Datenschutz newsbox

Ausgabe 8 2017

DATAKONTEXT

Editorial

Der Begriff der sog. Filterblase wurde im Jahre 2012 von dem Internetaktivisten Elo Pariser ins Leben gerufen. Er verwendete den Begriff „Filter Bubble" in seinem Buch „The Filter Bubble: What the Internet Is Hiding from You“ im Sinne einer eingeschränkten Weltsicht. Diese eingeschränkte Weltsicht kann bspw. durch vorgefilterte Inhalte verstärkt werden.
Nutzt ein Datenschutz-Interessierter oder ein Datenschutzbeauftragter beispielsweise Soziale Medien wie Twitter, ist es nicht unwahrscheinlich, dass es in seiner Timeline seit einigen Jahren verstärkt um die neuen Anforderungen der sogenannten Europäischen Datenschutz-Grundverordnung und seiner Umsetzung gehen wird. Auf Grund dieses Umstandes anzunehmen, dass der „Rest der Welt da draußen" ebenfalls so interessiert an dieser Thematik ist wie man selbst, kann sich aber durchaus als Trugschluss erweisen.
Der Händlerbund wollte in einer aktuellen Umfrage von Onlinehändlern wissen, was sie von dem neuen Gesetz (DS-GVO) halten und ob sie auf die neue Datenschutzgrundverordnung (DS-GVO) vorbereitet sind. Die Ergebnisse sind ernüchternd: Ein Drittel der befragten Onlinehändler gab an, noch nichts von der neuen Verordnung gehört zu haben. 72 Prozent der Befragten gestand, noch gar nicht oder nicht ausreichend über die neuen Richtlinien informiert zu sein. Nur 5 Prozent fühlten sich hinsichtlich der ab 25. Mai 2018 wirksam werdenden Verordnung gerüstet.

Bei den IT- und Digitalunternehmen sind die Werte auch eher durchwachsen. Nach einer im Juni 2017 durchgeführten Umfrage des BITKOM gab jedes fünfte IT- und Digitalunternehmen (19%) an, sich noch gar nicht mit dem Thema beschäftigt zu haben. Nur jedes dritte Unternehmen (34%) konnte angeben bereits erste Maßnahmen eingeleitet oder sogar schon umgesetzt zu haben. Vier von zehn Unternehmen (42%) beschäftigen sich zum Zeitpunkt der Umfrage mit dem Thema, hatten aber noch keine Maßnahmen begonnen, und 5% wollten oder konnten keine Angaben machen.
Offenbar kann eine Filterblase nicht nur zu einer eingeschränkten Weltsicht, sondern auch dazu führen, dass man die Außenwelt hinter der Filterblase nicht besonders realistisch einzuschätzen vermag.

Ihr Levent Ferik

Impressum

DATAKONTEXT GmbH
Augustinusstraße 9d
50226 Frechen

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

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

Maßnahmen gegen unerwünschte Werbung

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg hat das Merkblatt „Was Sie gegen unerwünschte Werbung tun können" aktualisiert (Stand 10. Mai 2017).
Dabei geht das Merkblatt sowohl auf die Offline-Werbung wie Briefpost als auch auf Belästigungen durch Online-Werbung wie EW-Mail, Telefax, SMS, MMS ein.
Auch auf die Telefonwerbung, die, wenn sie sich an Verbraucher richtet, besonders restriktiv behandelt wird, geht das Merkblatt ein. Hier scheint es noch Aufklärungsbedarf darüber zu geben, dass nur bei vorheriger ausdrücklicher Einwilligung in die entsprechende Datenerhebung und Nutzung zu Werbezwecken diese Art der Werbung zulässig ist (§ 7 Absatz 2 Nummer 2 UWG). Dabei muss die Einwilligung vor dem Werbeanruf vorliegen.
Im Abschnitt „Weitere allgemeine Hinweise: Was kann ich noch tun?" werden Verbraucher über mögliche Gegenmaßnahmen informiert.

Quelle: Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg

Neues Datenschutzrecht in der Umsetzung

Am 29. Juni und 7. Juli 2017 fanden die diesjährigen Informationstage der GDD bei der Vattenfall GmbH in Hamburg sowie im Schulungszentrum der Fraport AG in Frankfurt statt. Das Leitthema lautete „Neues Datenschutzrecht in der Umsetzung".
Nach der Begrüßung durch GDD-Vorstandsmitglied Barbara Broers in Hamburg bzw. dem Vorstandsvorsitzenden der GDD, Prof. Dr. Rolf Schwartmann in Frankfurt, berichtete GDD-Geschäftsführer Andreas Jaspers jeweils von den aktuellen Entwicklungen im Datenschutz und der GDD-Geschäftsstelle. Das Hauptaugenmerk lag hierbei natürlich auf den umfangreichen Umbauarbeiten, die nicht nur durch die Europäische Datenschutz-Grundverordnung (DS-GVO), sondern auch durch das nunmehr verkündete Datenschutzanpassungs- und Umsetzungsgesetz (DSAnpUG) notwendig werden. Die neuen Vorschriften müssen ab Mai 2018 von den Unternehmen befolgt werden.
Danach stellte Paul Gürtler, Datenschutzbeauftragter der Targo Bank und Mitglied des GDD-Arbeitskreises „DS-GVO-Praxis", die bislang erschienenen GDD-Praxishilfen zur DS-GVO vor. Seit Inkrafttreten der DS-GVO am 24. Mai 2016 erscheinen die Praxishilfen in neuem, klaren Design und mit neuer Zählung. Unter den bisher abgehandelten Themen findet sich der Datenschutzbeauftragte, die Auftragsverarbeitung, das Verzeichnis von Verarbeitungstätigkeiten und einiges mehr.
Nach einer Pause skizzierte Dr. Lorenz Franck von der GDD-Geschäftsstelle die neuen Transparenzpflichten nach den Artikeln 13 und 14 DS-GVO. Die neuen Vorschriften sehen Informationen an die Betroffenen vor, die wesentlich tiefer ins Detail gehen, als dies nach dem bisherigen Recht der Fall war.
Den Schluss machte Dr. Andreas Splittgerber, Rechtsanwalt bei ReedSmith LLP München, mit seinem Vortrag über die geplante ePrivacy-Verordnung. Diese soll die bisherige ePrivacy-Richtlinie ersetzen und ggf. noch zeitgleich mit der DS-GVO Geltung erlangen. Spannend bleibt, welche Änderungen sich beim Einsatz von Cookies, Website-Tracking und Werbemails ergeben werden.

Aus der Reihe: „Die Aufsichtsbehörde antwortet …"

Begriff der Belastbarkeit nach der DS-GVO

Frage des Erfa-Kreises Bayreuth:

Wie kann ich gemäß Artikel 32 (1) b) DS-GVO als Verantwortlicher oder Auftragsverarbeiter die „Belastbarkeit der Systeme und Dienste" sicherstellen und auch nachweisen?

Anwort BayLDA:

Die Anforderung der **„Belastbarkeit der Systeme und Dienste"** im Zusammenhang mit der Verarbeitung in Art. 32 DS-GVO ist zumindest als Wortlaut **neu** im Vergleich zum gegenwärtigen BDSG.
Nähere Ausführungen zur **Definition** des Begriffes sind in der DS-GVO jedoch **nicht** zu finden. Aus diesem Grund ist derzeit noch nicht final absehbar, welche konkreten Maßnahmen hierbei der Verantwortliche oder Auftragsverarbeiter tatsächlich zu treffen hat, um eine Sicherstellung auch hinsichtlich der Nachweisbarkeit zu gewährleisten.
Vorstellbar ist, dass der Begriff der Belastbarkeit eine **wesentliche Rolle im Bereich des Notfallmanagements** spielen kann. Die Datenschutzaufsichtsbehörden sind derzeit bemüht, auch diesen Begriff näher zu durchleuchten und die Anforderungen daran baldmöglichst zu veröffentlichen.

Neue Haftungsrisiken für den DSB nach der DS-GVO

Frage des Erfa-Kreises Bayreuth:

Welche Aufgaben und Haftungsrisiken ergeben sich für den Datenschutz-Beauftragten nach der DS-GVO? Muss sich der Datenschutzbeauftragte jetzt speziell gegen neue Risiken versichern?

Anwort BayLDA:

Die Aufgaben des DSB sind unter Nr. 4 des vorgenannten WP 243 näher beschrieben, ebenso in unserer Kurz-Information auf unserer Homepage. Der DSB hat in Zukunft nach Art. 39 Abs. 1 DS-GVO folgende Aufgaben:

- Unterrichtung und Beratung des Verantwortlichen und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Datenschutz-Pflichten;
- Überwachung der Einhaltung der Datenschutzvorschriften sowie der Strategien des Verantwortlichen für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen;
- Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO und Überwachung ihrer Durchführung;
- Zusammenarbeit mit der Aufsichtsbehörde;
- Anlaufstelle für die Aufsichtsbehörde;
- Hinzu kommt noch aus Art. 38 Abs. 4 DS-GVO die Beratung der betroffenen Personen zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte gemäß DS-GVO im Zusammenhang stehenden Fragen.
  Das WP 243 hält zur Verantwortlichkeit eines DSB schon in der Einführung unter Nr. 1 klarstellend fest:
  „DSB sind im Falle der Nichteinhaltung der DS-GVO nicht persönlich verantwortlich. Aus der DS-GVO geht klar hervor, dass es Aufgabe des Verantwortlichen oder des Auftragsverarbeiters ist, sicherzustellen und nachweisen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt (Artikel 24 Absatz 1). Für die Einhaltung der datenschutzrechtlichen Bestimmungen ist der Verantwortliche oder der Auftragsverarbeiter verantwortlich."
  Neue Haftungsrisiken bzw. den Bedarf einer Versicherung gegen neue Risiken sehen wir deshalb bei angestellten DSB nicht. Es wird nach unserer Ansicht weiterhin für den DSB im Beschäftigungsverhältnis die normale Arbeitnehmer-Haftung gelten.

Bestand alter Verfahrensverzeichnisse nach Wirksamwerden der DS-GVO

Frage des Erfa-Kreises Bayreuth:
Können alte Verfahrensverzeichnisse beibehalten werden oder müssen diese komplett neu erstellt werden? (Unverhältnismäßig hoher Bearbeitungsaufwand.) Wie wird „Verfahren" zukünftig definiert werden?

Anwort BayLDA:
Wenn die bisherigen Verzeichnisse eines Verantwortlichen schon alle Inhalte nach Art. 30 Abs. 1 DS-GVO abbilden, können diese Verzeichnisse weiterverwendet werden, andernfalls sind diese Verzeichnisse entsprechend zu ergänzen oder neu anzulegen.
Als Beispiele für „Verfahren" sehen wir für den Bereich Personal z. B. folgende Einzel-Verfahren (da unterschiedliche Zwecke und Dateninhalte etc.):

- Personalaktenführung/Stammdaten
- Lohn- und Gehaltsabrechnung
- Lohnfortzahlung bei Krankheit
- Lohn-/Gehaltspfändungen
- Arbeitszeiterfassung
- Urlaubsdaten
- Personalplanung/Skill-Datenbank
- Stammdaten zu ehemaligen Beschäftigten
- Betriebsbeteiligungen
- betriebliche Altersversorgung bzw. Betriebsrenten
- Nutzungsprotokollierungen IT/Internet/E-Mail
- Telefondatenerfassung
- Firmenparkplatzverwaltung
- Videoüberwachung an Arbeitsplätzen
- Dienstplanungen

DSB und kaufmännische Leitung in Personalunion

Frage des Erfa-Kreises Bayreuth:
Ein DSB ist in seiner/ihrer Hauptfunktion kaufmännischer Leiter/Leiterin und mit Prokura ausgestattet. Im Rahmen der weiteren Entwicklung wird er/sie auch zusätzlich zum Geschäftsleitungsmitglied ernannt. Das Unternehmen hat mehrere hundert Beschäftigte. Fragen: Wie schätzt das BayLDA die Unvereinbarkeit der Funktion DSB mit weiteren Aufgaben ein? Und reicht die Hauptfunktion kaufmännischer Leiter alleine schon als Ausschluss der zusätzlichen Tätigkeit als DSB aus?

Anwort BayLDA:
Im WP 243 der EU-Art.-29-Datenschutzgruppe heißt es dazu:
„Als Faustregel lassen sich zu den mit Interessenkonflikten einhergehenden Positionen solche des leitenden Managements (wie etwa Leiter des Unternehmens, Leiter des operativen Geschäftsbereichs, Finanzvorstand, leitender medizinischer Direktor, Leiter der Marketingabteilung, Leiter der Personalabteilung oder Leiter der IT-Abteilung) zählen, jedoch auch hierarchisch nachgeordnete Positionen, wenn die betreffenden Funktionen oder Aufgabenfelder die Festlegung von Zwecken und Mitteln der Datenverarbeitung mit sich bringen."
Nach diesen Grundsätzen ist die Tätigkeit des Geschäftsleitungsmitglieds oder kaufmännischen Leiters mit der Funktion des DSB wegen Interessenkollisionsgefahren unvereinbar.

Notfallplanung für eine Datenpanne nach DS-GVO

Frage des Erfa-Kreises Bayreuth:
Wie muss gewährleistet sein, dass die Datenpanne innerhalb 72 Stunden an Wochenenden / Feiertagen gemeldet wird? Muss hier eine Notfallplanung installiert werden?

Anwort BayLDA:
Nach Art. 33 DS-GVO ist eine Verletzung des Schutzes personenbezogener Daten binnen 72 Stunden der zuständigen Aufsichtsbehörde durch den Verantwortlichen zu melden, nachdem ihm die Verletzung bekannt wurde.
Erfolgt die Meldung an die Aufsichtsbehörde nicht innerhalb von 72 Stunden, so ist ihr eine entsprechende Begründung beizufügen.
Wir betrachten den angegebenen Zeitraum durchaus für ausreichend, um eine solche Meldung durchzuführen. Das BayLDA bietet hierfür seit letztem Jahr einen eigenen Online-Service an, mit dem sicher, schnell und bequem Vorfälle dieser Art ohne Registrierung gemeldet werden können.
Erfährt der Verantwortliche an Feiertagen oder an Wochenende davon, beginnt die 72-Stunden-Frist zu laufen.
In der Regel kann dann am darauffolgenden Werktag die Meldung noch innerhalb der Frist getätigt werden, so dass auch das BayLDA derzeit mit keinen Ausnahmen hierbei rechnet.
Verantwortliche sollten sich der Meldepflicht bewusst sein und entsprechende Vorbereitungen treffen, damit im „worst case" die richtigen Schritte eingeleitet werden, um den Schaden zu minimieren und den gesetzlichen Anforderungen zu genügen.

Überwachung mittels Keylogger – Verwertungsverbot

Der Einsatz eines Software-Keyloggers, mit dem alle Tastatureingaben an einem dienstlichen Computer für eine verdeckte Überwachung und Kontrolle des Arbeitnehmers aufgezeichnet werden, ist nach § 32 Abs. 1 BDSG unzulässig, wenn kein auf den Arbeitnehmer bezogener, durch konkrete Tatsachen begründeter Verdacht einer Straftat oder einer anderen schwerwiegenden Pflichtverletzung besteht.

Der Kläger war bei der Beklagten seit 2011 als „Web-Entwickler" beschäftigt. Im Zusammenhang mit der Freigabe eines Netzwerks teilte die Beklagte ihren Arbeitnehmern im April 2015 mit, dass der gesamte „Internet-Traffic" und die Benutzung ihrer Systeme „mitgeloggt" werde. Sie installierte auf dem Dienst-PC des Klägers eine Software, die sämtliche Tastatureingaben protokollierte und regelmäßig Bildschirmfotos (Screenshots) fertigte. Nach Auswertung der mit Hilfe dieses Keyloggers erstellten Dateien fand ein Gespräch mit dem Kläger statt. In diesem räumte er ein, seinen Dienst-PC während der Arbeitszeit privat genutzt zu haben. Auf schriftliche Nachfrage gab er an, nur in geringem Umfang und in der Regel in seinen Pausen ein Computerspiel programmiert und E-Mail-Verkehr für die Firma seines Vaters abgewickelt zu haben. Die Beklagte, die nach dem vom Keylogger erfassten Datenmaterial davon ausgehen konnte, der Kläger habe in erheblichem Umfang Privattätigkeiten am Arbeitsplatz erledigt, kündigte das Arbeitsverhältnis außerordentlich fristlos, hilfsweise ordentlich.

Die Vorinstanzen haben der dagegen gerichteten Kündigungsschutzklage stattgegeben. Die Revision der Beklagten hatte vor dem Zweiten Senat des Bundesarbeitsgerichts keinen Erfolg. Die durch den Keylogger gewonnenen Erkenntnisse über die Privattätigkeiten des Klägers dürfen im gerichtlichen Verfahren nicht verwertet werden. Die Beklagte hat durch dessen Einsatz das als Teil des allgemeinen Persönlichkeitsrechts gewährleistete Recht des Klägers auf informationelle Selbstbestimmung (Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG) verletzt. Die Informationsgewinnung war nicht nach § 32 Abs. 1 BDSG zulässig. Die Beklagte hatte beim Einsatz der Software gegenüber dem Kläger keinen auf Tatsachen beruhenden Verdacht einer Straftat oder einer anderen schwerwiegenden Pflichtverletzung. Die von ihr „ins Blaue hinein" veranlasste Maßnahme war daher unverhältnismäßig. Hinsichtlich der vom Kläger eingeräumten Privatnutzung hat das Landesarbeitsgericht ohne Rechtsfehler angenommen, diese rechtfertige die Kündigungen mangels vorheriger Abmahnung nicht.

Bundesarbeitsgericht
Urteil vom 27. Juli 2017 - 2 AZR 681/16 -

Fragebogen zum Stand der DS-GVO

Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) nahm den 25.05.2017 (1 Jahr vor Wirksamwerden der DS-GVO) zum Anlass, ca. 150 bayerischen Unternehmen unter Zugrundelegung des künftigen Rechts einen Prüffragebogen zuzuschicken, damit diese Unternehmen feststellen können, wie weit sie mit der Vorbereitung auf das neue Recht schon gekommen sind.
Dabei ging es dem BayLDA nicht darum einen Rücklauf zu den Fragen zu erhalten. In erster Linie sollten die Fragen als Gradmesser hinsichtlich Umsetzung intern eingesetzt werden.
Auf Grund zahlreicher Nachfragen hat sich das BayLDA entschlossen, den Fragebogen zur DS-GVO-Prüfung auch auf Englisch anzubieten.

Quelle: BayLDA

Datenübermittlung an Drittländer unter Beachtung der DS-GVO

Die Übergangszeit von zwei Jahren seit Inkrafttreten der DS-GVO bis zum Wirksamwerden nutzen die Aufsichtsbehörden, um Interessierten und Verantwortlichen die neuen Rechtsgrundlagen und deren Anforderungen näher zu bringen. Dazu haben einige Aufsichtsbehörden eigene Rubriken auf ihren Internetseiten gestartet. Bei der Umsetzung der Verordnung ist eine abgestimmte und einheitliche Sichtweise unabdingbar.
Als Ergebnis einer gemeinsamen Arbeit veröffentlicht die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) ab sofort gemeinsame Kurzpapiere zur DS-GVO.
Diese sollen als erste Orientierung, wie nach Auffassung der Datenschutzkonferenz die Datenschutz-Grundverordnung im praktischen Vollzug angewendet werden sollte, dienen. Dabei wird betont, dass diese Auffassung unter dem Vorbehalt einer zukünftigen –möglicherweise abweichenden –Auslegung durch den Europäischen Datenschutzausschuss stehe.
Auch das Kurzpapier Nr. 4 – Datenübermittlung an Drittländer dient als erste Orientierung insbesondere für den nichtöffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen –
möglicherweise abweichenden –Auslegung des Europäischen Datenschutz-ausschusses.
Die Datenschutzkonferenz hat ihre Reihe um folgende Kurzpapiere ergänzt:
– Kurzpapier Nr. 5 Datenschutz Folgenabschätzung
– Kurzpapier Nr. 6 Auskunftsrecht
– Kurzpapier Nr. 7 Marktortprinzip
– Kurzpapier Nr. 8 Maßnahmenplan

Quelle: Der Hessische Datenschutzbeauftragte

BSI erkennt ersten branchenspezifischen Sicherheitsstandard an

Mit dem branchenspezifischen Sicherheitsstandard (B3S) Wasser/Abwasser hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Eignung des ersten Sicherheitsstandards für einen KRITIS-Sektor festgestellt. Der Bescheid zur Eignung des Standards wurde von BSI-Präsident Arne Schönbohm an die Vertreter Prof. Dr. Gerald Linke und Otto Schaaf der für diesen Bereich regelsetzenden Verbände DVGW und DWA überreicht. Der DVGW ist der regelsetzende Verband für die Trinkwasserversorgung. Die DWA ist der regelsetzende Verband für die Abwasserbeseitigung.
Betreiber kritischer Infrastrukturen aus dem Sektor Wasser, die den Anforderungen des IT-Sicherheitsgesetzes unterliegen, müssen ihre Informationstechnologie nach dem Stand der Technik absichern und können dies nun anhand des B3S umsetzen. Der B3S Wasser/Abwasser enthält Rahmenanforderungen, die auf die tatsächlichen Gegebenheiten im KRITIS-Sektor Wasser zugeschnitten sind, eine Vorgehensweise zur Risikoanalyse sowie eine Sammlung von Sicherheitsmaßnahmen, um den identifizierten Risiken zu begegnen. Im B3S Wasser/Abwasser ist unter anderem ein Gesamtpaket von rund 140 Maßnahmen aus dem IT-Grundschutz des BSI enthalten.
Durch die Anwendung des branchenspezifischen Sicherheitsstandards können Betreiber aus dem KRITIS-Sektor Wasser (Branchen „Öffentliche Wasserversorgung" und „Öffentliche Abwasserbeseitigung") die Mindestanforderungen für IT-Sicherheit gemäß § 8a (1) BSI-Gesetz erfüllen. Auch Unternehmen aus dem KRITIS-Sektor Wasser, die nicht als Betreiber einer kritischen Infrastruktur im Sinne des BSIG gelten, können den Standard umsetzen und somit das IT-Sicherheitsniveau des Unternehmens erhöhen.

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Info-Seite zur DS-GVO

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz stellt im Rahmen seines Internetauftritts ausgewählte Informationen zum Thema DS-GVO bereit. Damit bietet der LfDIRlP neben seinem regelmäßig erscheinenden Newsletter eine gute Möglichkeit, sich über die wichtigsten Themen der DS-GVO zu informieren.
In der Kategorie FAQ werden die Antworten auf häufige Fragen zur Datenschutz-Grundverordnung und den durch sie bedingten Änderungen zusammengestellt. Die Seite enthält auch externe Verweise mit weiteren Infos zur DS-GVO, wie beispielsweise den Papieren der Artikel 29 Datenschutzgruppe oder den sogenannten Kurzpapieren zur Auslegung der Datenschutz-Grundverordnung, die von der Datenschutzkonferenz gepflegt werden.
Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz stellt damit, neben weiteren guten Anlaufstellen, eine empfehlenswerte Möglichkeit dar, sich über die Entwicklungen im Bereich der DS-GVO auf dem neuesten Stand zu halten.

Quelle: Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz

300.000 Euro Bußgeld für rechtswidrige Werbeanrufe

Die Bundesnetzagentur hat gegen die Energy2day GmbH das höchstmögliche Bußgeld von 300.000 Euro verhängt. Auslöser waren rechtswidrige Werbeanrufe für Energielieferverträge.
Bei der Bundesnetzagentur hatten sich rund 2.500 Verbraucher über Werbeanrufe der Energy2day GmbH beschwert. Zahlreiche Verbraucher berichteten, dass sich die Anrufer als ihr örtlicher Energieversorger ausgegeben oder behauptet haben, sie würden mit diesem zusammenarbeiten. Ziel war es, die Verbraucher zum Wechsel ihres Stromlieferanten zu bewegen.
Wettbewerber im Energiemarkt sahen sich wegen dieses Vorgehens der Energy2day GmbH bereits zu umfangreichen zivilrechtlichen Rechtsstreitigkeiten im gesamten Bundesgebiet gezwungen.
Die Energy2day GmbH hatte eine kaskadenartige Vertriebsstruktur aufgebaut und mit einer Vielzahl an Untervertriebspartnern u.a. auch im Ausland zusammengearbeitet, die als Subunternehmer Anrufe in Deutschland getätigt haben.
Wer Subunternehmen mit telefonischen Marketingkampagnen beauftragt, dem obliegen als Auftraggeber umfangreiche Aufsichtspflichten, so die BNetzA. Ist es in einer Vertriebsstruktur bereits zu Rechtsstreitigkeiten wegen unlauterem Marktverhalten gekommen, bestehen erst recht gesteigerte Aufsichtspflichten.
Im aktuellen Verfahren wurde der gesetzlich vorgesehene Bußgeldrahmen von der Bundesnetzagentur erstmals voll ausgeschöpft. Das Unternehmen hat ausgesagt, kein Telefonmarketing gegenüber Verbrauchern mehr zu betreiben. Die Bundesnetzagentur wird dies beobachten.
Die Geldbuße ist noch nicht rechtskräftig. Über einen möglichen Einspruch entscheidet das Amtsgericht Bonn.

Quelle: Bundesnetzagentur

Eigentumsordnung für Mobilitätsdaten

Das Bundesministerium für Verkehr und digitale Infrastruktur (BMVI) hat die während des Zukunftsforums Datensouveränität am 2. August 2017 vorgestellte Studie „‚Eigentumsordnung' für Mobilitätsdaten" zum Download bereitgestellt.
Die Studie wird einer breiten Fachkonsultation zugänglich gemacht, damit diese die Möglichkeit erhalten, ihre Stellungnahme zu der Studie abzugeben. Die Konsultation richtet sich an sämtliche Interessenträger u.a. aus der Wirtschaft, Wissenschaft, Verwaltung, Instituten und Verbraucherschutzorganisationen.
Die Stellungnahmen sollen im BMVI ausgewertet werden und zur Entwicklung eines transparenten und innovationsfreundlichen Datenrechts beitragen. Dieses soll entwickelt werden, um die wertvollen, im Bereich der Mobilität gesammelten Daten zusammenzuführen, bestmöglich zu nutzen und damit einen Mehrwert für die Verkehrsteilnehmer, Wirtschaft und den Verkehr zu schaffen.
Ein umfassendes Eigentum an Daten, wie man es vom Sacheigentum beispielsweise am Kfz kent, gibt es derzeit nicht, so das BMVI. Daten seien keine Sachen. In der geltenden Rechtsordnung existierten nur verstreute Schutz- und Abwehrrechte. Es gebe ein auf Abwehr gerichtetes Datenschutzrecht, aber kein auf Gestaltung angelegtes Datennutzungsrecht. In der Regel entscheide über die Datennutzung allein die faktische Zugriffsmöglichkeit.
Hier setze die Studie an. Sie zeigt konkrete Wege in Richtung eines neuen Datenrechtes auf. Auf diese Weise könnte ein neuer Zuordnungsansatz etabliert werden, der an die Erstellung der Daten und an die wesentlichen Investitionen anknüpft. Er ermöglicht mehr Transaktionen in einem Markt für Daten, größere Transparenz und Rechtssicherheit sowie eine höhere Souveränität der Marktteilnehmer.
Beiträge können **bis zum 2. November 2017** in einem gängigen Daten-Format und unter Verwendung folgender E-Mail-Adresse: Fachkonsultation-Datensouveraenitaet@bmvi.bund.de an das BMVI gesendet werden.

Quelle: Das Bundesministerium für Verkehr und digitale Infrastruktur (MBVI)

Betroffene können sich bezüglich Privacy Shield beschweren

Seit 1. August 2016 sind die zwischen der EU und den USA vereinbarten Neuregelungen für die Übermittlungen personenbezogener Daten in die USA in Kraft. Sie werden als EU-US Privacy Shield bezeichnet. Die Berliner Beauftragte für Datenschutz und Informationsfreiheit, Maja Smoltczyk, stellt ab sofort auf ihrer Internetseite Informationen zum Privacy Shield bereit, die auch einheitliche Beschwerdeformulare beinhalten.
Aufgrund der Neuregelungen können personenbezogene Daten an US-Unternehmen übermittelt werden, die eine gültige Privacy Shield-Zertifizierung besitzen. Personen aus Europa haben in diesem Fall gegenüber den zertifizierten US-Unternehmen eine Reihe von Rechten, wie das Recht auf Information, auf Auskunft, Berichtigung und – unter bestimmten Umständen – Löschung sowie auf Garantien für den Fall einer Weiterübermittlung. Diese Rechte können von Betroffenen direkt gegenüber den zertifizierten US-Unternehmen geltend gemacht werden. Daneben ist es auch möglich, sich jederzeit an die zuständige nationale
Datenschutzbehörde zu wenden. Um es Betroffenen zu erleichtern, sich zu informieren und gegebenenfalls eine Beschwerde einzureichen, veröffentlicht die Berliner Beauftragte für Datenschutz und Informationsfreiheit nun allgemeine Informationen zum Privacy Shield sowie unter den EU-Datenschutzbehörden abgestimmte Beschwerdeformulare.
Der Privacy Shield räumt europäischen Bürgern erstmals auch eine Überprüfungsmöglichkeit ein, wenn sie Zugriffe von US-amerikanischen Sicherheitsbehörden oder Nachrichtendiensten, unter Verstoß gegen geltende Bestimmungen, auf ihre aus Europa übermittelten Daten befürchten. Für die Untersuchung solcher Anträge wurde eine Ombudsperson im US-Außenministerium neu bestellt. Sie ist verpflichtet, Anträgen zur Überprüfung, die ihr von den europäischen Datenschutzbehörden zugeleitet wurden, nachzugehen.

Quelle: Berliner Beauftragte für Datenschutz und Informationsfreiheit

Haftungsrisiken in der IT unter Berücksichtigung der DS-GVO

Die IHK Schwaben in Kooperation mit dem aitiRaum e. V. stellen in einem aktuellen Leitfaden Haftungsrisiken dar, die klassischerweise in der IT auftreten. Der Leitfaden ist adressiert an Inhaber, Geschäftsführer und IT-Verantwortliche.
Wenn über Haftungsrisiken durch den Einsatz von Informationstechnologie und deren Absicherung nachgedacht wird, ist entscheidend, eine klare Gliederung der Verantwortungsbereiche und Handlungsfelder festzulegen, mit der Haftungsrisiken so gut als möglich reduziert werden können.
Im Kapitel „Verantwortung" wird beschrieben, dass die Absicherung von IT-Haftungsrisiken dem Vorstand bzw. der Geschäftsführung obliegt. Im schlimmsten Fall wird eine persönliche Verantwortung und Haftung möglich sein. Dabei geht der Leitfaden auch auf die strategischen Aufgaben und auch die konzeptionellen Aufgaben der Geschäftsführung ein. Im Rahmen des dabei zu erstellenden Sicherheit- und Datenschutzkonzepts widmet sich der Leitfaden auch den Vorgaben, die sich aus der DS-GVO ergeben.
Eine Checkliste für die Umsetzung der Vorgabe der Europäischen Datenschutz Grundverordnung (GVO) rundet den Leitfaden ab.

Quelle: IT-Gründerzentrum GmbH

Policy Paper zum Thema Datensparsamkeit

Das Prinzip der Datensparsamkeit wurde durch die neuesten Datenschutzregeln der Europäischen Union bekräftigt: Sowohl die europäische Datenschutz-Grundverordnung als auch die Richtlinie für den Datenschutz bei Polizei und Justiz, die beide ab Mai 2018 in den Mitgliedstaaten gelten bzw. von diesem umgesetzt sein müssen, enthalten die Forderung nach Minimierung der personenbezogenen Daten.

Das **Policy Paper „Datensparsamkeit"** bietet grundlegende Informationen über das Prinzip der Datensparsamkeit und diskutiert dessen Inhalt, Grundlagen, Vor- und Nachteile.
Das wissenschaftliche Expertengremium „Forum Privatheit" räumt in seinem neuesten Policy Paper mit einigen Missverständnissen auf und erklärt, warum Datensparsamkeit unions- und verfassungsrechtlich geboten ist und wie sie Wettbewerbsvorteile sichern kann.

Quelle: forum privatheit