Datenschutz newsbox

Ausgabe 03 2020

DATAKONTEXT

Editorial:

Ginge es darum, einem etwaigen Corona-Quarantäne-Koller dadurch entgehen zu wollen, in dem man den einzelnen Funktionen in einem Unternehmen, Figuren aus der griechischen Mythologie zuschreibt, ist es nicht unwahrscheinlich, dass der Vergleich „Kassandra" = Datenschutzbeauftragter fällt.

Kassandra erhielt danach vom Gott Apollon, aufgrund ihrer Schönheit, die Gabe der Weissagung. Als Apollon jedoch einen Korb von Kassandra bekam, wusste er sich in seiner toxischen Männlichkeit nicht anders zu behelfen, als sie und ihre Nachkommenschaft zu verfluchen, auf, dass niemand ihren Weissagungen Glauben schenken werde. Kassandra gilt in der antiken Mythologie daher als tragische Heldin, die immer das Unheil voraussah, aber niemals Gehör fand. Nachvollziehbar, dass deshalb ungehörte Warnungen als Kassandrarufe bezeichnet werden. Je nach dem welches Standing ein Datenschutzbeauftragter in einem Unternehmen genießt, können die Warnungen des DSB, die Teil seines Beratungs- und Überwachungsauftrags sind, als Kassandrarufe verhallen oder aber Gehör finden.

Gerade in Zeiten wie diesen, wenn die Bereitschaft groß ist, den Datenschutz und den Schutz der Persönlichkeitsrechte allzu vorschnell für vermeintlich höhere Güter aufzugeben. Es mag sein, dass Bewegungsdaten von Smartphone-Nutzern in einigen Ländern bereits im Kampf gegen die Bedrohung durch Corona eingesetzt werden. Zum Job von Datenschützern gehört es aber selbstverständlich, auch oder gerade in Situationen wie diesem, zu hinterfragen, ob beabsichtigte Datenverarbeitungen rechtmäßig sind. Es wäre bigott zu Schönwetterzeiten Staaten wie China wegen eines Datenschutzniveaus, das nicht europäischen Standards entspricht, zu kritisieren, aber es Ihnen gleich tun zu wollen, wenn die Lage nicht so sonnig ist. Es gilt, technische Innovationen mit den Datenschutz-Anforderungen in Einklang zu bringen, die wir uns als Europäer zum Maßstab gesetzt haben. Die Pauschalisierung, dass der Schutz vor Corona wichtiger ist als Datenschutz, kann diesem selbst auferlegten Standard nicht gerecht werden.

Die Aufsichtsbehörden und die Datenschutz-Community haben schnell und pragmatisch auf die datenschutzrechtliche Situation reagiert, die insbesondere im Bereich des Beschäftigtendatenschutzes durch Corona entstanden ist. Es liegt an den einzelnen Verantwortlichen und Beteiligten, die pragmatischen und sinnvollen Handlungsleitfäden umzusetzen, und wo nötig Nachbesserungen zu fordern, findet

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

Handreichung zum Stand der Technik

Sowohl das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“ (IT-Sicherheitsgesetz bzw. ITSiG) als auch die europäische Datenschutz-Grundverordnung (DS-GVO) erwähnen den Begriff des Stands der Technik als eine Forderung, an der sich die IT-Sicherheit orientieren soll.
Im Bereich des technischen Datenschutzes fordert die DS-GVO in Art. 32 DS-GVO zum Schutze der Rechte und Freiheiten natürlicher Personen technische und organisatorische Maßnahmen zu treffen, die zum einen risikoorientiert erfolgen sollen und zum anderen den „Stand der Technik“ berücksichtigen sollen. Hierzu haben Verantwortliche und Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen zu treffen.

Wie auch das ITSiG, sieht die DS-GVO jedoch keine Definition für das Tatbestandsmerkmal des Standes der Technik vor. Gleiches gilt ebenfalls für das Datenschutz-Anpassungs- und -Umsetzungsgesetz EU (DSAnpUG-EU) sowie die daraus resultierende Neufassung des BDSG (BDSG-neu).

Auch in Bezug auf Entwicklung, Gestaltung, Auswahl und Nutzung von Anwendungen, Diensten und Produkten, die entweder auf der Verarbeitung von personenbezogenen Daten beruhen oder zur Erfüllung ihrer Aufgaben personenbezogene Daten verarbeiten (Art. 25 DS-GVO), sollen die Hersteller von Produkte, Diensten und Anwendungen ermutigt werden, das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik sicherzustellen, dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen.
Das vom TeleTrusT – Bundesverband IT-Sicherheit e.V. veröffentlichte Dokument zum „Stand der Technik“ in der IT Security gibt vor diesem Hintergrund konkrete Hinweise und Handlungsempfehlungen. Die Handreichung soll Unternehmen, Anbietern und Dienstleistern Hilfestellung zur Bestimmung des Standes der Technik in der IT-Sicherheit geben und kann als Referenz z.B. für vertragliche Vereinbarungen, Vergabeverfahren bzw. für die Einordnung implementierter Sicherheitsmaßnahmen dienen. Durch die nun veröffentlichte englische Fassung des Dokumentes sollen Unternehmen in allen europäischen Ländern bei der Bestimmung des geforderten Sicherheitsstands in der IT-Sicherheit unterstützt werden.

Quelle: Bundesverband IT-Sicherheit e.V. (TeleTrusT)

LDI NRW aktualisiert FAQs zum Thema Inkasso und Datenschutz

Bereits am 23.03.2018 gab es einen Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) zur Einmeldung offener und unbestrittener Forderungen in eine Wirtschaftsauskunftei (Inkassounternehmen) unter Geltung der DS-GVO.
Die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW) hat unter der ständig aktualisierten Rubrik „Die Landesbeauftragte antwortet auf häufig gestellte Fragen" eine neue Broschüre zu diesem Themengebiet veröffentlicht.
„Seit Anwendungsbeginn der Datenschutz-Grundverordnung erreichen uns vermehrt Anfragen von Bürgerinnen und Bürgern, die durch ein Inkassounternehmen zum Ausgleich einer – häufig auch nur vermeintlich – offenen Forderung aufgefordert wurden", so die LfDI NRW.
Diese Broschüre, die einen Überblick über die häufig gestellten Fragen und die Antworten der Aufsichtsbehörde gibt, ist nun aktualisiert worden.
In der aktualisierten Broschüre antwortet die Landesbeauftragte auch auf Fragen zur Beitreibung im Ausland begangener Straßenverkehrsverstöße.

Quelle: Die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen

Musterlösungen zur Umsetzung der DS-GVO im Praxisalltag

Aus einer Kooperation des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz und der Kassenärztlichen Vereinigung Rheinland-Pfalz ist die Initiative „Mit Sicherheit gut behandelt" entstanden. Mittlerweile sind auch die Landesärztekammer Rheinland-Pfalz und die Landespsychotherapeutenkammer Rheinland-Pfalz der Initiative beigetreten.
Die Initiative stellt auf ihrer Homepage www.mit-sicherheit-gut-behandelt.de verschiedene Muster zur Umsetzung des sachgerechten Datenschutzes im Praxisalltag zur Verfügung. Diese wurden von den Kooperationspartnern der Initiative gemeinsam mit psychotherapeutischen und ärztlichen Pilotpraxen erarbeitet, um Praxisinhaber*innen die Gewährleistung des Datenschutzes noch weiter zu erleichtern.
Aufbereitet werden durch die Muster beispielsweise das Verzeichnis für Verarbeitungstätigkeiten, interne Arbeitsvorgaben sowie Einwilligungs- und Schweigepflichtentbindungserklärungen. Die vorgestellten Lösungsansätze und ihre Erläuterungen sind leicht nachvollziehbar, wurden im Praxisalltag erprobt, werden den datenschutzrechtlichen Anforderungen gerecht und können mit angemessenem Aufwand umgesetzt werden. Zwei Fortbildungsveranstaltungen im Juni 2020 sollen zugleich die Möglichkeit schaffen, im Beisein der beteiligten Pilotpraxen Fragen zu den Mustern, ihrer Entstehungsgeschichte und deren praktischem Nutzen zu stellen.

LDI NRW aktualisiert FAQ zum DSB

Mit dem Inkrafttreten der Datenschutz-Grundverordnung (DS-GVO) existiert erstmals eine europaweit verbindliche verpflichtende Regelung zur Bestellung betrieblicher und behördlicher Datenschutzbeauftragter. Während die EG-Datenschutzrichtlinie (95/46/EG) die Verpflichtung zur Bestellung von Datenschutzbeauftragten lediglich als Alternative vorsah, um die Meldepflicht gegenüber der Datenschutzaufsichtsbehörde entfallen zu lassen, wird sich mit Geltung der DS-GVO ab dem 25. Mai 2018 eine Bestellpflicht erstmals unmittelbar aus dem Europarecht ergeben. Das deutsche Erfolgsmodell der datenschutzrechtlichen Selbstkontrolle hat sich damit auch auf europäischer Ebene durchgesetzt. In Ergänzung zur europarechtlichen (Basis-) Bestellpflicht berechtigt die DS-GVO außerdem über eine Öffnungsklausel die Mitgliedstaaten, weitergehende Bestellpflichten auf nationaler Ebene vorzusehen. Neben den Regelungen über die Bestellpflicht enthält die DS-GVO Regelungen zur Stellung und zu den Aufgaben des Datenschutzbeauftragten, von denen der nationale Gesetzgeber grundsätzlich nicht abweichen darf.

Mit der Geltung der DS-GVO gehen auch viele Neuerungen für das Berufsbild der Datenschutzbeauftragten einher. Die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW) gibt in Ihren FAQs einen Überblick über die neuen Regelungen zu Datenschutzbeauftragten nach der Datenschutz-Grundverordnung und der JI-Richtlinie. Der Beitrag richtet sich sowohl an behördliche, als auch an betriebliche Datenschutzbeauftragte.

Datenschutzbeauftragte nehmen, so die LDI NRW, weiterhin für viele Behörden und Unternehmen eine zentrale Rolle ein, zumal sie diese dabei unterstützen, die Einhaltung der Regelungen zu gewährleisten. Datenschutzbeauftragte tragen erheblich dazu bei, ein effizientes Datenschutz-Managementsystem in der Behörde oder im Unternehmen zu implementieren. Sie sind darüber hinaus wichtige Vermittler zwischen den Beteiligten, wie z. B. Aufsichtsbehörden, Betroffenen und Behörden bzw. Unternehmen.

Die vollständigen Fragen und Antworten lassen sich hier herunterladen.

Akkreditierungen von Zertifizierungsstellen gemäß Art. 43 DS-GVO

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat bekannt gegeben, dass sie eine Kooperationsvereinbarung mit der DAkkS über die Akkreditierung von Zertifizierungsstellen im Sinne des Art. 43 DS-GVO geschlossen hat.
Die DAkkS ist die nationale Akkreditierungsstelle der Bundesrepublik Deutschland. Sie handelt nach der Verordnung (EG) Nr. 765/2008 und dem Akkreditierungsstellengesetz (AkkStelleG) im öffentlichen Interesse als alleiniger Dienstleister für Akkreditierung in Deutschland.
Die DAkkS arbeitet nicht gewinnorientiert. Gesellschafter der GmbH sind zu jeweils einem Drittel die Bundesrepublik Deutschland, die Bundesländer (Bayern, Hamburg und Nordrhein-Westfalen) und die durch den Bundesverband der Deutschen Industrie e. V. (BDI) vertretene Wirtschaft.
Gemäß Art. 43 Datenschutz-Grundverordnung (DS-GVO) und § 39 Bundesdatenschutzgesetz (BDSG) werden Stellen, die im Datenschutzbereich zertifizieren möchten, durch die Deutsche Akkreditierungsstelle (DAkkS) zusammen mit der Befugnis erteilenden, zuständigen Datenschutz-Aufsichtsbehörde (Aufsichtsbehörde) akkreditiert. Interessierte Stellen müssen dabei sowohl die Anforderungen aus der EN-ISO/IEC 17065/2012 erfüllen, als auch ergänzende Anforderungen aus dem Datenschutzbereich.
Mit der Kooperationsvereinbarung wird im Wesentlichen festgelegt, dass

a) die DAkkS die Akkreditierung von Zertifizierungsstellen i. S. d. Art. 43 DS-GVO im Einvernehmen mit den Aufsichtsbehörden durchführt,
b) die Aufsichtsbehörden im Rahmen der Akkreditierung die Begutachtung gemeinsam mit der DAkkS durchführen, an der Akkreditierungsentscheidung mitwirken, Mitglieder für den Akkreditierungsausschuss stellen sowie Vertreter in das relevante Sektorkomitee der DAkkS entsenden können, um die Fachkunde sicherzustellen.

Quelle: Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK)

Kardinalfehler bei der Umsetzung von Betroffenenrechten

Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) geht in seinem aktuellen Tätigkeitsbericht (9. Tätigkeitsbericht 2019) auch auf das Thema Betroffenenrechte ein und weist darauf hin, dass die Sicherstellung der Betroffenenrechte eine der Kernanforderung der DS-GVO an Verantwortliche darstellt.
Das BayLDA stellt in seinem Tätigkeitsbericht 7 Fehler vor (Ziffer 5.1), die die Aufsichtsbehörde als „No-Go" bewertet, die jedoch in der Praxis sowohl von den Verantwortlichen als auch von den betroffenen Personen begangen werden:

1. Fehler: Ignorieren von Auskunftsbegehren bei Identitätszweifeln
2. Fehler: Auskunft über ausschließlich Stammdaten als personenbezogene Daten
3. Fehler: Einreichen der Beschwerde vor Verstreichen der Frist
4. Fehler: Zweck des Rechts auf Auskunft außer Acht lassen
5. Fehler: Geltendmachung des Rechts auf Auskunft gegenüber dem Anwalt der Gegenseite
6. Fehler: Beschwerde ohne beweiskräftige Nachweise
7. Fehler: Berufung auf unverhältnismäßigen Aufwand ohne Darlegung der Umstände

Quelle: Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA)

Missbrauch von Kundendaten: Fristlose Kündigung

In seinem Urteil vom 15.01.2020 hat das Arbeitsgericht Siegen entschieden, dass der Missbrauch von Kundendaten durch einen IT-Mitarbeiter die fristlose Kündigung des Arbeitsverhältnisses rechtfertigen kann.

Nach Ansicht des Arbeitsgerichts ist ein IT-Mitarbeiter verpflichtet, sensible Kundendaten zu schützen und darf diese nicht zu anderen Zwecken missbrauchen. Ein Verstoß gegen diese Pflichten rechtfertige in der Regel eine fristlose Kündigung durch den Arbeitgeber.

Im vorliegenden Fall war der Kläger seit 2011 bei der Beklagten als SAP-Berater tätig. Der Kläger bestellte vom Rechner eines Spielcasinos aus Kopfschmerztabletten für zwei Vorstandsmitglieder einer Kundin der Beklagten, wobei er zwecks Zahlung per Lastschrift auf zuvor von einem verschlüsselten Rechner der Kundin auf einen privaten Memory-Stick heruntergeladene Namen, Anschriften und Bankverbindungsdaten von Kunden der Kundin zurückgriff.

Im Rahmen der Bestellung ließ der Kläger dem Vorstand dieser Kundin die Anmerkung zukommen, dass sie aufgrund der Bestellung sehen könnten, wie einfach Datenmissbrauch sei, was bei ihnen zu Kopfschmerzen führen müsste, wobei die bestellten Kopfschmerztabletten durchaus helfen könnten. Die Beklagte hatte er zuvor nicht über bestehende Sicherheitslücken bei der Kundin informiert. Der Kläger erhielt am 26.08.2019 eine fristlose Kündigung. Er erhob dagegen Kündigungsschutzklage.

Laut Pressemitteilung des Arbeitsgerichts Siegen wurde die Klage abgewiesen. Das Gericht entschied, dass die fristlose Kündigung gerechtfertigt sei. Durch sein Vorgehen habe der Kläger nach Überzeugung der 3. Kammer gegen seine Pflicht zur Rücksichtnahme auf die Interessen des Arbeitgebers eklatant verstoßen. Sensible Kundendaten seien zu schützen. Der Kläger habe seinen Datenzugriff missbraucht und eine Sicherheitslücke beim Kunden ausgenutzt. Die Kunden dürften der Beklagten und deren Mitarbeiter Schutz und keinesfalls Missbrauch von etwaigen Sicherheitslücken erwarten. Auch für das Aufdecken vermeintlicher Sicherheitslücken dürften Kundendaten nicht missbraucht werden. Der Kläger habe somit massiv das Vertrauen der Kundin in die Beklagte und deren Mitarbeiter gestört und damit die Kundenbeziehung massiv gefährdet. Dies rechtfertige eine fristlose Kündigung.

Die Entscheidung ist noch nicht rechtskräftig.

Quelle: Arbeitsgericht Siegburg – Aktenzeichen 3 Ca 1793/19 vom 15.01.2020.

Neuer Vorschlag der kroatischen Ratspräsidentschaft für eine ePrivacy-Verordnung

Am 21. Februar 2020 legte die kroatische Ratspräsidentschaft einen Vorschlag zur Neuregelung von Art. 6 und Art. 8 der ePrivacy-Verordnung vor. Die vorgeschlagenen Änderungen in Art. 8 („Schutz von Informationen im Zusammenhang mit Endeinrichtungen") berühren die wichtige Frage zum zulässigen Einsatz von Tracking-Technologien mittels Cookies.

Tracking als berechtigtes Interesse?

In Art. 8 Abs. 1 lit. g hat die Präsidentschaft einen Verarbeitungserlaubnistatbestand aufgrund berechtigter Interessen vorgeschlagen. Dieser Erlaubnistatbestand soll an den Einfügungen eines neuen Art. 8 Abs. 1a gemessen werden. In den Erwägungsgründen 20, 21, 21b und 21c wurden hierzu umfassende Änderungen vorgenommen.

Bisher nur Einwilligung

Bisher lag der Fokus der ePrivacy-Verordnung auf einer Einwilligung der betroffenen Person. Der neue Vorschlag beruft sich auf die bekannte Interessenabwägung der DS-GVO. Danach bedarf es einer Abwägung der berechtigten Interessen gegenüber den Interessen oder den Grundrechten und -freiheiten des Endnutzers. Die berechtigten Interessen sind nicht auf bestimmte Zwecke des Zugriffs beschränkt, was den Interessen der Websiteanbieter entgegenkommt. Cookies zum Zweck der Werbeausspielung könnten also zukünftig in Form eines berechtigten Interesses des Verantwortlichen gerechtfertigt sein.

Wann überwiegen Interessen des Endnutzers?

Wenn die Interessen des Endnutzers die Interessen des Diensteanbieters überwiegen, kann der vorgeschlagene Rechtmäßigkeitstatbestand keine Anwendung finden. Solche Fälle liegen vor, wenn der Endnutzer ein Kind ist, der Diensteanbieter die Informationen verarbeitet, speichert oder sammelt, um das Wesen und die Eigenschaften des Endnutzers zu bestimmen oder um ein individuelles Profil des Endnutzers zu erstellen.

Auslegungshilfe: Erwartungen der Endnutzer

Der Erwägungsgrund 21b verlangt eine Berücksichtigung der berechtigten Erwartungen der Endnutzer bei der Abwägung. So soll der Zugriff auf Informationen in Endgeräten zum Zweck der Behebung von Sicherheitslücken als vom berechtigten Interesse umfasst sein, wie auch Dienste (etwa eine Webseite) deren Inhalte ohne zusätzliche Zahlung zugänglich sind und teilweise oder gänzlich durch Werbung finanziert werden. Insbesondere Dienste zur Wahrung der Meinungs- und Informationsfreiheit, einschließlich zu journalistischen Zwecken, wie Online-Zeitungen oder anderen Presseveröffentlichungen, sollen hiervon profitieren können. In der Konsequenz müssten die genannten Anbieter eben keine Einwilligung von der betroffenen Person einholen.

Keine Weitergabe bei Verarbeitung aufgrund des berechtigten Interesses

Der neue Abs. 1a enthält einen Schutzmechanismus für Endnutzer, wenn ein Diensteanbieter die Interessenabwägung als Erlaubnis nutzen möchte. Nach ErwG 21c dürfen die gewonnenen Informationen nicht ohne vorherige Anonymisierung an Dritte weitergegeben werden. Auftragsverarbeiter nach Art. 28 DS-GVO bleiben hiervon unberührt, weil Auftragnehmer keine Dritten im datenschutzrechtlichen Sinne sind.