Datenschutz Kundeninformation

Ausgabe 7/2017

April 2017

Liebe Leserinnen und liebe Leser,

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

Themen in dieser Ausgabe:

ⓘ Quelle: https://www.datenschutz-notizen.de/edv-und-kirche-aenderung-im-katholischen-datenschutzrecht-2112773/

ⓘ Quelle: https://www.datenschutz-kirche.de/sites/default/files/file/download/vechta/KDO-DVO-2015-vechta.pdf

Datenschutz-Kontakt
datenschutzbeauftragter@factpartner.de

EDV und Kirche – Änderung im katholischen Datenschutzrecht

Zum 01.10.2015 erfuhr die Durchführungsverordnung zur Anordnung über den kirchlichen Datenschutz (KDO-DVO) eine erhebliche Änderung. Dem §6 KDO wurde eine 2. Anlage angefügt, die den Einsatz von Arbeitsplatzcomputern in kirchlichen Stellen regelt. Die wichtigsten Inhalte im Überblick:

Anlage 2 zu § 6 KDO

Mindestanforderungen

• Nennung des regelmäßigen Nutzers, des Standortes und der internen Kennzeichnungs-Nummer im Verfahrensverzeichnis.
• Verpflichtung aller an der Verarbeitung personenbezogener Daten beteiligten Personen auf das Datengeheimnis.
• Verwendung ausschließlich autorisierter Programme zu dienstlichen Zwecken und Verbot der Benutzung privater Programme.
• Orientierung der Schutzmaßnahmen an den BSI-IT-Grundschutzkatalogen bei der Verarbeitung von Daten aus den Melderegistern der kommunalen Meldebehörden in kirchlichen Rechenzentren.

Nicht elektronisch zu verarbeitende Daten

• Verbot der Verarbeitung von Daten an Arbeitsplatzcomputern, wenn diese dem Beicht-, Seelsorge- oder Adoptionsgeheimnis unterliegen und damit besonders schutzbedürftig sind.

Nutzung privater Datenverarbeitungssysteme zu dienstlichen Zwecken

• Verbot der Verarbeitung personenbezogener Daten zu dienstlichen Zwecken auf privaten Geräten.

Fremdzugriffe durch Externe

• Verpflichtung von Externen auf die KDO, unabhängig davon, ob es sich bei ihnen um kirchliche oder um nicht-kirchliche Stellen handelt.

IT-Richtlinien zur Umsetzung von Anlage 2

Zu den in der Anlage 2 definierten drei Datenschutzklassen werden die verschiedenen Schutzniveaus und die damit verbundenen Mindestanforderungen definiert. Davon unabhängig sind folgende Maßnahmen umzusetzen bzw. Aspekte zu beachten:

Erstellung und Umsetzung eines Datensicherungskonzeptes

• Bei der Nutzung von Cloud-Dienstleistungen ist der Auftragnehmer auf die KDO zu verpflichten; der physikalische Speicherort der Daten muss im Geltungsbereich des BDSG liegen.
• Im Falle einer im Ausnahmefall genehmigten Datenverarbeitung auf privaten Geräten, ist der Nutzer auf die Einhaltung der IT-Richtlinie zu verpflichten. Zudem muss er erklären, personenbezogene Daten durch die Dienststelle und auf deren Anforderung löschen zu lassen.

Wartungsarbeiten in der Dienststelle durch Externe

• Dem externen Wartungstechniker darf nicht die Möglichkeit eingeräumt werden, Kopien zu erstellen. Sofern diesem für die Wartungstätigkeit ein Passwort bekannt gegeben werden muss, ist dieses nach Abschluss der Wartungsarbeit unverzüglich zu ändern.

ⓘ Quelle: https://www.aok-verlag.info/de/pages/Themenbereich-Datenschutz/188/

ⓘ Quelle: https://www.aok-verlag.info/de/media_db_objects/inline/0x0/0/35117/Newsletter_DS_im_Blick_2017_01.pdf

Seriöse Aussagen zu den neuen datenschutzrechtlichen Vorgaben lassen sich bislang nur in Bezug auf die DSGVO selbst treffen.

Die Einigung der Gesetzgeber über nationalen Rechtsvorschriften steht noch aus.

Die EU-Datenschutz-Grundverordnung (DSGVO) – Was ändert sich dadurch in anderen Gesetzen?

Die neue EU-DSGVO ist am 25.05.2016 in Kraft getreten und mit einer zweijährigen Übergangsfrist am 25.05.2018 hat sie für alle EU-Mitgliedstaaten Rechtscharakter. Unklarheiten bestehen hingegen noch im Hinblick auf andere Gesetze, die durch die Einführung der DSGVO berührt werden.

Bundesdatenschutzgesetz (BDSG)

Das Bundesdatenschutzgesetz wird es ab Mai 2018 in der heutigen Fassung nicht mehr geben. Derzeit befindet sich ein Referentenentwurf für ein Gesetz zur Anpassung des Datenschutzrechts im Umlauf. Dieses wird ergänzende Regelungen enthalten, die DSGVO bleibt dadurch unberührt.

Klar zu sein scheint:
- Nicht öffentliche Stellen müssen weiterhin einen Datenschutzbeauftragten bestellen, wenn sie mindestens zehn Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigen oder wenn sie Verarbeitungen vornehmen, die deiner Datenschutzfolgeabschätzung nach DSGVO
- Auch das Verfahrensverzeichnis wird wohl weiterhin von den meisten Stellen vorgehalten werden müssen, auch wenn die DSGVO diesbezüglich in bestimmten Fällen für Stellen, die weniger als 250 Mitarbeiter beschäftigen, Ausnahmen vorsieht.

Telemediengesetz (TMG)

Auch im Hinblick auf das Telemediengesetz sind Änderungen zu erwarten. Die Regelungen einer neuen ePrivacy-Verordnung werden für Einrichtungen des Gesundheitswesens insbesondere in den Bereichen relevant werden, in denen Telemediendienste angeboten werden.

Strafgesetzbuch (StGB)

Obwohl es lange Zeit so aussah, als wären im StGB keine Änderungen zu erwarten, besteht nun Hoffnung:

- In einem Referentenentwurf soll der § 203 StGB künftig auch für Offenbarungen gegenüber Personen gelten, die an der beruflichen und dienstlichen Tätigkeit mitwirken, wenn diese Offenbarungen für die ordnungsgemäße Ausübung der Tätigkeit der mitwirkenden Personen erforderlich sind
- Der Entwurfsbegründung lässt sich entnehmen, dass hierdurch auch die klassischen Fälle der Auftragsdatenverarbeitung umfasst werden sollen („Einrichtung, Betrieb, Wartung und Anpassung der informationstechnischen Anlagen, Anwendungen und Systeme“).
- Aber auch für Dienstleister steigen die Anforderungen. Denn nach § 203 Abs. 4 S. 1 Alt. 1 StGB-E kommt auch eine Strafbarkeit der mitwirkenden Person in Betracht, sofern sie unbefugt ein fremdes Geheimnis offenbart.

Kirchengesetze

Selbst die datenschutzrechtlichen Regelungen innerhalb des Kirchenrechts werden vermutlich Änderungen erfahren. Hier wird es nach Art. 91 Abs. 1 DSGVO darauf ankommen, zu überprüfen, ob diese mit der DSGVO in Einklang stehen oder Änderungen erforderlich sind.

Sozialgesetzbuch (SGB) und Landesdatenschutzgesetze (LDSG)

Hier bleiben Änderungen, die es in naher Zukunft geben wird, zunächst abzuwarten.

Die DSGVO wird Mitte nächsten Jahres wirksam. Es ist jedoch auch erforderlich, insbesondere die o.g. weiteren Vorschriften im Blick zu behalten und deren Entwicklungen zu beobachten und diese zu gegebener Zeit im Umsetzungsprozess zu berücksichtigen.

Vorfälle und Wissenswertes

Änderungen im Telekommunikationsgesetz

Am 28.07.2016 ist eine Änderung des Telemediengesetzes in Kraft getreten. Danach wird die bisher nur für Festnetzbetreiber oder Hoster unter bestimmten Umständen geltende Haftungsbefreiung auch auf Anbieter freier WLANs ausgeweitet.

Das Haftungsprivileg umfasst dabei alle „fremde Informationen", deren Übermittlung vom Anbieter nicht veranlasst worden ist und er die Adressdaten der übermittelten Informationen nicht ausgewählt oder gar verändert hat. Somit soll in Zukunft die Einrichtung freier WLANs, die ohne Zugangsbeschränkung von jedermann genutzt werden können, erleichtert werden.

Das TMG schützt aber nicht ausdrücklich vor einer zivilrechtlichen Inanspruchnahme durch Abmahnungen von Seiten der Rechteinhaber, die beim Download von Musikdateien, Filmen oder Fotos ihr Urheberrecht verletzt sehen.

Zwar sieht die Gesetzesbegründung vor, dass die Haftungsprivilegierung des Diensteanbieters nach § 8 Absatz 1 und 2 TMG uneingeschränkt auch die verschuldensunabhängige Haftung im Zivilrecht nach der sog. Störerhaftung umfasst, und daher keine Verurteilung des Vermittlers zur Zahlung von Schadenersatz und ebenfalls keine Verurteilung zur Tragung der Abmahnkosten und der gerichtlichen Kosten im Zusammenhang mit der von einem Dritten durch die Übermittlung von Informationen begangenen Rechtsverletzung erfolgt. Im Wortlaut des Gesetzestextes ist diese Auffassung aber nicht umgesetzt worden. Trotzdem haben Gerichte bei der Auslegung von Gesetzesvorschriften auch die Absichten und Ziele des Gesetzgebers in ihre Entscheidungen mit einzubeziehen. Es bleibt also abzuwarten, ob die Rechtsprechung der Gesetzesbegründung folgen wird.

Vorsicht bei Autofill-Mechanismen

Chrome, Safari, Opera und Erweiterungen wie LastPass angreifbar

Der Sicherheitsspezialist Viljami Kuosmanen hat eine Methode entwickelt, die es ermöglicht, AutoFill-Mechanismen verschiedener Browser und deren Erweiterungen in die Irre zu führen, um private Daten abzugreifen. Über die AutoFill-Funktion werden häufig eingegebene Informationen wie Name, E-Mail-Adresse oder Telefonnummer gespeichert, um sie beim Ausfüllen von Web-Formularen in die entsprechenden Felder einzutragen. Wie der Sicherheitsexperte festgestellt hat, trägt AutoFill gespeicherte Daten auch in Eingabefelder ein, die für Nutzer gar nicht ersichtlich sind. So ist es möglich, verborgene Felder anzulegen, in die beispielsweise Kreditkarteninformationen eingetragen werden. Von der Schwachstelle betroffen sind die gängigen Browser Chrome, Safari und Opera. Firefox ist laut Kuosmanen immun gegen den Trick, weil dort der Anwender explizit jedes Formularfeld anklicken muss (11.01.2017)

ⓘ Quelle: 3.Jahresbericht 2016, Der Diözesandatenschutzbeauftragte des Erzbistums Hamburg, der Bistümer Hildesheim und Osnabrück und des Bischöflich Münsterschein Offizialats in Vechta i.O.

ⓘ Quelle: https://www.heise.de/security/meldung/Phishing-per-Autofill-Chrome-Safari-Opera-und-Erweiterungen-wie-LastPass-angreifbar-3593811.html

Datenschützer beanstanden Wearables/Smart Watches

ⓘ Quelle: http://www.lfd.niedersachsen.de/allgemein/presseinformationen/05122016-149204.html

ⓘ Quelle: Newsletter Information für betriebliche Datenschutzbeauftragte und IT-verantwortliche in kirchlichen Dienststellen Ausgabe 08/2016

Die Datenschutzaufsichtsbehörden der Länder Niedersachsen, Bayern, Brandenburg, Hessen, Nordrhein-Westfalen, Schleswig-Holstein haben zusammen mit der Bundesbeauftragten für den Datenschutz 16 Smart Watches, die insgesamt 70% des Angebotes abdecken, datenschutzrechtlich geprüft. Dabei wurde eine Reihe von nicht tolerierbaren Fehlern festgestellt.

- Die Gesundheitsdaten werden regelmäßig an den Anbieter und weitere Stellen weitergeleitet, ohne dass der Nutzer die Möglichkeit hat, dies zu verhindern.
- Eine Aufklärung über die Nutzung dieser Daten findet nicht in ausreichendem Maße statt. Die gesetzlich vorgeschriebene Aufklärung nach § 13 TMG findet nicht statt. So erfährt der Nutzer oftmals nicht, wer konkret Zugriff auf die Daten hat und wie lange sie gespeichert werden.
- Die einzelnen Informationen wie Körpergewicht, zurückgelegte Schritte, Herzfrequenz oder Dauer des Schlafes sind für sich betrachtet oft wenig aussagekräftig aber aufgrund der Fülle der über einen längeren Zeitraum erfassten Daten und der möglichen Verknüpfung mit Standortdaten entsteht jedoch ein erstaunlich präzises Bild über den Gesundheitszustand und über den Tagesablauf der Nutzer.

Im Rahmen ihrer Zuständigkeiten werden die Datenschutzaufsichtsbehörden nun an die Hersteller herantreten und diese auffordern, die Mängel zu beseitigen.

Wenn über geheime Patientendaten getratscht wird

ⓘ Quelle: http://www.sueddeutsche.de/bayern/klinikum-ingolstadt-wenn-ueber-geheime-patientendaten-getratscht-wird-1.3375020

Am Klinikum Ingolstadt reißt der Ärger nicht ab: Es geht um mutmaßlich schlechten Datenschutz und die Zahlung von „Schweigegeld" - diesmal im medizinischen Bereich.

Bereits im Jahr 2012 war eine Patientin, die an einer psychischen Erkrankung leidet, im Klinikum zur Behandlung. Nur ihr enges Umfeld wusste Bescheid und natürlich das Personal, das nach Ansicht der Patientin unter Schweigepflicht stehen müsste. Das sollte auch so bleiben. Nach ihrem Klinikaufenthalt habe ihre Schwiegermutter dann einen Anruf mit den geheimen Informationen erhalten - dem Verdacht der Patientin nach von einer eifersüchtigen Assistentin in der Klinik, die früher ein Verhältnis mit ihrem Gatten gehabt habe.
Der damalige Geschäftsführer habe die Sache geprüft und soll der Patientin daraufhin 5000 Euro angeboten haben. Eine Art Schweigegeld, glaubt die Betroffene. Ein Nachweis über die Zahlung des Klinikums im September 2014 liegt der Süddeutschen Zeitung vor. Sie habe - verunsichert - das Geld angenommen; nun will die Dame aber weiter vorgehen, weil sie regelmäßig auf ihre Krankheit angesprochen werde. Am Klinikum ist ein außergerichtliches Schreiben eingegangen - mit der Forderung nach Schadenersatz. Der Anwalt der Patientin rechtfertigt die Schadensersatzansprüche bis in sechsstelliger Höhe.

Nach SZ-Informationen wurde wegen eines ähnlichen Falls am Landgericht Ingolstadt Klage eingereicht. (...)

Impressum
FAC'T GmbH
Hohenzollernring 72
48145 Münster

info@factpartner.de
www.factpartner.de

Telefon 0251 935-3700
Telefax 0251 935-4075