Ausgabe 6/2016

Dezember 2016

Datenschutz Kundeninformation

Liebe Leserinnen und liebe Leser,

in unserer aktuellen Ausgabe möchten wir Sie wieder über einige spannende Themen im Datenschutz informieren.

Themen in dieser Ausgabe:

- Organisation des kirchlichen Datenschutzes
- Nutzung öffentlicher Hotspots
- Facebook und Datenschutz
- Datenschutzverstöße aus der Praxis
- aktuelle Rechtsprechungen

Kirche organisiert Datenschutz neu – Start des katholischen Datenschutzzentrums für NRW

Mit Wirkung zum 16.09.2016 ist das katholische Datenschutzzentrum (KDSZ) für NRW mit Sitz in Dortmund an den Start gegangen. Geleitet wird das Zentrum vom neuen Diözesandatenschutzbeauftragten Steffen Pau, der mit seinem Amtsantritt die Aufgaben des Diözesandatenschutzbeauftragten für den Bereich der (Erz-) Diözesen Köln, Paderborn, Aachen, Essen und den in NRW gelegenen Teil des Bistums Münster wahrnimmt.

Anlass für die Errichtung des KDSZ sind europarechtliche Vorgaben, insbesondere ein Urteil des europäischen Gerichtshofes sowie die europäische Datenschutzgrundverordnung.

Als Datenschutzaufsicht berät das Katholische Datenschutzzentrum die kirchlichen Stellen in Fragen des Datenschutzes und steht als Ansprechpartner für den Umgang mit personenbezogenen Daten zur Verfügung. Weiterhin geht es Hinweisen oder Beschwerden nach, die es zum Umgang mit personenbezogenen Daten in kirchlichen Einrichtungen erhält. Damit sollen eventuell bestehende Verbesserungsmöglichkeiten im Umgang mit den Daten in den kirchlichen Einrichtungen gefunden und umgesetzt werden.

Für die (Erz-)Bistümer Hildesheim, Osnabrück, Hamburg und den oldenburgischen Teil des Bistums Münster ist der Diözesandatenschutzbeauftragte Andreas Mündelein zuständig.

Welche Folgen hat das?

Die Diözesandatenschutzbeauftragten kommen bereits gezielt ihrer Verpflichtung nach und fordern die kirchlichen Stellen zur Herausgabe von Informationen zur Aktenverwaltung in den Krankenhäusern auf.
Dies beinhaltet u.a. folgende Informationen:

- Eingesetzte IT-Systeme zur Verarbeitung von Patientendaten
- Betrieb der IT-Systeme und deren Wartung / Fernwartung
- Speicherung von Daten / Archivierung / Scannen von Papierakten
- Aktenvernichtung
- Externe Leistungsabrechnung

Bei der Beteiligung externer Firmen sind entsprechende Nachweise (ADV-Verträge/Dienstleistungsverträge einzureichen).

ⓘ Quelle: http://www.erzbistum-paderborn.de/38-Nachrichten/20254,Katholisches-Datenschutzzentrum-geht-an-den-Start.html

Datenschutz-Kontakt
datenschutzbeauftragter@factpartner.de

Nutzung von öffentlichen Hotspots

Quelle: http://www.express.de/news/politik-und-wirtschaft/recht/datenschutz--rechtslage-so-schuetzen-sie-ihre-daten-im-offenen-wlan-22427232

Die Kommunikation bei öffentlichen Hotspots läuft oft komplett unverschlüsselt ab.

Mal eben von unterwegs noch eine E-Mail senden, oder im Café oder am Flughafen noch ein wenig arbeiten, bevor es zum nächsten Termin geht…

Öffentliche WLAN-Netze sind praktisch, bergen aber auch Gefahren, da die Kommunikation nach der erfolgreichen Anmeldung bei öffentlichen Hotspots oft komplett unverschlüsselt abläuft. Die Gefahr: Jeder Hacker, der mit einem Notebook oder Smartphone im Umkreis von einigen Dutzend Metern sitze, könne alles im Klartext mitlesen. Ohne Verschlüsselung sind die E-Mail-Zugangsdaten ebenso einsehbar, wie die Nachrichten selbst. Wie also kann man sich nun schützen?

Verschlüsselung

Von öffentlichen Netzwerken ohne Verschlüsselung sollte man grundsätzlich die Finger lassen, warnt das Bundesamt für Sicherheit in der Informationstechnik (BSI). Hier kann theoretisch jeder mitlesen. Besser sind verschlüsselte Netze, doch auch hier ist prinzipiell ein Ausspähen möglich. Gibt es keine Alternative zum öffentlichen Netzwerk, helfen ein VPN-Dienst oder eine SSL-gesicherte Verbindung, den Datenstrom per Verschlüsselung zu schützen.

Fehlermeldungen

Fehlermeldungen zu Zertifikaten (zum Beispiel die Meldung im Browser: „Es besteht ein Problem mit dem Sicherheitszertifikat der Seite. Es wird empfohlen, dass Sie die Webseite schließen und nicht zu dieser Webseite wechseln.“) sollten Internetnutzer im Allgemeinen nicht auf die leichte Schulter nehmen. In öffentlichen Funknetzen ist das Risiko, dass sich dahinter ein Hackerangriff verbirgt, besonders hoch.

Passwörter

Passwörter sind komplex auszuwählen und für verschiedenen Konten sind auch verschiedene Passwörter zu verwenden.

Freigaben

Datei- und Verzeichnisfreigaben sollten deaktiviert werden. Denn je nach Konfiguration des Hotspots kann es möglich sein, dass das Gerät im Netzwerk für andere sichtbar ist.

Automatik

Auch die automatische Anmeldung an bekannten Hotspots sollte deaktiviert werden. Den Namen seines WLANs kann ein Betreiber frei wählen. „Daher ist es denkbar, dass Betrüger WLANs errichten, diese ‚Telekom‘ oder ‚Free Wifi“ nennen, und dann darauf warten, dass sich Smartphones einbuchen“, warnt das BSI.

Facebook und Datenschutz – Einbindung des „Gefällt mir" Button

Per Abmahnung hat die Verbraucherzentrale NRW bereits bei einigen Unternehmen darauf gepocht, den „Gefällt mir"-Button von Facebook datenschutzkonform umzustellen.

Ein dickes Dislike gab es bereits für einige Unternehmen, die auf ihren Webseiten den „Gefällt mir"-Button von Facebook integriert haben. Per Abmahnung hat die Verbraucherzentrale NRW darauf bestanden, diese Schaltfläche datenschutzkonform umzustellen. Denn schon allein durch die Einbindung des Like-Buttons liest das soziale Netzwerk automatisch bei jedem bloßen Aufruf dieser Seiten mit. Darüber werden Besucher jedoch vorher weder ausdrücklich informiert noch können sie der Datenweitergabe widersprechen.

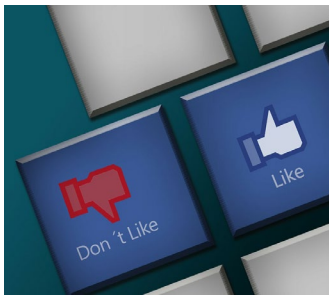
Hintergrund: Mit dem „Gefällt mir"-Button setzt Facebook sogenannte Cookies auf die Rechner der Seitenbesucher. So werden ihre Daten automatisch an Facebook weitergegeben, weil der Browser eine Verbindung mit den Servern dieses Netzwerks aufbaut. Das widerspricht deutschen und europäischen Datenschutzstandards, die eine Weitergabe stets nur mit ausdrücklicher Einwilligung der Betroffenen erlauben.

Allein der Besuch einer Seite mit einem „Gefällt mir"-Button bedeutet noch nicht, dass der Surfer mit der anschließenden automatischen Übertragung, Speicherung und Auswertung seines Surfverhaltens einverstanden ist. Weiterhin werden selbst Informationen von Nutzern abgegriffen, die überhaupt keinen Facebook-Account haben: Tatsächlich können die IP-Adressen mit Hilfe der Cookies wiedererkannt und daraus anonyme Surferprofile angelegt werden. Auf die kann Facebook dann zurückgreifen, wenn sich Nutzer dort irgendwann anmelden sollten.

Ein bloßer Hinweis der Anbieter in den Datenschutzbestimmungen, dass eine solche Weiterleitung der Daten an Facebook erfolgt, genügt nicht. Ebenso wenig wie der Verweis auf die Datenschutzbestimmungen von Facebook. Notwendig ist eine echte Aufklärung über die Datensammlung und -verwertung. Alles mit dem Ziel, Verbraucher in ihrer Entscheidungs- und Verhaltensfreiheit zu schützen.

Impressumspflicht

Das Landgericht Aschaffenburg hat in einem Urteil vom 19.08.2016 (2 HK O 54/11) bestätigt, dass auch Facebookseiten ein Impressum benötigen.



Ein Impressum muss vor allem die folgenden Bedingungen erfüllen:

- **Einfach erkennbar** – Ein durchschnittlich aufgeklärter Nutzer muss sofort erkennen können, wo sich das Impressum befindet. Mittlerweile hat Facebook eine Impressumsrubrik für Seiten eingeführt.
- **Unmittelbar erreichbar** – Das Impressum muss von jeder Seite des Angebotes mit 2-Klicks erreichbar sein.
- **Eindeutig** – Wenn auf das Impressum der Unternehmenswebsite verlinkt wird, darf der Betreiber der Facebook-Seite nicht anders lauten, als die Angabe in dem Impressum auf der Website.
- **Ständig verfügbar** – Das Impressum muss permanent erreichbar sein. Das gilt auch, wenn sich die Fanseite gerade erst im Aufbau befindet.

Datenschutzkonforme Einstellungen bei der Verlinkung auf Facebook

Quelle: http://www.verbraucherzentrale.nrw/likebutton

Impressum auch bei Facebook unverzichtbar

Quelle: http://allfacebook.de/policy/abmahnwelle-wegen-impressumsfehlern-sichern-sie-ihre-fanseite-in-5-min

Datenschutzverstöße aus der Praxis

Promi-Krankenakten in verlassener Klinik gefunden

Zahlreiche Krankenakten von Prominenten sind auf dem Gelände einer ehemaligen Klinik in Münsing am Starnberger See gefunden worden. Die Befunde unter anderem von Klausjürgen Wussow („Die Schwarzwaldklinik) lägen noch heute in der seit zehn Jahren geschlossenen Klinik, berichten übereinstimmend „Münchner Merkur" und „tz".
Ein Fotograf, der bevorzugt Bildserien von verlassenen Orten aufnimmt, hat den Berichten zufolge etwa Röntgenaufnahmen von Wussow gefunden.

Das Gelände sei frei zugänglich, heißt es in den Berichten. Kürzlich habe in dem Gebäude sogar eine Party stattgefunden. Nach den Informationen ließen sich in der Privatklinik einst Stars wie Inge Meysel, Heinz Rühmann und Harald Juhnke behandeln. Die Polizei war schon vor einigen Wochen auf Krankenakten der Klinik aufmerksam geworden, als Befunde eines früheren Patienten von Passanten auf der Straße gefunden wurden.

Patientenakten sind „sensibles Material", sagte Thomas Petri, bayerischer Datenschutzbeauftragter, dem „Münchner Merkur". Die Anforderungen für den Schutz seien besonders hoch. Krankenhäuser müssten die Unterlagen nach der abgeschlossenen Behandlung in ein passives Archiv verschieben, das nicht frei zugänglich ist. „Leider müssen wir immer wieder Mängel feststellen", sagt Petri.

ⓘ Quelle: http://www.spiegel.de/panorama/leute/klausjuergen-wussow-krankenakten-am-starnberger-see-gefunden-a-1100670.html

Aktuelle Rechtssprechungen

Urteil des BGH: Arzt hat keinen Anspruch auf Löschung seiner Daten aus Bewertungsportal

Das hat der Bundesgerichtshof (BGH) in einem Urteil vom 23.September 2014 (AZ: VI ZR 358/13) entschieden. Konkret ging es um die Löschung seiner Daten aus dem Online-Ärztebewertungsportal „jameda".
Gestützt auf sein allgemeines Persönlichkeitsrecht verlangte der Mediziner von den Betreibern des Portals die Unterlassung der Veröffentlichung aller ihn betreffenden Daten sowie die vollständige Löschung seines Profils auf der Internetseite. Auch Daten wie seinen Namen, die Fachrichtung und Anschrift sowie die Bewertungen über ihn wollte er von der Plattform entfernen lassen.
Zur Begründung verwies er auf sein allgemeines Persönlichkeitsrecht und den Datenschutz und war der Ansicht, die Speicherung seiner personenbezogenen Daten durch „jameda" sei unzulässig. Er habe weder in die Speicherung seiner Daten eingewilligt noch sei diese von Gesetzes wegen gestattet.

Das BGH wies seine Klage jedoch mit der Begründung zurück, dass das Recht des Arztes auf informationelle Selbstbestimmung nicht höher zu bewerten ist als das Recht des beklagten Bewertungsportals auf Kommunikationsfreiheit.

Fazit: Die Entscheidung des Bundesgerichtshofs bedeutet Klarheit und Sicherheit für Bewertungsportale: Angehörige freier Berufe wie Ärzte oder Anwälte haben keinen Anspruch auf das Löschen von Online-Bewertungen.

ⓘ Quelle: https://www.ecovis.com/medizin/bgh-arzt-hat-keinen-anspruch-auf-loeschung-seiner-daten-aus-bewertungsportal/

ⓘ Quelle: http://www.dzw.de/artikel/arzt-hat-keinen-anspruch-auf-loeschung-seiner-daten-aus-bewertungsportal

Impressum
FAC'T GmbH
Hohenzollernring 72
48145 Münster

info@factpartner.de
www.factpartner.de

Telefon 0251 935-3700
Telefax 0251 935-4075