NEWS BOX DATENSCHUTZ

AUSGABE
4/2021

INHALTSVERZEICHNIS

DATAKONTEXT

Levent Ferik

EDITORIAL

Was ist der Unterschied zwischen der Berliner Beauftragten für Datenschutz und Informationsfreiheit und der Katholischen Datenschutzaufsicht (KDSA)? Das scheint nur auf den ersten Blick eine einfache Frage zu sein. Vielen war oder ist ggf. gar nicht bekannt, dass es eine Katholische Datenschutzaufsicht gibt. Die Antwort ist auf jeden Fall: Die eine Aufsicht hält Zoom für „zulässig", die andere jedoch, und das ist ja nun hinlänglich bekannt, ist der Auffassung, dass die Nutzung rechtswidrig ist. Grundsätzlich ist das immer noch ein nicht ganz so einfaches Thema. Einen Kriterienkatalog zu datenschutzkonformen Videokonferenzsystemen gibt es übrigens nicht nur von der DSK, sondern auch aus der Feder der Datenschutzaufsicht der Evangelischen Kirche in Deutschland (EKD).
Und wussten Sie, dass auch die Datenschutz-Aufsichtsbehörden nicht davor gefeit sind, „getrollt" zu werden? Wie sonst wäre es wohl zu erklären, dass der LfDI BaWü auf seinem Mastodon-Auftritt davon berichtet, mit folgender Eingabe konfrontiert worden zu sein: „Sind Grabsteine eigentlich DS-GVO-konform?".
Warum die Frage mit „Ja" zu beantworten ist, erfahren Sie ebenfalls auf Mastodon. Vielleicht ist die mutmaßliche Troll-Attacke ja die „ausgleichende Gerechtigkeit" dafür, dass sich die Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen in ihrem 3. Jahresbericht mit einer datenschutzrechtlichen Problematik beschäftigt (Ziffer 9.7), die durch ein „unzulässiges, schulisch organisiertes ‚Freundebuch' der Klasse" entstanden ist? Durch ein solches Verhalten „bestehe gerade bei Kindern im Grundschulalter die Gefahr, dass auch besonders sensible personenbezogene Daten Eingang in das Buch finden, wie etwa die Religionszugehörigkeit der Familie eines Kindes, wenn zum Beispiel ein sonntäglicher Kirchenbesuch geschildert würde".
Wenn es aber tatsächlich ein solches „Instant-Karma" für datenschutzrechtliche Verfehlungen gäbe, würde es wohl auch den Gesundheitsminister treffen müssen, und zwar für seine Pläne, eine Triage-Software einzuführen, die Notfälle in den Krankenhäusern sortieren soll (Artikel 22 DS-GVO lässt grüßen ...).
Damit kommen wir in diesem Editorial zu den einzigen zwei „positiven" Datenschutz-Innovation: Eine wunderschön vertonte Datenschutzinformation für eine Homepage in professioneller Hörbuch-Qualität sowie eine Möglichkeit, alle Webseiten der deutschen Datenschutzbehörden über nur ein Suchfeld durchsuchen (credit goes to https://twitter.com/kleibold23) zu können.

Bleiben Sie gesund,
Ihr Levent Ferik

Sagen Sie uns Ihre Meinung
kundenservice@datakontext.com

Foto: Pixel-Shot, Adobe Stock

Korruptionsbekämpfung und Datenschutz

Datenschutzbeauftragte sind zumeist „Allrounder". Das müssen sie auch oftmals sein, da sie im Unternehmen als Schnittstelle fungieren (müssen). Sie müssen die Prozesse der Marketingabteilung genauso gut kennen, wie die Welt der IT oder der IT-Sicherheit und natürlich auch die der Personalabteilung, um ihrer originären Aufgabe (Beratung und Überwachung) nachkommen zu können. Das hat seine Ursache darin, dass das Datenschutzrecht in immer größerem Maße zu einem Querschnittsrecht der Informations- und Wissensgesellschaft wird.
Viele Unternehmen bekennen sich zur weltweiten Bekämpfung von Korruption in all ihren Erscheinungsformen, unterstützen nationale und internationale Anstrengungen und lehnen jegliches korruptes Verhalten ab.

Wie bei allen anderen im Unternehmen anstehenden Aufgaben kann die Geschäftsleitung den Aufbau und den Betrieb eines Compliance-Management-Systems delegieren. In der Regel übernimmt diese Aufgabe ein Compliance-Officer oder, je nach Ausgestaltung und Größe des Unternehmens, ein Chief Compliance Officer, welche dann als Hauptakteure eines Compliance-Management-Systems (CMS) für die Einhaltung von gesetzlichen Vorschriften eintreten, in dem sie zusammen mit allen anderen Beschäftigten des Unternehmens dafür Sorge tragen, dass sowohl unternehmensinterne Richtlinien/Anweisungen als auch gesetzliche Regelungen sichergestellt und überwacht werden.
Die damit einhergehende Verarbeitung von teilweise sehr sensiblen Informationen über die betroffenen Personen bedingt, dass der Datenschutzbeauftragte auch im Bereich der Compliance intensiv eingebunden werden muss.
Insbesondere unter diesem Aspekt kann die aktuelle Publikation „Korruptionsbekämpfung – Ein Leitfaden für Unternehmen" auch für alle Datenschutzbeauftragten als Lektüre empfohlen werden. Der Leitfaden ist als Gemeinschaftsprojekt unter Beteiligung von Alliance for Integrity, Deutsches Global Compact Netzwerk sowie des Deutschen Instituts für Compliance e.V. entstanden. Auf mehr als 100 Seiten beleuchten nationale Compliance-Expertinnen und Experten verschiedene Aspekte rund um das Thema Korruptionsprävention, darunter rechtliche Grundlagen, Whistleblowing, Compliance in Grauzonen, Digitalisierung und vieles mehr.
Für Datenschutzbeauftragte besonders interessant dürfte das Kapitel 3.7 „Interne Untersuchungen" sein. Aber auch die Lektüre der übrigen Kapitel dürfte dem Datenschutzbeauftragten ein größeres „Systemverständnis" und eine bessere „Schnittstellenarbeit" ermöglichen, sodass der gesamte Leitfaden nicht nur Datenschutzbeauftragten empfohlen werden kann, die „über den Tellerrand schauen" wollen, sondern generell allen Beteiligten, die eine Schnittstelle zum unternehmenseigenen Compliance-Management-System darstellen.

Live Online-Schulung

Foto: fotogestoeber, Adobe Stock

GDD-BASIS-SCHULUNG TEIL 1

Einführung in den Datenschutz für die Privatwirtschaft

3. – 4. Mai, 6. – 7. Mai und 11. Mai 2021 | online
Referenten: RA Andreas Jaspers,
Prof. Dr. Rolf Schwartmann, Thomas Müthlein

Schwerpunkte:

- ✓ Einführung in das Datenschutzrecht: Im Fokus Arbeitnehmer- und Kundendatenschutz (inkl. Fallübungen)
- ✓ Umsetzung des Datenschutzes in der Praxis

Jetzt anmelden:
www.datakontext.com

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT

Foto: Tierney, Adobe Stock

Vermerk zu Abdingbarkeit von Art. 32 DS-GVO

Eine als Vermerk veröffentlichte Publikation des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI) fand in den letzten Tagen in Datenschutzkreisen große Beachtung. Darin beschäftigt sich der HmbBfDI mit der Frage, ob betroffene Personen in ein niedrigeres Schutzniveau einwilligen können als rechtlich geboten ist. Es geht also um die Frage, ob oder inwieweit es sich bei den Vorgaben des Art. 32 DS-GVO um zwingende, nicht zur Disposition der betroffenen Person stehende Vorgaben handelt. Die Frage, ob Art. 32 DS-GVO zwingendes, nicht zur Disposition stehendes Recht darstellt, ist besonders praxisrelevant, weil dies teilweise mit dem Argument bejaht wird, dass die DS-GVO einen europäischen Mindeststandard des Systemdatenschutzes schaffen wolle.

Auf der anderen Seite würde es jedoch eine erhebliche Beschränkung der Entscheidungsfreiheit der betroffenen Personen bedeuten, wenn eine Verarbeitung ihrer personenbezogenen Daten, die sie ausdrücklich wünschen, mit Verweis auf den Systemdatenschutz nicht durchgeführt werden kann. Als praxisrelevantes Beispiel werden in dem Vermerk Arztpraxen, Steuerberater oder Anwälte genannt, bei denen ein undifferenziertes Festhalten an dieser Auffassung dazu führen würde, dass die Auskünfte oder die Übermittlung dringend benötigter Unterlagen per einfacher E-Mail nicht durchgeführt würden, da sie befürchten müssten, Art. 32 DSGVO zuwiderzuhandeln, selbst wenn die betroffene Person ausdrücklich in die unsichere Übermittlungsart einwilligt hat.
Aufgrund dieser widerstreitenden Interessen sei die Frage der Abdingbarkeit des Systemdatenschutzes daher nicht pauschal zu beantworten. Die Antwort müsse insbesondere zwischen dem Verantwortlichen oder Auftragsverarbeiter und der betroffenen Person differenzieren.
Der HmbBfDI zieht nach einer ausführlichen Betrachtung der Sach- und Rechtslage folgendes Fazit:
„Der Verantwortliche und der Auftragsverarbeiter haben die nach Art. 32 DS-GVO erforderlichen Maßnahmen zwingend umzusetzen und vorzuhalten. Betroffene Personen können in die Herabsetzung des nach Art. 32 DS-GVO vorgesehenen Schutzniveaus, allerdings bezogen auf ihre eigenen Daten, im Einzelfall einwilligen, wenn die Einwilligung freiwillig im Sinne des Art. 7 DS-GVO erfolgt. Dies setzt jedoch voraus, dass der Verantwortliche die nach Art. 32 DS-GVO erforderlichen Schutzvorkehrungen grundsätzlich vorhält und der betroffenen Person auf Verlangen zur Verfügung stellt, ohne dass der betroffenen Person Nachteile dadurch entstehen."
Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI)

Foto: WhataWin, Adobe Stock

Meldung einer Datenpanne infolge des „Hafnium Hacks"

Nach ErwG 85 der DS-GVO kann eine Verletzung des Schutzes personenbezogener Daten – wenn nicht rechtzeitig und angemessen reagiert wird – einen physischen, materiellen oder immateriellen Schaden für natürliche Personen nach sich ziehen, wie etwa Verlust der Kontrolle über ihre personenbezogenen Daten oder Einschränkung ihrer Rechte, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die betroffene natürliche Person.

Deshalb soll nach dem Willen des Verordnungsgebers der Verantwortliche, sobald ihm eine Verletzung des Schutzes personenbezogener Daten bekannt wird, die Aufsichtsbehörde von der Verletzung des Schutzes personenbezogener Daten unverzüglich und, falls möglich, binnen höchstens 72 Stunden, nachdem ihm die Verletzung bekannt wurde, unterrichten, es sei denn, der Verantwortliche kann im Einklang mit dem Grundsatz der Rechenschaftspflicht nachweisen, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen führt.

Vor dem Hintergrund, dass bei einem erfolgreichen Angriff über den sog. „Hafnium Hack" die Möglichkeit der Ausführung von Schadsoftware besteht und die Angreifer über die Sicherheitslücke Zugriff auf das Unternehmensnetzwerk erlangen können, haben sich die Datenschutzaufsichtsbehörden dahingehend geäußert, dass im Fall eines festgestellten Datenabflusses ein Data Breach bei der zuständigen Datenschutz-Aufsichtsbehörde gemeldet werden muss. Darüber hinaus könne in einem solchen Fall zudem eine Benachrichtigungspflicht an betroffene Personen bestehen.

Zur Beseitigung der Unsicherheiten, die sich aus den diversen Stellungnahmen der Aufsichtsbehörden zum Thema „Meldung einer Datenpanne infolge eines Hafnium Hacks" bei den Verantwortlichen ergeben haben, hat sich eine Unterarbeitsgruppe des AK Datenschutzes der Bitkom mit der Auslegung der Art. 33 und 34 DSGVO auseinandergesetzt, um Unternehmen bei Meldungen von Datenschutzverletzungen fachlich zu unterstützen. Insbesondere wurde die herrschende Meinung über den Begriff des »Bekanntwerdens« einer Verletzung des Schutzes personenbezogener Daten untersucht, mit dem Ziel, der Harmonisierung der Auslegung durch Unternehmen und den Behörden.

Als Ergebnis dieser Bemühungen hat der BITKOM den Leitfaden „Datenschutzverletzung und Meldung im Kontext des ‚Hafnium Hacks'" veröffentlicht.

Bitkom e.V.
www.bitkom.org

Foto: Production Perig, Adobe Stock

BSI nun auch auf Mastodon (daten-schutzfreundliche Twitter-Alternative) vertreten

Im November 2017 richtete der Landesbeauftragte für den Datenschutz und die Informationsfreiheit (LfDI), Dr. Stefan Brink, einen Twitter-Account für seine Behörde ein und twitterte mit großem Erfolg zu aktuellen Themen aus der Welt des Datenschutzes und der Informationsfreiheit. Mit dem Angebot wollte der LfDI seine Zielgruppen noch besser mit aktuellen Informationen erreichen, in direkten Dialog mit den Bürgerinnen und Bürgern treten und sich besser mit anderen Institutionen und öffentlichen Stellen vernetzen. Dies gelang ihm auch von Beginn an.

Nach eigenen Angaben war die Twitternutzung dabei eingebettet in ein ganzes Maßnahmenpaket, mit dem die Behörde ihrer Richtlinie zur Nutzung Sozialer Medien gerecht werden wollte. Ende Dezember 2019 jedoch gab der LfDI BW seinen Rückzug von Twitter bekannt. Brink sah sich vor dem Hintergrund der Entscheidung des Bundesverwaltungsgerichts BVerwGE 6 C 15.18 nicht mehr in der Lage, den Auftritt seiner Behörde auf Twitter vertreten zu können.

Nach Urteilen des Europäischen Gerichtshofes und des Bundesverwaltungsgerichts sind unter anderem Behörden beim Betrieb einer Fanpage oder eines Twitter-Accounts ebenso als Mitverantwortliche zu sehen wie die Plattformbetreiber selbst. Sie sind rechenschaftspflichtig und müssen erklären können, welche Daten auf dem Account oder der Fanpage erhoben und wie sie verarbeitet werden. Das führt auch dazu, dass zwischen den beiden gemeinsam Verantwortlichen ein Vertrag gemäß Artikel 26 DS-GVO abgeschlossen werden muss, in dem die Wahrnehmung der Pflichten durch die Parteien, wie beispielsweise die Information gegenüber Betroffenen, transparent und eindeutig geregelt wird. Da solche Verträge in datenschutzgerechter Form nicht vorlagen und bis heute nicht vorliegen und damit unklar bleibt, was mit Daten geschieht, die bei Twitter landen, hat sich der Landesbeauftragte von dort zurückgezogen.

Eine neue digitale Heimat fand der LfDI auf der Social Media Plattform Mastodon. Seit dem 19. Januar 2021 nutzt der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg die Social Media Plattform Mastodon (https://bawü.social/@lfdi). Nutzer_innen können dem Landesbeauftragten unter: **@lfdi@bawü.social** folgen.

Anders als bei Twitter ist Mastodon dezentral organisiert. Es gibt somit keine zentralen Server, die alle Nutzer_innen gleichermaßen erfassen, sondern eine Vielzahl von kleinen Servern, die miteinander vernetzt sind. Dem übergeordnet ist das Fediverse – ein föderiertes Netzwerk, bei dem sich diverse Plattformen untereinander verbinden können. Mastodon ist Teil dieses Fediverse. Die Nachrichten in dem Netzwerk werden „Toots“ oder auf Deutsch „Tröts“ genannt und können aus bis zu 500 Zeichen bestehen.

Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist seit dem 31.03.2021 auf dem Mikroblogging-Dienst Mastodon präsent. Damit ist das BSI die zweite Bundesbehörde überhaupt, die diese auf freier Software basierende, datenschutzfreundliche Alternative zum Kurznachrichtendienst Twitter nutzt.

Das BSI gibt bekannt, bei Mastodon unter anderem regelmäßig Kurznachrichten zu verschiedenen technischen Themen wie Zwei-Faktor-Authentifikation zu veröffentlichen.

Das BSI nutzt die Instanz des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit in Deutschland (BfDI) social.bund.de, die 2020 als datenschutzkonforme Alternative zu Twitter gestartet wurde. So beabsichtigen BSI und BfDI auf ihren Mastodon-Präsenzen auch über gemeinsame Vorhaben zu informieren.

Der Link zur Mastodon-Präsenz des BSI lautet:
https://social.bund.de/@bsi


Foto: Looker_Studio, Adobe Stock

Datenschutz und Homeoffice

vom Provisorium zum Dauerzustand

5. Mai 2021 | online Referent:
Dr. Niels Lepperhoff

Online-Kompaktkurs

Schwerpunkte:

✓ Datenschutzrisiken im Homeoffice
✓ Risiken für die Vertraulichkeit, Integrität und Verfügbarkeit personenbezogener Daten
✓ Nutzung privater Geräte

Jetzt anmelden: www.datakontext.com

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT

Datenschutz-Anforderungen beim Outsourcing von IT

Foto: Tuomas Kujansuu, Adobe Stock

Der Bayerische Datenschutzbeauftragte für den Datenschutz (BayLfD) hat einen Leitfaden zum Outsourcing kommunaler IT herausgegeben. Der Leitfaden soll die Kommunen bei der Auslagerung der kommunalen Informationstechnologie unterstützen. Es richtet sich daher zwar explizit an Kommunen, die eine solche Auslagerung in Betracht ziehen. Jedoch kann der Leitfaden auch für Unternehmen aus der Privatwirtschaft eine gute Hilfe sein.
Unter Ziffer „2.2 Allgemeine Kriterien aus dem Datenschutzrecht“ geht das BayLfD auch auf die allgemeinen Kriterien für eine Auslagerung der IT ein, die sich insbesondere aus Art. 28 DS-GVO ergeben. Als zu erfüllende Mindestinhalte einer Auftragsverarbeitung nach Art. 28 DS-GVO geht der Leitfaden daher ausführlich auf folgende Punkte ein:

1. Sorgfältige Auswahl des Auftragsverarbeiters
2. Wahrung des Datengeheimnisses
3. Sicherstellung des Zugriffs auf die Daten
4. Tatsächliche Überprüfungen
5. Erteilung fachkundiger Weisungen
6. Sicherstellung von Prüfungsrechten
7. Regelung einer Rückgabe der Daten
8. Technisch-Organisatorische Aspekte

Ein beigefügtes Ablaufschema für eine geplante Auslagerung von IT-Dienstleistungen rundet den Leitfaden ab.

Whistleblowing zwischen Gesellschaftsrecht, Arbeitsrecht und Datenschutz

Foto: DOC RABE Media, Adobe Stock

Eine Kooperation aus der Universität Bonn, der TH Köln, der GDD e.V. sowie dem Berufsverband der Compliance Manager lädt am Mittwoch, den 5. Mai 2021, zu einem Diskussionsnachmittag ein. Das Leitthema lautet: „**Hinweisgeberschutzgesetz: Whistleblowing zwischen Gesellschaftsrecht, Arbeitsrecht und Datenschutz – Herausforderungen anlässlich der Umsetzung der Richtlinie 2019/1937/EU –** “ Die Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden (Richtlinie (EU) 2019/1937), muss 2021 umgesetzt werden. Hierzu existiert bereits ein Referentenentwurf. Doch was genau muss getan werden? Was kann die Praxis bereits jetzt tun? Diese und andere Fragen werden in einem Diskussionsnachmittag am 5. Mai 2021 ab 14:00 Uhr online besprochen. Mitwirken werden u.a. Prof. Dr. Rolf Schwartmann, Vorsitzender der GDD, und Prof. Dr. Gregor Thüsing, Vorstandsmitglied der GDD.

Es setzt sich zunehmend die Erkenntnis durch, dass ein erhebliches öffentliches Informationsinteresse an den Hinweisen von Whistleblowern besteht. Dazu tragen die verschiedenen Skandale bei, die sich in der letzten Zeit in großen deutschen Unternehmen ereignet haben. Europa hat nun gehandelt. Die Richtlinie muss 2021 umgesetzt werden und es existiert bereits ein Referentenentwurf. Doch was genau muss getan werden? Was kann die Praxis bereits jetzt tun?

Diese und andere Fragen zu diskutieren laden die Kooperationspartner zu einer kostenlosen Diskussionsveranstaltung ein. Die Veranstaltung erfolgt per Zoom.

Foto: wladimir1804, Adobe Stock

Anforderungen an eine datenschutzkonforme Kontaktverfolgungs-App

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) hat Erfordernisse für eine datenschutzkonforme Kontaktverfolgungs-App zur Bewältigung der Corona-Pandemie in einer Stellungnahme zusammengefasst. Die DSK betont die Notwendigkeit, Kontaktverfolgung mithilfe von Apps im Einklang mit datenschutzrechtlichen Vorgaben zu entwickeln.

Das könne, nach Meinung der DSK, insbesondere mit einer möglichst dezentralen Speicherung der erfassten Daten und einer sicheren Verschlüsselung sowie Schlüsselverwaltung gelingen. Für erforderlich hält sie auch, die Einhaltung der zentralen Sicherheitsmaßnahmen nachzuweisen bzw. zu dokumentieren.
Bislang gibt es für eine bundesweit einheitliche, datensparsame digitale Infektionsnachverfolgung keine gesetzliche Regelung. Die Beauftragten regen die Schaffung einer solchen gesetzlichen Regelung an.
Die App Luca des Unternehmens culture4life GmbH hat dabei in den vergangenen Wochen besonderes mediales Interesse erfahren. Culture4life hat bei mehreren Aufsichtsbehörden um ein datenschutzrechtliches Votum zu der Lösung ersucht. Darüber hinaus haben einige Länder und Landkreise die Absicht bekundet, diese App einzuführen und dann eine Verbindung zu den jeweiligen Gesundheitsämtern herzustellen.
Die DSK fordert das Unternehmen dennoch auf, weitere Anpassungen an dem System vorzunehmen, um den Schutz der teilnehmenden Personen weiter zu erhöhen.
Die DSK gibt zudem bekannt, dass sie außerdem eine eigenständige Orientierungshilfe für alle Betreiber solcher Kontaktverfolgungssysteme mit allgemeinen Anforderungen für die digitale Kontaktnachverfolgung erarbeiten und kurzfristig veröffentlichen werde. Die DSK fordert die Gesetzgeber auf Landes- und Bundesebene auf, bundeseinheitliche gesetzliche Regelungen zur digitalen Kontaktnachverfolgung zu schaffen. Dabei sei auch zu prüfen, inwieweit mit datensparsameren Verfahren das Ziel der Kontaktnachverfolgung im Rahmen der aktuellen Pandemiebekämpfung erreicht werden kann.

mit Muster Löschkonzept + weitere Arbeitshilfen zum Download

Löschen nach DS-GVO
in der Praxis
Sascha Kremer

1. Auflage 2020
122 Seiten / DIN A 4
ISBN: 978-3-89577-851-3
99,99 € inkl. E-Book
und Arbeitshilfen
(PDF Excel, Word)

Bestellen Sie direkt unter:
datakontext.com/loeschkonzepte

DATAKONTEXT

Foto: ty, Adobe Stock

Per E-Mail generiertes Double-Opt-In hat keine Gültigkeit für Telefon-Werbung

Für Anrufe bei Verbrauchern zu Zwecken der Direktwerbung sieht das UWG (§ 7 Abs. 2 Nr. 2) keine Ausnahme vom Einwilligungserfordernis vor, sodass ein solches Nutzen von Telefonnummern ohne vorherige Einwilligung wegen der besonderen Auswirkungen dieser Werbeform (stärkere Belästigung/Störung) datenschutzrechtlich an den überwiegenden schutzwürdigen Interessen der betroffenen Personen, gemäß Art. 6 Abs. 1 Satz 1 lit. f DS-GVO, scheitert.

Bei Werbung mit einem Telefonanruf gegenüber einem sonstigen Marktteilnehmer (B2B) kommt es für die Zulässigkeit, gemäß § 7 Abs. 2 Nr. 2 UWG, darauf an, dass von dessen zumindest mutmaßlicher Einwilligung ausgegangen werden kann. Im B2B-Bereich stehen deshalb bei einem Nutzen von Telefonnummern für Werbeanrufe datenschutzrechtlich nicht von vorneherein überwiegende schutzwürdige Interessen der telefonisch anzusprechenden Gewerbetreibenden nach Art. 6 Abs. 1 Satz 1 lit. f DS-GVO entgegen (vgl. Orientierungshilfe der Aufsichtsbehörden zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der Datenschutz-Grundverordnung (DS-GVO)).

In einem Rechtsstreit vor dem OVG Saarlouis wurde auch über die Frage verhandelt, ob sich der Werbende auf eine mutmaßlich im Double-Op-in Verfahren eingeholte Einwilligung berufen kann, wenn der betrachtete Werbekanal ein Telefonanruf ist.

Die Werbetreibende gab an, dass eine Einwilligung in die Telefonwerbung vorliege, welche jedoch im Rahmen eines Gewinnspiels für Zwecke des Direktmarketings durch ein vollständig durchlaufenes Double-Opt-In-Verfahren eingeholt wurde. Belegen wollte dies die Werbetreibende mit dem Ausdruck einer Online-Registrierung. Darin waren auch eine E-Mail-Adresse und der Eingang einer Bestätigungsmail vermerkt. Da aber die Betroffenen angaben, weder die genannte Internetadresse noch die E-Mail-Adresse zu kennen, musste das Gericht feststellen, dass der vorgelegte Ausdruck rein technisch betrachtet nichts darüber aussagt, ob der Inhaber der betreffenden E-Mail-Adresse auch Besitzer der angegebenen Rufnummer ist.

Rechtsprechungsdatenbank Saarland:
www.recht.saarland.de

Foto: peterschreiber.media, Adobe Stock

Gutachten zum vorbeugenden Rechtsschutz bei Bußgeldern

Angesichts der drastischen Bußgeldhöhen, die in den meisten Fällen geeignet wären, den Jahresgewinn eines Unternehmens abzuschöpfen, stellen Bußgelder nicht nur eine latente Sanktionsgefahr dar, sondern enorme, unter Umständen gar existenzielle, finanzielle Risiken für die Verantwortlichen.

Die bloße Verwicklung in ein Bußgeldverfahren begründet regelmäßig bereits eine nachhaltige und teilweise irreparable Rufschädigung, die selbst ein „Freispruch" nicht wiedergutzumachen vermag. Aufgrund dieser im schlimmsten Fall image- und wirtschaftlich Existenz-vernichtenden Auswirkungen, entfalten Bußgeldandrohungen im datenschutzrechtlichen Bereich eine enorme Abschreckungswirkung. Konflikte entstehen hierdurch für die Verantwortlichen vor allem in Anbetracht der teils scharfen Sanktionspraxis einiger Datenschutzaufsichten.
Schutz könnte hier der Verwaltungsrechtsweg bieten. Danach kann unter bestimmten Voraussetzungen verwaltungsgerichtlicher Rechtsschutz zur vorbeugenden Abwehr von Bußgeldern in Anspruch genommen werden. Solange die Behörden nämlich auch bei ungesicherter Rechtslage unmittelbar Bußgelder verhängen, ohne zuvor auf mildere verwaltungsrechtliche Maßnahmen wie Anweisung und Anordnung zurückzugreifen, werden die Verantwortlichen den Rechtspositionen der Behörde aus wirtschaftlichen Gründen grundsätzlich Folge leisten müssen. Durch ihr Vorgehen spricht sich die Aufsicht faktisch eine Art Deutungshoheit über die Auslegung der unbestimmten Rechtsbegriffe der DS-GVO zu.
Hierzu hat der Vorstandsvorsitzende der GDD und Leiter der Forschungsstelle Medienrecht der TH Köln, Professor Rolf Schwartmann, zusammen mit Lucia Burkhardt das Gutachten „Vorbeugender verwaltungsgerichtlicher Rechtsschutz zur Abwehr drohender Bußgeldverfahren im Datenschutzrecht" im Auftrag der Freenet AG verfasst, welches Sie auf den Seiten der Gesellschaft für Datenschutz und Datensicherheit (GDD e.V.) frei verfügbar abrufen können.

Foto: weyo, Adobe Stock

Sozialdatenschutz nach Geltung der DS-GVO

Ein neues Arbeitspapier des Bayerischen Landesbeauftragten für den Datenschutz (BayLfD) stellt das Nebeneinander von datenschutzrechtlichen Regelung und bereichsspezifischen Regelungen des deutschen Sozialrechts dar, die auch nach dem Wirksamwerden der DS-GVO nach wie vor im Bereich des Sozialrechts bestehen (Der Sozialdatenschutz unter Geltung der Datenschutz-Grundverordnung).
Das sog. Sozialgeheimnis gibt jeder Person einen Anspruch darauf, dass die sie betreffenden Sozialdaten von den Leistungsträgern nicht unbefugt verarbeitet werden (§ 35 Abs. 1 S. 1 SGB I). Die Regelung zum Schutz des Sozialgeheimnisses wurde bereits lange vor Wirksamwerden der DS-GVO (1976) eingeführt.

Durch DS-GVO wird auch im Bereich des Sozialrechtes der Datenschutz gestärkt. Der Bundesgesetzgeber hat das Sozialgeheimnis und die zentralen Vorschriften des Sozialdatenschutzes im Zehnten Buch Sozialgesetzbuch (SGB X) sowie die übrigen Fachgesetze den vorrangigen europäischen Vorgaben angepasst.
Aufgabe des Sozialdatenschutzrechts ist es, das grundrechtlich geschützte Interesse des Einzelnen auf Geheimhaltung der ihn betreffenden, besonders schützenswerten Sozialdaten und das staatliche Interesse an einer funktionsfähigen Sozialverwaltung weitestgehend in Einklang zu bringen. Dazu hat der Gesetzgeber mit den datenschutzrechtlichen Regelungen im Sozialgesetzbuch Normen geschaffen, die zwar das Recht auf informationelle Selbstbestimmung im notwendigen Umfang einschränken, den Betroffenen aber gleichzeitig durch eindeutige Grenzen dieser zulässigen Einschränkungen vor den nachteiligen Folgen einer Datenverarbeitung schützen (vgl. auch BfDI – Info 03 – „Sozialdatenschutz“ – Die Bürger und ihre Daten im Netz der sozialen Sicherheit).
Das Arbeitspapier des BayLfD gibt dem Leser zu Beginn einen Überblick über die bislang erfolgten Reformschritte und eine Darstellung der beibehaltenen Strukturen. Danach werden die wesentlichen Änderungen des Sozialgesetzbuches, ausgewählte Datenschutzfragen sowie Entscheidungen der Sozialgerichtsbarkeit behandelt. Abschließende Praxishinweise runden das Arbeitspapier ab.

Bayerischer Landesbeauftragter für den Datenschutz (BayLfD)

Impressum

DATAKONTEXT GmbH
Augustinusstraße 9d
50226 Frechen

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

kundenservice@datakontext.com
www.datakontext.com

Geschäftsführung:
Hans-Günter Böse, 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