DOSB FÜHRUNGS AKADEMIE

FA Datenschutzportal

DSP Info-Brief

Nr. 45 / April 2017

INHALT

Herausgeber
Führungs-Akademie des DOSB

Kontakt FA
Führungs-Akademie des DOSB
Willy-Brandt-Platz 2 / 50679 Köln
Tel. 0221 – 221 275 94 /// Fax: 0221 – 221 220 13
www.fuehrungs-akademie.de
niewerth@fuehrungs-akademie.de

Technische Umsetzung
Führungs-Akademie des DOSB

Redaktion
Toni Niewerth / Robert Graf

Kontakt SVBG
Sachverständigenbürogemeinschaft Mülot:Graf
Westfalenweg 2
33449 Langenberg
www.muelot.de/
graf@muelot-Graf.de / muelot@muelot-graf.de

DATENSCHUTZPORTAL INTERN

1 Themen und Inhalte des Live-Chats vom 26.4.2017

Zugriff auf Mail-Postfächer von „Ehemaligen"

FRAGE
Es gibt in unserem Verein keine Vereinbarung zur privaten E-Mail-Kommunikation. Unter den aktuellen Bedingungen ist eine Dienstvereinbarung dazu auch nicht in Sicht.

Ausscheidenden Mitarbeitern haben wir bisher ein Formular vorgelegt, in dem wir uns ihr Einverständnis zur Einsicht haben geben lassen. Bei uns hat das bisher auch immer problemlos geklappt. Allerdings ist dies ja nicht zwingend. Der Ausscheidende kann diese Zustimmung natürlich auch verweigern.

Um dem vorzubeugen, möchten wir diese Einverständniserklärung zukünftig sofort bei Neueinstellungen unterzeichnen lassen. Sollte der neue Mitarbeiter die Zusage später widerrufen, hätten wir zumindest für den Zeitraum der Zusage die Möglichkeit, auf das Postfach zugreifen zu können.

Gibt es gegen diese Regelung aus Ihrer Sicht datenschutzrechtliche Bedenken?

ANTWORT
Sie haben vollkommen Recht, der Zugriff auf die E-Mailkonten, die privat genutzt werden können, unterliegt den Einschränkungen des Telekommunikationsgesetzes und des Telemediengesetzes. Auch das Strafgesetzbuch hat hier eine Relevanz bezüglich des Brief- und des Fernmeldegeheimnisses. Das bedeutet, dass auf diese E-Mail Konten (E-Mails, Kontakte, Termine, Aufgaben etc.), nicht zugegriffen werden kann, ohne Gefahr zu laufen sich strafbar zu machen, da man private Informationen zur Kenntnis genommen hat.

Als Notmaßnahme kann man natürlich die Mitarbeiter beim Ausscheiden bitten, in den Zugriff auf das Postfach einzuwilligen. Sinnvoller ist sicher ihr Vorschlag, sich schon bei der Einstellung die Einwilligung zum Zugriff geben zu lassen. Bitte beachten Sie aber, dass der Verein / Verband für diejenigen, die diese Einwilligung nicht unterzeichnen, eine Regelung geben muss, die ihnen die private Nutzung der E-Mailkonten untersagt.

Ein Problem könnte sich ab Mai 2018 ergeben, da hier jeder Einwilligung auch eine Widerspruchsmöglichkeit zugehört. Generell ist es nach wie vor empfehlenswert, die private Nutzung von betrieblicher Infrastruktur generell zu untersagen.

Bitte beachten Sie auch die zunehmende Synchronisation der oben genannten Informationen mit Smartphones. Daraus folgt, dass auch die private Nutzung von Smartphones zu regeln ist. [R. Graf]

Umgang mit Absenderdaten bei weitergeleiteten E-Mails

FRAGE
Um nicht dem Vorwurf ausgesetzt zu sein, Informationen nicht an die 'richtige' Stelle weitergeleitet zu haben, neigen in unserer Geschäftstelle immer noch viele Mitarbeiter

dazu, E-Mails einfach weiterzuleiten. Die Absenderdaten der ursprünglichen E-Mail werden dabei vermutlich in der Regel nicht beachtet und mit weitergeleitet.

Gibt es datenschutzrechtlich Einschränkungen bei der Weitergabe von E-Mails mit Absenderdaten? Müssen Absenderdaten eventuell sogar teilweise oder komplett gelöscht werden?

ANTWORT
Verbleiben die weitergeleiteten E-Mails innerhalb der Geschäftsstelle, ist aus datenschutzrechtlicher Sicht kein besonderes Problem zu erwarten. Aus inhaltlich-organisatorischer Sicht bleibt die nicht-ziel- und zweckgerichtete Weiterleitung natürlich trotzdem ein auch Zeit und Geld kostendes Problem.

Gehen E-Mails an Empfänger außerhalb der Geschäftsstelle, gilt es zu prüfen, ob der Sender berechtigt ist, die darin enthaltenen personenbezogenen Daten weiterzugeben. Dies hängt sowohl vom Zweck der erhaltenen E-Mail als auch vom Zweck der Weitergabe ab. Wenn die Weiterleitung einer E-Mail den Zweck hat, bestimmte Informationen eines Absenders (Inhalt und Absenderdaten) einer anderen Person zur Kenntnis zu geben, dann hängt es davon ab, ob die Absenderdaten benötigt werden, um diese Information zu beschreiben. Sind die Absenderdaten nicht notwendig, ist das Entfernen der Absenderdaten in jedem Falle empfehlenswert, um die Vertraulichkeit zu gewährleisten. [R. Graf]

Cloud basiertes Office für Deutschland

FRAGE
Bei uns wird - zum wiederholten Male - die Anschaffung des Cloud basierten MS Office 365 diskutiert.

Als DSB habe ich wegen der Frage der Standorte der Server bisher immer Einspruch gegen die Anschaffung erhoben.

Bei der letzten Vorstandssitzung hat jemand darauf hingewiesen, dass es ein spezielles Angebot "Office 365 Deutschland" gibt.

Gibt es zu diesem Angebot bereits Stellungnahmen von Datenschützern bzw. Datenschutzbehörden (im Netz habe ich dazu nichts gefunden) und wie schätzen Sie die datenschutzrechtlichen Konsequenzen ein?

ANTWORT
Sie haben recht, die Verwendung von Office 365 hat aufgrund der unklaren Standorte der Microsoft Server und aufgrund der Ausführungen in den "OST, Online Service Terms (AGB´s)" von Microsoft erhebliche datenschutzrechtliche Bedenken erzeugt.

Es gab in der Vergangenheit auch schon Anordnungen von Aufsichtsbehörden, die den Einsatz von Office 365 untersagten.

Microsoft hat nun mit der Telekom (T-Systems) eine Vereinbarung getroffen, dass die für "Office 365 Deutschland" zur Verfügung gestellten Server nur von der Telekom verwaltet werden (Daten Treuhänderschaft). Diese Server stehen in Deutschland, und es gibt hierfür ein entsprechendes Angebot der Telekom.

Ich kann Ihnen hier die aktuelle Ausgabe der Zeitschrift c't, Ausgabe 9 vom 15.4.2017 sehr empfehlen. Hier wird in einem Artikel speziell auf Office 365 eingegangen.

In dieser Zeitschrift gibt es noch weitere interessante Artikel, die sich mit der Problematik der US-Clouds und dem rechtlich riskanten Datentransfer in die USA beschäftigt. Darüber hinaus beleuchtet die Zeitschrift in einigen Beiträgen auch neue Entwicklungen der rechtlichen Situation in den USA, so u.a. zur Bedeutung von Privacy Shield, dem Nachfolgeabkommen zu Safe Harbor. [R. Graf]

IN DER DISKUSSION – NEUIGKEITEN RUND UM DEN DATENSCHUTZ

2 Verstärkte Videoüberwachung in der Diskussion

Notwendige Sicherheitsmaßnahme oder ungerechtfertigter Eingriff in das Persönlichkeitsrecht

Im Zuge der neu entfachten Debatte um angemessene Sicherheitskonzepte ist auch das Thema Videoüberwachung von öffentlichen Plätzen und (Massen)Veranstaltungen wieder stärker in den Blick geraten. Nach dem Anschlag auf den Mannschaftsbus von Borussia Dortmund dürfte diese Debatte zunehmend auch bei den Organisatoren von Sportveranstaltungen eine Rolle spielen.

Vor dem Hintergrund der Überlegungen der Ampel-Koalition in Rheinland-Pfalz zum verstärkten Einsatz von Videokameras bei großen Veranstaltungen hat der Datenschutzbeauftrage des Landes, Dieter Kugelmann, seine Bedenken gegen eine zu große Ausweitung der Videoüberwachung geäußert. Neben einem konkreten Anlass fordert Kugelmann auch eine genaue Kennzeichnung der Überwachung durch Kameras. Schließlich sei "Videoüberwachung … immer noch ein Eingriff in das Persönlichkeitsrecht, weil ich eben … nicht ausweichen kann". Als Beispiel einer vertretbaren Videoüberwachung bei Großveranstaltungen verwies er auf große Konzerte wie etwa Rock am Ring. "Wenn das entsprechend gekennzeichnet ist und die Leute das entsprechend wissen (....), da gibt es gute Gründe, das zu machen." Es müsse aber festgelegte Kriterien für den Einsatz geben. …

Kugelmann kritisierte die erleichterte Möglichkeit für mehr Videoüberwachung in Deutschland vor allem für private Betreiber in Einkaufszentren oder vor Fußballstadien. Der Bundestag hatte im März als Konsequenz aus mehreren Gewalttaten im vergangenen Jahr den Weg dafür freigemacht. Bei der Entscheidung erhalten Sicherheitsaspekte in Zukunft ein größeres Gewicht als bisher. "Da wird noch ein Ball mehr in die Seite der Wahrung der Sicherheit geschmissen und wir sehen nicht ein, warum", sagte Kugelmann. "Das ist ein Videoüberwachungs-Verschlechterungsgesetz."

Der Datenschutzbeauftragte warnte vor einer flächendeckenden Überwachung in Einkaufszentren. Die Datenschutzbehörden könnten von den Betreibern einen Grund für die Installation einer Überwachungskamera verlangen. "Da hätten wir auch die Befugnis zu sagen: hängt ab!", sagte er. "Das können wir anordnen gegebenenfalls mit Bußgeld." Gute Gründe gebe es aber zum Beispiel beim Einsatz von Videokameras in Einkaufszentren in der Nähe von Geldautomaten. [Fundort: heise online v. 20.4.17 / Oliver von Riegen, dpa)

Zur aktuellen Diskussion vgl. auch den Beitrag zur Diskussion in Thüringen: Keine Generalerlaubnis für mehr Videoüberwachung [Fundort: heise online v. 20.4.17] *[BE: TN]*

MEDIEN –TECHNIK – SICHERHEIT

3 Datenschutzprobleme mit Windows 10

Die aktuelle Version steht ebenso wie die Vorgängerversionen in der Kritik in erheblichem Umfang Daten der Nutzer an Microsoft zu übertragen. Da Windows 10 in immer mehr Organisationen als Standard Betriebssystem eingeführt wird, stellt sich auch verstärkt die Frage, welche datenschutzrechtlichen Aspekte zu berücksichtigen sind.

Microsoft wertet an verschiedenen Stellen in Windows 10 das Nutzerverhalten aus und überträgt diese Daten in die USA. In den Standardeinstellungen sind diese Datensammlungen eingeschaltet und müssen, sofern der Betroffene dies nicht wünscht, explizit ausgeschaltet werden.

Während der Nutzung von Windows 10 werden natürlich auch personenbezogene Daten verarbeitet, zum einen vom Nutzer, zum anderen gegebenenfalls über Personen, die im Rahmen der Tätigkeiten (Briefe schreiben, Anfragen an Cortana (den Sprachassistenten von Windows 10), Surfverhalten, Standorterfassung etc.) verarbeitet werden. Dadurch, dass diese Daten ohne Einwilligung des Betroffenen bzw. ohne eine Rechtsgrundlage in die USA übertragen werden, ergeben sich die entsprechenden datenschutzrechtlichen Probleme, die u.U. auch dazu führen können, dass sich der Nutzer damit strafbar machen kann.

Um sich einen Überblick über die umfangreiche Datensammlung von Windows 10 zu verschaffen, können Sie z.B. das kostenlose Antispy-Tool „O&O ShutUp10" einsetzen. Das Programm ist ein nützliches Werkzeug, das zum einen analysiert, welche Daten gesammelt werden, und das Ihnen auf der anderen Seite die Möglichkeit bietet, diese Datensammlung abzuschalten [Link zum Programm]. *Bitte beachten Sie, dass diese Empfehlung ohne Gewährleistung gemacht wird.*

Der Einsatz von Windows 10 kann in Organisationen auch über den Einsatz von Gruppenrichtlinien modifiziert werden. Diese werden serverseitig konfiguriert und legen damit die Regeln für die lokalen Betriebssysteme fest. Bitte wenden Sie sich hier an ihren IT Verantwortlichen.

Eine aus unserer Sicht gute Übersicht über die zu beachtenden Einstellungen bietet u.a. die Website des baden-württembergischen Landesdatenschutzbeauftragten: *„Datenschutzeinstellungen bei Windows 10 – Wie Sie Windows 10 datenschutzfreundlich nutzen können*".

Ergänzende Informationen zum Thema Datenschutz bei der Nutzung von Windows 10 finden Sie u.a auf den nachfolgend aufgeführten Websites.

- https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2016/04/2016-04_leitfaden_win10.pdf
- https://www.youtube.com/watch?v=J8J1UGEloGo
- https://www.youtube.com/watch?v=S-gbINru_9s
- http://www.n-tv.de/technik/Hat-Windows-10-ein-Datenschutz-Problem-article15661606.html
- https://www.computerbase.de/2016-10/windows-10-datenschutz-probleme-firmen/

[R. Graf]

4 Schnell und sicher informiert – Bürger-Cert: Der Newsletter des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

Viele, vielleicht sogar die meisten von Ihnen werden die Sicherheitsinformationen und den 14tägigen Newsletter des Bürger-Cert kennen. Aus aktuellem Anlass möchten wir an dieser Stelle noch einmal auf diesen Service hinweisen.

Das Bürger-CERT ist ein Projekt des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Das Bürger-CERT informiert und warnt Bürger und kleine Unternehmen schnell und kompetent vor Viren, Würmern und anderen Sicherheitslücken – natürlich kostenfrei und absolut neutral. Das CERT Team analysiert und bewertet die Sicherheitslage im Internet rund um die Uhr und verschickt bei konkretem Handlungsbedarf aufgrund von Sicherheitslücken im Internet Warnmeldungen und Sicherheitshinweise per E-Mail.

Das Bürger-CERT wurde im Jahr 2006 als ein Gemeinschaftsprojekt des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und Mcert Deutsche Gesellschaft für IT-Sicherheit gestartet. Zur Finanzierung des Projekts haben die öffentliche Hand und Partner aus der Wirtschaft ein starkes Bündnis zum Nutzen der Bürger geschlossen. Seit Juni 2007 werden die Dienstleistungen des Bürger-CERT allein durch das BSI bereitgestellt. [LINK]

Schwerpunkt der aktuellen Ausgabe des Newsletters sind Sicherheitshinweise u.a. zu Trojanern, Pishing-E-Mails und zum vielgenutzten Programm ‚Joomla':

1. Gefälschte Super Mario App sammelt Kreditkartendaten: Trojaner:
2. Internet-Kriminelle nutzen Pixel-Tracking für Datensammlung: Phishing:
3. Unechte Amazon E-Mails im Umlauf: Phishing-Welle:
4. Updates installieren: Google Chrome und Firefox Browser:
5. Sicherheitshinweis für IT-Administratoren: Joomla:
6. Sicherheitslücken mit Updates schließen: Foxit Reader und PhantomPDF:
7. Passwortmanager aktualisieren: LastPass:
8. Auto-Updater aktivieren: Fritzbox-Firmware:
9. Angebliche Support-Mitarbeiter möchten Fernzugriff auf Ihr System: Betrugsversuch:
10. Automatische Likes von Apps abschalten: Facebook:
11. BSI als Partner freut sich über Bewerberinnen: Nationaler Pakt für Frauen in MINT-Berufen:
12. IT-Sicherheitsnachwuchs oder Cyber-Kriminelle

5 Was tun, wenn die Polizei vor der Türe steht?

Je nachdem, wie die Polizei Kontakt aufnimmt, ergeben sich unterschiedliche Vorgehensweisen.

Im Falle der telefonischen Kontaktaufnahme stellt sich die Frage nach der Identifikation des Anrufers. Da man sich am Telefon keinen Ausweis zeigen lassen kann, empfiehlt sich der Rückruf bei der Behörde. Sollte der Anrufer eine Telefonnummer vorgeben, ist zu prüfen, oder diese auch wirklich zur angegeben Behörde gehört. Auf keinen Fall sollte eine Mobilfunknummer akzeptiert werden. Am besten sucht man sich die Telefonnummer selbst heraus und sucht den Kontakt dann über die Behörde.

Der weitere Informationsaustausch sollte dann entweder schriftlich oder im persönlichen Gespräch erfolgen.

Informationen am Telefon sollten nach Authentifizierung des Anrufers (siehe oben) – wenn überhaupt – nur von dazu berechtigten Personen erfolgen. Bei mündlichen Aussagen besteht zudem immer die Problematik der Beweisbarkeit.

Die schriftliche Anfrage muss konkret die Fragestellung unter Bezug auf die Rechtsgrundlage enthalten. Wichtig ist darüber hinaus, dass innerhalb des Vereines oder des Verbandes festgelegt werden sollte, wer berechtigt ist, entsprechende Anfragen zu beantworten.

Im Falle, dass die Polizei tatsächlich vor der Tür steht und ggf. die Gefahr der Beschlagnahme von z. B. PC´s oder Servern steht, sollte unbedingt ein Rechtsbeistand hinzugezogen werden.

Dieser kann im Falle einer Hausdurchsuchung bzw. Beschlagnahme unterstützen und ggf. den vorliegenden richterlichen Beschluss, der für solche Fälle vorliegen muss anfechten und ggf. größeren Schaden verhindern oder verringern. [R. Graf]

GESETZGEBUNG

6 Neues Bundesdatenschutzgesetz senkt datenschutzrechtliche Standards und ist europarechtswidrig

Quelle: Pressemitteilung der Landesbeauftragten für den Datenschutz Niedersachsen vom 28.04.2017 [Link]

„Das gestern vom Bundestag beschlossene neue Datenschutzgesetz stellt bewährte datenschutzrechtliche Standards in Frage und ist europarechtlich zweifelhaft", so Barbara Thiel, Landesbeauftragte für den Datenschutz in Niedersachsen und gegenwärtig Vorsitzende der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder. Anlass des so genannten Datenschutz-Anpassungs- und -Umsetzungsgesetz EU (DSAnpUG-EU), das an die Stelle des Bundesdatenschutzgesetzes treten soll, ist das neue EU-Datenschutzrecht. Bis Mai 2018 müssen die Mitgliedsstaaten ihr nationales Recht an die europarechtlichen Vorgaben anpassen.

Thiel: „Das Gesetz missachtet an einigen Stellen das Europarecht. Das gilt etwa für die Vorgaben zur Verarbeitung besonders sensibler personenbezogener Daten wie Gesundheitsdaten oder genetische Daten." Auch schränkt das Gesetz die Informations-, Auskunfts- und Löschrechte der betroffenen Personen erheblich ein. „Gegenüber dem gegenwärtigen Schutzniveau ist das ein Rückschritt", so Thiel.

Nicht überzeugen kann auch die Regelung zur Vertretung der Aufsichtsbehörden im Europäischen Datenschutzausschuss (EDSA). Dem EDSA kommt zukünftig eine zentrale Bedeutung zu, kann dieser doch Beschlüsse treffen, die für alle Datenschutz-Aufsichtsbehörden bindend sind. Thiel: „Hier werden die Länderinteressen unzureichend berücksichtigt. In Angelegenheiten, in denen allein die Aufsichtsbehörden der Bundesländer sachlich zuständig sind, sollte den Landesbehörden auch das Recht zur Vertretung auf europäischer Ebene zugestanden werden."

Bevor das Gesetz in Kraft treten kann, muss sich auch noch der Bundesrat abschließend mit den geplanten Neuregelungen befassen. Thiel hofft daher, dass noch Korrekturen vorgenommen werden: „Anderenfalls droht Deutschland wegen der europarechtswidrigen Regelungen die Einleitung eines Vertragsverletzungsverfahrens durch die Europäische Kommission", so die Landesdatenschutzbeauftrage abschließend.

Einige Kritikpunkte am neuen Datenschutzgesetz zusammengefasst:

- Hersteller von IT-Anwendungen werden nicht in die Regelungen aufgenommen. Nur wenn die Software es zulässt kann der Datenverarbeiter seine datenschutzrechtlichen Pflichten erfüllen. Es fehlt die Konkretisierung der Pflichten zu datenschutzfreundlichen Produkten.
- Die strenge Zweckbindung bei der Verarbeitung wird aufgeweicht mit der Möglichkeit Daten auch in kompatiblen Zwecke zu verarbeiten. Damit ergibt sich die Schwierigkeit der Abgrenzung.
- Einschränkung der Betroffenenrechte zugunsten privater Datenverarbeiter. Diese sollen nur dann Auskunft geben oder Daten löschen müssen, wenn dies keinen „unverhältnismäßigen Aufwand" bedeute.

- Schwächung der Aufsichtsbehörden: Diese sollen keine Vorort-Kontrollen bei Berufsgeheimnisträgern mehr vornehmen dürfen (Rechtsanwälte, Ärzte, Steuerberater, etc.). Damit würden ganze Branchen, wie z. B. der Gesundheitssektor ausgenommen.
- Der Gesetzesentwurf sieht keine zusätzlichen Personalstellen für die Behörden vor, obwohl diese zahlreiche neue Aufgaben übernehmen müssen, wie Zertifizierungen und Datenschutzfolgeabschätzungen. *[BE: R.G.]*

7 Diskussion um den Entwurf der Bundesregierung zur Anpassung des BDSG an die EU-DSGVO

Am 01.02.2017 hat die Bundesregierung den Entwurf des Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – (DSAnpUG-EU) beschlossen. Damit sollen die nationalen Regelungen zum Datenschutz in Deutschland an die EU-Datenschutzgrundverordnung (EU-DSGVO) angepasst werden, die ab dem 25.5.2018 in Kraft tritt. Die ersten beiden Entwürfe des Bundesinnenministeriums (BMI) wurden im September und November 2016 stark kritisiert und danach erneut überarbeitet.

Das Bundesinnenministerium selbst sieht in dem Entwurf „einen großen Schritt zur Angleichung der Datenschutzregelungen in Europa und damit zu einem harmonisierten digitalen Binnenmarkt". Gleichzeitig stellt es heraus, dass durch die schnelle Verabschiedung des Entwurfes „allen Beteiligten genug Zeit" bleibe, „sich auf die neue Rechtslage vorzubereiten." Die viel diskutierten Öffnungsklauseln, die den nationalen Gesetzgebern die Möglichkeit geben, eigene Regelungen zu treffen, sieht der Bundesinnenminister mit diesem Entwurf als gut genutzte „Spielräume der Datenschutz-Grundverordnung" zur Sicherstellung von „Rechtssicherheit" und zu einem „angemessenen Ausgleich der Interessen." (Quelle)

Die vom Innenministerium als positiv eingeschätzten Aspekte des DSAnpUG-EU werden allerdings von Datenschutzexperten und Betroffenen ebenso wie von Kommentaren politischer Institutionen sehr kontrovers diskutiert und teilweise scharf kritisiert.

So bedauerte der Bundesrat in seiner Stellungnahme vom 10. März, das „ihm eine umfassende Bewertung der vorgeschlagenen Neufassung des Bundesdatenschutzgesetzes nicht möglich" sei, weil „notwendige Anpassungen des vorrangigen Fachrechts bislang weder erfolgt noch konkret absehbar" seien, „so dass der konkrete Anwendungsbereich des Gesetzentwurfs in weiten Teilen im Unklaren" bleibe.

Der Bundesrat, so die Stellungnahme weiter, „bedauert, dass die ausstehende Anpassung des bereichspezifischen Datenschutzrechts des Bundes beispielsweise in den Prozessordnungen oder im Sozialdatenschutzrecht auch für die Rechtsanwender in öffentlichen Stellen der Länder und Kommunen erhebliche Unsicherheiten über ihre … Anpassungspflichten erwarten lässt. Der Bundesrat bittet deshalb die Bundesregierung, die Länder zum frühestmöglichen Zeitpunkt umfassend in die Vorbereitung der notwendigen Änderungen des Fachrechts einzubinden. [Quelle]. Auf insgesamt 46 Seiten werden anschließend in insgesamt 57 Punkten die Änderungswünsche des Bundesrates formuliert. [Die PDF-Datei finden Sie auch im Portal im Verzeichnis EU-DSGVO [Link]

Noch deutlich schärfer formuliert der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern, Heinz Müller, seine Kritik am z.T. missglückten und unzureichenden Entwurf. Müller zufolge beschränkt sich der Entwurf im Wesentlichen auf „oberflächliche Schönheitsreparaturen", der zudem die Voraussetzungen und Anforderungen der bereits angesprochenen Öffnungsklauseln verkenne. Die daraus entstehenden Einschränkungen des Betroffenenrechts sowie die Privilegierung von öffentlichen Stellen hinsichtlich der Vollstreckung, bewertet er zudem als „problematisch". (Quelle)

Auch aus der Sicht anderer Datenschutzexperten lässt der neue Entwurf „viel zu wünschen übrig". So bemängeln sie die durch viele Verweise selbst für Experten schwer verständliche, hohe Komplexität des geplanten Gesetzes, (Quelle) die durch die Anzahl der Einzelregelungen zusätzlich noch erhöht werde. Mit insgesamt 84 Paragraphen enthält das neue Gesetz nahezu doppelt so viele wie das bisherige BDSG. Hinzu kommen 99 Artikel der DSGVO, was insgesamt 183 Paragraphen und Artikel ergibt. Zusätzliche 173 Erwägungsgründe komplettieren die DSGVO und verstärken damit den Eindruck einer in der praktischen Umsetzbarkeit nur sehr schwer beherrschbaren Komplexität. Inhaltliche Kritik äußerten Sachverständige und Experten unter anderem auch beim Betroffenenrecht und bei Passagen betreffend der Polizei- und JustizRL. (Quelle)

Neben der Kritik an den Inhalten werden von einigen Autoren auch die aus ihrer Sicht damit verbundenen zu hohen Kosten kritisiert. „Nach Schätzung der Bundesregierung entstehen für die Wirtschaft jährliche Bürokratiekosten aus Informationspflichten in Höhe von rund 17,2 Millionen Euro. Darüber hinaus soll bei deutschen Unternehmen nach Einschätzung der Regierung ein einmaliger Erfüllungsaufwand in Höhe von rund 58,9 Millionen Euro anfallen. Experten schätzen auf der Grundlage von Erfahrungen aus bisherigen Projekten zur Umsetzung der DSGVO allerdings, dass die tatsächlichen Kosten eines solchen deutschen Alleingangs deutlich höher liegen dürften. " (Quelle)

Abschließend lässt sich sagen, dass die Hoffnungen und Erwartungen, die an diesen Gesetzesentwurf gestellt wurden, nicht erfüllt wurden. Aus allen Richtungen hagelt es Kritik. Aufsichtsbehörden, Bundesdatenschutzbeauftragte, Datenschutzexperten sowie Magazine und Fachforen äußerten sich mehr als kritisch zu der geplanten Anpassung.

Als höchst problematisch wird darüber hinausgesehen, dass die Bundesregierung bestrebt zu sein scheint, den Entwurf trotz aller handwerklichen Mängel und trotz der heftigen Kritik an den inhaltlichen Schwächen schnellstmöglich zu verabschieden, um diesen noch vor dem Wahlkampf und damit „bevor sich die Öffentlichkeit mit dem Inhalt des Entwurfs befasst," (Quelle) durchzudrücken. Peter Schaar, Vorsitzender der Europäischen Akademie für Informationsfreiheit und Datenschutz e.V., warnte daher eindringlich auch vor einem „Rufverlust Deutschlands", wenn man ein solches Gesetz durch den Bundestag „peitschen" würde, zumal nicht klar sei, ob es „der europäischen Prüfung Stand halte. Zudem würde durch den derzeitigen Entwurf die Intentionstrias des europäischen Gesetzgebers im Bereich Datenschutz, also Harmonisierung, Stärkung der Betroffenenrechte sowie Schaffung einer effektiven und effizienten Aufsicht, nicht erreicht." (Quelle)

Vor diesem Hintergrund sehen einige Kritiker dem Gesetzesvorhaben schon leicht resigniert entgegen. Hin und hergerissen zwischen der begründeten Kritik und dem Unmut über die mangelnde Qualität des Entwurfes auf der einen Seite und dem knappen Zeitrahmen zur Umsetzung in die Praxis auf der anderen Seite stellen sie die Frage, welche Prioritäten jetzt gesetzt werden sollten: Denn, so der Hamburger Datenschutzbeauftragte,

Prof. Dr. Johannes Caspar, „wenn nicht kurzfristig ein Gesetz verabschiedet wird, ist die verbleibende Frist für die Verantwortlichen zur Umsetzung zu knapp. Vielleicht sollten wir also aufhören, uns zu echauffieren und (erst einmal) mit dem leben, was uns der Gesetzgeber anbietet.“ (Quelle)

Fasst man die Reaktionen zusammen, entsteht ein sehr skeptischer bis negativer Eindruck. Es scheint fraglich, „ob das hohe datenschutzrechtliche Niveau in Deutschland aufrechterhalten wird. Es wird auch interessant werden, wie sich die Aufsichtsbehörden für den Datenschutz zu den europarechtlich problematischen Regelungen positionieren werden“, die in diesem neuen Entwurf enthalten sind. (Quelle) *[L. Schwank]*

AKTUELLE URTEILE

8 Facebook darf personenbezogene Daten deutscher WhatsApp-Nutzer vorerst nur bei Vorliegen einer entsprechenden Einwilligung verwenden

Quelle: Verwaltungsgericht Hamburg, Beschluss vom 24.04.2017; AZ: 13 E 5912/16 –
Fundort: © kostenlose-urteile.de (ra-online GmbH), Berlin 25.04.2017; Dok. Nr.: Dokument-Nr. 24167

Schutz personenbezogener Daten stellt grundrechtlich geschütztes Rechtsgut dar

Das Verwaltungsgericht Hamburg hat entschieden, dass Facebook vorerst nur personenbezogene Daten deutscher WhatsApp-Nutzer verwenden darf, wenn hierfür eine den deutschen Datenschutzvorschriften entsprechende Einwilligung vorliegt.

Dem Verfahren lag folgender Sachverhalt zugrunde: Ende August 2016 hat WhatsApp Inc., die 2014 von der Facebook Unternehmensgruppe übernommen worden ist, eine Aktualisierung seiner Nutzungsbedingungen und Datenschutzrichtlinien bekannt gegeben, durch die eine - bis dahin nach den Nutzungsbedingungen nicht zugelassene - Weitergabe von personenbezogenen Daten an die Facebook Unternehmensgruppe vorgesehen ist. Mit sofort vollziehbarem Bescheid vom 23. September 2016 untersagte der Hamburgische Beauftragte für Datenschutz und Informationssicherheit … der Facebook Ireland Ltd. … – dem internationalen Hauptsitz der Facebook Unternehmensgruppe –, die personenbezogenen Daten deutscher WhatsApp-Nutzer zu erheben und zu speichern, soweit und solange ein den deutschen Datenschutzvorschriften entsprechende Einwilligung nicht vorliege (Ziffer 1). Zugleich ordnete der Datenschutzbeauftragte die Löschung von personenbezogenen Daten an, die ohne die notwendige Einwilligung erhoben worden sind, sowie die Dokumentation der Löschung (Ziffer 2 und 3). Gegen diese Verfügung legte Facebook Widerspruch ein und beantragte einstweiligen Rechtsschutz beim Verwaltungsgericht Hamburg. [Link zum vollständigen Beitrag] *[BE: TN]*

---

9 Google-Adword-Kampagne: Werbender haftet als "Störer" bei Erscheinen von Werbeanzeigen mit geschützter Unternehmensbezeichnung

Quelle: Schleswig-Holsteinisches Oberlandesgericht, Urteil vom 22.03.2017; AZ: 6 U 29/15
Fundort: © kostenlose-urteile.de (ra-online GmbH), Berlin 25.04.2017; Dok. Nr.: Dokument-Nr. 24158

Verletzung des Markengesetzes beruht auf konkreter Ausgestaltung der Anzeige und nicht auf Verwendung bestimmter Schlüsselwörter

Ist eine Google-Adword-Kampagne so eingerichtet, dass bei der Eingabe einer geschützten Unternehmens-bezeichnung eine Werbeanzeige einer anderen Person (Werbender) erscheint, so steht dem Inhaber der geschützten Unternehmensbezeichnung auch dann ein Unterlassungsanspruch gegen den Werbenden zu, wenn dieser nicht für die Einblendung seiner Anzeige verantwortlich ist, hiervon aber wusste. Dies entschied das Schleswig-Holsteinische Oberlandesgericht.

Der Kläger des zugrunde liegenden Falls nutzt die geschäftliche Bezeichnung "W... C... T...". Die Beklagten sind in derselben Branche tätig wie der Kläger. Durch eine Adword-Kampagne der Beklagten erschien bei der Eingabe des Suchbegriffs "W... C... T..." im Suchfeld der Suchmaschine Google eine Anzeige der Beklagten. Der Kläger nahm die Beklagten daraufhin gerichtlich auf Unterlassung in Anspruch. Das Landgericht Kiel hat der Unterlassungsklage des Klägers in der ersten Instanz stattgegeben.

Diese Entscheidung bestätigte nun das Schleswig-Holsteinische Oberlandesgericht. Zur Begründung führte das Gerichts aus, dass dem Kläger gegen die Beklagten ein Unterlassungsanspruch aus §§ 5 Abs. 2, 15 Abs. 4, Abs. 2 MarkenG zusteht. Die Beklagten haben die geschäftliche Bezeichnung des Klägers "W... C... T..." unbefugt in einer Weise benutzt, die zu Verwechslungen führen kann. Bei der Eingabe des Suchbegriffs "W... C... T..." im Suchfeld der Suchmaschine Google erschien nicht eine Anzeige des Klägers, sondern eine solche der Beklagten, die mit den Worten "Anzeige zu w...c...t..." überschrieben war. Nach dem Erscheinungsbild haben die Beklagten damit das Unternehmenskennzeichen des Klägers als Werbung für sich benutzt, denn für den durchschnittlichen Internetnutzer ist nicht erkennbar, ob eine – tatsächlich nicht bestehende – geschäftliche Verbindung zwischen den Beklagten und dem Kläger besteht. Vielmehr erweckt die Überschrift der Anzeige den Eindruck, dass die Anzeige eine solche des Klägers ist. [Link zum vollständigen Beitrag] *[BE: TN]*

10 Vorratsdatenspeicherung: Weitere Eilanträge erfolglos

Quelle: *Bundesverfassungsgericht, Beschluss vom 26.03.2017 ; AZ: 1 BvR 3156/15 und 1 BvR 141/16*
Fundort: *© kostenlose-urteile.de (ra-online GmbH), Berlin 13.04.2017*; Dok.-Nr.: *24121*

Verfassungsrechtliche Fragen im Eilrechtschutzverfahren nicht zu klären

Die Eilanträge auf Erlass einer einstweiligen Anordnung gegen das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten waren erneut erfolglos. Dies hat das Bundesverfassungsgericht nunmehr bekannt gegeben.

In den vorliegenden Verfahren haben sich die Antragsteller mit ihren Anträgen auf Erlass einer einstweiligen Anordnung erneut gegen das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10. Dezember 2015 gewandt.

Sie wollten insbesondere mit Blick auf das Urteil des Gerichtshofs der Europäischen Union vom 21. Dezember 2016 (Rs. C-203/15 und C-698/15) erreichen, dass die durch dieses Gesetz eingeführte Vorratsdatenspeicherung von Telekommunikations-Verkehrsdaten zu Zwecken der öffentlichen Sicherheit außer Kraft gesetzt wird.

Das Bundesverfassungsgericht hat die Anträge auf Erlass einer einstweiligen Anordnung abgelehnt. Auch nach der Entscheidung des Gerichtshofs der Europäischen Union stellen sich hinsichtlich der verfassungsrechtlichen Bewertung der angegriffenen Regelungen Fragen, die nicht zur Klärung im Eilrechtschutzverfahren geeignet sind. *[BE: RG]*

Führungs-Akademie
des Deutschen Olympischen Sportbundes
Willy-Brandt-Platz 2
50679 Köln

Tel. 0221/221 220 13
Fax: 0221/221 220 14
info@fuehrungs-akademie.de
www.fuehrungs-akademie.de