NEWS BOX DATENSCHUTZ

INHALTSVERZEICHNIS

AUSGABE 7/2022

DATAKONTEXT

Levent Ferik

EDITORIAL

Der Anwendungsbereich des Datenschutzrechts ist groß und wird gefühlt jährlich größer. Datenschutzrecht ist zum grundlegenden Querschnittsrecht der Informations- und Wissensgesellschaft geworden. Um in diesem stetig größer werdenden Anwendungsbereich des Datenschutzrechts weiterhin erfolgreich tätig zu sein, müssen auch Datenschutzbeauftragte ihre Qualifikation auf einem hohen Stand erweitern.
Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. fasst es in seiner Publikation „Das berufliche Leitbild der Datenschutzbeauftragten“ gut zusammen, wenn in der Ankündigung zum Leitbild gefordert wird: *„Datenschutzbeauftragte tragen große Verantwortung. Sie begleiten Unternehmen und Behörden auf dem Weg der Digitalisierung. Dabei haben sie einerseits das Grundrecht auf Schutz persönlicher Daten, andererseits die Bedürfnisse und Entwicklung von Firmen und Verwaltungen im Blick.*

Datenschutzbeauftragte helfen also nicht nur, Gesetze einzuhalten, sondern sorgen mit Fachwissen und Erfahrung dafür, dass die besten Prozesse mit einer sicheren Lösung zum Erfolg für alle werden.
Aus diesem doppelten Blick heraus tragen Datenschutzbeauftragte entscheidend zur Glaubwürdigkeit von Firmen und Verwaltung bei. Ein funktionierender Datenschutz baut Vertrauen bei Kunden und Partnern auf, schützt Unternehmenswerte und stärkt Marken. Damit wird Datenschutz zu einem wichtigen Wettbewerbsvorteil.

Um diese Herausforderungen zu meistern, ist eine hervorragende Qualifikation der Datenschutzbeauftragten unabdingbar. Insbesondere ist Fachwissen erforderlich für Prozesse und Organisation, IT-Systeme und Applikationen Datenschutzrecht.“

Ihr Levent Ferik

Sagen Sie uns Ihre Meinung
kundenservice@datakontext.com

Sommer, Sonne, (Timmendorfer) Strand
15. GDD Sommerworkshop 2022

Foto: kasto, Adobe Stock

Egal ob Unternehmen, Behörde oder medizinische Einrichtung – jede Organisation arbeitet täglich mit personenbezogenen Daten und ist verpflichtet diese zu schützen. Der Datenschutz und die korrekte Umsetzung der DS-GVO bleiben für Unternehmen eine andauernde Aufgabe. Häufig herrschen Unsicherheiten über die neueste Rechtsprechung und die fehlerfreie Umsetzung des Datenschutzes, wie zum Beispiel über die aktuelle IT-Sicherheitsgesetzgebung, die praktischen Umsetzung von „Schrems II" oder auch über den Beschäftigtendatenschutz im Zeitalter der Digitalisierung. Mit dem TTDSG gibt es seit Dezember 2021 zudem ein neues Datenschutzrecht für Telekommunikation & Telemedien. Daher ist die Fort- und Weiterbildung in einem dynamischen Thema wie dem Datenschutz essenziell für die ordentliche Aufgabenerfüllung des betrieblichen Datenschutzbeauftragten oder des Datenschutzberaters.

Datenschutz und Fachaustausch direkt an der Ostsee

Die GDD bietet mit ihrem 15. Sommerworkshop betrieblichen Datenschutzbeauftragten, externen Datenschutzdienstleistern sowie beratenden Datenschützern eine Möglichkeit zur kompakten Weiterbildung. Vom 8. bis 10. August 2022 präsentieren Experten in Timmendorfer Strand die neuesten Entwicklungen im Datenschutz. Virulente Themen wie der rechtmäßige Einsatz von Google Analytics, die praktische Gewährleistung des Rechts auf Auskunft/Datenkopie, Verbraucherverträge über digitale Produkte sowie die aktuellen Standardvertragsklauseln zur Drittstaatenübermittlung werden in Vorträgen und Fachdiskussionen behandelt und erörtert. Die Vortragenden stehen nach ihren Ausführungen auch für Diskussionen und individuelle Fragestellungen der Teilnehmenden bereit.

Kompetente Referenten zeigen Problemstellungen und Lösungswege auf

Zu den hochkarätigen Referenten aus dem Datenschutz gehören insbesondere Vertreter mehrerer Aufsichtsbehörden aus ganz Deutschland. GDD und DATAKONTEXT dürfen die Landesbeauftragten für Datenschutz aus Hamburg **Thomas Fuchs**, aus Niedersachsen **Barbara Thiel** und aus Schleswig-Holstein **Marit Hansen** begrüßen. Neben den fachlichen GDD-Experten **Prof. Dr. Rolf Schwartmann, Prof. Dr. Rainer W. Gerling, RA Andreas Jaspers und RAin Yvette Reif** und **Kristin Benedikt** liefern die Vertreter aus der Praxis – **Philipp Quiel, RA Sascha Kremer, Michael Bödelt und RA Boris Reibach** – Ihnen weiteren wertvollen Input und praxisnahes Wissen. Stellen Sie unseren Top-Experten Ihre Fragen und genießen Sie die den Ostseestrand. Neben zahlreichen Fachvorträgen bietet DATAKONTEXT am letzten Veranstaltungstag auch ein fachlich wie politisches Diskussionsforum, bei der sich auch alle Teilnehmenden einbringen können, an.

Fachkundenachweis am Strand und Zeit für Vernetzung

Der Sommerworkshop verschafft wichtigen Input für Datenschutzbeauftragte und -berater sowie Datenschutzdienstleister und stellt zugleich auch einen Nachweis der gem. Art. 38 Abs. 2 DS-GVO, §§ 5, 6, 38 BDSG geforderten gesetzlichen Fachkunde gegenüber den jeweiligen Auftraggebern, Arbeitgebern und den Aufsichtsbehörden dar. Nach rund 2 Jahren Corona-Pandemie kann nun nach dem fachlichen Miteinander auch der zwischenmenschliche Austausch stattfinden. Zum Sommerworkshop gehört deswegen auch die Einladung am 1. Abend zu einer gemeinsamen Abendveranstaltung als Möglichkeit zum Networking. Eine detaillierte Übersicht inklusive Ablaufplan über den angebotenen Workshop und alle weitere Informationen finden Sie hier

Foto: pictworks, Adobe Stock

Betriebliches Eingliederungsmanagement: Weitergabe von Gesundheitsdaten an Betriebsrat

Die Öffnungsklauseln der DS-GVO lassen nationale Regelungen zur Datenverarbeitung im Beschäftigungskontext öffentlicher Stellen zu (siehe Artikel 6 Absatz 2 und Absatz 3 Buchstabe b DS-GVO sowie Artikel 88 DS-GVO). Der Bundesgesetzgeber hat unter anderem mit den spezialgesetzlichen Regelungen in den Sozialgesetzbüchern hiervon Gebrauch gemacht.

Weiter auf DataAgenda lesen

EuGH: Sonderkündigungsschutz für DSB ist mit EU-Recht vereinbar

Seit dem Wirksamwerden 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.

Zum Schutz des Datenschutzbeauftragten gewährleistet die DS-GVO Abberufungsschutz sowie ein Benachteiligungsverbot (Art. 38 Abs. 3 Satz 2 DS-GVO): Der Datenschutzbeauftragte darf von dem Verantwortlichen oder dem Auftragsverarbeiter wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden. Möglich ist jedoch nach der DS-GVO ein betriebsbedingter Wegfall der Benennung.

Weiter auf DataAgenda lesen

Foto: Zerbor, Adobe Stock

Aufsichtsbehörden veröffentlichen FAQ zu Facebook-Fanpages

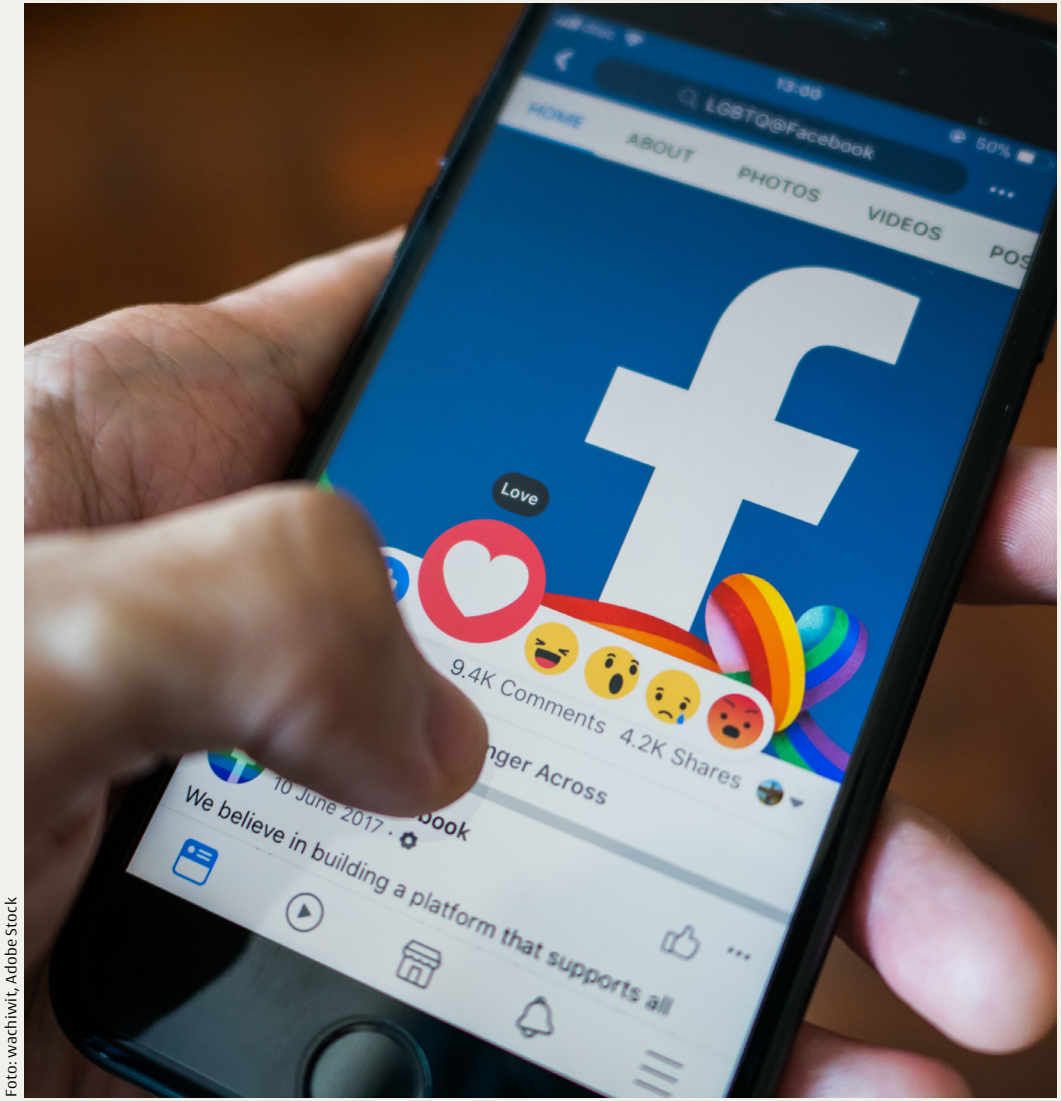

Foto: wachiwit, Adobe Stock

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat am 22. Juni 2022 eine FAQ-Liste zur Nutzung von Facebook-Fanpages verabschiedet.

Die DSK beantwortet darin unter anderem, warum der Betrieb von Facebook-Fanpages datenschutzrechtlich problematisch ist und warum Verantwortliche in der aktuellen Situation den datenschutzkonformen Betrieb einer Facebook-Fanpage nicht gewährleisten können. Das Dokument geht auf oft gestellte datenschutzrechtliche Fragen ein. Verantwortliche müssen nach der Auffassung des DSK davon ausgehen, dass die rechtlichen Aspekte sinngemäß ebenso für andere soziale Netzwerke und Plattformen gelten. Maßgebliche Rechtsprechung gebe es bisher allerdings nur zu Facebook-Fanpages.

Die rechtlichen Probleme beim Betrieb einer Facebook-Fanpage hatte die DSK zudem im Einzelnen in einem Kurzgutachten dargestellt. Die FAQ-Veröffentlichung sei als Reaktion und Hilfsangebot in Bezug auf das große Interesse an Hinweisen zu rechtssicherem Handeln bei der Nutzung von Social Media-Angeboten zu sehen. Gleichzeitig sollen beaufsichtigte Stellen schnell und verständlich über die gemeinsame Rechtsauffassung der Datenschutzaufsichtsbehörden informiert werden.

Quelle: DSK

Foto: dennizn, Adobe Stock

Datenschutzproble-matik Office 365

Nach Auffassung des LfDI Rheinland-Pfalz gründet die mit der Nutzung von Office 365 verbundene Problematik auf technischen und rechtlichen Faktoren. Bspw. lassen sich nach Bewertung der Aufsichtsbehörde bei der Nutzung weder eine Übermittlung bestimmter Nutzungsdaten, wie bspw. die IP-Adresse vermeiden, noch die Verwendung bestimmter Nutzungsdaten vom Anbieter für eigene Zwecke oder gar die Weitergabe an Werbepartner vermeiden, obwohl hierfür ggf. keine rechtliche Grundlage angeführt werden könne.
Auch wenn die Weitergabe aus gesetzlichen Übermittlungsbestimmungen oder über die Möglichkeit der Inanspruchnahme eines Auftragsverarbeiters nach Art. 28 Abs. 3 DS-GVO legitimieren ließe, bliebe nach dem sog. Schrems II-Urteil des EuGH als grundsätzliches Problem, dass in die USA übermittelte personenbezogene Daten unter rechtlichen Bedingungen verarbeitet werden, die nicht dem europäischen Datenschutzniveau entsprechen.

Nachfolgend geht der LfDI Rheinland-Pfalz auf folgende Fragestellungen ein:

- Warum reicht die von Microsoft angebotene Option, Daten auf europäischen Servern zu verarbeiten, für einen datenschutzkonformen Betrieb nicht aus?
- Warum stellt der US-amerikanische CLOUD-Act ein Datenschutzproblem dar?
- Unter welchen Voraussetzungen ist ein datenschutzkonformer Einsatz von Microsoft Office 365 denkbar?
- Welche „Nutzungsdaten“ werden bei Microsoft Office 365 übermittelt?
- Welche technisch-organisatorischen Maßnahmen können getroffen werden, um eine Übermittlung von Diagnosedaten an Microsoft zu vermeiden?
- Wie ist die Nutzung von Microsoft Office 365 auf Tablets oder Smartphones zu bewerten?

Auch wenn die Antworten auf diese häufig gestellten Fragen letztliche keine tatsächliche Lösung für die brennenden Probleme der Verantwortlichen bringen dürften, kann die FAQ zumindest als kompakte Zusammenfassung der aktuell diskutierten Themen einen gewissen Mehrwert bieten.

Quelle: LfDI Rheinland-Pfalz

Live Online-Schulung

Big Data-Analysen nach DS-GVO und BDSG

29. August 2022 | online
Referenten: Prof. Dr. Rolf Schwartmann, Fritz-Ulli Pieper

Schwerpunkte:

- ✓ Was bedeutet Big Data – Abgrenzung zu Profiling und CRM
- ✓ Methoden der Big Data-Analysen
- ✓ Rechtsrahmen für die Nutzung nach DS-GVO und BDSG
- ✓ Anwendungsfälle und deren Lösungen

Jetzt anmelden:
www.datakontext.com

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT

DATA AGENDA PODCAST

Der **Experten-Talk** mit Prof. Schwartmann

Folge #**19** (Teil 1 und 2)

Onlinedatenschutz im Spannungsfeld zwischen Wirtschaft und Aufsicht


Dr. Stefan Hanloser


Dr. Nina Herbort


RAin Yvette Reif

DataAgenda Podcast Folge 19: Onlinedatenschutz im Spannungsfeld zwischen Wirtschaft und Aufsicht

Das TTDSG ist für den Onlinedatenschutz zentral. Im Juli 2022 haben Wirtschaft und Aufsicht erste Erfahrungen mit dem neuen Gesetz gesammelt. Eine zentrale Norm ist § 25 TTDSG, der den Zugriff auf Endgeräte regelt.
Dr. Stefan Hanloser, Vice President Data Protection Law bei der ProSiebenSat.1 Group, Dr. Nina Herbort, beim Berliner Beauftragten für Datenschutz und Informationsfreiheit zuständig für Telemedien und Webtracking und RAin Yvette Reif, LL.M., stellv. Geschäftsführerin der GDD diskutieren mit Professor Dr. Rolf Schwartmann.

Teil 1:
Die Grundlagen des TTDSG und die Grundzüge von § 25 TTDSG. Wie weit geht die Reichweite der Einwilligung nach Abs. 1 im Verhältnis zu den gesetzlichen Erlaubnissen nach Abs. 2? Und wie ist das Zusammenspiel der Norm mit der DS-GVO?
Zum Podcast bitte hier klicken.

Teil 2:
Beantwortung von Spezialfragen zu § 25 TTDSG und um die Orientierungshilfe der DSK. Konkret diskutieren wir über Cookie-Banner, die Zulässigkeit des „Zahlens mit Daten" und den Tatbestand der „unbedingten Erforderlichkeit". Schließlich befassen wir uns mit der Differenzierung zwischen Basis- und Zusatzdienste der DSK
Zum Podcast bitte hier klicken.

Weitere Folgen unter DataAgenda.de/podcast

Foto: freshidea, Adobe Stock

Orientierungshilfe „Das Recht auf Löschung nach der DS-GVO“

Die Datenschutz-Grundverordnung (DS-GVO) als gesetzliche Regelung zur Verarbeitung personenbezogener Daten hat den Datenschutz nachhaltig verändert und geprägt. Sie verpflichtet jedes Unternehmen – unabhängig von seiner Größe – zur Implementierung eines Datenschutzmanagementsystems (DSMS). Jeder Verantwortliche hat deswegen eine Datenschutzorganisation vorzuweisen, die in der Lage ist, die Einhaltung datenschutzrechtlicher Pflichten zu gewährleisten. Eine der maßgeblichen Anforderungen ist die Pflicht personenbezogenen Daten korrekt zu löschen nach DS-GVO.

Aufgrund des Prinzips der Datenminimierung (Art. 5 Abs. 1 lit. c DS-GVO) und des Grundsatzes der Zweckbindung besteht nach Wegfall der Erforderlichkeit kein Rechtsgrund mehr zur weiteren Speicherung. Doch daran anschließende gesetzliche Aufbewahrungspflichten laufen dieser grundsätzlichen Löschregel häufig zuwider.

Der Bayerische Landesbeauftragte für den Datenschutz gibt an, dass sich in der Prüfungs- und Beratungspraxis rund um das Recht auf Löschung zahlreiche Fragen ergeben. Diese betreffen die verschiedenen Löschungsgründe sowie die Reichweite der Ausnahmetatbestände, jedoch auch etwa das Verhältnis von Löschungsrecht und Löschungspflicht oder die praktische Umsetzung entsprechender Ersuchen, so der BayLfD.
Der Bayerische Landesbeauftragte für den Datenschutz hat daher eine Orientierungshilfe „Das Recht auf Löschung nach der Datenschutz-Grundverordnung“ erarbeitet, die den bayerischen öffentlichen Stellen (aber auch Verantwortlichen in anderen Bundesländern) wie auch interessierten Bürgerinnen und Bürgern anhand praktischer Anwendungsfälle aus dem öffentlichen Sektor eine umfassende Erläuterung der einschlägigen Vorgaben bietet. Die in die Ausführungen eingestreuten Praxisbeispiele runden die Orientierungshilfe ab.

Quelle: Der Bayerische Landesbeauftragte für den Datenschutz (BayLfD)

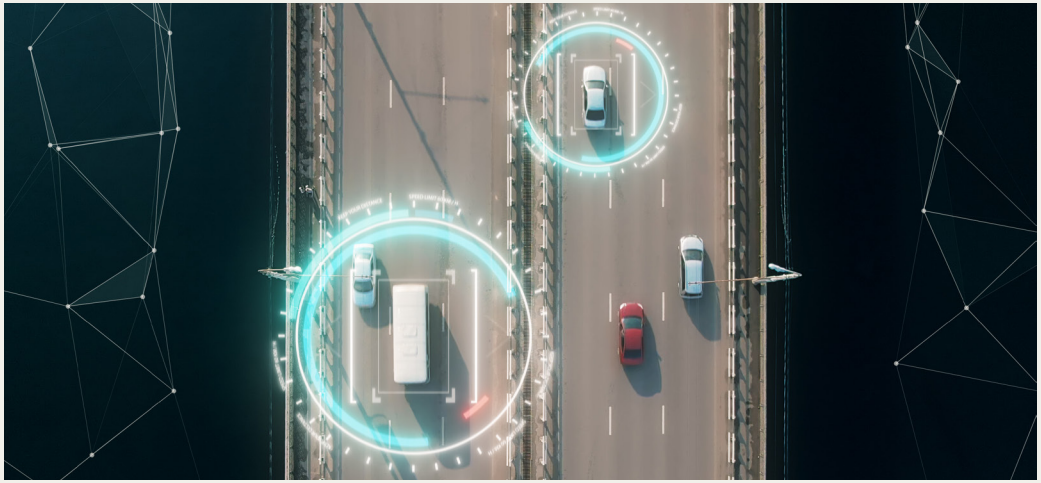

Foto: flashmovie, Adobe Stock

Zwecke für GPS-Tracking im Beschäftigungsverhältnis

GPS-Tracking im Beschäftigtenverhältnis kann datenschutzrechtlich zulässig sein, soweit die Interessen des Arbeitgebers und das Persönlichkeitsrecht der Beschäftigten in einen angemessenen Ausgleich gebracht werden und es auf das erforderliche Maß beschränkt ist.

In seinem 50. Tätigkeitsbericht geht der Hessische Datenschutzbeauftragte auf mögliche Zwecke eines GPS-Trackings ein und schildert anhand eines von der Behörde geprüften Falles, welche Anforderungen an die Erforderlichkeit der einzelnen möglichen Zwecke gestellt werden müssten (Abschnitt 11.3).

Damit bieten die Ausführungen eine gute Orientierung für Verantwortliche, die sich mit dieser Thematik auseinandersetzen wollen oder müssen. Folgende Einsatzzwecke werden näher betrachtet:

- Schnelle Störungsbehebung und Effizienzsteigerung bei der Routenplanung
- Einhaltung steuerrechtlicher Vorschriften
- Sicherheit der Fahrer (Unfall/Pannenhilfe)
- Sicherheit der Fahrzeuge (Diebstahlschutz)
- Effizienzsteigerung in der Beschaffung (Qualität, Abnutzung der Fahrzeuge)
- Sicherstellung der Einhaltung arbeitsrechtlicher Vorgaben (Missbrauch der Tankkarte
- Anlasslose präventive Kontrollmaßnahmen zur Überprüfung der Einhaltung von bestehenden arbeitsrechtlichen Pflichten
- Anlassbezogene repressive Mitarbeiterkontrolle bei konkretem zu dokumentierendem Anfangsverdacht

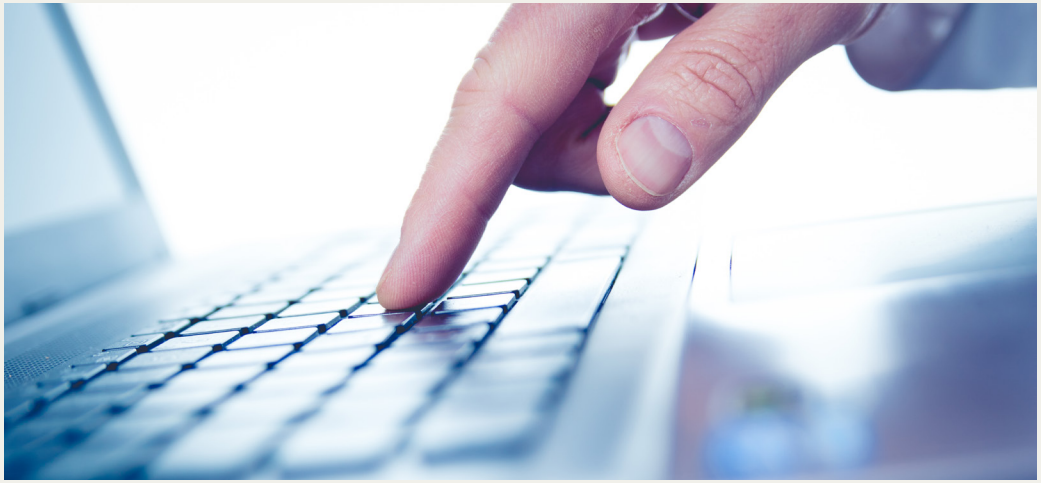

Foto: CreaFoto, Adobe Stock

Datenschutzverstöße durch „Mitarbeiterexzess“

Regel: Unternehmen haften für Datenschutzverstöße ihrer Beschäftigten

Nach Auffassung der Datenschutzkonferenz (DSK) als Gremium der deutschen Datenschutzaufsichtsbehörden sollen Unternehmen im Rahmen von Art. 83 DS-GVO für Datenschutzverstöße eines jeden Beschäftigten haften, wenn der Mitarbeiter nicht im Exzess (für eigene Zwecke) gehandelt hat. Dabei sei nicht erforderlich, dass für die Handlung ein gesetzlicher Vertreter oder eine Leitungsperson verantwortlich ist. Zurechnungseinschränkende Regelungen im nationalen Recht würden dem widersprechen. Diese Haftung für Mitarbeiterverschulden ergebe sich aus der Anwendung des sogenannten funktionalen Unternehmensbegriffs des europäischen Primärrechts. Der funktionale Unternehmensbegriff aus dem Vertrag über die Arbeitsweise der Europäischen Union (AEUV) besage, dass ein Unternehmen jede wirtschaftliche Einheit unabhängig von ihrer Rechtsform und der Art ihrer Finanzierung ist.

Nach der Rechtsprechung zum funktionalen Unternehmensbegriff haften Unternehmen für das Fehlverhalten ihrer Beschäftigten:

- ohne dass eine Kenntnis oder Anweisung der Geschäftsführung
- oder eine Verletzung der Aufsichtspflicht für die Zurechnung erforderlich sind.

Ausnahme: Beschäftigter geriert sich als Verantwortlicher (Mitarbeiterexzess)

In bestimmten Fällen kann aber auch der Arbeitnehmer unmittelbar Adressat einer aufsichtsbehördlichen (Sanktions-)Maßnahme sein. Dafür muss der Beschäftigte als „Verantwortlicher“ im Sinne des Art. 4 Nr. 7 DS-GVO zu qualifizieren sein. Die DSK hat in seiner Entschließung vom 3.4.2019 („Unternehmen haften für Datenschutzverstöße ihrer Beschäftigten!“) betont, dass sogenannte „Exzesse“ der Beschäftigten, die bei verständiger Würdigung nicht der unternehmerischen Tätigkeit zugeordnet werden können, nicht von der Haftung des Unternehmens erfasst sind.

In seinem 50. Tätigkeitsbericht (Ziffer 6.3) schildert der Hessische Datenschutzbeauftragte mehrere Fälle des sog. Mitarbeiterexzesses, die dazu führten, dass Geldbußen direkt gegen die Beschäftigten des Verantwortlichen verhängt wurden. Dabei ging es beispielsweise um Sachverhalte im Zusammenhang mit der zweckwidrigen Datenverwendung aus den sogenannten „Corona-Listen“ in der Gastronomie oder in Corona-Testcentern durch die dortigen Mitarbeiter und um Verstöße durch hessische Polizeibedienstete.

Weiter auf DataAgenda lesen

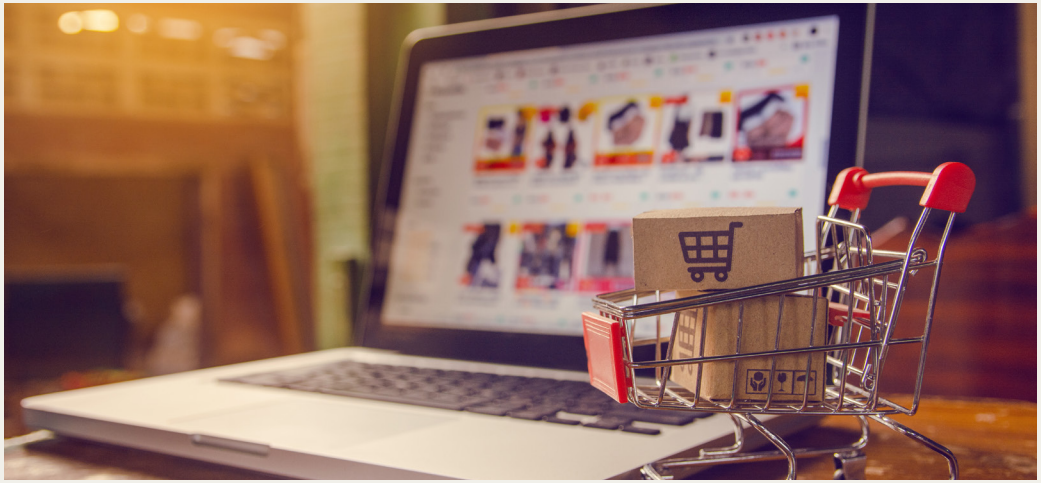

Foto: NaMaKuKj, Adobe Stock

GDD-Stellungnahme: Datenschutzkonformer Online-Handel mittels Gastzugang

Die Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. hat sich zum DSK-Beschluss „Datenschutzkonformer Online-Handel mittels Gastzugang“ im Rahmen einer detaillierten und differenzierten Stellungnahme geäußert.
Anlasspunkt für die aktuelle Stellungnahme der GDD sind zum einen der am 24.03.2022 veröffentlichte DSK-Beschluss „Datenschutzkonformer Online-Handel mittels Gastzugang “ sowie zum anderen die Berichterstattung durch die Tagespresse, dass es im Rahmen der DSK Bestrebungen gebe, den Handel mit Adressen einzuschränken. Mit ihrer Stellungnahme möchte die GDD zu einem differenzierten und sachlichen Diskurs über die Verarbeitung personenbezogener Daten zum Zwecke der Werbung und des Adresshandels beitragen.

Anders als das BDSG a.F. enthalte die DS-GVO keinen spezifischen Erlaubnistatbestand für die Verarbeitung personenbezogener Daten für Werbezwecke. Entscheidend seien damit die allgemeinen Erlaubnistatbestände, insbesondere Art. 6 Abs. 1 lit. f) DS-GVO (sog. Interessenabwägung). Angesichts des Wortlauts von Erwägungsgrund 47 S. 7 DS-GVO lasse sich dabei nicht infrage stellen, dass auch Direktwerbung grundsätzlich ein berechtigtes Interesse im Sinne der DS-GVO darstellen kann. Denn der zitierte Satz besage explizit: „Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden.“ Welche werblichen Verarbeitungen konkret noch über die Interessenabwägung legitimiert werden könnten und welche der Einwilligung der betroffenen Person bedürfen, sei allerdings strittig.

„Die Zulässigkeit des Adresshandels bzw. der Datenweitergabe zu Werbezwecken allgemein betreffen schließlich Grundsatzfragen der Auslegung der DS-GVO, bezüglich derer es zunächst einer Abstimmung der Aufsichtsbehörden auf europäischer Ebene (EDSA) bedarf“, so die GDD in ihrer Stellungnahme. Die GDD weist darauf hin, dass ein Alleingang der deutschen Behörden in Form einer restriktiven Auslegung nicht zielführend im Sinne einer einheitlichen Auslegung der DS-GVO in den Mitgliedstaaten wäre und dazu führen würde, dass die nationalen Unternehmen in einer ohnehin schwierigen wirtschaftlichen Gesamtsituation nicht unerheblich belasten würden.

Foto: NDABCREATIVITY, Adobe Stock

Datenschutz im Vereinsleben

Mit der Broschüre „Datenschutz im Verein“, die die Landesbeauftragte für Datenschutz und Informationsfreiheit NRW (LDI LNRW) nun in der zweiten Auflage veröffentlicht, versucht die LDI die Wissenslücken weiter zu schließen, die es beim Umgang mit personenbezogenen Daten innerhalb der Vereine geben kann.

In Anbetracht der Tatsache, dass in Deutschland 620.000 Vereine mit über 50 Millionen Vereinsmitgliedern existieren, scheinen die Adressaten der Broschüre auch für die Betrachtungen einer Datenschutz-Aufsichtsbehörde nicht ganz unbedeutend zu sein. Personenbezogene Daten werden in Vereinen viel häufiger verarbeitet, als man vielleicht denkt. Zu der klassischen Datenverarbeitung bei der Pflege der Mitgliederkartei, über Adresslisten der Fördernden, Veröffentlichungen im Internet, Veröffentlichungen von Fotos aus Vereinsveranstaltungen oder der Frage, was mit den Daten der Ex-Mitglieder zu passieren hat, wenn sie ausgetreten sind, dürfte pandemiebedingte Fragen, wie zu Verarbeitungstätigkeiten im Rahmen von 3G-Regelungen, hinzugekommen sein.

Wie die LDI NRW bereits im Vorwort ihrer Broschüre herausarbeitet, wird die Umsetzung der DS-GVO gerade in den zumeist ehrenamtlich geführten kleineren Vereinen häufig als besondere Herausforderung empfunden. Vielfach sind weder Zeit noch Mittel für eine umfangreiche Prüfung und Umsetzung der Anforderungen der DS-GVO vorhanden. Dies auch deshalb, weil es zwar zahlreiche Hilfestellungen zur Umsetzung der DS-GVO – etwa im Internet – gibt, aber häufig unklar bleibt, inwieweit diese für Vereine relevant sind.
Die Broschüre kann unter folgendem Link abgerufen werden:

Es sei darauf hingewiesen, dass auch das BayLDA einige nützliche Informationen für Vereine zur Verfügung stellt. In seinem Praxisratgeber DS-GVO Anforderungen für Vereine findet sich ein kurzer Überblick über die wichtigsten Themen und Vorkehrungen sowie Templates für ein Verzeichnis der Verarbeitungstätigkeiten und andere praxisrelevante Muster:

www.lda.bayern.de/media/muster_1_verein.pdf
www.lda.bayern.de/media/muster_1_verein_verzeichnis.pdf

Foto: prima91, Adobe Stock

Hessische Aufsichtsbehörde: Zoom unter Einhaltung von Auflagen nutzbar

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) hatte im August 2021 die Senatskanzlei der Freien und Hansestadt Hamburg (FHH) offiziell gewarnt, die Videokonferenzlösung von Zoom Inc. in der sog. on-demand-Variante zu verwenden. Dies verstoße gegen die DS-GVO, da eine solche Nutzung mit der Übermittlung personenbezogener Daten in die USA verbunden sei. In diesem Drittland bestehe kein ausreichender Schutz für solche Daten. Dies sei durch den Europäischen Gerichtshof in der Entscheidung Schrems II bereits vor über einem Jahr (C-311/18) festgestellt worden und das bis dahin geltende Privacy-Shield als Übermittlungsgrundlage außer Kraft gesetzt. Ein Datentransfer sei daher nur unter sehr engen Voraussetzungen möglich, die bei dem geplanten Einsatz von Zoom durch die Senatskanzlei nicht vorliegen. Die Daten von Behördenbeschäftigten und externen Gesprächsbeteiligten würden auf diese Weise der Gefahr einer anlasslosen staatlichen Massenüberwachung in den USA ausgesetzt, gegen die keine ausreichenden Rechtsschutzmöglichkeiten bestehen.

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit (HBDI) sieht diese Probleme ebenfalls, stellt aber eine „Lösung“ vor, die bei Einhaltung des „Hessischen Modells“ dazu führen kann, dass Zoom datenschutzkonform und sicher von Hessischen Hochschulen genutzt werden könne.

Beim „Hessischen Modell“ stellen die Hochschulen sicher, dass sie

- einen von Zoom unabhängigen Auftragsverarbeiter mit Sitz in der EU beauftragen, damit Videokonferenzsysteme auf Servern in der EU zu betreiben und mit ihnen abzurechnen sind,
- eine Ende-zu-Ende-Verschlüsselung aller Inhaltsdaten zur Verfügung zu stellen,
- den Abfluss personenbezogener Daten von Studierenden in die USA und den Zugriff auf solche Daten aus den USA heraus verhindern,
- die Nutzung von Zoom auf Lehrveranstaltungen beschränken,
- ein alternatives datenschutzkonformes Videokonferenzsystem für andere Zwecke oder für Lehrpersonen, die nicht mit Zoom arbeiten wollen, anbieten,
- die Lehrenden und Studierenden über weiterführende, unterstützende Maßnahmen zum Schutz der informationellen Selbstbestimmung ausführlich informieren.

Setzen die Hessischen Hochschulen dieses hier beschriebene „Hessische Modell“ in der praktischen Nutzung von Zoom um, bewertet der HBDI das verbleibende Risiko für die Teilnehmenden an Zoom-Videokonferenzen bei den bestehenden Wahlmöglichkeiten mit den datenschutzrechtlichen Vorgaben als vereinbar.

Impressum

DATAKONTEXT GmbH
Augustinusstraße 9d
50226 Frechen

Telefon: +49 2234 98949-30
Fax: +49 2234 98949-32

kundenservice@datakontext.com
www.datakontext.com

Geschäftsführung:
Dr. Karl Ulrich
Amtsgericht Köln, HRB 82299

Newsletter

Möchten Sie bei Erscheinen der aktuellen Datenschutz Newsbox informiert werden und so keine Ausgabe mehr verpassen? Dann tragen Sie sich unverbindlich und kostenlos ein unter:
www.datakontext.com/newsletter