Datenschutz
newsbox

Ausgabe
10
2018

DATAKONTEXT

Editorial

Seit Mai 2018 gilt die Europäische Datenschutz-Grundverordnung (DS-GVO). Die Berichterstattung in den Medien und das Rauschen in sozialen Netzwerken schüren unaufhörlich Panik vor den horrenden Geldbußen, den drakonischen Befugnissen der Aufsichtsbehörden, der perfiden Abmahnindustrie und den ausufernden Rechten der betroffenen Personen.

Da werden Schulzeugnisse plötzlich wieder von Hand geschrieben, Erinnerungsphotos geschwärzt und Kunstaktionen gestoppt. Selbst die EU-Kommission hat bereits die flächendeckende Verbreitung von Fehlinformationen in Bezug auf das neue europäische Datenschutzrecht kritisiert.

Die neueste Gruselmeldung betrifft die recht unverdächtig erscheinenden Klingelschilder am Eingang von Mietshäusern. Ein Mieter in Wien hatte sich darüber beschwert, dass ein Schild mit seinem Namen an der Gegensprechanlage angebracht war. Die Datenschutzbehörde in Österreich prüfte den Sachverhalt und verfügte, dass die Namen entfernt werden müssten. Prompt schwappt die Debatte auch nach Deutschland. Doch die Sorge ist unbegründet: Die DS-GVO gilt ausweislich ihres Artikels 2 Absatz 1 überhaupt nicht für Klingeltafeln. Mindestens aber ist die Anbringung im Rahmen berechtigter Interessenwahrnehmung gestattet. Die Aufsichtsbehörde ist im konkreten Fall schlicht über's Ziel hinausgeschossen.

Diese Ansicht vertritt nunmehr auch der Präsident des Bayerischen Landesamtes für Datenschutzaufsicht Thomas Kranig: "Ich finde es sehr problematisch und auch sehr schade, dass durch diese unsinnigen Behauptungen die sehr gute Datenschutz-Grundverordnung als Begründung für etwas herangezogen wird, was sie gar nicht fordert und sie damit als "weltfremdes europäisches Recht" diskreditiert wird."

Selbstverständlich dürfen Vermieter weiterhin die Namen der Mietparteien am Eingang anbringen. Genauso ist der namentliche Aufruf von Patienten im Wartezimmer gestattet, und wenn das Friseurstudio einen Termin reserviert, muss hierfür nicht extra Einwilligung eingeholt werden. Es gibt vielfältige interessante Fragestellungen im Datenschutzrecht, doch sollte die Energie auf die Lösung komplexer rechtlicher Probleme verwendet werden.

Zu Risiken und Nebenwirkungen fragen Sie Ihren Datenschutzbeauftragten oder die GDD-Geschäftsstelle. Die GDD tritt als gemeinnütziger Verein für einen sinnvollen, vertretbaren und technisch realisierbaren Datenschutz ein. Sie hat zum Ziel, die Daten verarbeitenden Stellen – insbesondere auch die Datenschutzbeauftragten - bei der Lösung und Umsetzung der vielfältigen mit Datenschutz und Datensicherheit verbundenen rechtlichen, technischen und organisatorischen Anforderungen zu unterstützen.

Ihre GDD e.V.

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

GDD-Ratgeber zum betrieblichen DSB nach DS-GVO und BDSG

Das GDD-Institut für Datenschutzbeauftragte befasst sich kontinuierlich mit Aufgaben und Rechtsstellung von Datenschutzbeauftragten sowie der Entwicklung von Standards zur Aus- und Weiterbildung von Datenschutzverantwortlichen. In jüngerer Zeit lag ein Schwerpunkt der Arbeit des Instituts darin, die DS-GVO-Regelungen zur/zum Datenschutzbeauftragten (Art. 37 ff. DS-GVO) zu analysieren und relevante Unterschiede zu den Be-stimmungen im BDSG 2018 zu ermitteln. Ebenso bedurfte es einer Interpretation der Regelung in § 38 BDSG 2018 und ihres Zusammenspiels mit den DS-GVO-Bestimmungen. Besondere Aufmerksamkeit galt dabei der Auseinandersetzung mit der zwischenzeitlich erschienenen zahlreichen Kommentarliteratur sowie der Analyse der "Leitlinien in Bezug auf Datenschutzbeauftragte ("DSB")" (WP 243 rev.01), die von der Art. 29-Datenschutzgruppe beschlossen und später vom Europäischen Datenschutzausschuss bestätigt wurden.
Die Ergebnisse der Tätigkeit sind eingeflossen in die Überarbeitung des GDD-Ratgebers zum/zur betrieblichen Datenschutzbeauftragten. Der bewährte Ratgeber beleuchtet detailliert, unter welchen Voraussetzungen ein/e Datenschutzbeauftragte/r zu benennen ist und welche Aufgaben und welche Rechtsstellung diesem dieser zukommen.

Der Ratgeber greift im Einzelnen u.a. folgende Themen auf:

- Rechtsgrundlagen in der DS-GVO und im BDSG 2018 zum/zur Datenschutzbeauftragten
- Die Benennung eines/einer Datenschutzbeauftragten
- Kriterien für das Eingreifen der Pflicht zur Benennung
- Anforderungen an die Benennung
- Veröffentlichung/Mitteilung der Kontaktdaten des/der Datenschutzbeauftragten
- Möglichkeit der Benennung eines/einer externen Datenschutzbeauftragten
- Exkurs: Rechtsanwälte als Datenschutzbeauftragte
- Möglichkeit der Benennung eines/einer gemeinsamen Datenschutzbeauftragten
- Fortgeltung von Altbestellungen
- Anforderungen an den/die Datenschutzbeauftragte/n
- Berufliche Qualifikation, insbes. Fachwissen
- Fähigkeit zur Aufgabenerfüllung, insbes. keine Interessenkonflikte
- Aufgaben des/der Datenschutzbeauftragten

Die gesamte Inhaltsangabe können Sie hier einsehen:
https://www.rdv-online.com/news/gdd-ratgeber-zum-betrieblichen-dsb-nach-ds-gvo-und-bdsg
Abgerundet werden die Ausführungen durch praxisrelevante Muster und Materialien. So enthält der Ratgeber ein Musterschreiben zur Benennung des/der Datenschutzbeauftragten so-wie eine dieses Schreiben ergänzen-de umfassende Stellenbeschreibung für Datenschutzbeauftragte.
Der Materialienteil des Ratgebers gibt schließlich ausgewählte Papiere der nationalen und europäischen Aufsichtsbehörden zum/zur Datenschutzbeauftragten wieder, nämlich das Kurzpapier Nr. 12 der Datenschutzkonferenz und das bereits er-wähnte WP 243 rev.01.
>> Hinweis: Der Ratgeber steht GDD-Mitgliedern ab Mitte November als Download im Mitgliederservice-Bereich zur Verfügung.

Quelle: Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V.

Mustervertrag zur Auftragsverarbeitung im Gesundheitswesen

Die Europäische Datenschutz-Grundverordnung (DS-GVO) regelt die Anforderungen hinsichtlich der vertraglichen Gestaltung von Verträgen zur Auftragsverarbeitung. Um den Umgang mit diesen Anforderungen zu erleichtern, überarbeitete eine gemeinsame Arbeitsgruppe der Verbände Berufsverband der Datenschutzbeauftragten Deutschlands e. V. (Arbeitskreis Medizin), Bundesverband Gesundheits-IT e. V. (Arbeitsgruppe Datenschutz & IT-Sicherheit), Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V. (Arbeitsgruppe "Datenschutz und IT-Sicherheit im Gesundheitswesen"), Deutsche Krankenhausgesellschaft e. V., Gesellschaft für Datenschutz und Datensicherheit e. V. (Arbeitskreis "Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen") den bisherigen Muster-Vertrag zur Auftragsverarbeitung für das Gesundheitswesen.
Die Überarbeitung ist nunmehr abgeschlossen, der Muster-Vertrag zur Auftragsverarbeitung steht zur freien Verfügung unter einer Creative Commons (CC) Lizenz, genauer unter der CC BY (Namensnennung 4.0 International).

Quelle: Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie (GMDS) e.V.

Kundenzufriedenheitsbefragung ohne Einwilligung

Der BGH hat in seinem Urteil vom 10.07.2018 (Az.: VI ZR 225/17) entschieden, dass die Verwendung von elektronischer Post für die Zwecke der Werbung ohne Einwilligung des Empfängers grundsätzlich einen Eingriff in seine geschützte Privatsphäre und damit in sein allgemeines Persönlichkeitsrecht darstellt.
Dabei falle eine Kundenzufriedenheitsbefragung in einer E-Mail auch dann unter den Begriff der (Direkt-) Werbung, wenn mit der E-Mail die Übersendung einer Rechnung für ein zuvor gekauftes Produkt erfolge. Dem Verwender einer E-Mail-Adresse zu Werbezwecken nach Abschluss einer Verkaufstransaktion sei es zumutbar, bevor er auf diese Art mit Werbung in die Privatsphäre des Empfängers eindringe, diesem - wie es die Vorschrift des § 7 Abs. 3 UWG verlange - die Möglichkeit zu geben, der Verwendung seiner E-Mail-Adresse zum Zwecke der Werbung zu widersprechen. Ansonsten sei der Eingriff grundsätzlich rechtswidrig.
Der Entscheidung lag folgender Sachverhalt zugrunde: Der Kläger nahm die Beklagte, bei der er über die Internet-Plattform "Amazon Marketplace" Waren bestellt hatte, auf Unterlassung der Zusendung von E-Mails in Anspruch, in denen der Dank für den Kauf eines Gegenstandes mit der Bitte verknüpft wurde, an einer Kundenzufriedenheitsumfrage teilzunehmen. Der Kläger bestellte am 9. Mai 2016 bei der Beklagten ein Ultraschallgerät zur Schädlingsvertreibung, wobei die Abwicklung nicht direkt zwischen den Parteien, sondern über Amazon erfolgte. Eine Rechnung erhielt er zunächst nicht. Am 24. Mai 2016 erhielt er diese von der Beklagten durch eine E-Mail mit dem Betreff "Ihre Rechnung zu Ihrer Amazon Bestellung ... " und folgendem Inhalt:

"Sehr geehrte Damen und Herren, anbei erhalten Sie Ihre Rechnung im PDF-Format. Vielen Dank, dass Sie den Artikel bei uns gekauft haben. Wir sind ein junges Unternehmen und deshalb auf gute Bewertungen angewiesen. Deshalb bitten wir Sie darum, wenn Sie mit unserem Service zufrieden waren, uns für Ihren Einkauf eine 5-Sterne Beurteilung zu geben. Sollte es an dem gelieferten Artikel oder unserem Service etwas auszusetzen geben, würden wir Sie herzlich darum bitten, uns zu kontaktieren. Dann können wir uns des Problems annehmen. Zur Bewertung: über folgenden Link einfach einloggen und eine positive 5-Sterne Beurteilung abgeben (…)".

Der Kläger sah in der E-Mail eine unaufgeforderte unerlaubte Zusendung von Werbung, die in sein allgemeines Persönlichkeitsrecht eingreife. Das Amtsgericht wies die Klage ab. Die hiergegen gerichtete Berufung hat das Berufungsgericht zurückgewiesen. Mit der vom Berufungsgericht zugelassenen Revision verfolgt der Kläger sein Klagebegehren weiter.

Quelle: Bundesgerichtshof

Blacklists für Datenschutz-Folgeabschätzungen

Wie der Europäische Datenschutz-Ausschuss, EDPB, (European Data Protection Board) bekanntgab, wurde bei der letzten Sitzung eine Einigung bzgl. der 22 Stellungnahmen erzielt, die die einzelnen Länder zum Thema erarbeitet hatten. Die Stellungnahme beschäftigten sich mit der Festlegung gemeinsamer Kriterien für die Erarbeitung von Blacklist für die Datenschutz-Folgenabschätzung (DSFA) nach Art. 35 DS-GVO.
Um die Arten der Verarbeitungstätigkeiten festzulegen, die eine DPIA erfordern könnten, fordert die DS-GVO die nationalen Aufsichtsbehörden auf, Listen der Arten von Verarbeitungstätigkeiten zu erstellen und zu veröffentlichen, die ein hohes Risiko mit sich bringen können. Der Europäische Datenschutz-Ausschuss hat 22 nationale Listen mit insgesamt 260 verschiedenen Verarbeitungstätigkeiten erhalten. Die Vorsitzende der EDPB, Andrea Jelinek, sagte: "Es war eine enorme Aufgabe alle diese Listen zu prüfen und gemeinsame Kriterien dafür festzulegen, was eine DSFA auslöst und was nicht. Es war eine ausgezeichnete Gelegenheit für den Europäischen Datenschutz-Ausschuss die Konsistenz der erarbeiteten Kriterienkataloge, die eine DSFA auslösen können, einem Praxistest zu unterziehen. Die DS-GVO erfordert keine vollständige Harmonisierung oder eine "EU-Liste", sondern vielmehr eine Kohärenz, die wir in diesen 22 Stellungnahmen erreicht haben, indem wir uns auf eine gemeinsame Sichtweise geeinigt haben."
Die 22 Meinungen zu den DPIA-Listen ergeben sich aus Art. 35 Abs. 4 und Art. 35 Abs. 6 DS-GVO und stehen im Einklang mit früheren Leitlinien der Artikel-29-Arbeitsgruppe.

Quelle: European Data Protection Board

Auskunftsbegehren innerhalb des Konzerns

Frage des GDD Erfa-Kreises Würzburg:

Wenn ein Betroffener Auskunft bei einer Firma verlangt und diese zu einem Konzern gehört, ist dann die jeweilige rechtlich selbständige Einheit verpflichtet, den Betroffenen hinzuweisen, dass möglicherweise seine Daten auch bei anderen rechtlichen Einheiten der Gruppe gespeichert sein könnten. Es werden zwar keine Daten weitergegeben (es können also keine Empfänger genannt werden) in der Praxis ist aber wohl den Betroffenen oft nicht ganz klar, dass es mehrere rechtlich Einheiten gibt. Die Betroffenen googeln meist nach der Zentrale und richten ihre Auskunft an den dort benannten Mutterkonzern. Auf der einen Seite sind die Betroffenenrechte durch die EU-DS-GVO gestärkt, d. h. aufgrund des "überlegenen Wissens" könnte eine Informationspflicht bestehen, andererseits müssten die betroffenen Personen gerade aufgrund der umfassenden Transparenzpflichten in der Lage sein, ein "qualifiziertes Auskunfts-verlangen" zu formulieren.

Antwort des BayLDA:

Die Auskunftspflicht nach Art. 15 DS-GVO betrifft zunächst nur den Verantwortlichen im Sinne von Art. 4 Nr. 7 DS-GVO, also die angegangene Firma als juristische Person. Ausnahmen sind bei einer gemeinsamen Verantwortlichkeit nach Art. 4 Nr. 19 und Art. 26 DS-GVO gegeben. Allerdings soll der Verantwortliche der betroffenen Person nach Art. 12 Abs. 2 Satz 1 DS-GVO die Ausübung ihrer Rechte gemäß den Art. 15 bis 22 erleichtern, woraus auch hergeleitet werden kann, dass der Verantwortliche sein "überlegenes Wissen" über die Datenverarbeitung in dem Konzern der anfragenden betroffenen Person insoweit zukommen lassen muss, damit diese ihr Auskunftsrecht gegenüber Konzernunternehmen sach- und zielgerecht ausüben kann. Eine andere Verhaltensweise könnte als Verstoß gegen Treu und Glauben nach Art. 5 Abs. 1 lit. a DS-GVO bzw. unfaire Verfahrensweise im Sinne von Nr. 60 ErwGr. DS-GVO gewertet werden.

Leitfaden macht DS-GVO für Vereine überschaubarer

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern und die Stiftung für Ehrenamt und bürgerschaftliches Engagement in Mecklenburg-Vorpommern haben in Zusammenarbeit einen Leitfaden "Datenschutz – Orientierungshilfe für Vereine in Mecklenburg-Vorpommern" veröffentlicht.
Der Text dieses Leitfadens basiert zu großen Teilen auf der Orientierungshilfe "Datenschutz im Verein nach der Datenschutzgrundverordnung (DS-GVO)" und dem "Praxisratgeber Datenschutz im Verein nach der DS-GVO" des Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg. Erklärtes Ziel des Leitfadens ist es die seit Wirksam Werden der DS-GVO entstandene Verunsicherung, insbesondere bei kleinen Vereinen zu reduzieren. Der Leitfaden soll Hilfestellung bieten bei den Fragen, welche Neuerungen anstehen bzw. welche Neuerungen an sie gestellt werden. Darüber hinaus bietet der Leitfaden aber auch eine Anleitung wie die Anforderungen konkret umgesetzt werden können. Muster und Checklisten runden den Leitfaden ab.
Der Leitfaden ist in zwei Teile untergliedert. Im ersten Teil: "DS-GVO light" gibt es einen Praxisratgeber für die schnelle Orientierung mit häufig gestellten Fragen, einer Checkliste sowie Mustern und Formulierungshilfen. Der zweite Teil "DS-GVO Vertiefung" enthält eine ausführliche Orientierungshilfe zu Einzelfragen.
Der Leitfaden steht ab heute auf den Homepages des Landesdatenschutzes und der Ehrenamtsstiftung zum kostenlosen Download zur Verfügung. Mit Unterstützung des Landtages wird die Orientierungshilfe demnächst auch in gedruckter Form zur Verfügung stehen.

Quelle: Stiftung für Ehrenamt und bürgerschaftliches Engagement in Mecklenburg-Vorpommern & Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern

Fax von der "Datenschutz-Auskunftszentrale"

Vermehrt berichten Betroffene und Verantwortliche ein Fax von einer sog. "Datenschutz-Auskunftszentrale" erhalten zu haben. Diese suggeriert, dass das beigefügte Formular unbedingt bis zum 9. Oktober ausgefüllt werden müsse (hier dürften die meisten bereits reflexartig an die mit den DS-GVO oftmals in Verbindung gebrachten Geldbußen denken..).
Das ausgefüllte Formular solle bis zum 9. Oktober "gebührenfrei" zurückgefaxt werden. Mag das Fax auch gebührenfrei sein, so wird dem Leser erst beim Studium des Kleingedruckten klar, dass er für Unterlagen und Infomaterial rund um die DS-GVO 498 EUR (Netto) zahlen soll. Durch die Unterzeichnung werde die Leistung für drei Jahre verbindlich bestellt. Dafür erhalte der Besteller das Leistungspaket Basisdatenschutz, welches Informationsmaterial, ausgefüllte Muster, Formulare und Anleitungen zur Umsetzung der Vorgaben der DS-GVO enthalte.
Es sei darauf hingewiesen, dass viele Informationen zur Umsetzung der DS-GVO frei verfügbar zum Download bereitstehen. Diese können bei den Aufsichtsbehörden und diversen anderen Institutionen und Verbänden abgerufen werden. Mehr Infos zum Thema:

Quelle: Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Schleppende Umsetzung der DS-GVO

Nach einer aktuellen Studie des Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) hat erst ein Viertel (24 Prozent) der befragten 500 Unternehmen in Deutschland die DS-GVO vollständig umgesetzt. Weitere 40 Prozent geben an, die Regeln größtenteils umgesetzt zu haben, drei von zehn (30 Prozent) teilweise. 5 Prozent der befragten Unternehmen gaben an gerade erst mit den Anpassungen begonnen zu haben.
Die große Mehrheit der Unternehmen beklagt höhere Aufwände durch die DS-GVO im laufenden Betrieb. Acht von zehn Unternehmen (78 Prozent) geben an, höhere Aufwände durch die DS-GVO im laufen Betrieb zu haben. Nur jedes fünfte befragte Unternehmen (19 Prozent) rechnet mit gleichbleibendem Aufwand im laufenden Betrieb, vier Monate zuvor waren es noch 34 Prozent. Die Unternehmen nannten die erweiterten Dokumentations- und Informationsplichten, die die DS-GVO mit sich bringt, am häufigsten, wenn es darum ging, was die größten Aufwände generiert. So hat für 96 Prozent der Aufwand für die Erfüllung der Dokumentationspflichten zugenommen, 87 Prozent bestätigen dies für die Erfüllung der Informationspflichten. Acht von zehn (78 Prozent) geben an Mühe damit zu haben, das eigene Personal zu den neuen Datenschutzregeln zu schulen.

Quelle: BITKOM

Dokumentation von telefonisch eingeholten Opt-Ins

Frage des GDD Erfa-Kreises Würzburg:

Wie müssen telefonisch eingeholte Opt-Ins nach Ansicht der Aufsichtsbehörde dokumentiert werden (Dokumentations- und Rechenschaftspflichten)? Muss der Agent jeweils eine Tonbandaufnahme der Einwilligungserklärung des Betroffenen fertigen und (z. B. bis zum Widerspruch) aufbewahren oder wäre es hier – auch im Sinne der Datensparsamkeit und zur leichteren Abwicklung von Betroffenenansprüchen – ausreichend, wenn der Agent im CallCenter nach umfassender Aufklärung selbst ein Kreuz im Protokoll (mit Datumsangabe) an entsprechender Stelle setzt.

Antwort des BayLDA:

Für uns als Aufsichtsbehörde würde die Variante 2, Ankreuzen im Protokoll mit Datumsangabe und Namenszeichen, für den Regelfall als Beleg eines opt-in genügen, es sei denn, diese Regelvermutung wird durch schlüssig dargelegte Beschwerden betroffener Personen bei uns über fingierte Einwilligungen erschüttert. Wie Gerichte in dortigen Verfahren die Beweissituation bewerten, können wir nicht beurteilen.

BSI-Bericht 2018: Die Lage der IT-Sicherheit in Deutschland

Mit dem Lagebericht zur IT-Sicherheit 2018 legt das Bundesamt für Sicherheit in der Informationstechnik (BSI) als nationale Cyber-Sicherheitsbehörde einen umfassenden und fundierten Überblick über die Bedrohungen Deutschlands, seiner Bürgerinnen und Bürger und seiner Wirtschaft im Cyber-Raum vor. Zudem werden Gegenmaßnahmen des BSI und die gemeinsam mit Partnern gefundenen Lösungsansätze für die Akteure in Staat, Wirtschaft und Gesellschaft dargestellt.
Nach Einschätzung des BSI ist die Gefährdungslage weiterhin hoch. Im Vergleich zum vorangegangen Berichtszeitraum hat sie sich weiter verschärft und ist zudem vielschichtiger geworden. Es gibt nach wie vor eine hohe Dynamik der Angreifer bei der Weiterentwicklung von Schadprogrammen und Angriffswegen. Darüber hinaus gibt es z. B. mit den entdeckten Schwachstellen in Hardware eine neue Qualität der Bedrohung, wie bei den Sicherheitslücken Spectre/Meltdown und Spectre NG, die ohne einen Austausch der Hardware nicht vollständig geschlossen werden können.
In diesem Bericht wird die Gefährdungslage der IT-Sicherheit in Deutschland im Zeitraum 1. Juli 2017 bis 31.Mai 2018 beschrieben. Das Kapitel "Gefährdungslage" ist gegliedert in die Bereiche Bundesverwaltung, Kritische Infrastrukturen/Wirtschaft und Gesellschaft. Zudem wird auf Angriffsmethoden und Angriffsmittel der Angreifer sowie auf Rahmenbedingungen und Ursachen eingegangen. Anhand zahlreicher Beispiele wird erläutert, wie durch Angriffe auf die IT-Sicherheit das Leben in einer digitalisierten Gesellschaft beeinträchtigt werden kann.
Im zweiten Kapitel beschäftigt werden unter Bezug auf die aktuelle Gefährdungslage der IT-Sicherheit anhand ausgewählter Themen Lösungsansätze und Angebote des BSI dargestellt – gegliedert nach den drei Aufgabenbereichen Staat/Verwaltung, Wirtschaft/Kritische Infrastrukturen und Gesellschaft/Bürger. Um diese Angebote praktisch nutzbar zu machen, wird über Links auf zahlreiche Publikationen und Internetangebote des BSI verwiesen.

Quelle: Bundesamt für Sicherheit in der Informationstechnik

Bußgeld gegenüber Mitarbeitern nach der DS-GVO

Frage des GDD Erfa-Kreises Würzburg:
Die Verpflichtung auf das Datengeheimnis ist zwar nicht explizit in der EU-DS-GVO genannt und im BDSG-neu nur für Behörden, allerdings sollen die Unternehmen aus eigenen Interesse ja weiterhin die Mitarbeiter darauf verpflichten. Bei dem Muster nach dem BDSG wurden die Bußgeld-Paragraphen immer angehängt. Da die EU-DS-GVO aber keine Bußgelder ggü. den Mitarbeitern enthält, fragen wir uns, ob wir diese dann komplett weglassen oder die vom BDSG-neu heranziehen? Was empfehlen Sie?

Antwort des BayLDA
Zur Erläuterungen für eine Verpflichtung von Beschäftigten unter Geltung der DS-GVO verweisen wir auf unser Info-Blatt "Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach der DS-GVO" unter https://www.lda.bayern.de/media/info_verpflichtung_beschaeftigte_dsgvo.pdf
Dass Geldbußen nach der DS-GVO nur gegen Unternehmen verhängt werden können, sehen wir nicht so. Nr. 150 ErwGr. Der DS-GVO führt im Satz 4 wie folgt aus: "Werden Geldbußen Personen auferlegt, bei denen es sich nicht um Unternehmen handelt, so sollte die Aufsichtsbehörde bei der Erwägung des angemessenen Betrags für die Geldbuße dem allgemeinen Einkommensniveau in dem betreffenden Mitgliedstaat und der wirtschaftlichen Lage der Personen Rechnung tragen.

Hilfe bei DDoS-Attacken

Wenn die Unternehmens-Webseite nicht mehr erreichbar ist, interne Netzwerkdienste ausfallen oder kritische Geschäftsprozesse wegen Überlastung blockiert werden, ist oftmals ein sogenannter DDoS-Angriff die Ursache. Diese Distributed-Denial-of-Service-Angriffe werden von Cyber-Kriminellen genutzt, um ihre Opfer zu erpressen oder um gezielt Schaden anzurichten. Ein prominentes Beispiel unter vielen ist der Angriff auf den Internet-Infrastruktur-Dienstleister Dyn, der 2016 zum Ausfall von Online-Diensten wie Twitter, Netflix oder PayPal führte. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat nun eine Reihe qualifizierter DDoS-Mitigation-Dienstleisteridentifiziert, die Unternehmen und Organisationen Schutz vor solchen Cyber-Angriffen bieten können.

Basierend auf den ebenfalls veröffentlichten Auswahlkriterien für qualifizierte Dienstleister wurde ein wettbewerbsneutrales Verfahren entwickelt, durch das erste geeignete DDoS-Mitigation-Dienstleister identifiziert werden konnten. Anhand der nun veröffentlichten Liste geeigneter Dienstleister und der transparenten Gestaltung der Auswahlkriterien, werden Unternehmen in die Lage versetzt, geeignete Hilfe durch externe Experten anzufordern. Weiteren Interessenten steht das Verfahren jederzeit offen.
Ein vergleichbares Verfahren für APT-Response-Dienstleister wird derzeit im BSI umgesetzt.
Weitere Informationen finden sich auf der Webseite des BSI.