Datenschutz newsbox

Ausgabe 8 2019

DATAKONTEXT

Editorial:

Es gibt Themen, die werden jedes Jahr auf das Neue diskutiert: Zum Beginn der Feiertage wettern Autofahrer darüber, dass ganz unabgesprochen und zufällig die Benzinpreise steigen.
Alle klagen über Dürre und Hitze, wenn es länger als drei Tage gutes Wetter gibt und über das miese Wetter, wenn es im Sommer auch mal regnet.

Weihnachten kommt jedes Jahr unerwartet und überraschend, so dass viele in Stress geraten, wenn sie durch überlaufene Einkaufshäuser hetzend, letzte Besorgungen machen müssen. Alle paar Jahre wird die Fußball National-Mannschaft zum Ärger Vieler nicht Weltmeister. Auch die Umstellung der Sommerzeit/Winterzeit sorgt jedes Jahr für Verdruss: Kurz, einige finden immer einen Anlass, um sich zu ärgern.

Vergleichbares lässt sich momentan rund um das Thema DS-GVO oder das Thema Datenschutz schlechthin beobachten. Saisonal bedingt und kurz vor Schulbeginn steht wieder einmal Thema "Zulässigkeit von Fotos" im Blickpunkt.

Mancherorts gibt es dieses Jahr keine Erinnerungs-Fotos an die Einschulung. Der Ärger ist groß, vermeintlich daran "schuld": Die DS-GVO und "der Datenschutz".

Wie bei allen Missverständnissen ist ein Mittel dagegen, das der Aufklärung. Dafür setzen sich dankenswerterweise Aufsichtsbehörden, aber auch Blogs unermüdlich ein.

Sollte es nicht gelingen diese und andere Datenschutz-Themen für die Bevölkerung verständlich und rechtssicher aufzubereiten, steht zu befürchten, dass Eltern und Großeltern auch die nächsten Jahre zur Einschulung über die DS-GVO schimpfen werden.

Ihr Levent Ferik

DATAKONTEXT

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

Datenschutz
newsbox

Hinweise zum Fotografieren bei Schulveranstaltungen

Mit Inkrafttreten der DS-GVO ist bei der Anfertigung und Veröffentlichung von Fotos und Videos, die auf Digitaltechnik basieren, der Anwendungsbereich der DS-GVO eröffnet. Die Anfertigung von Foto- und Videoaufnahmen stellt die Verarbeitung personenbezogener Daten im Sinne von Artikel 4 DS-GVO dar. Somit ist für die Anfertigung der Aufnahmen und die weitere Verarbeitung die DS-GVO einschlägig. Bei Veröffentlichung kommen die spezialgesetzlichen Regelungen des KUG zur Anwendung.

Der Landesbeauftragte für den Datenschutz Sachsen-Anhalt arbeitet in seiner aktuellen Orientierungshilfe die komplexe Rechtslage in Bezug auf das Fotografieren anlässlich von Schulveranstaltungen auf. Die DS-GVO stellt in datenschutzrechtlicher Hinsicht die europäischen Rahmenbedingungen. Weiter können Aspekte des Hausrechts, des Kunsturheberrechts oder des Zivilrechts eine Rolle spielen.

Nach Ansicht des Landesbeauftragten kann es infolge der persönlichen Betroffenheit der fotografierten Veranstaltungsgäste nach Abwägung der Interessen ein Anliegen der Schule sein, dem Fotografieren anlässlich von Schulveranstaltungen entgegenzuwirken.

Quelle: Der Landesbeauftragte für den Datenschutz Sachsen-Anhalt

Zulässigkeit von Weihnachtsgrüßen per E-Mail

Frage GDD-Erfa-Kreis Coburg:
Einmal im Jahr verschickt unsere Schwesterfirma an Weihnachten Weihnachtsgrüße per E-Mail. Hierbei handelt es sich um Interessenten aus Kaltakquisen, Stammkunden und gekauften Adressen. Ist dies ohne vorherige Einwilligung rechtlich zulässig?

Antwort des BayLDA:
Bei bestehenden Kontakt-/Kundenbeziehungen ("Bestandskunden") ist E-Mail- oder SMS-Werbung, Newsletter-Zusendung, usw. (weiterhin) zulässig, wenn die elektronischen Kontaktdaten im Zusammenhang mit den bisherigen Kontakten, einer Newsletter-Bestellung oder einer Vertragsabwicklung (Verkauf einer Ware oder Dienstleistung) erlangt worden sind, (nur) für eigene ähnliche Waren oder Dienstleistungen geworben oder hierzu informiert wird, dem bisher nicht widersprochen wurde und bei jeder Werbe-Mail bzw. -SMS klar und deutlich auf das Widerspruchsrecht hingewiesen wird. Siehe dazu die Regelung in § 7 Abs. 3 UWG.

Auch Weihnachtsgrüße sind nach unserer Auffassung wegen des in der Rechtsprechung weit ausgelegten Begriffs der Werbung nach diesen Maßstäben zu bewerten.
Werbe-E-Mails an gekaufte personenbezogene E-Mail-Adressen ("Kaltakquisen") sind wettbewerbsrechtlich und datenschutzrechtlich unzulässig.

Berliner Datenschutzbeauftragte verhängt hohe Bußgelder

Die Behörde der Berliner Beauftragten für Datenschutz und Informationsfreiheit hat bestätigt, dass sie jüngst zwei Bußgeldbescheide gegen ein Unternehmen in Höhe von insgesamt 200 000 Euro verhängt hat. Zudem befindet sie sich gerade in einem Verfahren, wonach es in absehbarer Zeit ein Bußgeld in bis zu zweistelliger Millionenhöhe wegen Verstößen gegen die Datenschutz-Grundverordnung (DS-GVO) geben soll.
Die Berliner Datenschutzbeauftragte Maja Smoltczyk will die bereits sanktionierte betroffene Firma nicht nennen. Diese kann noch gegen die Bußgeldbescheide Rechtsmittel einlegen. Gleiches gilt für das Unternehmen, dem ein sieben- oder gar achtstelliges Bußgeld droht. Öffentlich geworden sind die bereits verschickten Bescheide ebenso wie die weiteren bevorstehenden Sanktionierungen durch eine Mitteilung an den Haushaltsausschuss des Berliner Abgeordnetenhauses. Aus diesem Gremium gelangten die Nachrichten, die allesamt von der Berliner Landesbeauftragten bestätigt wurden.

Fragen zur DS-GVO an 50 Unternehmen

Die Landesbeauftragte für den Datenschutz Niedersachsen (LfD), Barbara Thiel, hatte ab Ende Juni eine Prüfung begonnen, wie gut sich die niedersächsischen Unternehmen bisher auf die seit dem 25. Mai geltende Datenschutzgrundverordnung (DS-GVO) eingestellt haben. In einer branchenübergreifenden Querschnittsprüfung schrieb Thiels Behörde in diesen Tagen 50 Unternehmen unterschiedlicher Größe an, die Fragen zu zehn Bereichen des Datenschutzes beantworten sollen. Die Prüfung steht nun kurz vor dem Abschluss. Als Hilfestellung für alle interessierten Unternehmen veröffentlicht die LfD schon jetzt ihren detaillierten Bewertungskatalog.
Um die geprüften Unternehmen einheitlich bewerten zu können, wurde zu den zehn Fragekomplexen ein Katalog mit circa 200 Einzelkriterien entwickelt. Mit der Veröffentlichung der Kriterien macht die LfD Niedersachsen transparent, was ein Verantwortlicher beachten muss, um die DS-GVO korrekt anzuwenden.

"Ich möchte mir zunächst einen Überblick darüber verschaffen, wie die Firmen die zweijährige Übergangszeit bis zur Geltung der DS-GVO genutzt haben", so Barbara Thiel in der Pressemitteilung Juni 2019. "Mein Hauptanliegen dabei ist es zu identifizieren, ob es bei den verantwortlichen Stellen noch Nachholbedarf gibt. Außerdem möchte ich mit dieser Prüfung das Bewusstsein für Datenschutz im Allgemeinen und die Vorschriften der DS-GVO im Speziellen stärken. Es geht zum jetzigen Zeitpunkt also nicht vorrangig darum, möglichst viele Fehler zu finden und Bußgelder zu verhängen. Stattdessen möchten wir aufklären, sensibilisieren und wertvolle Hinweise geben. Trotzdem kann es natürlich zu einem entsprechenden Verfahren kommen, wenn wir während der Prüfung Verstöße gegen die DS-GVO feststellen."
Der Kriterienkatalog zur Querschnittsprüfung als PDF-Download.

Quelle: Die Landesbeauftragte für den Datenschutz Niedersachsen

Handlungsempfehlung zum "Fashion-ID-Urteil" des EuGH

Der Europäische Gerichtshof (EuGH) hat in seinem Urteil vom 29. Juli 2019 in der Rechtssache C-40/17 Fashion ID GmbH & Co. KG gegen die Verbraucherzentrale NRW e.V., grundlegende Aussagen im Hinblick auf die Einbindung von Plugins von Drittanbietern in Websites getroffen.
Rechtsanwender sind dringend angehalten, die Feststellungen des EuGH auf die derzeitige Rechtslage anzuwenden und erforderlichenfalls kurzfristig Maßnahmen zu ergreifen, um bei dem Einsatz von Drittanbieter-Plugins auf ihren Websites keine sanktionsfähigen Verstöße gegen die DS-GVO zu begehen und so das Risiko von etwaigen Verbandsklagen und Abmahnungen zu minimieren.
Auf Grund des Zeitpunkts der Klageerhebung im Ausgangsverfahren setzt sich der EuGH in seinen Entscheidungsgründen zwar mit der bis zum 25. Mai 2018 geltenden Rechtslage auseinander. Allerdings finden sich die streitgegenständlichen Aspekte – wie bspw. Transparenzpflichten des Verantwortlichen – nahezu unverändert oder sogar verschärft in der DS-GVO wieder; zumal auch die ePrivacy-Richtlinie noch nicht durch die ePrivacy-Verordnung ersetzt wurde.

Die Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. hat hierzu Handlungsempfehlungen auf ihrer Webseite zur Verfügung gestellt:

https://www.gdd.de/aktuelles/startseite/eugh-urteil-mit-starker-breitenwirkung

EU-Kommission verklagt Griechenland und Spanien wegen fehlender Datenschutzgesetze

Die Europäische Kommission hat beschlossen, Griechenland und Spanien vor dem Gerichtshof der Europäischen Union (EuGH) zu verklagen, weil beide Länder es versäumt haben, die zur DS-GVO zugehörige JI-Richtlinie umzusetzen. Anders als die DS-GVO als unmittelbar geltende Verordnung musste die JI-Richtlinie in nationales Recht umgesetzt werden. Die Richtlinie war bis zum 6. Mai 2018 in nationales Recht umzusetzen.
Ziel der Richtlinie ist es, einen hohen Schutz der personenbezogenen Daten sicherzustellen und gleichzeitig den Austausch von personenbezogenen Daten zwischen den zuständigen Behörden auf der Grundlage strenger Datenschutzgarantien zu vereinfachen. Die Richtlinie enthält Bestimmungen über die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung. Damit soll gewährleistet werden, dass der Schutz der Daten von Opfern, Zeugen, Verdächtigen und Straftätern im Rahmen strafrechtlicher Ermittlungen ordnungsgemäß gewahrt wird. Darüber hinaus werden stärker harmonisierte Rechtsvorschriften die grenzübergreifende Zusammenarbeit von Polizei, Staatsanwaltschaft und Justiz im Interesse einer wirksameren Bekämpfung von Kriminalität und Terrorismus in Europa erleichtern. Diese EU-Vorschriften tragen damit zur Vollendung eines Raums der Freiheit, der Sicherheit und des Rechts bei. Durch die fehlende Umsetzung der Richtlinie ist der Datenschutz der betroffenen Personen in Spanien und Griechenland nicht vollumfänglich gewährleistet. Zudem wird der Datenaustausch zwischen den Mitgliedstaaten, die die Richtlinie umgesetzt haben, und Griechenland/ Spanien beeinträchtigt. Die Vertragsverletzungsverfahren gegen Griechenland und Spanien wurden bereits im Juli 2018 durch die Kommission eingeleitet. Der Kommission liegen bislang keine Mitteilungen über die Annahme der zur Umsetzung der Richtlinie erforderlichen Maßnahmen von Griechenland und Spanien vor.
Die Kommission fordert den EuGH auf, folgende finanzielle Sanktionen gegen Griechenland zu verhängen: ein Pauschalbetrag von 5287,50 € pro Tag zwischen dem Tag nach Ablauf der in der Richtlinie festgelegten Umsetzungsfrist und der Einhaltung der Vorschriften durch Griechenland bzw. dem Tag des Urteils, wobei der Pauschalbetrag insgesamt mindestens 1 310 000 € betragen sollte. Hinzu kommt ein tägliches Zwangsgeld in Höhe von 22 169,70 € ab dem Tag des ersten Urteils bis zur vollständigen Einhaltung der Vorschriften oder bis zum zweiten Urteil des Gerichtshofs. Für Spanien stellt sich ein ähnliches Bild dar: hier ist ein Pauschalbetrag von 21 321 € pro Tag zwischen dem Tag nach Ablauf der in der Richtlinie festgelegten Umsetzungsfrist und der Einhaltung der Vorschriften durch Spanien bzw. dem Tag des Urteils beantragt, wobei der Pauschalbetrag insgesamt mindestens 5 290 000 € betragen sollte. In Ergänzung dessen ist ein tägliches Zwangsgeld in Höhe von 89 548,20 € ab dem Tag des ersten Urteils bis zur vollständigen Einhaltung der Vorschriften oder bis zum zweiten Urteil des Gerichtshofs beantragt.

Praxishilfe zum Datenschutzbeauftragten nach der DS-GVO aktualisiert

Mit dem Inkrafttreten der Datenschutz-Grundverordnung (DS-GVO) existiert erstmals eine europaweit verbindliche verpflichtende Regelung zur Benennung betrieblicher und behördlicher Datenschutzbeauftragter. Während die EG-Datenschutzrichtlinie (95/46/EG) die Verpflichtung zur Benennung von Datenschutzbeauftragten lediglich als Alternative vorsah, um die Meldepflicht gegenüber der Datenschutzaufsichtsbehörde entfallen zu lassen, ergibt sich mit der Geltung der DS-GVO erstmals eine Benennungspflicht unmittelbar aus dem Europarecht.

Das deutsche Erfolgsmodell der datenschutzrechtlichen Selbstkontrolle hat sich damit auch auf europäischer Ebene durchgesetzt. In Ergänzung zur europarechtlichen (Basis-)Benennungspflicht berechtigt die DS-GVO außerdem über eine Öffnungsklausel die Mitgliedstaaten dazu, weitergehende Benennungspflichten auf nationaler Ebene vorzusehen. Von dieser Regelungsmöglichkeit hat der deutsche Gesetzgeber mit § 38 Bundesdatenschutzgesetz (BDSG) Gebrauch gemacht.

Neben den Regelungen über die Benennungspflicht enthält die DS-GVO Regelungen zur Rechtsstellung und zu den Aufgaben des Datenschutzbeauftragten, von denen der nationale Gesetzgeber nicht abweichen darf. Das vorliegende Papier gibt einen Überblick über die Regelungen zur Benennung von Datenschutzbeauftragten sowie deren Aufgaben und Stellung.

Die aktualisierte Praxishilfe der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. hat seine Praxishilfe zum Thema "Der Datenschutzbeauftragte nach der Datenschutz-Grundverordnung " nun aktualisiert. Die Praxishilfe berücksichtigt bereits jetzt die Fassung des § 38 Abs. 1 Satz 1 BDSG, aufgrund Beschlussfassung des Bundestages vom 27. Juni 2019 zum Zweiten Datenschutz-Anpassungs- und Umsetzungsgesetz EU (2. DSAnpUG-EU).
Die Regelung tritt am Tag nach der Verkündung im Bundesgesetzblatt in Kraft. Letztere setzt noch die Zustimmung des Bundesrats nach der Sommerpause sowie die Unterzeichnung und Freigabe durch den Bundespräsidenten voraus.
Nach § 38 Abs. 1 Satz 1 BDSG haben Verantwortliche und Auftragsverarbeiter nunmehr ergänzend zu den Vorgaben der DS-GVO einen Datenschutzbeauftragten zu bestellen, soweit sie in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen.

Näheres finden Sie im neuen Praxisleitfaden der GDD.

150.000 € Bußgeld wegen Datenverarbeitung auf falscher Rechtsgrundlage

Ein jüngst von der griechischen Datenschutz-Aufsichtsbehörde verhängtes Bußgeld richtet sich gegen die Fa. PricewaterhouseCoopers (Pwc). Das Bußgeld in Höhe von 150.000 verhängte die Aufsichtsbehörde nicht etwa weil der Verantwortliche für die relevante Datenverarbeitung keine zulässige Rechtsgrundlage angeben konnte, sondern weil sich die Datenverarbeitung nach Auffassung der Behörde auf eine "falsche" Rechtsgrundlage stützte.
Konkret ging es darum, dass PwC die relevante Verarbeitung personenbezogener Daten von Beschäftigten auf eine Einwilligung stützte, obwohl diese Rechtsgrundlage nicht einschlägig war. Damit verstieß PwC nach Ansicht der Aufsichtsbehörde gegen einen Grundsatz des Artikels 5 Abs. 1 lit a DS-GVO (Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz). Nach Artikel 5 Abs. 2 DS-GVO ist der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können ("Rechenschaftspflicht"), was PwC in diesem Falle nicht möglich war.

Quelle: European Data Protection Board

Neues EuGH-Urteil zur gemeinsamen Verantwortlichkeit

Der Europäische Gerichtshof (EuGH) in Luxemburg hat Ende Juli 2019 ein neues Urteil (C-40/17) zur Gemeinsamen Verantwortlichkeit erlassen. Ausgangspunkt war das Einbinden des "Gefällt mir"- Buttons von Facebook auf einer Internetseite eines deutschen Online-Händler für Modeartikel. Dies hatte zur Folge, dass beim Aufrufen der Website die personenbezogenen Daten dieses Besuchers an Facebook Ireland übermittelt werden. Offenbar erfolgte diese Übermittlung im Verborgenen, ohne dass sich der Besucher dessen bewusst ist und unabhängig davon, ob er Mitglied des sozialen Netzwerks Facebook ist oder den "Gefällt mir"-Button angeklickt hat.

Das mit dem Rechtsstreit im Ausgangsverfahren befasste Oberlandesgericht (OLG) Düsseldorf hat dem EuGH sechs Vorlagefragen vorgelegt. Damit verfolgte das Gericht die Auslegung einer Reihe von Bestimmungen der früheren EG-Datenschutzrichtlinie von 1995. Diese wurde durch die neue Datenschutz-Grundverordnung (DS-GVO) mit Wirkung vom 25. Mai 2018 ersetzt. Dennoch sind die Aussagen der EuGH-Rechtsprechung von Bedeutung, da sich die Gemeinsame Verantwortlichkeit auch in der DS-GVO in Art. 26 wiederfindet.

Die Entscheidung widmet sich nicht allein der Gemeinsamen Verantwortlichkeit. Nicht zu übersehen im EuGH-Urteil ist, dass es Verbänden zur Wahrung von Verbraucherinteressen ("Verbraucherschutzverbände") erlaubt ist, gegen den mutmaßlichen Verletzer von Datenschutzregeln Klage zu erheben. Der Gerichtshof weist darauf hin, dass die neue DS-GVO nunmehr ausdrücklich diese Möglichkeit vorsieht.

Mit der Einbindung des "Gefällt mir"-Buttons in eine Website scheint der Mode-Händler stillschweigend in das Erheben personenbezogener Daten seiner Webseiten-Besucher und deren Weitergabe eingewilligt zu haben. Deswegen kann die entsprechende Firma, Fashion ID, für die Vorgänge des Erhebens der in Rede stehenden Daten und deren Weiterleitung durch Übermittlung an Facebook Ireland als gemeinsam mit Facebook verantwortlich angesehen werden. Schließlich kann davon ausgegangen werden kann, dass Fashion ID und Facebook Irland gemeinsam über die Zwecke und Mittel entscheiden. Die Gemeinsame Verantwortlichkeit hat aber Grenzen. Fashion ID kann für alle Datenverarbeitungsvorgänge, die Facebook Ireland nach der Übermittlung der Daten vornimmt, nicht als mitverantwortlich angesehen werden kann. Es erscheint nach Auffassung des EuGH nämlich auf den ersten Blick ausgeschlossen, dass Fashion ID über die Zwecke und Mittel dieser Vorgänge entscheidet.

Konsequenzen einer Gemeinsamen Verantwortlichkeit

Neben der von Art. 26 DS-GVO verlangten transparenten Vereinbarungen hat der EuGH nun noch weitere Folgen einer Gemeinsamen Verantwortlichkeit definiert. Der Gerichtshof betont, dass der Betreiber einer Website wie Fashion ID für bestimmte Vorgänge wie das Erheben der Daten und deren Übermittlung an Facebook Ireland als (Mit)Verantwortlicher seinen Besuchern bestimmte Informationen zu geben hat, wie beispielsweise seine Identität und die Zwecke der Verarbeitung. Diese Informationen sind – genauso wie bei den Informationspflichten nach Art. 13 DS-GVO – "zum Zeitpunkt des Erhebens" bereitzustellen.

Datenschutz-Wegweiser für Bürgerinnen und Bürger

Datenschutz ist nicht nur Sache der Datenschutz-Aufsichtsbehörden. Jede Bürgerin und jeder Bürger ist gefordert, wenn es um die Sicherung des eigenen Freiheitsraums in einer zunehmend digitalisierten Welt geht. Das vom Bayerischen Landesbeauftragten für den Datenschutz herausgegebene Buch "Meine Daten, die Verwaltung und ich – Wegweiser durch die Welt der Datenschutz-Grundverordnung" soll das hierfür erforderliche Know-How vermitteln.
Der Datenschutz-Wegweiser für Bürgerinnen und Bürger ist kostenlos erhältlich. Eine PDF-Version steht auf der Internetpräsenz des Bayerischen Landesbeauftragten für den Datenschutz https://www.datenschutz-bayern.de in der Rubrik "Datenschutzreform 2018" zum Download bereit.

Der Datenschutz-Wegweiser für Bürgerinnen und Bürger führt zunächst in die wichtigsten Grundstrukturen und Begriffe des Datenschutzrechts ein. Im Zentrum stehen dann die Betroffenenrechte der Datenschutz-Grundverordnung. Dazu zählen unter anderem die Rechte auf Auskunft, Berichtigung und Löschung sowie das Widerspruchsrecht. Ein Blick auf die Datenschutzaufsicht und das Beschwerderecht zeigt, wie betroffene Personen ihre Datenschutzrechte verteidigen können.

Quelle: Der Bayerische Landesbeauftragte für den Datenschutz
Weiteres Know-How finden Sie auch in unseren DataAgenda Arbeitspapieren.

Unverschlüsselter Datenaustausch per E-Mail

Das BayLDA beantwortet eine Frage des GDD-Erfa-Kreises Coburg zum Thema unverschlüsselter Datenaustausch per E-Mail:
Im Rahmen der neuen Anforderungen der DS-GVO stellt sich die Frage, inwieweit ein Datenaustausch von personenbezogenen Daten per E-Mail mit z.B. Geschäftspartnern noch erfolgen kann. Aufgrund unterschiedlicher Verschlüsselungen kann ein verschlüsselter Versand nicht stets gewährleistet werden. Der aktuellen GDD-Praxishilfe DS-GVO XIII zur Einwilligung ist zu entnehmen, dass die betroffene Person stets die Wahl zwischen unverschlüsseltem und verschlüsseltem Versand/Postversand haben muss.
Muss ein verschlüsselter Versand bei jeder Art von Kommunikation (z.B. auch beim Austausch von Kontaktdaten) gewährleistet werden? Muss vorab die Einwilligung des Geschäftspartners eingeholt werden, wenn ein unverschlüsselter Versand erfolgt? Wäre es ausreichend, den Geschäftspartner über den unverschlüsselten Versand zu informieren und wenn dieser einen verschlüsselten Versand wünscht, dies beim Vertragspartner geltend zu machen? In welchem Umfang muss der Geschäftspartner informiert werden, dass ein unverschlüsselter Versand erfolgt? Wäre es ausreichend, diese Informationen in den Datenschutzhinweis nach Art. 13 DS-GVO aufzunehmen?

Antwort des BayLDA:
Da die E-Mail-Provider inzwischen regelmäßig Transportverschlüsselung für E-Mails einsetzen, können E-Mails mit "normalem" geschäftlichem Inhalt aus unserer Sicht ohne Ende-zu-Ende-Verschlüsselung (Inhaltsverschlüsselung) versandt werden. Nur bei sensiblen Daten (z. B. Gesundheitsdaten beim Arzt oder Krankenhaus) fordern wir eine Inhaltsverschlüsselung).
Ein "Abweichen" von gebotenen Datensicherheitsmaßnahmen per Einwilligung sehen wir allerdings als kritisch an.

Verschlüsselungstrojaner im Krankenhaus

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz nimmt einen aktuellen Sicherheitsvorfall im Krankenhaus zum Anlass, um darauf hinzuweisen, wie verwundbar Krankenhäuser mit der zunehmenden Digitalisierung ihrer Abläufe werden und welchen Risiken ihre IT-Strukturen und Behandlungsprozesse dabei ausgesetzt sind.
Eine Reihe von Einrichtungen der DRK Trägergesellschaft Südwest wurde jüngst Opfer eines Befalls mit Schadsoftware. Die durch diese erfolgte Verschlüsselung von Daten im IT-Verbund der Trägergesellschaft hatte zu weitreichenden Beeinträchtigungen des Krankenhausbetriebs geführt. Entsprechend der Verpflichtung aus Art. 33 der EU Datenschutz-Grundverordnung hat die Trägergesellschaft die Verletzung des Schutzes personenbezogener Daten dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit (LfDI) als zuständige Aufsichtsbehörde angezeigt.
"IT-Strukturen und Patientendaten müssen daher über eine ausreichende Widerstandsfähigkeit gegenüber Cyber-Attacken und einen angemessenen Schutz verfügen. Andernfalls drohen Schäden für die Gesundheit und den Datenschutz von Patientinnen und Patienten und wirtschaftliche Schäden", so der Landesbeauftragte für den Datenschutz und die Informationsfreiheit, Prof. Dr. Kugelmann.

Der LfDI Rheinlad-Pfalz weist darauf hin, dass auch Einrichtungen unterhalb der KRITIS-Schwelle geeignete Schutzmaßnahmen nach dem Stand der Technik vorsehen müssen, um personenbezogene Daten zu schützen.

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