gerade im Gegensatz zur langjährigen Regelung zukünftig zur Abnahmeerklärung. Darauf sollten Auftraggeber insbesondere ihre Vorgehensweisen in Projekten anpassen.

Praxistipp: Verkäufer von ITK-Leistungen sollten ihre Verträge und ihre Kalkulation rechtzeitig an die gesetzlichen Änderungen anpassen. Auftraggeber von Werk-leistungen sollten ihre Verträge überarbeiten und auch Vorgehensweisen in der Abnahmephase von Projekten, um „ungewollte" Abnahmeerklärungen zu vermeiden.

Martin Schweinoch, München
m.schweinoch@skwschwarz.de

Online-Test zur Datenschutz-Grundverordnung

Am 25. Mai 2018 endet die Übergangsfrist, die der europäische Gesetzgeber Unternehmen für die Umstellung ihrer Prozesse auf die Datenschutz-Grundverordnung (DS-GVO) eingeräumt hat. Ab diesem Zeitpunkt können Aufsichtsbehörden bei Verstößen Bußgelder in Höhe von bis zu 4 % des weltweiten Unternehmensumsatzes verhängen und Abmahnungen drohen.Viele Unternehmen scheinen das Problem aber noch nicht auf der Agenda zu haben. So hat eine Umfrage des Branchenverbands Bitkom ergeben, dass bislang nur jedes 4. Unternehmen zusätzliches Personal für die Umsetzung der DS-GVO einsetzt. Neueinstellungen gab es dazu bei 5 % der Befragten, 20 % gaben an, vorhandenes Personal einzusetzen.

Auch das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) hat festgestellt, dass der Umsetzungsstand der neuen gesetzlichen Anforderungen im Datenschutzrecht bei bayerischen Unternehmen längst noch nicht so weit ist, wie erhofft. Daher hat das BayLDA einen Online-Test unter dem Motto „Weg zur DS-GVO - Selbsteinschätzung" entwickelt, der auch auf Englisch verfügbar ist.

Mit diesem Online-Test soll eine spielerische Standortbestimmung zur Verfügung gestellt werden, so dass Unternehmen selbst einschätzen können, an welcher Stelle man sich zur richtigen Umsetzung der neuen europäischen Datenschutzanforderungen befindet.

Als Ergebnis erhält jeder Teilnehmer eine detaillierte Auswertung zu den gewählten Anforderungen sowie eine Beschreibung, wie nach Ansicht des BayLDA die Anforderungen zur DS-GVO umzusetzen wären.

Praxistipp: Es kann davon ausgegangen werden, dass bei Datenschutzprüfungen durch Aufsichtsbehörden ab Mai 2018 auf Bereiche dieser Fragen abgezielt werden. Mit Durchführung des Online-Tests können Unternehmen selbst prüfen, wie weit sie auf dem Weg zur Erfüllung der neuen gesetzlichen europäischen Forderungen fortgeschritten sind. Unternehmen verbleiben nur noch 6 Monate Schonfrist, bis das neue europäische Datenschutzrecht im Unternehmen umgesetzt werden muss.

Dr. Oliver Hornung, Frankfurt/Main
o.hornung@skwschwarz.de

Urteil des Bundesgerichtshofs zur Zulässigkeit der Speicherung von dynamischen IP-Adressen

Der BGH hat am 16. Mai 2017 entschieden, dass dynamische IP-Adressen personenbezogene Daten sind und dass sie unter bestimmten Umständen von Website-Betreibern über den temporären Seitenabruf hinaus gespeichert werden dürfen (Urteil vom 16. Mai 2017, Az.: VI ZR 135/13). Damit unterfallen IP-Adressen grundsätzlich den datenschutzrechtlichen Regelungen.

Über den Personenbezug von dynamischen IP-Adressen in der Hand des Website-Betreibers kann man sich deshalb streiten, weil es sich aus Sicht des Website-Betreibers zunächst einmal nur um eine Nummer handelt, die aus sich heraus keinen Rückschluss auf den Nutzer zulässt. Darüber hinaus wird diese Nummer bei Internetanschlüssen von Endverbrauchern bei jeder Einwahl ins Internet oder in der Regel zumindest einmal täglich neu vergeben. Die Zuordnung zu einer Person ist damit nicht dauerhaft möglich. Es stellt sich daher die folgende Frage: Wann ist der Nutzer hinter der IP-Adresse bestimmbar?

Der BGH legte diese Frage vor einiger Zeit dem Europäischen Gerichtshof (EuGH) vor.

Der EuGH wählte einen Mittelweg: Danach kann eine dynamische IP-Adresse für den Website-Betreiber ein personenbezogenes Datum darstellen, wenn er über „rechtliche Mittel“ verfügt, mit deren Hilfe er die betroffene Person bestimmten bzw. bestimmen lassen kann (Urteil vom 19. Oktober 2016, Az.: C-582/14).

Auf Grundlage dieser Vorabentscheidung des EuGH entschied nun der BGH, dass eine Speicherung von IP-Adressen dann erfolgen könne, wenn sie erforderlich sei, um die generelle Funktionsfähigkeit der Dienste zu gewährleisten. Für die vom EuGH angesprochene Interessenabwägung seien insbesondere Feststellungen über das Gefahrenpotential bei dem konkreten Online-Dienst notwendig. Dabei müssten auch die Gesichtspunkte der Generalprävention und der Strafverfolgung gebührend berücksichtigt werden.

Die Entscheidung des BGH gibt den Gerichten viel Spielraum für eine präzise Einzelfallentscheidung. Da im zu entscheidenden Fall die notwendige Tatsachengrundlage vom Berufungsgericht nicht ausreichend erforscht wurde, konnte der BGH keine abschließende Abwägung vornehmen.

Praxistipp: Website-Betreibern ist zu empfehlen, IP-Adressen nur insoweit zu speichern, als diese tatsächlich für die Funktionsfähigkeit des Dienstes erforderlich sind. Zudem sollte die Entscheidung des Berufungsgerichts abgewartet werden, bei der eine weitere Konkretisierung der Kriterien für die Speicherung der IP-Adressen zu erwarten ist.

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

Aufsichtsbehörden veröffentlichen 10-Punkte-Papier zur Datenschutz-Grundverordnung

Unternehmen haben noch knapp ein Jahr bis die Datenschutz-Grundverordnung in allen Mitgliedstaaten zwingend zu beachten ist. Datenschutz ist dann eine Führungsaufgabe und die Nichtbeachtung wird teuer. Dies gilt sowohl in Großunternehmen und im Mittelstand als auch in kleinen Betrieben sowie in Vereinen.

Um Konformität mit der Verordnung herzustellen, sind Prozesse und Strukturen zum Teil erheblich anzupassen. Zur Vorbereitung hatten die Verantwortlichen zwei Jahre Zeit. Nunmehr ist die Hälfte der Zeit bereits abgelaufen. Aus diesem Grunde sollten Verantwortliche dringend prüfen, ob sie die erforderlichen Maßnahmen getroffen haben. Sofern dies noch nicht der Fall ist, müssen dringend entsprechende Maßnahmen getroffen werden.

Nachdem bereits das Bayerische Landesamt für Datenschutzaufsicht einen Fragebogen zur Umsetzung der Datenschutz-Grundverordnung veröffentlicht hat (wir berichteten), haben die Aufsichtsbehörden nunmehr in einem 10-Punkte-Papier Anregungen für Unternehmen zur Vorbereitung auf die Datenschutz-Grundverordnung zusammengestellt.

Danach sollten im Unternehmen zunächst in die relevanten Personen Gruppen – Geschäftsführung, Datenschutzbeauftragte und andere für das Thema Datenschutz zuständige Personen – dafür sensibilisiert werden, dass die Datenschutz-Grundverordnung direkte Auswirkung auf das Unternehmen als datenverarbeitende Stelle hat. Anschließend empfehlen die Aufsichtsbehörden eine Bestandsaufnahme durchzuführen. Dies entspricht auch dem Vorgehen welches SKW Schwarz Rechtsanwälte seinen Mandanten bei der Beratung von Datenschutz-Grundverordnungs-Projekten empfiehlt.

Als wichtige Themen der Datenschutz-Grundverordnung nennen die Aufsichtsbehörden die Rechtsgrundlage für die Verarbeitung personenbezogener Daten, personenbezogene Daten von Kindern sowie den Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen. Zudem raten die Aufsichtsbehörden dazu Verträge, insbesondere zur Auftragsverarbeitung, zu überprüfen und überarbeiten. Wichtig ist auch, dass Unternehmen die Betroffenenrechte und Informationspflichten ordnungsgemäß umsetzen. Schließlich sind Prozesse zur Datenschutzfolgenabschätzung, zu Melde- und Konsultationspflichten sowie zur ordnungsgemäßen Dokumentation zu implementieren und organisieren.

Praxistipp: Ab dem 25. Mai 2018 müssen Verantwortliche die Datenschutz-Grundverordnung einhalten. Anderenfalls drohen Bußgelder und Schadensersatzforderungen in Millionenhöhe. Das 10-Punkte-Papier der Aufsichtsbehörden gibt Unternehmen einen Überblick und Anregungen zur Vorbereitung auf die Datenschutz-Grundverordnung. Die dort genannten Punkte sollten im Rahmen eines Projektes im Unternehmen innerhalb des nächsten Jahres umgesetzt werden. Sofern dies noch nicht geschehen ist, sind Unternehmen dringend dazu angehalten ein Projekt zur Umsetzung der Datenschutz-Grundverordnung zu starten.

SKW Schwarz Rechtsanwälte hat eine Taskforce gebildet und berät aktuell bereits viele Mandanten vom klassischen deutschen Mittelständler bis hin zum multinationalen Großunternehmen in Umsetzungsprojekten zur Datenschutz-Grundverordnung.

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

BNetzA setzt Vorratsdatenspeicherung aus

Seit dem 1. Juli 2017 sind Erbringer öffentlich zugänglicher Telekommunikationsdienste zur Vorratsdatenspeicherung verpflichtet. Die Bundesnetzagentur (BNetzA) hat nun entschieden, diese Pflicht vorerst nicht durchzusetzen.

In einer öffentlichen Mitteilung zur Speicherpflicht nach § 113b TKG hat die BNetzA angekündigt, von Anordnungen und sonstigen Maßnahmen zur Durchsetzung der Pflicht zur Vorratsdatenspeicherung einstweilen abzusehen. Vorerst drohen Anbietern von Telekommunikationsdiensten damit auch keine Bußgelder, wenn sie Verkehrs- und Inhaltsdaten nicht wie vorgeschrieben speichern.

Als Grund für die Aussetzung nennt die Behörde den Beschluss des OVG Nordrhein-Westfalen vom 22.06.2017 (Az. 13 B 238/17), wonach die gesetzliche Pflicht zur Vorratsdatenspeicherung EU-Recht verletze. Anlass für die Gerichtsentscheidung war der Eilantrag eines Internetproviders, vorläufig von der Pflicht zur Speicherung von Kundendaten befreit zu werden.

Wegen der über den Einzelfall hinausgehenden Tragweite dieser Entscheidung wird die BNetzA bis zum rechtskräftigen Abschluss eines Hauptsacheverfahrens zur Überprüfung der Rechtmäßigkeit der Speicherpflicht keine Maßnahmen zur Durchsetzung der Vorratsdatenspeicherung unternehmen.

Praxistipp: Ob eine mangelnde Umsetzung der Vorratsdatenspeicherung für Anbieter von Telekommunikationsdiensten bis zur rechtskräftigen Entscheidung in dem Hauptsacheverfahren tatsächlich absolut folgenlos bleibt, ist damit nicht sichergestellt: So könnten etwa Konkurrenten zur Abmahnung der Anbieter berechtigt sein, welche die Speicherpflicht nicht umsetzen.

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

Gesetz zur Netzwerk- und Informationssicherheit in Kraft

Zum 30.06.2017 sind Änderungen des BSI-Gesetzes zur Erhöhung des Sicherheitsstandards von Netzwerk- und Informationssystemen in Kraft getreten. Anbieter „digitaler Dienste“ in Deutschland sind zukünftig zum Schutz Ihrer Systeme verpflichtet und müssen Sicherheitsvorfälle an das BSI melden.

Mit der Gesetzesänderung setzt Deutschland die EU-Richtlinie zur Gewährleistung eines hohen Sicherheitsstandards von Netzwerk- und Informationssystemen (NIS-Richtlinie) in nationales Recht um. Zu diesem Zweck ändert das Umsetzungsgesetz in erster Linie Bestimmungen des BSI-Gesetzes und des Telekommunikationsgesetzes.

Welche neuen Pflichten gibt es?

Ab dem 10.05.2018 sind nicht mehr nur Betreiber kritischer Infrastrukturen, sondern erstmals auch Anbieter so genannter „digitaler Dienste“ verpflichtet, Maßnahmen zum Schutz der von ihnen eingesetzten Netzwerk- und Informationssysteme zu ergreifen. Außerdem müssen Sicherheitsvorfälle unverzüglich an das BSI gemeldet werden, wenn sie im Einzelfall erhebliche Auswirkungen auf die Erbringung des Digitalen Dienstes haben können.

Wer ist betroffen?

Zu den „digitalen Diensten“ zählen Suchmaschinen, Online-Marktplätze und Cloud-Dienste. Die Sicherheits- und Meldepflichten gelten für Anbieter digitaler Dienste, die ihren Hauptsitz in Deutschland haben, einen Vertreter in Deutschland benannt haben oder Netzwerk- und Informationssysteme in Deutschland betreiben, um digitale Dienste zu erbringen.

Ausblick

Die EU-Kommission erarbeitet derzeit spezifische Anforderungen an Sicherheitsmaßnahmen zum Schutz von Anbietern digitaler Dienste eingesetzten IT-Systeme und Kriterien für die Meldung von Sicherheitsvorfällen. Erste Ergebnisse werden im August 2017 erwartet.

In Deutschland ist das BSI für die Durchsetzung der Pflichten nach dem BSI-Gesetz zuständig. Erfüllt ein Anbieter digitaler Dienste die neuen Anforderungen nicht, drohen Bußgelder von bis zu EUR 50.000,00.

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

Fünf weitere DSK-Kurzpapiere zur DS-GVO veröffentlicht

Die Deutschen Datenschutzbehörden stimmen sich aktuell in Kurzpapieren zur Auslegung der DS-GVO gemeinsam ab und veröffentlichen diese.
Die ersten drei DSK-Kurzpapiere betrafen folgende Themen:

• Verzeichnis von Verarbeitungstätigkeiten
• Aufsichtsbefugnisse / Sanktionen
• Verarbeitung personenbezogener Daten für Werbung

(vergleiche unseren Beitrag Auslegungshilfen der deutschen Aufsichtsbehörden zum neuen europäischen Datenschutzrecht vom 6. Juli 2017)

Mit dem Kurzpapier Nr. 4 wird über den Datentransfer in Drittländer informiert. Die DS-GVO sieht hierzu folgende Möglichkeiten vor:

• Festlegung der Angemessenheit des Datenschutzniveaus im Drittland durch EU- Kommission (Art. 45 DS-GVO)
• Vorliegen geeigneter Garantien (Art. 46 DS-GVO) oder
• Ausnahmen für bestimmte Fälle (Art. 49 DS-GVO)

Aktuell wurden vier weitere DSK-Kurzpapiere zur DS-GVO veröffentlicht und zwar zu folgenden Themen:

• Datenschutz-Folgenabschätzung
• Auskunftsrecht
• Marktortprinzip
• Maßnahmenplan

Interessant ist insbesondere das Kurzpapier für einen Maßnahmenplan zur DS-GVO für Unternehmen. Denn viele Unternehmen sind nach Auffassung der Datenschutzaufsichtsbehörden noch nicht auf die DS-GVO und deren Auswirkungen auf die Unternehmensprozesse vorbereitet. Daher haben die Datenschutzaufsichtsbehörden einige Tipps zur Erstellung eines Maßnahmenplans für Unternehmen zusammengestellt.

Die aktuellen Kurzpapiere Nr. 4 bis Nr. 8 sind unter folgendem Link abrufbar:
www.lda.bayern.de/de/datenschutz_eu.html.

Dr. Oliver Hornung, München
o.hornung@skwschwarz.de

Gesetz zur Vorratsdatenspeicherung nicht mit Unionsrecht vereinbar

Die ab dem 1. Juli 2017 geltende Pflicht zur anlasslosen Speicherung von Verkehrs- und Standortdaten („Vorratsdatenspeicherung“) verstößt gegen EU-Recht.

§ 113b TKG verpflichtet Erbringer öffentlich zugänglicher Telekommunikationsdienste mit Wirkung zum 1. Juli 2017, Verkehrsdaten für zehn und Standortdaten für sechs Wochen zu speichern. Nach Auffassung des Oberverwaltungsgerichts Nordrhein-Westphalen ist diese Vorratsdatenspeicherung

nicht mit dem Unionsrecht vereinbar (Beschluss v. 22.06.2017, Az. 13 B 238/17).

Anlass für die Entscheidung war der gerichtliche Eilantrag eines Internetproviders, vorläufig von der Pflicht zur Speicherung von Kundendaten befreit zu werden. Während das Verwaltungsgericht Köln den Antrag noch abgelehnt hatte (Beschluss v. 25.01.2017, Az.: 9 L 1009/16) hat das Oberverwaltungsgericht der Beschwerde des Internetproviders nunmehr stattgegeben.

§ 113b TKG verstößt danach gegen die so genannte Datenschutzrichtlinie vom 12.07.2002 (Richtlinie 2002/58/EG). Nach den Vorgaben des Europäischen Gerichtshofs (Urteil v. 21.12.2016, Rs. C-203/15 und C-698/15) sei eine Pflicht zur Vorratsdatenspeicherung allenfalls dann rechtmäßig, wenn der betroffene Personenkreis von vornherein auf Fälle beschränkt sei, bei denen ein Zusammenhang mit der Verfolgung schwerer Straftaten oder der Abwehr schwerwiegender Gefahren bestehe. Da § 113b TKG eine solche Einschränkung nicht vorsehe, sei die Vorschrift nicht mit EU-Recht vereinbar.

*Praxistipp: Bindende Wirkung hat die Entscheidung des Oberverwaltungsgerichts nur für den rechtssuchenden Internetprovider. Es ist deswegen nicht auszuschließen, dass andere Gerichte bei einem vergleichbaren Verfahren zu einer abweichenden Rechtsauffassung gelangen. Das Bundesverfassungsgericht hat es jüngst **abgelehnt**, vor dem 1. Juli 2017 über die Verfassungsgemäßheit der Vorratsdatenspeicherung zu entscheiden.*

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

Pflicht zur Softwareaktualisierung gegen geplante Obsoleszenz

Das EU-Parlament fordert die Einführung eines „angemessenes Nutzungszeitraums“ für Software, in dem Softwarehersteller zur Bereitstellung von Sicherheitsupdates verpflichtet sind.

In einer am 04.07.2017 verabschiedeten Entschließung zur Lebensdauer von Produkten schlägt das EU-Parlament Maßnahmen zum Schutz von Verbrauchern gegen Software-Obsoleszenz vor. Insbesondere sollen Softwarehersteller und -lieferanten zu mehr Transparenz beim Vertrieb von Software verpflichtet werden.

So sollen Hersteller von Betriebssystemen in Softwareverträgen zukünftig eine Mindestdauer angeben, für die Sicherheitsaktualisierungen bereitgestellt werden. Zu dem Zweck schlägt das EU-Parlament vor, eine „angemessene Nutzungsdauer“ für Softwareprodukte zu definieren. Durch diese Maßnahmen soll verhindert werden, dass Softwarehersteller die Lebensdauer ihrer Produkte bewusst verkürzen, indem sie deren Pflege einstellen.

Die Entschließung sieht überdies eine Pflicht von Softwareherstellern vor, die Abwärtskompatibilität von Softwareupdates sicherzustellen und Nutzern stets zu ermöglichen, installierte Updates selbst rückgängig zu machen.

Praxistipp: Die Vorschläge des EU-Parlaments sind nicht bindend. Es bleibt daher abzuwarten, ob die EU-Kommission die Vorschläge aufgreift und ein entsprechendes Gesetzgebungsverfahren einleitet.

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

Auslegungshilfen der deutschen Aufsichtsbehörden zum neuen europäischen Datenschutzrecht

Die deutschen Aufsichtsbehörden befassen sich aktuell intensiv mit den neuen Rechtsgrundlagen der EU-Datenschutz-Grundverordnung (DS-GVO), deren Anforderungen und stimmen eine einheitliche Sichtweise ab. Erste Ergebnisse dieses Prozesses sind verabschiedete Kurzpapiere zur DS-GVO, die die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) seit dem 3. Juli 2017 veröffentlichen. Diese Kurzpapiere dienen als erste Orientierungshilfe, wie nach Auffassung der DSK die Verordnung im praktischen Vollzug angewendet werden sollte.

Die ersten drei Kurzpapiere befassen sich mit den Themen:

- Verzeichnis von Verarbeitungstätigkeiten,
- Aufsichtsbefugnisse/Sanktionen,
- Verarbeitung personenbezogener Daten für Werbung.

Diese Kurzpapiere können auf den Internetseiten der Aufsichtsbehörden abgerufen werden.

Die Datenschutzkonferenz betont, dass die Auslegungshilfen zum neuen europäischen Datenschutzrecht unter dem Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegungshilfe durch den europäischen Datenschutzausschuss stehen.

Praxistipp: Neben den Stellungnahmen und Interpretationsleitfäden der Artikel-29-Datenschutzgruppe, die regelmäßig auf ihrer Website veröffentlicht werden, liegen nunmehr auch erste abgestimmte Auslegungshilfen der deutschen Aufsichtsbehörden zur DS-GVO vor. Damit erhalten Unternehmen für ihr Projekt zur Umsetzung der DS-GVO Hilfestellungen bei der Auslegung der Vorschriften zum neuen europäischen Datenschutzrecht.

Dr. Oliver Hornung, München
o.hornung@skwschwarz.de

Whitepaper zur Pseudonymisierung unter Berücksichtigung der Vorgaben der DS-GVO

Personenbezogene Daten sind der Rohstoff der Zukunft. Das neue europäische Datenschutzrecht der Datenschutz-Grundverordnung (DS-GVO) gibt der Wirtschaft die Verantwortung für den Schutz personenbezogener Daten, indem sie von den verantwortlichen Unternehmen verlangt, Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen zu gewährleisten. Ein probates Mittel dazu stellt nach der DS-GVO die Pseudonymisierung von personenbezogenen Daten dar.

Die Fokusgruppe Datenschutz der Plattform Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft hat im Rahmen des Digital-Gipfels 2017 ein White-paper mit Leitlinien für die rechtssichere Nutzung von Pseudonymisierungslösungen unter Berücksichtigung der Vorgaben der DS-GVO veröffentlicht.

Das Whitepaper erläutert, in welchem Zusammenhang die Pseudonymisierung unter der Vorgaben

der DS-GVO eine Rolle spielen kann und gibt anschauliche Hinweise und Praxisbeispiele für den rechtssicheren Einsatz.

Praxistipp: Art. 25 DS-GVO verpflichtet Verantwortliche dazu, den vorgeschriebenen Datenschutz auch durch die Gestaltung der von ihnen eingesetzten IT und durch datenschutzfreundliche Voreinstellungen umzusetzen. Ein Beispiel hierfür ist die möglichst frühe und umfassende Pseudonymisierung personenbezogener Daten. Hierfür liefert das Whitepaper anschauliche Maßnahmen, um drohende Bußgelder vermeiden zu können.

Dr. Oliver Hornung, München
o.hornung@skwschwarz.de