Datenschutz newsbox

Ausgabe 06 2020

Editorial: 2

Datenschutzrechtliches Auskunftsrecht im Arbeitsverhältnis 3

Websites datenschutzkonform gestalten (Anzeige) 3

Corona-Warn-App und Datenschutz im Beschäftigungsverhältnis 4

GDD vergibt Wissenschaftspreis für Datenschutz und Datensicherheit 4

Best-Practice-Prüfkriterien im Sinne von Art. 32 DS-GVO 5

Corona-Warn-App, Fiebermessen, Dokumentationspflichten – F.A.Q. zur Kontrolle von Beschäftigten, Kunden und Besuchern (Anzeige) 5

Datenschutz im Homeoffice: Selbst-Check des BayLDA 6

GDD nimmt Stellung zur Änderung des Telemediengesetzes 6

Orientierungshilfe für datenschutzkonforme Nutzung von E-Mail 7

Einführung in den Datenschutz (Anzeige) 7

Datenschutzbeauftragte werden auch in Zeiten der Kurzarbeit gebraucht 8

Datenschutz bei Inkassounternehmen 8

DATAKONTEXT

Editorial:

Am 15. Juni 2020 erblickte die Corona-Warn-App nach 50 Tagen das Licht der Welt und war sowohl über den Apple App Store als auch den Google Play Store beziehbar. Je nachdem wen man fragt, verzeichnete die App bereits oder erst nach vier Tagen fast acht Millionen Downloads (Stand: 18.06.2020).

Der Steckbrief der App ist voller Superlative: Es wird als das „größte Open-Source-Projekt" der Bundesregierung angepriesen. Die App entstand in enger Zusammenarbeit von Branchenriesen wie SAP und Deutsche Telekom sowie weiteren Partnern. Ob der Umstand, dass der Steuerzahler wohl insgesamt 68 Millionen Euro für die Corona-Warn-App zahlen muss, vor dem Hintergrund von „unglücklichen Vorhaben" wie Pkw-Maut oder Berliner Großflughafen, tatsächlich noch als Negativ-Superlativ ins Gewicht fällt, darf bezweifelt werden.

Auch in puncto Datenschutz und IT-Sicherheit wollte man offensichtlich nichts dem Zufall überlassen. Die Entwicklung der Corona-Warn-App erfolgte in enger Zusammenarbeit mit den entscheidenden, öffentlichen Institutionen, wie dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI). Beide Behörden zeigen sich mit dem Ergebnis zufrieden. Das sich sogar der Sprecher des Chaos Computer Clubs bei der Bewertung der Corona-Warn-App mangels wesentlicher Kritikpunkte in „einer ungewohnten Situation wiederfindet", mag dann wohl als „Ritterschlag" für die Aspekte Datensicherheit bewertet werden.

Auch bei der Nutzerakzeptanz wollte man keine Fehler machen und hat versucht, den „Nutzer abzuholen". Dezentral, freiwillig und ohne Identifizierbarkeit der Nutzer – das waren laut dem Nürnberger Institut für Marktentscheidungen die wichtigsten Wünsche der Deutschen an eine Corona-Tracing-App und wurden erfüllt. Sogar der Wunsch nach Barrierefreiheit wurde bei der Entwicklung berücksichtigt.

Kein Wunder, dass man bei der Entwicklung der App so viel wie möglich richtig machen wollte, werden doch bei dem Kampf gegen die Pandemie große Hoffnungen in die Corona-Warn-App gesetzt. Zentral in der Bekämpfung jeder Pandemie ist das Unterbrechen der Infektionsketten. Die Corona-Warn-App kann dazu einen wichtigen Beitrag leisten und die zentrale Arbeit der Gesundheitsämter beim Nachverfolgen der Kontakte unterstützen, so auch das RKI.

Bei aller berechtigten Freude über einen gelungenen Start der Corona-Warn-App ist jedoch auch gut, dass die Datenschutz-Aufsichtsbehörden direkt zum Start vor dem Erwachen neuer Begehrlichkeiten und vor Missbrauchsszenarien mit aller Deutlichkeit warnen, 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

Datenschutzrechtliches Auskunftsrecht im Arbeitsverhältnis

Nach Art. 15 Abs. 1 DS-GVO steht der betroffenen Person ein abgestuftes Auskunftsrecht zu. Dazu gehört das Recht von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob der Verantwortliche sie betreffende personenbezogene Daten verarbeitet. Falls der Verantwortliche entweder keine Daten zu dieser Person verarbeitet oder personenbezogene Daten unumkehrbar anonymisiert hat, hat die betroffene Personen das Recht eine „Negativauskunft" zu erhalten. Des Weiteren steht der betroffenen Person das Recht zu, ganz konkret Auskunft darüber verlangen zu können, welche personenbezogenen Daten vom Verantwortlichen verarbeitet werden.

Unterlassene oder nicht vollständige Auskunftserteilungen an betroffene Personen sind nach Art. 83 Abs. 5 lit. b DS-GVO mit einer hohen Geldbuße bedroht.

Das Recht auf Auskunft ist natürlich auch im Bereich des Beschäftigtendatenschutzes anwendbar.

Das ArbG Düsseldorf hatte im Rahmen einer arbeitsgerichtlichen Entscheidung (u.a.) darüber zu befinden, ob einem Arbeitnehmer ein Schadensersatzanspruch gegen seinen Arbeitgeber zustehen kann, wenn dieser ihm keine vollständige Auskunft nach Art. 15 DS-GVO erteilt hat.

Der Arbeitnehmer, der unter anderem die seiner Ansicht nach nicht vollständige Auskunft nach Art. 15 DS-GVO vor Gericht geltende machte, wollte einen Schadensersatz in Höhe von 140.000,- EUR erstreiten (ca. 12 Monatsgehälter).

In dem Fall hielt das ArbG Düsseldorf einen Schadensersatz in Höhe von 5.000,- EUR für die nicht vollständige Datenauskunft für angemessen.

Quelle: *ArbG Düsseldorf, Urt. v. 05.03.2020 – Az.: 9 Ca 6557/18*

Corona-Warn-App und Datenschutz im Beschäftigungsverhältnis

Die Veröffentlichung der Corona-Warn-App hat eine Menge datenschutzrechtlicher Fragen aufgeworfen, die Arbeitgeber und Arbeitnehmer genauso beschäftigen wie Datenschutzbeauftragte. Eine der Fragen ist:

Kann der Arbeitgeber Beschäftigte verpflichten, eine Corona-Warn-App auf seinem privaten Smartphone zu installieren und vorzuzeigen oder diese auf dienstlichen Smartphones einsetzen und auswerten?

Diese und viele andere Fragen hat die Gesellschaft für Datenschutz und Datensicherheit (GDD e.V.) als FAQ auf ihrer Seite gesammelt und stellt ihre rechtliche Einschätzung zu diesen Fragen zur Verfügung.

Die FAQ befassen sich insbesondere mit den derzeit relevanten Fragen rund um die Verarbeitung personenbezogener Daten bei der Kontrolle von Beschäftigten und deren datenschutzrechtlicher Zulässigkeit. Die Ausführungen in Bezug auf eine Corona-Warn-App orientieren sich ausschließlich an der App der Bundesregierung.

Darüber hinaus stellt die GDD angesichts gehäufter Anfragen zu datenschutzrechtlichen Fragestellungen im Zusammenhang mit der Corona-Pandemie (Covid-19) eine stetig aktualisierte Linksammlung zu aktuellen Ansichten der Aufsichtsbehörden, Beiträgen von Datenschutzexperten sowie den Themen Datenschutz und Datensicherheit bereit.

Quelle: *Gesellschaft für Datenschutz und Datensicherheit*

GDD vergibt Wissenschaftspreis für Datenschutz und Datensicherheit

Auch in diesem Jahr vergibt die Gesellschaft für Datenschutz und Datensicherheit (GDD e.V.) erneut einen Wissenschaftspreis für herausragende wissenschaftliche Arbeiten in den Bereichen Datenschutz und Datensicherheit. Der Preis beträgt 5.000,00 €. Der Preis kann auch zwischen mehreren Arbeiten geteilt werden.
Der Preis soll bevorzugt an Nachwuchswissenschaftler vergeben werden. Es sollen fertiggestellte oder in der Fertigstellung befindliche Abschlussarbeiten oder Doktorarbeiten ausgezeichnet werden. In Betracht kommen neben Arbeiten aus den Rechtswissenschaften, Wirtschaftswissenschaften und der Informatik auch aus anderen Wissenschaftsdisziplinen, in denen Fragen aus den Bereichen Datenschutz und Datensicherheit behandelt werden. Voraussetzung für die Vergabe des Wissenschaftspreises ist die Erfüllung der wissenschaftlichen Exzellenzkriterien.
Die Arbeiten müssen mit Befürwortung des betreuenden Hochschullehrers bei der
GDD-Geschäftsstelle bis zum **31. Juli 2020** eingereicht werden.
Nähere Informationen zum Wissenschaftspreis stehen als
und Word-Dokument als Download zur Verfügung.

Best-Practice-Prüfkriterien im Sinne von Art. 32 DS-GVO

Nach Informationen des Bundesamts für Sicherheit in der Informationstechnik (BSI) waren 2019 etwas weniger als zehn Prozent der Krankenhäuser in Deutschland beim BSI als Kritische Infrastrukturen (KRITIS) im Sinne des IT-Sicherheitsgesetzes registriert.

Neben Einrichtungen anderer Sektoren waren Krankenhäuser und andere medizinische Einrichtungen zuletzt wiederholt Betroffene gravierender IT-Sicherheitsvorfälle. Neben der Bedrohung durch Ransomware-Angriffe standen dabei auch sensible Patientendaten im Mittelpunkt.

Das BSI hat Oktober 2019 die Eignung eines branchenspezifischen Sicherheitsstandards (B3S) festgestellt, mit dem Krankenhäuser ihre IT-Sicherheitsmaßnahmen nach dem Stand der Technik ausrichten können. Vorgelegt wurde der B3S von der Deutschen Krankenhausgesellschaft (DKG).

Das Bayerische Landesamt für Datenschutzaufsicht (BayLfD) und der Bayerische Landesbeauftragte für den Datenschutz (BayLDA) greifen diese Thematik vor dem Hintergrund der aktuellen Pandemie auf und weisen in einem gemeinsamen Papier darauf hin, wie wichtig ein funktionierendes Gesundheitssystem ist. Krankenhäuser, Arztpraxen und medizinische Labore seien herausgefordert, die medizinische Versorgung der Bevölkerung sicherzustellen. Bereits ein erfolgreicher Cyberangriff könne aber die Funktionsfähigkeit einer medizinischen Einrichtung für Tage oder Wochen massiv beeinträchtigen – und im schlimmsten Fall sogar komplett lahmlegen.

Zur Überprüfung ihrer Cybersicherheitsmaßnahmen stellen der BayLfD und das BayLDA daher den medizinischen Einrichtungen in Bayern eine Best-Practice-Checkliste zur Verfügung.

Der Fokus des Dokuments liegt auf der Verfügbarkeit der Daten bzw. Dienste bezüglich Angriffe aus dem Internet und weniger auf deren Vertraulichkeit und Integrität, die aus Datenschutzsicht jedoch ebenfalls zu beachten sind. Die beiden Aufsichtsbehörden sehen das Papier als eine Hilfestellung zur schnellen Überprüfung der eigenen Sicherheit hinsichtlich der Verfügbarkeit der eigenen Datenverarbeitung im Sinne von Art. 32 DS-GVO. Der Anwendungsbereich umfasst sowohl den nicht-öffentlichen als auch den öffentlichen Bereich.

Die Checkliste kann kostenlos unter www.datenschutz-bayern.de/best_practice_medizin sowie unter www.lda.bayern.de/best_practice_medizin abgerufen werden.

Datenschutz im Homeoffice: Selbst-Check des BayLDA

Die Corona-Pandemie hat dafür gesorgt, dass das Thema Homeoffice auch bei Unternehmen, die sich bislang nicht intensiv damit beschäftigt haben, in den Vordergrund gerückt ist. Im „Normalfall" stellt sich die Einrichtung eines Home-Office-Arbeitsplatzes als eine wohlüberlegte und gut geplante Maßnahme dar. Damit auch im Falle einer pandemiebedingten, schnelleren Umsetzung der Verlagerung der Datenschutz am heimischen Arbeitsplatz nicht auf der Strecke bleibt, haben auch Datenschutz-Aufsichtsbehörden eine ganze Reihe von Leitfäden veröffentlicht, so bspw. Das ULD oder auch der BfDI.

Die aktuellste Veröffentlichung kommt von dem BayLDA in Form eines „Selbst-Check: Datenschutzrechtliche Regelungen bei Homeoffice".

Das BayLDA möchte mit seiner Handreichung einen Überblick über die wichtigsten Praxismaßnahmen im Homeoffice entsprechend den geltenden gesetzlichen Datenschutzvorgaben geben. Im Sinne einer gezielten Prävention von Datenschutzverstößen soll damit im momentanen „neuen Alltag" eine gesteigerte Sensibilisierung für dieses Thema erreicht und mit konkreten Prüffragen der eigene Stand der Umsetzung unterstützt werden, so das BayLDA.
Die aufgeführten Prüfpunkte sieht das BayLDA nicht als abschließend an, sondern stellt einen Best-Practice-Ansatz dar, der beispielsweise vonseiten der Geschäftsführung oder des Datenschutzbeauftragten im Sinne einer Soll-Ist-Überprüfung verwendet werden kann.

Eine gut sortierte Sammlung zum Thema Datenschutz und Home-Office bietet die GDD mit weiteren nützlichen Links zum Thema.

Quelle: *Bayerisches Landesamt für Datenschutzaufsicht*

GDD nimmt Stellung zur Änderung des Telemediengesetzes

Die Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD) nahm zur geplanten Änderung des Telemediengesetzes im Rahmen der Umsetzung einer EU-Richtlinie Stellung.

Am 1. April 2020 hat die Bundesregierung den vom Bundesministerium für Wirtschaft und Energie vorgelegten Entwurf eines Gesetzes zur Änderung des Telemediengesetzes und weiterer Gesetze im Kabinett beschlossen. Mit dem Entwurf werden die Änderungen der europäischen Richtlinie über audiovisuelle Mediendienste (AVMD-Richtlinie) in deutsches Recht umgesetzt. Die Regelungen sollen noch vor Ende der Umsetzungsfrist am 19. September 2020 in Kraft treten. Mit dem von der Bundesregierung beschlossenen Artikelgesetz werden weitere Anforderungen der AVMD-Richtlinie umgesetzt. So sieht die Richtlinie auch Einschränkungen der Werbung für Tabakerzeugnisse und elektronische Zigaretten vor. Dies erfordert Änderungen im Tabakerzeugnisgesetz. Die inhaltsbezogenen Anforderungen der Richtlinie für Fernsehen und audiovisuelle Mediendienste auf Abruf, die z.B. die Werbung, den Jugendschutz oder die Einhaltung einer europäischen Quote betreffen, gelten auch für die Deutsche Welle.
Aus Sicht der GDD sind vor allem die geplanten Änderungen des TMG von besonderer Relevanz. Videosharingplattformen müssen, laut der vorliegenden Drucksache, in Zukunft ein Melde- und Abhilfeverfahren für Nutzerbeschwerden wegen Verstößen gegen Werbe- und Jugendschutzvorschriften einrichten. Abseits der AVMD-Richtlinie soll es jedoch keine weiteren Anpassungen oder Änderungen des TMG geben. Hierzu hat die GDD Stellung bezogen, die allen Mitgliedern des federführend zuständigen Ausschusses für Wirtschaft und Energie im Deutschen Bundestag vorgelegt wird.
Die vollständige Stellungnahme können Sie hier abrufen.

Orientierungshilfe für datenschutzkonforme Nutzung von E-Mail

E-Mail ist neben dem World Wide Web ein wichtiger Internetdienst, nicht zuletzt, weil es durch E-Mails möglich ist, Textnachrichten ebenso wie digitale Dokumente (also z. B. Grafiken oder Office-Dokumente) typischerweise in wenigen Sekunden rund um die Erde zu senden.
Ihren Siegeszug trat die E-Mail bereits in dem Jahre 1984 an und ihre Beliebtheit hält trotz diverser Messenger und Sozialer Dienste weiter an.

Insbesondere wenn mit der E-Mail personenbezogene Daten übermittelt werden (über die ohnehin vorhandenen Metadaten des Versenders hinaus), existieren auch datenschutzrechtliche Anforderungen, die insbesondere Verantwortliche und Auftragsverarbeiter beachten müssen. Sie sind gesetzlich gehalten, die Risiken, die sich aus ihren Verarbeitungen personenbezogener Daten ergeben, hinreichend zu mindern.

Das betrifft auch Risiken, die durch die Übermittlung personenbezogener Daten per E-Mail entstehen. Der gesetzlich gebotene Schutz personenbezogener Daten im Zuge der Übermittlung von E-Mail-Nachrichten erstreckt sich sowohl auf die personenbezogenen Inhalte als auch die Umstände der Kommunikation, soweit sich aus letzteren Informationen über natürliche Personen ableiten lassen.

Sowohl Transportverschlüsselung als auch Ende-zu-Ende-Verschlüsselung mindern für ihren jeweiligen Anwendungszweck Risiken für die Vertraulichkeit und Integrität der übertragenen personenbezogenen Daten. Der Einsatz von Transportverschlüsselung bietet lediglich einen Basis-Schutz und stellt eine Mindestmaßnahme zur Erfüllung der gesetzlichen Anforderungen dar. Der durchgreifendste Schutz der Inhaltsdaten wird hingegen durch Ende-zu-Ende-Verschlüsselung erreicht. Verantwortliche müssen beide Verfahren in der Abwägung der notwendigen Maßnahmen berücksichtigen. In einer von der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder mehrheitlich verabschiedeten Orientierungshilfe werden die Anforderungen an die Verfahren zum Versand und zur Entgegennahme von E-Mail-Nachrichten erläutert.

Quelle: *Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder*

Datenschutzbeauftragte werden auch in Zeiten der Kurzarbeit gebraucht

Kurzarbeit im Arbeitsverhältnis bedeutet die vorübergehende Verringerung der regelmäßigen Arbeitszeit in einem Betrieb aufgrund eines erheblichen Arbeitsausfalls. Von der Kurzarbeit können alle oder nur ein Teil der Arbeitnehmer des Betriebes betroffen sein.

Was bedeutet dies für die Tätigkeit der/des Datenschutzbeauftragten? Hat der/die Beauftragte für den Datenschutz beispielsweise während einer Pandemie weniger zu tun und muss daher auch in Kurzarbeit beschäftigt werden?

Mit Fragen rund um dieses Thema beschäftigt sich die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW) in ihrer neuesten Veröffentlichung und stellt fest, dass der Beratungs- und Prüfauftrag eines Datenschutzbeauftragten bei einer Krisensituation wie einer Pandemie sogar steigen kann und von gesteigerter Bedeutung sein kann.
Mit den Maßnahmen gegen die Bekämpfung der Pandemie gehen nicht selten Datenverarbeitungen einher, die es so vorher nicht gegeben hat. Solche Maßnahmen sind mit vielen neuen datenschutzrechtlichen Fragestellungen konfrontiert, die sich aus der Corona-bedingten Änderung bisheriger Arbeitsabläufe in einem Unternehmen ergeben. Die Neuorganisation von Arbeitsprozessen, die Zunahme der elektronischen Datenverarbeitung, das Arbeiten im Homeoffice, in Tele-Arbeit und mittels Videokonferenzsystemen sowie nicht zuletzt Fragen des Gesundheitsdatenschutzes bei Beschäftigten, Kundinnen und Kunden erfordern die Einbindung der betrieblichen Datenschutzbeauftragten.

Die LDI NRW weist auch darauf hin, dass eine angeordnete Kurzarbeit auch an der Benennungspflicht nach dem Bundesdatenschutzgesetz (BDSG) nichts ändert. Zwar kommt es nach § 38 Abs. 1 BDSG darauf an, dass Personen „in der Regel (…) ständig" mit der Verarbeitung personenbezogener Daten beschäftigt sind. Mit dieser Formulierung ist aber gerade nicht gemeint, dass kurzzeitige Veränderungen berücksichtigt werden, sondern dass es auf eine langfristige Betrachtung ankommt, so die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen.

Quelle: *Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen*

Datenschutz bei Inkassounternehmen

Die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW) weist in einer aktuellen Veröffentlichung auf eine Praxis von Inkassounternehmen hin, die schwerwiegende Nachteile für Betroffene begründen kann.

Nach den Erfahrungen der LDI NRW kommt es offenbar nicht selten vor, dass Personen von Inkassounternehmen angeschrieben werden, obwohl den Betroffenen die zugrundeliegende Forderung nicht bekannt ist. Teilweise stelle sich im Verlauf der Kommunikation mit dem Inkassounternehmen und der betroffenen Person heraus, dass eine schlichte Verwechslung von Personen die Ursache hierfür ist.
In ihrer aktuellen Veröffentlichung stellt die LDI NRW die möglichen Gründe für derlei Verwechslungen dar und gibt praxistaugliche Ratschläge, wie Betroffene im Falle einer Personenverwechslung reagieren sollten.
Dabei spielt neben dem Bestreiten einer Forderung, die Möglichkeit des Auskunftsanspruchs nach Art. 15 DS-GVO eine wesentliche Rolle. Die Aufsichtsbehörde geht auch auf die Frage ein, ob und wie die verwechselte Person eine Löschung ihrer Daten vom Inkassounternehmen verlangen kann, ohne dass die Aufsichtsbehörde bei der Beantwortung dieser Frage vernachlässigt, die kollidierenden Interessenslagen deutlich zu machen.

Quelle: *Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW)*