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 02/2019

Der IT-Ticker 02/2019 informiert Sie über folgende Themen:

EuGH: Keine TKG-Überwachungspflichten für Gmail – für SkypeOut hingegen schon

Der EuGH entschied am 13. Juni 2019, dass der internetbasierte Emaildienst Gmail nicht als „elektronischer Kommunikationsdienst“ im Sinne von Art. 2 Buchst. C der Rahmenrichtlinie (RL 2002/21 EG in der durch RL 2009/140/EG geänderten Fassung) einzuordnen ist.

Diese Einordnung gilt für einen internetbasierten Emaildienst, der keinen Internetzugang vermittelt und nicht ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze besteht. Bei Gmail handelt es sich um einen sogenannten „Over-the-top-Dienst“ (OTT), d. h. einen über das Internet zur Verfügung stehender Dienst, ohne dass ein traditioneller Internet-Service-Provider involviert ist. Zwar nehme Gmail eine Übertragung von Signalen vor, indem von Inhabern eines Gmail-Kontos in Datenpakete zerlegte Emails über ihre Email-Server in das offene Internet eingespeist und aus diesem empfangen werden. Dies stelle allerdings keine „überwiegende“ Übertragung von Signalen dar. Nicht Gmail, sondern die Internetzugangsanbieter der Absender/Empfänger und die Betreiber der verschiedenen Netze, aus denen das offene Internet besteht, seien für die Übertragung verantwortlich. Der Umstand, dass Google auch eigene elektronische Kommunikationsnetze in Deutschland betreibt, verändere dieses Ergebnis nicht. Dem Urteil liegt ein langjähriger Rechtsstreit zwischen der Google LLC und der Bundesrepublik Deutschland über einen Bescheid der Bundesnetzagentur zugrunde, in welchem Gmail als Telekommunikationsdienst eingeordnet und zur Einhaltung der Meldepflicht nach § 6 Telekommunikationsgesetz (TKG) aufgefordert wurde.

Im Gegensatz dazu ordnete der EuGH in seiner Entscheidung vom 5. Juni 2019 den Dienst SkypeOut – der kein OTT Dienst ist – als elektronischen Kommunikationsdienst ein. Es handelt hierbei sich um eine Zusatzfunktion zur Kommunikationssoftware „Skype“, welche unter Verwendung von „Voice over IP (VoIP)“-Technik (Stimmübertragung über Internetprotokoll) Telefonanrufe von einem Endgerät an einen Festnetz- oder Mobilfunkanschluss ermöglicht. Die Bereitstellung einer Software mit einer „VoIP“ -Funktion, mit der der Nutzer von einem Endgerät über das öffentliche Telefonnetz (PSTN) eines Mitgliedstaats eine Festnetz- oder Mobilfunknummer eines nationalen Rufnummernplans anrufen kann, sei als „elektronischer Kommunikationsdienst“ einzustufen. Dies gelte, wenn zum einen dem Herausgeber der Software für die Bereitstellung des Dienstes Entgelt gezahlt werde und zum anderen den Abschluss von Vereinbarungen des Herausgebers des Dienstes mit für die Übertragung und die Terminierung von Anrufen in das PSTN ordnungsgemäß zugelassenen Telekommunikationsdienstleistern beinhalte. SkypeOut ist kostenpflichtig, da die Nutzung entweder von einer Vorauszahlung oder einem Abonnement abhängig ist. Im Gegensatz zu Gmail trete SkypeOut als Verantwortlicher für die Übertragung auf, da ohne die Vereinbarungen zwischen Skype und den PSTN Telekommunikationsdienstleistern die Übermittlung der Sprachsignale nicht erfolgen könne. Dem steht nicht entgegen, dass die Standard Skype-Software auch ohne die Zusatzfunktion SkypeOut genutzt werden kann oder dass in den allgemeinen Vertragsbedingungen

von SkypeOut die Verantwortung für die Übertragung von Signalen an die Nutzer ausgeschlossen wird. Vergleichbar mit dem deutschen Ausgangsverfahren bei Gmail liegt diesem Urteil ein Rechtsstreit zwischen Skype Communications und dem Belgischen Institut für Post und Fernmeldewesen (IBPT) zugrunde. IBPT hatte eine Geldbuße wegen Bereitstellung eines elektronischen Kommunikationsdienstes durch Skype Communications ohne Einhaltung der erforderlichen Meldepflicht verhängt.

Sowohl Gmail als auch SkypeOut wollten eine Einordnung als elektronischer Kommunikationsdienst stets vermeiden, da die rechtlichen Verpflichtungen nach dem TKG sehr weitreichend sind. Nach §§ 110, 113 TKG müssen elektronische Kommunikationsdienstleister nach staatlicher Anordnung die Überwachung und Aufzeichnung der Telekommunikation eines Beschuldigten ermöglichen. Zudem müssen sie (bei einem Kundenstamm von mehr als 100.000) für die Auskunft von Bestandsdaten eine gesicherte elektronische Schnittstelle bereitstellen. Nach der Gmail Entscheidung müssen OTT Dienste diesen Pflichten nicht nachkommen, SkypeOut dagegen schon.

Praxistipp:
Für Betreiber von OTT Diensten (Messengerdienste wie WhatsApp, Telegramm und Threema) gilt somit, dass diese keine „elektronischen Kommunikationsdienste" sind. Für Betreiber kostenpflichtiger (Nicht-OTT-) Dienste, die mit SkypeOut vergleichbar sind, muss die Einordnung sorgfältig geprüft werden. Allerdings ist zu bedenken, dass die aktuelle Einordnung des EuGH nicht bis „ans Ende aller Tage" gilt. Die Urteile beziehen sich auf Regelungen, die nur noch bis Ende 2020 Anwendung finden, da bereits seit Dezember 2018 die neue Richtlinie über den europäischen Kodex für die elektronische Kommunikation in Kraft ist. In Deutschland wird aktuell der entsprechende Gesetzesentwurf zur Umsetzung der Richtlinie erarbeitet.

Hannah Mugler, Berlin
h.mugler@skwschwarz.de
Nikolaus Bertermann, Berlin
n.bertermann@skwschwarz.de

Das Bundeskartellamt fordert mehr Flexibilität und Spielräume für Facebook-Nutzer

Das Bundeskartellamt hat der Facebook Inc. und der Facebook Germany GmbH („Facebook") weitreichende Beschränkungen bei der Verarbeitung von Nutzerdaten auferlegt. Es fordert Facebook auf, den Nutzern die Möglichkeit der Einwilligung in die konzernübergreifende Datenverarbeitung entsprechend der DSGVO und nicht mittels der allgemeinen Nutzungsbedingungen einzuräumen. Facebook würde diese Nutzungsbedingungen aufgrund der in Deutschland vorherrschenden Marktmacht zu starr entwerfen. Der jeweiligen Nutzer würde dadurch in unzulässiger Weise zu stark eingeschränkt.

Facebook ist hingegen der Ansicht, dass das Bundeskartellamt das Wettbewerbsrecht in verfehlter Weise anwende, indem es Sonderanforderungen aufstelle, die nur für ein einziges Unternehmen gelten würden.

Die Entscheidung des Bundeskartellamts verwundert nicht und entspricht ständiger Rechtsprechung.

Die Facebook Inc. gewinnt – bei Betrachtung der Key Performance Indikatoren – jährlich an Nutzern dazu und ist im Alltag vieler Millionen Deutscher angekommen und zu Hause. Das soziale Netzwerk Facebook, die sehr beliebte Video- und Foto-Sharing App Instagram und die dazugehörigen Messengerdienste (WhatsApp und FB-Messenger) sind die vier beliebtesten Dienste bei den Nutzern. 75 % der Zeit, die Nutzer mit Apps verbringen, verbringen sie im Durchschnitt mit Applikationen der Facebook Inc.

Die Durchdringung des deutschen Marktes ist dabei als sehr hoch zu bewerten. Das soziale Netzwerk Facebook hat mit 23 Mio. täglichen und 32 Mio. monatlichen Nutzern einen Marktanteil von über 95 % bei den täglich aktiven Nutzern und von über 80 % bei den monatlich aktiven Nutzern. In WhatsApp sind es sogar 42 Mio. täglich aktive Nutzer und 46 Mio. pro Woche. Dies entspricht nahezu allen mündigen Personen in Deutschland ab dem Geburtsjahr 1955.

In der Vergangenheit waren diese Dienste eigenständig und sammelten somit auch eigenständig

Nutzerdaten und Mitgliedschaften. Aufgrund des rapiden Wachstums von WhatsApp und Instagram übernahm die Facebook Inc. diese in weiser Voraussicht und erhielt in den folgenden Jahren immer weitreichendere Marktdurchdringung.

Aus wirtschaftlichen Gründen – insbesondere der Kosteneinsparung, Effizienz und Effektivität – möchte das Unternehmen die derzeit dezentrale Sammlung von Nutzerdaten in einem Facebook-Nutzerkonto zentral kollektivieren und verarbeiten.

In Zuge dessen verabschiedete das Unternehmen neue Nutzungsbedingungen für seine Plattformen. Danach könnte der Nutzer nun entscheiden, ob er Produkte der Facebook Inc. nutze und damit einer kollektiven Verarbeitung seiner Daten zustimme oder nicht. Grundsätzlich wäre diese Praxis durch die Privatautonomie eines jeden Einzelnen gedeckt. Die Nutzer sollen und können selbst im Rahmen der Rechtsordnung eigenverantwortlich und rechtsverbindliche Regelungen treffen.

Aufgrund der Marktdurchdringung und Beherrschung der beliebtesten Apps – die fast alle dem Facebook-Konzern angehören – musste das Bundeskartellamt jedoch als Korrektiv tätig werden, damit die Grundsätze der Privatautonomie nicht konterkariert werden und der Nutzer geschützt wird.

Die Nutzungsbedingungen der Facebook Inc. würden die Nutzer zu stark in ihren Rechten einschränken, da soziale Medien und Nachrichtendienste – insbesondere Facebook, Instagram und WhatsApp – das soziale Gefüge der gegenwärtigen Gesellschaft prägen. Eine starre vertragliche Bindung würde die Nutzer daher vor die Wahl stellen, am Kreis der Aktiven und vernetzten 40 Mio. Deutschen teilzunehmen oder sich als Minderheit aus der Interaktion und dem sozialen Umfeld zurückziehen.

Damit würde die Privatautonomie aus praktischen Gesichtspunkten zu stark beschränkt. Die Nutzer könnten zwar eigenverantwortlich und rechtsverbindlich eine Willenserklärung abgeben, jedoch nur unter hohem sozialen Druck und nicht aus freiem Entschluss.

Das Bundeskartellamt agiert hier im Sinne der ständigen Rechtsprechung des Bundesgerichtshofs. Danach können nicht nur überhöhte Preise, sondern auch die Unangemessenheit von vertraglichen Regelungen und Konditionen eine missbräuchliche Ausbeutung darstellen.

Regelungen und Konditionen seien angemessen, wenn die Nutzer selbst über die Verarbeitung ihrer Daten entscheiden könnten. Die Behörde verbietet Facebook nicht, weiterhin gewerblich tätig zu sein und Daten plattformübergreifend – oder auch über Dritte mittels Cookies, Pixeln und Verlinkungen – einzusammeln und zu verarbeiten. Dies soll weiterhin zulässig sein, jedoch unter der Voraussetzung, dass der jeweilige Nutzer Facebook seine Einwilligung erteilt.

Die Entscheidung des Bundeskartellamts hat ein großes Medienecho hervorgerufen. Sie entspricht inhaltlich jedoch der üblichen Spruchpraxis und war daher absehbar.

Wir empfehlen die weitere Entwicklung abzuwarten. Wir gehen davon aus, dass dieser Fall verschiedene Gerichte beschäftigen wird.

Dr. Stefan Peintinger, München
s.peintinger@skwschwarz.de

Cookies & Co. vor dem faktischen Aus?

Neue Orientierungshilfe der Datenschutzkonferenz (DSK) und anstehende Entscheidung des EuGH zu Cookies. Schon lange gibt es die Diskussion, ob die Nutzung von Cookies und anderen Technologien zum Zwecke der Webanalyse, des Trackings und der individualisierten Werbung die ausdrückliche Einwilligung der Betroffenen erfordert oder ob diese auch auf ein berechtigtes Interesse gestützt werden kann. Zu dieser Frage haben sich sowohl der Generalanwalt beim EuGH also auch die deutsche Datenschutzkonferenz (DSK) jüngst geäußert. Beide Äußerungen sprechen sich im Kern dafür aus, dass eine Einwilligung erforderlich ist und ein berechtigtes Interesse in den allermeisten Fällen nicht (mehr) ausreichend sein soll.

Bisher wurde in der Praxis häufig von der Einholung einer Einwilligung unter Verweis auf § 15 Abs. 3 TMG abgesehen und eine Opt-Out Lösung praktiziert. Alternativ werden häufig auch so genannte Cookie-Consent-Banner eingesetzt, die versuchen, aus dem Verhalten des Nutzers eine Einwilligung abzuleiten.

Verfahren vor dem EuGH

Vor dem Europäischen Gerichtshof streiten die Planet49 GmbH und der Bundesverband der Verbraucherzentralen (Rs C-673/17) darüber, ob die Einholung einer aktiven Einwilligung bei der Verwendung von Cookies erforderlich ist.

Einen Vorgeschmack auf die mögliche Entscheidung des EuGH lieferten am 21. März 2019 die Schlussanträge des Generalanwalts Maciej Szpunar in der genannten Angelegenheit. Der Generalanwalt äußerte sich dahingehend, dass nach der E-Privacy Richtlinie und der Datenschutzgrundverordnung die Diensteanbieter eine Einwilligung für die Nutzung von Cookies einholen müssten. Diese Einwilligung könne aber nicht durch eine vorausgewählte Checkbox eingeholt werden. Zudem müssten Nutzer über die Funktionsdauer von Cookies sowie darüber informiert werden, ob Dritte Zugriff auf die Cookies haben (sog. Third-Party Cookies).

Diesen Äußerungen des Generalanwalts kommt besondere Bedeutung zu, da der EuGH – jedenfalls bisher – im Regelfall den Schlussanträgen des Generalanwalts folgt. Die Folge einer entsprechenden Entscheidung wäre, dass bei jedem neuen Rechtsstreit zur Cookie-Thematik die nationalen Gerichte die Rechtsprechung des EuGH zwingend berücksichtigen müssten.

Orientierungshilfe der DSK

Besonders relevant ist vor diesem Hintergrund auch die am 5. April 2019 veröffentlichte Orientierungshilfe für Anbieter von Telemedienste der Datenschutzkonferenz (DSK), worin sich die Datenschutzaufsichtsbehörden des Bundes und der Länder unter anderem ganz konkret zur Einwilligungsfrage bei Cookies äußern. Auch aus Sicht der DSK ist ein Opt-Out Verfahren für eine Einwilligung vor dem Hintergrund des Erwägungsgrundes 32 DSGVO nicht ausreichend. Die Aufsichtsbehörden fordern sogar ausdrücklich, dass beim Öffnen der Webseite im Cookie-Banner alle einwilligungsbedürftigen Verarbeitungsvorgänge unter Nennung der beteiligten Akteure und deren Funktionen erklärt und über ein Auswahlmenü aktiviert werden müssen. Sie stellen darüber hinaus klar, dass die Auswahlmöglichkeiten nicht „aktiviert“ voreingestellt werden dürfen. Während das Banner angezeigt wird, sollen alle weitergehenden Skripte einer Webseite oder Web-App, die potenziell Nutzerdaten erfassen, mit technischen Maßnahmen blockiert werden. Erst durch die aktive Einwilligung darf die Datenverarbeitung tatsächlich beginnen.

Darüber hinaus hat sich die DSK in ihrem Papier auch zu der Frage der Anwendbarkeit der datenschutzrechtlichen Vorschriften des TMG seit Geltung der DSGVO geäußert und diese abgelehnt. Grundsätzlich könnten diese Vorschriften nur dann neben der DSGVO zur Anwendung kommen, wenn es sich dabei um Umsetzungen der ePrivacy-Richtlinie (2002/58/EG) handeln. Die Voraussetzungen dafür sieht die DSK als nicht gegeben.

Die DSK macht in Ihrer Orientierungshilfe umfangreiche Ausführung zum berechtigten Interesse nach Art. 6 Abs.1 lit. f) DSGVO. Die Aufsichtsbehörden erkennen dabei durchaus an, dass beispielsweise an einer Reichweitenmessung oder an statistischen Analysen ein berechtigtes Interesse bestehen kann. Im Rahmen der Abwägung mit den Rechten der betroffenen Personen messen sie Letzteren aber sehr hohe Bedeutung zu. Als Kriterien im Rahmen der Interessenabwägung stellen die Aufsichtsbehörden u.a. auf vernünftige Erwartung der betroffenen Personen und Transparenz, Interventionsmöglichkeiten der betroffenen Person, Verkettung von Daten, beteiligte Akteure, Dauer der Beobachtung, Kreis der Betroffenen, Datenkategorien und Umfang der Datenverarbeitung ab und betonen, dass diesbezüglich die jeweiligen Erwägungsgründe der DSGVO heranzuziehen seien.

Als konkretes Beispiel für die Reichweitenmessung wird angeführt, dass die Interessenabwägung zugunsten des Verantwortlichen Webseitenbetreibers ausfalle, wenn lediglich statistische Angaben für die Messung verwendet werden und keine umfangreiche Profilbildung und Weitergabe von Daten an Dritte erfolge, da dies dann für den Nutzer vorhersehbar sei. Zur Interessenabwägung bei Einsatz von Tracking-Pixeln von sozialen Netzwerken legt die DSK ausführlich dar, dass die Rechte der betroffenen Personen vor den Interessen der Webseitenbetreiber überwiegen, da sich der

durchschnittliche Nutzer sozialer Netzwerke nicht über die Profilbildung durch die Betreiber mittels Einbindung „unsichtbarer“ Pixel im Klaren sei, keine Möglichkeit zum Widerspruch habe und Nutzungsdaten über einen längeren Zeitraum zur Profilbildung gespeichert würden.

Stellungnahme

Nach unserer Einschätzung sind die Ansichten des Generalanwalts und der DSK ausgesprochen streng und die Umsetzung aller Vorgaben zur Ausgestaltung der Telemedienangebote teilweise praxisfern. Allerdings bringen die Ausführung gerade mit Blick auf das Verhältnis von DSGVO und TMG mehr Klarheit in die langjährige Diskussion. Es ist für Webseitenbetreiber und auch andere Anbieter von Telemedien also durchaus wichtig, sich mit den Ansichten der Aufsichtsbehörden auseinanderzusetzen und diese bei der Ausgestaltung der Webseite / Web-App zu berücksichtigen.

Die von den Aufsichtsbehörden angeführten Kriterien für die Interessenabwägung ermöglichen es sowohl den Anbietern von Telemedienangeboten als auch den Entwicklern von Anwendungen zur Reichweitenmessung, zur Analyse des Benutzerverhaltens oder zur Werbesteuerung ihre Angebote anhand der aufgestellten Kriterien zu bewerten, gegebenenfalls Anpassungen vorzunehmen oder eigene Argumente für einen anderen Ausgang der Interessenabwägung zu dokumentieren. Die Frage der Zulässigkeit des Einsatzes von Cookies & Co wird weiterhin eine Einzelfallenscheidung bleiben. Kurzfristige neue Impulse durch die E-Privacy-Verordnung erwarten wir nicht. Selbst wenn der Rat im Juni seine Position zu den streitigen Punkten verkünden sollte, werden die Wahlen und der anschließende Trilog eine schnelle Einigung und eine schnelle Anwendbarkeit der E-Privacy-Verordnung verhindern.

Praxistipp:
Vor dem Hintergrund der Stellungnahme des Generalanwalts und der Orientierungshilfe der DSK rechnen wir damit, dass kurzfristig differenziertere Lösungen für die Einwilligung erforderlich sein werden. Ein pauschales „Mit der Nutzung der Webseite stimmen Sie allen Cookies zu.“ wird nicht mehr ausreichend sein (falls es das jemals gewesen ist). Daher raten wir dazu, den Einsatz von Cookies und Trackingtechniken zu überprüfen und sich darauf einzustellen, dass sehr viel häufiger als bisher eine aktive Einwilligung der Nutzer erforderlich sein wird. Auch müssen voraussichtlich die Informationstexte überarbeitet werden, um die geforderte Transparenz zu schaffen. Am Markt sind sowohl kostenlose als auch kostenpflichtige Tools verfügbar, die ein aktives Consent Management anbieten. Viele dieser Tools ermöglichen einen Start der Webseite mit deaktivierten Cookies und einfache Einstellungen für Einwilligungen.

Hannah Mugler, Berlin
h.mugler@skwschwarz.de
Nikolaus Bertermann, Berlin
n.bertermann@skwschwarz.de

IT-Sicherheitsgesetz 2.0: Referentenentwurf des BMI

Die Befugnisse des BSI sollen erweitert und Meldepflichten bei IT-Sicherheitsvorfällen ausgedehnt werden. Bei Verletzungen von IT-Sicherheitspflichten sieht der Entwurf Bußgelder nach Vorbild der DSGVO vor. Das Bundesministerium des Innern, für Bau und Heimat (BMI) hat Ende März einen Referentenentwurf für das „Zweite Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0)“ in die Ressortabstimmung eingebracht. Anknüpfend an das im Juni 2015 in Kraft getretene IT-Sicherheitsgesetz und dessen Ergänzung durch die EU NIS-Richtlinie soll der Schutz informationstechnischer Systeme in der öffentlichen Verwaltung und in der Privatwirtschaft damit weiter verbessert werden.

Der Referentenentwurf sieht zu diesem Zweck insbesondere Anpassungen von BSIG, TMG und TKG, sowie die Schaffung neuer Straftatbestände mit Bezug zur IT-Sicherheit vor. Einige wesentliche Aspekte des aktuellen Entwurfs sind im Folgenden zusammengefasst.

Ausweitung der Vorgaben an IT-Sicherheit und der Meldepflichten bei Sicherheitsvorfällen

Die Pflichten zur Einhaltung eines Mindeststandards an IT-Sicherheit und zur Meldung von IT-Sicherheitsvorfällen soll erheblich ausgeweitet werden. Der Referentenentwurf definiert dazu weitere KRITIS-Sektoren und soll künftig auch Zulieferer von KRITIS-Betreibern unmittelbar gesetzlich

verpflichten. Zugleich sollen die Anforderungen an die Maßnahmen zum Schutz der Informationstechnik verschärft werden, etwa durch eine Pflicht zum Einsatz von Systemen zur Angriffserkennung.

Neue Meldepflicht für Hersteller von IT-Produkten

Zudem sollen auch Hersteller von IT-Produkten verpflichtet werden, erhebliche Störungen ihrer IT-Produkte an das BSI zu melden, wenn diese zu Beeinträchtigungen von KRITIS-Anlagen oder von Anlagen führen können, die für „Infrastrukturen im besonderen öffentlichen Interesse“ genutzt werden. Neue Meldepflichten sieht der Entwurf darüber hinaus für Hersteller so genannter „KRITIS-Kernkomponenten“ vor. Was „KRITIS-Kernkomponenten“ sind, soll durch eine Rechtsverordnung spezifiziert werden.

Weitere Kompetenzen des BSI

Die Kompetenzen und Aufgaben des BSI sollen weiter ausgebaut werden. So enthält der Referentenentwurf weitere Befugnisse des BSI, etwa zur Prüfung „öffentlich erreichbarer informationstechnischer Systeme“ auf Schadprogramme und Sicherheitslücken, und sieht die Einführung eines IT-Sicherheitskennzeichens vor, dessen Nutzung des BSI Herstellern von IT-Produkten gestatten kann. Das IT-Sicherheitskennzeichnen soll Verbrauchern relevante Informationen zur Sicherheit eines IT-Produkts verschaffen.

Bußgelder nach Vorbild der DSGVO

Schließlich soll der Bußgeldrahmen für Verstöße von IT-Sicherheitspflichten substantiell angehoben werden. Insbesondere wenn Unternehmen vollziehbaren Anordnungen des BSI zur IT-Sicherheit nicht nachkommen, sieht der Referentenentwurf einen Bußgeldrahmen von bis zu EUR 20.000.000,00 oder 4 % des jährlichen Unternehmensumsatzes vor. Andere Verstöße sollen im Höchstmaß immerhin noch mit EUR 10.000.000,00 oder 2 % des Unternehmensumsatzes geahndet werden können.

Praxistipp:
Der Referentenentwurf des BMI befindet sich in einem frühen Stadium. Ob und in welcher Form der Entwurf einem formalen Gesetzgebungsverfahren zugeleitet wird, wird maßgeblich auch von Kommentierungen und Stellungnahmen durch Unternehmen und Branchenverbände abhängen. Unklar ist aktuell außerdem, wie sich der Entwurf in die durch den Cyber Security Act im März beschlossene Regelungskompetenz der ENISA einfügen wird.

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

Welche Maßnahmen zur Zugangssicherung sind von Online-Diensten zum effektiven Schutz der Nutzerdaten zu treffen?

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (kurz: Datenschutzkonferenz, DSK) ist ein Gremium, das sich mit aktuellen Fragen des Datenschutzes in Deutschland befasst und zu ihnen Stellung nimmt. Eine der Hauptaufgaben der DSK ist die Erreichung einer einheitlichen Anwendung des europäischen und nationalen Datenschutzrechts. Die Beschlüsse und Stellungnahmen der DSK haben zwar keinen bindenden Charakter, sind jedoch von den Verantwortlichen unbedingt bei der Umsetzung der gesetzlichen Vorgaben zu berücksichtigen, da sie die Sichtweise der Aufsichtsbehörden zu datenschutzrechtlichen Fragen konkretisieren.

Am 5. April 2019 hat der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Datenschutzkonferenz eine Orientierungshilfe zu Maßnahmen zur Zugangssicherung von Online-Diensten veröffentlicht. Das Dokument richtet sich an Anbieter von Online-Diensten, die personenbezogene Daten von Nutzern verarbeiten. Solche Unternehmen fallen unter die Regelungen der DSGVO und haben folglich insbesondere die Vorschriften zur Sicherheit der Verarbeitung (Art. 32 DSGVO) zu beachten. Hierzu gehören auch Maßnahmen zur Sicherung des Zugangs zu den Diensten. Die im Dokument beschriebenen Maßnahmen entsprechen nach Ansicht der Datenschutzaufsichtsbehörden dem Stand der Technik und gewährleisten einen effektiven Schutz der personenbezogenen Daten der Nutzer.

Folgende Maßnahmen sind in der Orientierungshilfe beschrieben:

- Passwortstärke messen und anzeigen
- Passwortwechsel nur in Sonderfällen erzwingen
- Vorgang zum Umgang mit fehlgeschlagenen Anmeldeversuchen
- Umgang mit kompromittierten Diensten
- Sinnvolle Benachrichtigungen
- Sicheres Passwort-Reset
- Passwörter verschlüsselt übertragen
- Passwörter verschlüsselt speichern
- Passwort-Datenbanken vor unbefugtem Zugriff sichern
- Schulung der Beschäftigten
- Zwei-Faktor-Authentisierung anbieten
- Trennung von Authentifikations- und Nutzdaten
- Über Passwort-Manager informieren
- Sicherheit als integrierte Aufgabe

Über die vorstehend genannten Maßnahmen hinaus verweist die DSK ausdrücklich auf die Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) im IT-Grundschutz-Kompendium zum Identitäts- und Berechtigungsmanagement (u.a. Basisanforderung ORP.4.A8 „Regelung des Passwortgebrauchs“ oder ORP.4.A11 „Zurücksetzen von Passwörtern“).

Die nun veröffentlichte Orientierungshilfe ist insbesondere deshalb von Anbietern von Online-Diensten zu beachten, weil schon Anfang Februar das Bayerische Amt für Datenschutzaufsicht (BayLDA) als Aufsichtsbehörde geprüft hat, wie Website-Betreiber mit den Passwörtern ihrer Nutzer umgehen (Link zur Prüfung des BayLDA: https://www.lda.bayern.de/media/sid_ergebnis_2019.pdf). 20 Online-Dienste, die in Deutschland sehr beliebt sind, wurden hierfür näher untersucht – von sozialen Netzwerken über Videostreaming-Portale bis hin zu Online-Shops. Im Ergebnis hat die Behörde festgestellt, dass bei keinem dieser Dienste starke Passwörter vom Nutzer gefordert werden und oft sogar sehr schwache Passwörter wie „123456“, „Passwort“ oder sogar „0000“ möglich sind. Zusätzliche Sicherheitsmaßnahmen und Hilfestellungen zum Schutz des Accounts hatten zudem nur eine überschaubare Anzahl an Diensten angeboten. Es ist deshalb mehr als wahrscheinlich, dass die Aufsichtsbehörden weiter auf die Sicherheit der Gewährleistung eines sicheren Zuganges zu den Diensten achten werden und entsprechende Überprüfungen durchführen werden. In diesem Zusammenhang erwarten die Aufsichtsbehörden die Umsetzung von ausreichenden Maßnahmen zur Zugangssicherung.

Praxistipp:
Anbietern von Online-Diensten ist dringend zu empfehlen, die Sicherheit des Zuganges zu den Diensten zu überprüfen. Dabei sollten die von der DSK und dem BSI empfohlenen Maßnahmen berücksichtigt werden.

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

Der Schutz von Gesundheitsdaten – Empfehlung des Europarats vom 27.03.2019

Mobile health Apps und andere technische Anwendungen im Gesundheitssektor werden immer populärer. Ob Herzfrequenz, Gewicht, Medikamenteneinnahme, Schlafphasen oder Laborwerte; in Health-Apps dreht sich alles um Gesundheitsdaten. Gesundheitsdaten sind alle Daten, die sich auf den Gesundheitszustand einer natürlichen Person beziehen und aus denen Informationen über den früheren, gegenwärtigen und zukünftigen körperlichen oder geistigen Gesundheitszustand der Person hervorgehen (siehe Erwägungsgrund 35 DSGVO). Solche Gesundheitsdaten sind personenbezogene Daten, die als besonders sensibel gelten. Regelungen zur Nutzung von Gesundheitsdaten finden sich in Artikel 9 DSGVO. Die Regelungen stoßen jedoch auf praktische Umsetzungsprobleme und Unsicherheiten in der Anwendung, insbesondere bei den neuen technischen Anwendungen im Gesundheitssektor. Konkrete Leitlinien wären für viele Anbieter von technischen Anwendungen im Gesundheitssektor wünschenswert.

Der Europarat hat am 27.03.2019 eine Empfehlung veröffentlicht, um den Mitgliedstaaten Leitlinien für die Regulierung der Verarbeitung gesundheitsbezogener Daten zur Verfügung zu stellen (abrufbar unter new guidelines). Die Empfehlung des Europarates enthält Ausführungen zu Grundsätzen zum Schutz von Gesundheitsdaten. Behörden sollen die Leitlinien den Akteuren innerhalb des Gesundheitssystems, die Gesundheitsdaten verarbeiten zur Verfügung stellen.

Praxistipp:
Anbieter von Mobile Health Apps und anderen technischen Anwendungen im Gesundheitssektor sollten die aktuellen Stellungnahmen und Empfehlungen der Behörden verfolgen. Möglicherweise werden bald klarstellende Informationen zur Verfügung gestellt, nach denen sich Anbieter von technischen Anwendungen im Gesundheitssektor richten können.

Yvonne Schäfer, Frankfurt/Main
y.schaefer@skwschwarz.de