NEWS BOX DATENSCHUTZ

INHALTSVERZEICHNIS

AUSGABE 3/2021

DATAKONTEXT

Levent Ferik

EDITORIAL

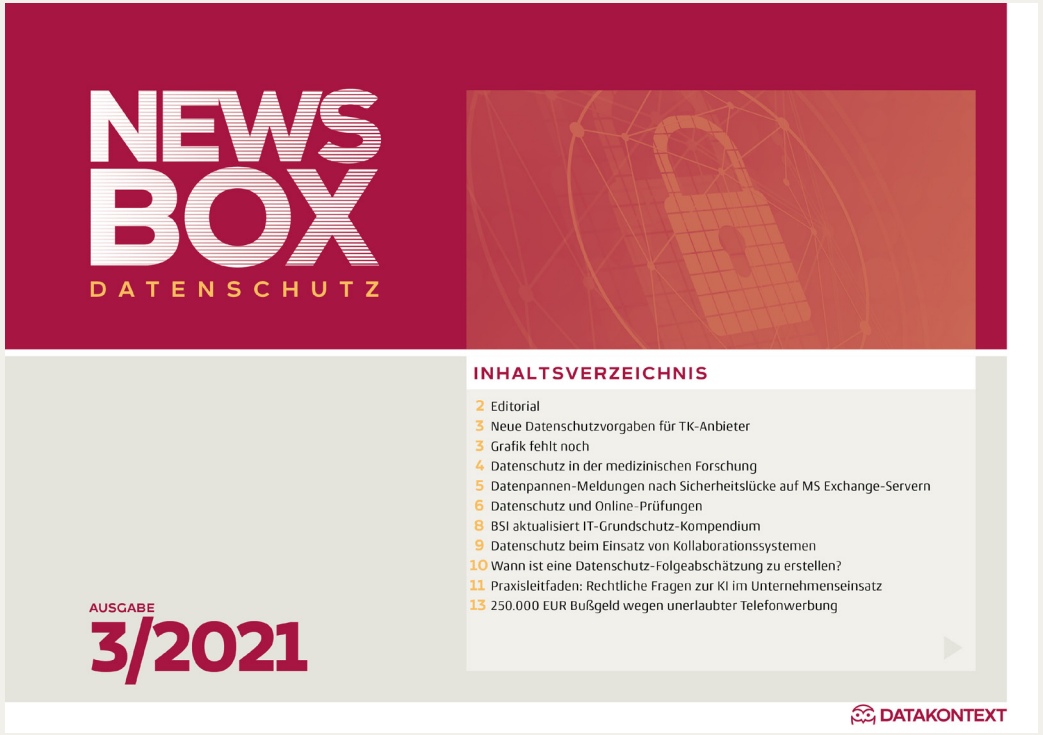
Der Gedanke, dass dem Datenschutzrecht durchaus auch eine selbstregulierende Wirkung innewohnen kann, ist zu vermuten und wäre im Bejahensfall auch nicht kritikwürdig.

Ob, aber die DS-GVO und insbesondere das Verhalten der Datenschutz-Aufsichtsbehörden zu sog. „chilling effects" führt, und damit eine „einschüchternde" oder „abschreckenden" Wirkung auf die Zivilgesellschaft hat, dürfte wohl weiter zu diskutieren sein.

Spätestens die Äußerung „der Datenschutz habe sich aufgrund seiner einschüchternden Wirkung zu einer ernsten Gefährdung der freiheitlichen Ordnung entwickelt – und zwar ganz unabhängig davon, wie bestimmte Einzelfälle zu bewerten sind", dürfte wohl nicht nur bei Vertretern der Aufsichtsbehörden zu Widerworte führen, hofft

Ihr Levent Ferik

Sagen Sie uns Ihre Meinung
kundenservice@datakontext.com



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

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

Foto: Blue Planet Studio, Adobe Stock

Neue Datenschutzvorgaben für TK-Anbieter

Am 10.02.2021 hat das Bundeskabinett den Entwurf für ein Telekommunikations-Telemedien-Datenschutzgesetz (TTDSG) beschlossen. Mittels des geplanten Gesetzes sollen die Datenschutzvorgaben für Telemedien und Telekommunikationsdienste zusammengeführt und an das geltende europäische Recht angepasst werden.

Mit dem TTDSG soll u.a. das Setzen und Auslesen von Cookies und die Verwendung von vergleichbaren Techniken zur Wiedererkennung von Nutzern, wie z.B. das Browser Fingerprinting, geregelt werden. Anders als noch der vorhergehende Referentenentwurf für ein TTDSG, zu dem die GDD im Rahmen der Verbändeanhörung eine Stellungnahme abgegeben hat, orientiert sich der Regierungsentwurf bezüglich der „Cookie-Regelung“ (§ 24 TTDSG-E) dabei unmittelbar am Wortlaut der ePrivacy-Richtlinie (2002/58/EG).

Eine Einordnung des Entwurfes bietet die Geschäftsstelle der GDD auf Ihrer Webseite.

Quelle: DataAgenda

Datenschutz in der medizinischen Forschung

In jüngster Vergangenheit ist der Datenschutz nicht selten Prügelknabe für politische Versäumnisse, wirtschaftliche Fehlplanungen oder persönliche Defizite gewesen.

Foto: vegefox.com, Adobe Stock

Thilo Weichert vom Netzwerk Datenschutzexpertise nimmt die aktuellen Diskussionen, ob der Datenschutz tatsächlich der Hemmschuh der Pandemiebekämpfung ist, zum Anlass, diese Frage näher zu beleuchten:

„Es liegt nicht am Datenschutz, dass es nicht vorangeht; es liegt daran, dass keine nachhaltigen digitalen Strukturen bestehen und dass einheitliche grundrechtsfreundliche Regelungen fehlen. Mit einem Medizinischen Forschungsgesetz könnte beides geschaffen werden“, so der ehemalige Datenschutzbeauftragte des Landes Schleswig-Holstein (2004 bis 2015).

In der neuesten Veröffentlichung des Netzwerks Datenschutzexpertise („Plädoyer für ein medizinisches Forschungsgesetz zwecks Beseitigung von Forschungshindernissen und Schutzdefiziten“) machen die Autoren Vorschläge für eine bundesweit einheitliche Regulierung im Bereich der Gesundheitsforschung. Die Corona-Krise wird dabei nur als überdeutliches Zeichen gesehen, dass in Deutschland eine nationale medizinische Forschungsinfrastruktur und dazu eine einheitliche moderne Regulierung fehlen.

Die Autoren beschreiben in ihrer Veröffentlichung die Defizite und sehen eine Möglichkeit der nachhaltigen Beseitigung in der Ausarbeitung eines „Medizinischen Forschungsgesetzes“ (MedForschG), das den bisher bestehenden gesetzlichen Wildwuchs im Bund und bei den Ländern beende und zugleich den Datenschutz der Patientinnen und Patienten sicherstellen soll. Der Vorschlag knüpft an die bestehenden vom Bundesgesundheitsministerium initiierten Regelungen eines Digitale-Versorgung-Gesetzes (DVG) mit der Schaffung eines Forschungsdatenzentrums (FDZ) und des Patientendatenschutzgesetzes (PDSG).

Quelle: Netzwerk Datenschutzexpertise

Foto: Egor, Adobe Stock

Datenpannen-Meldungen nach Sicherheitslücke auf MS Exchange-Servern

Bereits am 05.03.2021 informierte das Bundesamt für Sicherheit in der Informationstechnik (BSI) über eine neue und außerordentlich kritische Gefährdungslage, die den weit verbreiteten Microsoft Exchange Server betrifft.

Das BSI gab bekannt, dass zehntausende Exchange-Server in Deutschland nach Informationen des IT-Dienstleisters Shodan über das Internet angreifbar und mit hoher Wahrscheinlichkeit bereits mit Schadsoftware infiziert seien. Betroffen seien Organisationen jeder Größe. Infolgedessen begann das BSI, potenziell Betroffene zu informieren und empfahl, allen Betreibern von betroffenen Exchange-Servern sofort die von Microsoft bereitgestellten Patches einzuspielen.

Die Gefährdungslage wurde dabei mit der höchsten „IT-Bedrohungslage Rot" eingestuft, sodass ein sofortiges Handeln aller betroffenen Unternehmen und Institutionen als notwendig angesehen wurde.

Vor dem Hintergrund, dass bei einem erfolgreichen Angriff die Möglichkeit der Ausführung von Schadsoftware besteht und die Angreifer über die Sicherheitslücke Zugriff auf das Unternehmensnetzwerk erlangen können, erhält die Gefährdungslage auch eine datenschutzrechtliche Dimension. Über die Schwachstellen können Angreifer beispielsweise eine Webshell auf den betroffenen Systemen einrichten. Damit erlangen sie potenziell Zugriff auf sämtliche Daten des angegriffenen Exchange Servers. E-Mail-Postfächer und Adressbücher können somit ausgelesen und gesteuert werden.

Alle Datenschutzaufsichtsbehörden, die sich zu dem Fall geäußert haben, sind daher der Meinung, 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. Eine Zusammenfassung der Aufsichtsbehörden, die sich zu dieser Fragestellung positioniert haben, finden Sie hier. Eine FAQ zum Thema Sicherheitslücken bei Microsoft Exchange-Mail-Servern hat das BayLDA zusammengestellt.

Foto: vegefox.com, Adobe Stock

Datenschutz und Online-Prüfungen

Bereits im DataAgenda-Arbeitspapier 19 „Das digitale Semester FAQ“ führte Prof. Dr. Rolf Schwartmann, Leiter der Kölner Forschungsstelle für Medienrecht (TH Köln), zum Thema Klausuren, die per Videokonferenz beaufsichtigt werden sollen, wie folgt aus:

„[…] Im Regelbetrieb ist es prüfungsrechtlich demgegenüber nicht machbar, per Videokonferenz von unterschiedlichen Orten Klausuren schreiben zu lassen. Ein Problem ist die Aufsicht. Selbst wenn alle Studierenden während der Klausur ihre Kameras einschalten würden, wäre diese Maßnahme – vom Datenschutz abgesehen – ungeeignet, Täuschungsversuche auszuschließen. Schon auf der gegenüberliegenden Seite des Tisches könnte ein Team von „Prüfungs-Helfern“ sitzen.

Deren Mitwirkung wäre selbst dann im Sinne der Prüfungsgerechtigkeit verboten und nicht wirksam auszuschließen, wenn man eine „Open-Book-Prüfung“ gestattet. Wer sich bei Klausuren akustische Kontrolle über bei allen Prüflingen aktivierten Mikrofonen verspricht, muss sich die unvermeidbare Kakofonie aller Hintergrundgeräusche vorstellen, die ungestörtes Arbeiten zur Farce macht. Da von der Hochschule weder sichergestellt noch überprüft werden kann, dass alle privaten Computer der Studierenden mit passenden Mikrofonen und Kameras ausgestattet sind, scheitert die Klausur per Videokonferenz auch an der Prüfungsgleichheit. Die Beschwerde nur eines Studierenden oder spätestens ein Eilverfahren vor dem Verwaltungsgericht würde zum unkalkulierbaren Risiko.“

Die prognostizierten Beschwerden von Studierenden ließen nicht lange auf sich warten. Gegen die sogenannte Corona-Ordnung der Fernuniversität Hagen wehrte sich ein Student der Fernuniversität mit einem Eilantrag beim Oberverwaltungsgericht (OVG) Nordrhein-Westfalen. Ziel war es, dass die für den 8. März 2021 geplante Prüfung nicht aufgezeichnet, sondern allenfalls mittels Videoübertragung beobachtet wird.

Die Fernuniversität sieht in ihrer Corona-Prüfungsordnung als alternative Möglichkeit neben Präsenzprüfungen, die zurzeit nicht durchgeführt werden, videobeaufsichtigte häusliche Klausurprüfungen vor. Danach werden die Prüflinge durch prüfungsaufsichtsführende Personen über eine Video- und Tonverbindung während der Prüfung beaufsichtigt. Die Video- und Tonverbindung sowie die Bildschirmansicht des Monitors werden vom Beginn bis zum Ende der Prüfung aufgezeichnet und gespeichert. Die Prüfungsaufzeichnung wird nach dem Ende der Prüfung gelöscht. Dies gilt nicht, wenn die Aufsicht Unregelmäßigkeiten im Prüfungsprotokoll vermerkt hat oder der Student eine Sichtung der Aufnahme durch den Prüfungsausschuss beantragt. In diesem Fall erfolgt die Löschung der Aufzeichnung erst nach Abschluss des Rechtsbehelfsverfahrens.

Mit Beschluss vom 04.03.2021 (Aktenzeichen: 14 B 278/21.NE) hat das Oberverwaltungsgericht den Normenkontroll-Eilantrag abgelehnt. Die Rechtmäßigkeit der Aufzeichnung und Speicherung könne im Eilverfahren nicht geklärt werden, so das OVG. Allerdings räumte das OVG ein, dass die DS-GVO die Datenverarbeitung erlaube, wenn sie für die

Wahrnehmung einer Aufgabe erforderlich sei, die im öffentlichen Interesse liege oder in Ausübung öffentlicher Gewalt erfolge, die dem Verantwortlichen übertragen worden sei.

Wenn Hochschulen der Pflicht zur Durchführung von Prüfungen nachkommen, hätten sie in Wahrnehmung dieser Aufgabe dem prüfungsrechtlichen Grundsatz der Chancengleichheit Geltung zu verschaffen. Dieser verlange, dass für vergleichbare Prüflinge so weit wie möglich vergleichbare Prüfungsbedingungen gälten, um allen Teilnehmern gleiche Erfolgschancen zu bieten. Insbesondere sei zu verhindern, dass einzelne Prüflinge sich durch eine Täuschung über Prüfungsleistungen einen Chancenvorteil gegenüber den rechtstreuen Prüflingen verschafften.

Ebenfalls ohne Erfolg blieb der Versuch eines Studierenden der Christian-Albrechts-Universität zu Kiel (CAU), mithilfe des Schleswig-Holsteinischen Oberverwaltungsgerichts (Az. 3 MR 7/21) durchzusetzen, dass die von ihm in elektronischer Form abzulegenden Prüfungen ohne die vorgesehene Videoaufsicht stattfinden. Insbesondere sah das OVG das Recht auf Unverletzlichkeit der Wohnung (Art. 13 Abs. 1 GG) nicht als betroffen an, da dieses nur vor einem (digitalen) „Eindringen" in die Wohnung schütze. Die Videoaufsicht erfolge jedoch nicht gegen den Willen der Studierenden. Sie könnten frei entscheiden, ob sie an der elektronischen Prüfung teilnähmen mit der Folge, Kamera und Mikrofon ihres Computers für die Aufsicht zu aktivieren, oder ob sie später eine Präsenzprüfung ablegten. Obwohl diese derzeit nicht durchgeführt werden dürften, sei die Freiwilligkeit ihrer Entscheidung ausreichend gesichert.

BSI aktualisiert IT-Grundschutz-Kompendium

Mit dem IT-Grundschutz-Kompendium richtet sich das Bundesamt für Sicherheit in der Informationstechnik (BSI) gezielt an alle Unternehmen und Behörden, die sich grundlegend mit IT-Sicherheit befassen möchten oder müssen.

Foto: hkama, Adobe Stock

Zusammen mit den BSI-Standards bildet es die Basis für eine umfassende Betrachtung der Informationssicherheit.

Das in aktueller Auflage komplett überarbeitete Kompendium beinhaltet 97 Bausteine, die sich nicht nur mit technischen, sondern auch mit infrastrukturellen, organisatorischen sowie personellen Aspekten der IT-Sicherheit befassen. Neu hinzugekommen sind die IT-Grundschutz-Bausteine CON.10 Entwicklung von Webanwendungen und INF.11 Allgemeines Fahrzeug.

Ziel des Bausteins CON.10 ist es, sichere Webanwendungen zu entwickeln sowie Informationen zu schützen, die durch eine Webanwendung verarbeitet werden.

Der neue Baustein INF.11 beschreibt spezifische Gefährdungen, die zu beachten sind, wenn Institutionen Fahrzeuge mit IT-Komponenten einsetzen oder Fahrzeuge im Allgemeinen als IT-Arbeitsplätze verwenden. Darauf aufbauend legt der Baustein fest, welche Anforderungen von Fahrzeugnutzern und -haltern zu erfüllen sind, um den optimalen Betrieb eines Fahrzeugs aus Sicht der Informationssicherheit zu gewährleisten.

Neben Maßnahmen selbst finden sich Umsetzungshinweise zum vertiefenden Verständnis. Sie beschreiben, wie die Anforderungen der Bausteine umgesetzt werden können und erläutern im Detail geeignete Sicherheitsmaßnahmen. Diese Umsetzungshinweise werden ständig vom BSI aktualisiert und aktuellen Gegebenheiten angepasst. Bei der Überarbeitung wird Wert darauf gelegt, dass auch die Belange von kleinen und mittelständischen Unternehmen angemessen adressiert werden.

Quelle: Bundesamt für Sicherheit in der Informationstechnik

Foto: metamorworks, Adobe Stock

Datenschutz beim Einsatz von Kollaborationssystemen

Der öffentlich-rechtliche Rundfunk in Deutschland muss, gemäß Artikel 5 Abs. 1 S. 2 GG und der Rechtsprechung des Bundesverfassungsgerichts, staatsfern organisiert sein. Er unterliegt deshalb einer autonomen Datenschutzaufsicht, die an die Stelle der staatlichen Datenschutzkontrolle tritt.

In Deutschland treten neben den Landesdatenschutzbehörden und den Bundesbeauftragten bereichsspezifisch die Rundfunkdatenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten, die Datenschutzaufsicht der Landesmedienanstalten über die privaten Rundfunkveranstalter und die kirchlichen Kontrollorgane.

Maßgebend für die Datenschutzkontrolle im öffentlich-rechtlichen Rundfunk sind die Vorgaben des Art. 51 der DS-GVO sowie die für die jeweilige Rundfunkanstalt geltenden gesetzlichen Vorschriften. Die Rechtsstellung der oder des jeweiligen Rundfunkdatenschutzbeauftragten entspricht der der staatlichen Datenschutzbeauftragten.

Die sogenannten Rundfunkdatenschutzkonferenz (quasi das Äquivalent zur Datenschutzkonferenz, also dem Zusammenschluss der unabhängigen Datenschutzbehörden des Bundes und der Länder) hat im Februar 2021 ein eigenes Positionspapier veröffentlicht, in dem sich die Beteiligten mit den datenschutzrechtlichen Eckpunkten beschäftigen, die bei einem Einsatz von Kollaborationssystemen Beachtung finden sollten.

Ausgehend von der Feststellung, dass bei dem Einsatz derartiger Plattformen, in der Regel Namen und Kontaktdaten der Nutzenden, personenbezogene Inhalte der Videokonferenz, also Ton und (Bewegt-) Bilder, ggf. sogar besonders sensible Daten im Sinne von Art. 9 DS-GVO sowie natürlich Metadaten (z. B. körperliche Eigenschaften, politische Einstellungen etc.) eine Rolle spielen können, stellt die Rundfunkdatenschutzkonferenz eine Reihe datenschutzrechtlicher Anforderungen für den Betrieb der betrachteten Kollaborationssysteme auf.

Die Anforderungen werden mittels einer Schutzbedarfsfeststellung konkretisiert und auch vor dem Hintergrund des genutzten Betriebsmodells bewertet. Abgerundet wird das Positionspapier durch zahlreiche Hinweise bezüglich der zu beachtenden organisatorischen Maßnahmen zur Einhaltung von Datenschutz und Informationssicherheit sowie durch weitere hilfreiche Ausführungen zu dem oftmals vernachlässigten Thema Dokumentation und Information.

Quelle: Rundfunkdatenschutzkonferenz (RDSK)

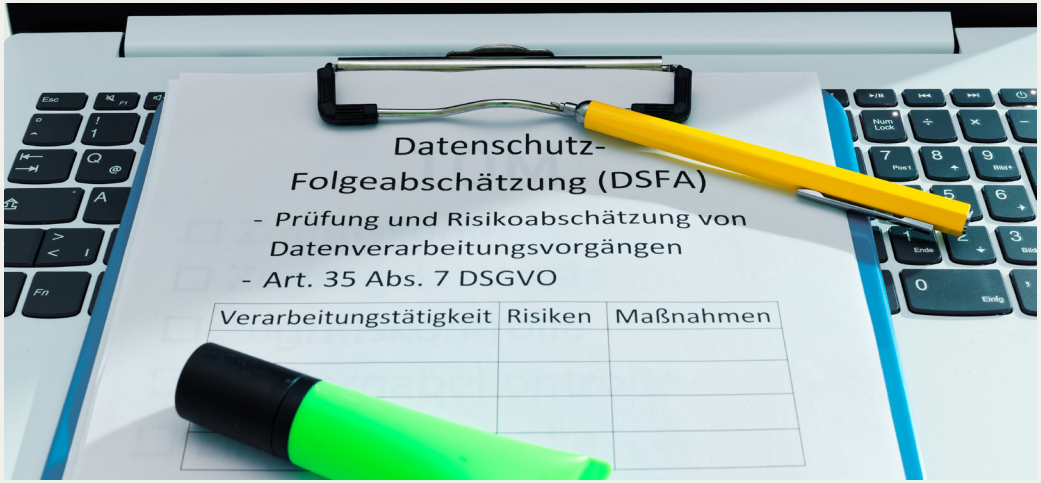


Foto: DatenschutzStockfoto, Adobe Stock

Wann ist eine Datenschutz-Folgeabschätzung zu erstellen?

Die Risiken für die Rechte und Freiheiten natürlicher Personen – mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere – können aus einer Verarbeitung personenbezogener Daten hervorgehen, die zu einem physischen, materiellen oder immateriellen Schaden führen könnte.

Die Datenschutz-Folgenabschätzung (DSFA, Art. 35 DS-GVO) ist Ausdruck des risikobasierten Ansatzes der DS-GVO. Soweit eine Datenverarbeitung hohe Risiken für die Rechte und Freiheiten natürlicher Personen beinhaltet, sollen diese mithilfe der DSFA frühzeitig erkannt werden, um sie durch geeignete Schutzmaßnahmen technischer und/oder organisatorischer Art von Anfang an eindämmen zu können.

Zweck der DSFA ist es, im Falle von besonders riskanten Datenverarbeitungsvorgängen, die voraussichtlichen Risiken für die persönlichen Rechte und Freiheiten betroffener Personen zu identifizieren.

Die Artikel-29-Arbeitsgruppe (WP29) hat Leitlinien mit neun Kriterien (WP248) veröffentlicht, die als Indikatoren für die Feststellung eines „wahrscheinlich hohen Risikos" dienen können. In den meisten Fällen weist eine Kombination von zwei dieser Faktoren auf die Notwendigkeit einer DSFA hin.

Wie die Landesbeauftragte für den Datenschutz (LfD) Niedersachsen berichtet, erreichen die Behörde immer wieder Anfragen, wann eine DSFA konkret durchzuführen ist. Um Anwendern die Beantwortung dieser Frage zu erleichtern, stellt die LfD ein Prüfschema zur Verfügung, womit Datenverarbeiter für ihren Verantwortungsbereich prüfen können, ob die Durchführung einer DSFA erforderlich ist. Neben einer Checkliste und einem umfangreichen Glossar der wichtigsten Begriffe enthält das Schema auch Hinweise auf weitere Hilfestellungen zum Thema Datenschutz-Folgenabschätzung. Das Prüfschema lässt sich hier herunterladen.

Die Datenschutzstelle Fürstentum Liechtenstein stellt ebenfalls seit geraumer Zeit eine sehr nützliche Checkliste (Excel-Dokument) für die Prüfung der Notwendigkeit der Durchführung einer Datenschutz-Folgenabschätzung (DSFA) zur Verfügung. Die Checkliste zur Prüfung der Notwendigkeit der Durchführung einer Datenschutz-Folgenabschätzung (DSFA) gliedert sich in sechs Abschnitte. Jeder Abschnitt umfasst mehrere Hauptfragen, mit deren Beantwortung festgestellt wird, ob die Notwendigkeit der Durchführung einer DSFA für eine bestimmte Verarbeitungstätigkeit besteht.

Foto: RS-Studios, Adobe Stock

Praxisleitfaden: Rechtliche Fragen zur KI im Unternehmenseinsatz

Die „Künstliche Intelligenz“ (KI) ist in unserem Alltag angekommen. Egal ob in Wirtschaft, Wissenschaft oder im gesellschaftlichen Diskurs – wir kommen kaum noch um sie herum. Unternehmen nutzen KI, um Effizienzgewinne oder Wettbewerbsvorteile zu erlangen. Auf der anderen Seite gibt es angesichts der technischen Komplexität und der undurchsichtigen Datenverarbeitung aber auch kritische Stimmen.

Die Datenethikkommission der Bundesregierung versteht KI als Sammelbegriff für Technologien und Anwendungen. Diese greifen auf digitale Methoden zurück, die mit potenziell sehr großen und heterogenen Datensätzen arbeiten. Damit ermitteln sie, einem komplexen und die menschliche Intelligenz gleichsam nachahmenden maschinellen Verarbeitungsprozess, ein Ergebnis.

Schließlich gibt es auch abseits dessen Hürden für die Nutzung Künstlicher Intelligenz. Der Einsatz von KI als Teilgebiet der Informatik ist nicht nur aus technischer Sicht eine Herausforderung. Hinzu kommt eine starke Unsicherheit über den (datenschutz-)rechtlichen Rahmen.

Das Datenschutzrecht stellt bereits ohne die Anwendung von KI eine enorme Herausforderung für jede datenverarbeitende Stelle dar. Spätestens seit der Datenschutz-Grundverordnung (DS-GVO) kann sich kein Unternehmen aufgrund der drakonischen Bußgelder mehr erlauben, den Datenschutz nicht ordentlich umzusetzen. Häufig werden beim Einsatz Künstlicher Intelligenz personenbezogene Daten in komplexer Art

und Weise verarbeitet. Dies potenziert die vielfältigen Anforderungen des Datenschutzrechts noch weiter.

Die automatisierte Verarbeitung sehr großer und heterogener Datensätze kollidiert mit dem Zweckbindungsgrundsatz und vor allem mit dem Prinzip der Datenminimierung. Aus den Regelungen der DS-GVO und des Bundesdatenschutzgesetzes (BDSG) ergeben sich beim Einsatz von Künstlicher Intelligenz aufgrund der großen Datenmengen, die möglicherweise aus verschiedenen Datenquellen stammen, Fragen nach den Verantwortlichkeiten für die Datenverarbeitungen. Auch die durch Datenschutzerklärung bekannten Transparenzanforderungen der DS-GVO sind bei Anwendungen mit KI schwer zu erfüllen. Datenschutzrechtliche Regelungen sind also für den optimalen Einsatz Künstlicher Intelligenz von enormer Relevanz.

Eine aktuelle Veröffentlichung der Bertelsmann Stiftung möchte („KI in Unternehmen – Ein Praxisleitfaden zu rechtlichen Fragen") eine handlungsorientierte Unterstützung zu diesem Thema geben. Sie richtet sich an Projektverantwortliche und Praktiker:innen in KMU, die Systeme speziell des Maschinellen Lernens in die betrieblichen Abläufe einfügen wollen. Eine rechtliche Grundorientierung wird als wichtig erachtet, weil viele rechtliche Aspekte möglichst frühzeitig im Projekt adressiert und damit die Weichen richtig gestellt werden müssen.

Darin beschäftigen sich die Autoren nicht nur mit Fragen wie:

„Wann darf ich Inhalte für Trainingszwecke verwenden? Wem gehören die Arbeitsergebnisse einer KI?", sondern auch mit datenschutzrechtlichen Fragestellungen:

„Welche Anforderungen bestehen an das System bei Umgang mit personenbezogenen Daten? Welche Daten darf ich für Trainingszwecke verwenden? Wie vermeide ich Diskriminierungen durch das System?".

Abgerundet wird der Leitfaden mit Fragen, die sich im Bereich der Haftungsrisiken und arbeitsrechtlichen Aspekte bewegen.

Quelle: Bertelsmann Stiftung

Foto: shock, Adobe Stock

250.000 EUR Bußgeld wegen unerlaubter Telefonwerbung

Die Bundesnetzagentur hat gegen den Energieversorger mivolta GmbH wegen unerlaubter Telefonwerbung eine Geldbuße von 250.000 Euro verhängt. Die Palette der illegalen Machenschaften zulasten der Verbraucherinnen und Verbraucher ging in diesem Fall von unerlaubten Werbeanrufen bis zu unterstellten Vertragsabschlüssen.

Das Unternehmen setzte Vertriebspartner ein, die die Betroffenen hartnäckig und gegen deren erklärten Willen immer wieder kontaktierten. Die Anrufe erfolgten teilweise auch mit unterdrückter Rufnummer, sodass die Aufdeckung der unerlaubten Anrufe bzw. die Beschwerde durch die Betroffenen aufgrund der anonym erfolgenden Anrufe erschwert wurde.

Einige der Betroffenen wurde in die Irre geführt, in dem die Anrufer in Einzelfällen sogar suggerierten, dass sie im Auftrag der Bundesnetzagentur anrufen.

In mehreren Fällen wurde auch der eigentliche Anrufzweck, Produkte der mivolta zu vertreiben, zunächst verschleiert. Die Anrufer gaben vor, allgemein angebliche Kosteneinsparpotenziale beim Energieverbrauch aufzeigen zu wollen.

Die Bundesnetzagentur hat in ihren Ermittlungen festgestellt, dass ein erheblicher Teil der Werbeeinwilligungen nach dem jeweils betreffenden Telefonanruf datiert war. Weitere der verwendeten Einwilligungserklärungen, die die mivolta über Online-Gewinnspiele bezogen hatte, waren seitens der Gewinnspielanbieter intransparent vorformuliert und gestaltet.

Teilweise gaben sich die Anrufer auch gezielt als Mitarbeiter des aktuellen Energieversorgers der Angerufenen aus. Auf diese Weise versuchten sie, von den Betroffenen gerade die Informationen wie die Zählernummer zu erhalten, die erforderlich sind, um einen Lieferantenwechsel anstoßen zu können.

Zu den konkreten Formen der Direktwerbung, also dem Kontaktweg zu den betroffenen Personen (Ansprache per Telefonanruf, E-Mail, Fax etc.), regelt das Wettbewerbsrecht, § 7 des Gesetzes gegen den unlauteren Wettbewerb (UWG), in welchen Fällen von einer unzumutbaren Belästigung der Beworbenen auszugehen und eine Werbung dieser Art unzulässig ist.

Weil Art. 6 Abs. 1 Satz 1 lit. f DS-GVO eine Verarbeitung personenbezogener Daten nur für zulässig erklärt, soweit die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen, sind auch bei der datenschutzrechtlichen Beurteilung einer Verarbeitung personenbezogener Daten für Zwecke der Direktwerbung die Wertungen in den Schutzvorschriften des UWG für die jeweilige Werbeform mitzuberücksichtigen. Wenn für den werbenden Verantwortlichen ein bestimmter Kontaktweg zu einer betroffenen Person danach nicht erlaubt ist, kann die Interessenabwägung nach Art. 6 Abs. 1 Satz 1 lit. f DS-GVO auch nicht zugunsten der Zulässigkeit einer Verarbeitung dieser Kontaktdaten für Zwecke der Direktwerbung ausfallen. (DSK: www.datenschutz-bayern.de Orientierungshilfe der Aufsichtsbehörden zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der Datenschutz-Grundverordnung).

Quelle: Bundesnetzagentur