LOSCHELDER

Newsletter Datenschutzrecht

März 2020

Sehr geehrte Damen und Herren,

das Coronavirus hat mittlerweile auch Deutschland fest im Griff. Aber seien Sie unbesorgt: Diesen Newsletter können Sie auch weiterhin ganz ohne Mundschutz und nachträgliches Händewaschen konsumieren!

Wir befassen uns in unserem ersten Beitrag mit der aktuellen Frage, ob Unternehmen private und gesundheitsbezogene Informationen von Lieferanten, Geschäftspartnern oder Dienstleistern einholen dürfen, um Corona-Infektionsrisiken im Betrieb vorzubeugen. In unserem zweiten Beitrag geht es um die mittlerweile weit verbreitete Praxis, gesetzlichen oder vertraglichen Auskunftsansprüchen das Datenschutzrecht entgegenzuhalten. In unserem dritten Beitrag zeichnen wir für Sie die aktuellen Entwicklungen zum Datenverkehr und KI im EU-Binnenmarkt nach. Und zu guter Letzt wollen wir Ihnen auch in diesem Monat die besonders interessanten Bußgeldfälle und besonders kurios gelagerte Sachverhalte nicht vorenthalten.

Inhalt

Corona: Wie weit dürfen Präventionsmaßnahmen gehen?

Welche Maßnahmen dürfen Unternehmen treffen, um eigene Mitarbeiter vor einer Infektion durch das Coronavirus zu schützen und eine Betriebsschließung durch Behörden zu verhindern? Dürfen Lieferanten, Boten oder Dienstleister und Besucher vor dem Zutritt zum eigenen Gebäude zu ihrem Gesundheitszustand und etwaigen Aufenthalten in Risikogebieten befragt werden? Darf man diesen Personen bei entsprechenden Antworten den Zugang zum Gebäude verwehren und welche Folgen hat das Ganze? Das wollen wir in diesem Beitrag näher beleuchten.

Das allgemeinen Hausrecht (§§ 903, 1004 BGB) erlaubt es Unternehmen, den Zutritt zum Gebäude zu reglementieren. Dies umfasst auch das Recht, einzelnen Personen den Zutritt zu verwehren.

Verweigert man allerdings dem Mitarbeiter eines Vertragspartners oder einem Dienstleister den Zutritt, wird das Konsequenzen für die bestehenden vertraglichen Beziehungen nach sich ziehen. Können infolge des Zutrittsverbotes Dienstleistungen nicht erbracht werden oder Produkte nicht ausgeliefert werden, kann dies zulasten des Unternehmens gehen, das den Zutritt verweigert hat. Je nach vertraglicher Gestaltung, kommt in diesen Fällen ein sog. Annahmeverzug des Gläubigers in Betracht. Infolge der Zutrittsverweigerung muss das Unternehmen seinem Schuldner dann etwa dadurch entstandene Mehraufwendungen wie die Kosten einer zweiten Anlieferung ersetzen (§ 304 BGB) oder auch für einen Untergang der Sache haften. Gleichzeitig müssen Unternehmen Leistungen nicht annehmen, wenn dies für sie unzumutbar ist. Das mag der Fall sein, wenn die anbietende Person offensichtliche Symptome des Coronavirus zeigt und bekannt ist, dass sich diese Person in der Vergangenheit in einem Risikogebiet aufgehalten hat. Die Verweigerung des Zutritts kann daher nachteilige zivilrechtliche Folgen für Auftraggeber und Auftragnehmer haben und alle daraus erwachsenden Rechtsfragen sollten schon aus diesem Grund sorgsam geprüft werden. Unternehmen auf beiden Seiten tun daher gut dran, die Risiken vorab abzuwägen und es nicht zu einer Konfrontation am Werkstor kommen zu lassen.

Durch die Abfrage von Informationen im Rahmen der Zutrittskontrolle tritt eine weitere wesentliche rechtliche Schranke hinzu: das Datenschutzrecht. Will ein Unternehmen von externen Besuchern Informationen erhalten, wo sich diese in den letzten Wochen aufgehalten haben und ob sie bestimmte Krankheitssymptome aufweisen, so werden damit personenbezogene Daten erhoben. Geschieht dies rechtswidrig, drohen auch aufsichtsbehördliche Sanktionen und im schlimmsten Fall hohe Bußgelder. Die Beachtung der datenschutzrechtlichen Grenzen ist daher von mindestens ebenso gewichtiger Bedeutung. Hierbei gilt:

1. Das Datenschutzrecht ist dann anwendbar, wenn die personenbezogenen Daten automatisiert erhoben werden, also z.B. über ein an der Pforte angebrachtes Tablet. Wenn diese Daten nicht-automatisiert erhoben werden, also etwa über handschriftlich zu beantwortende „Ausfüllzettel", ist das Datenschutzrecht nur dann anwendbar, wenn die ausgefüllten Zettel im Nachgang systematisch gespeichert werden sollen, z.B. alphabetisch oder chronologisch in Ordnern. Im Umkehrschluss bedeutet dies: Fragen Sie handschriftlich am Eingang Informationen ab und vernichten die Zettel im Nachgang sofort, spricht viel dafür, dass der Anwendungsbereich des Datenschutzrechts nicht eröffnet ist und ohne Berücksichtigung der nachfolgenden Ausführungen kein Bußgeld droht.

2. Ist das Datenschutzrecht anwendbar, dürfen Informationen von den Besuchern nur erhoben werden, wenn und soweit dafür eine Erlaubnisgrundlage zur Verfügung steht.

   Denkbar ist dies zunächst mit einer wirksamen Einwilligung der Betroffenen. Wirksam ist eine solche Einwilligung aber nur dann, wenn sie freiwillig und informiert erfolgt. Die Freiwilligkeit dürfte hier oftmals eine kaum überwindbare Hürde darstellen, wenn sich etwa Arbeitnehmer „gezwungen sehen", zu antworten, um ihre Arbeit ordnungsgemäß zu erbringen und keine Nachteile zu erleiden. Wenn eine nachweislich freiwillige Situation geschaffen werden kann, ist das Nachfragen auch datenschutz- und zivilrechtlich erlaubt. Das erfordert eine sorgsame Gestaltung und eine gute und sensible Kommunikation. Verweigert ein Betroffener die

Antworten, darf ihm bei dieser Gestaltung nicht deshalb der Zutritt verwehrt werden.

Im Ausgangspunkt sind die Gesundheit einer jeden Person und auch etwaige Fragen darüber von dem Allgemeinen Persönlichkeitsrecht umfasst. Ein Betroffener darf selbst entscheiden, ob und wie viel er in diesem Zusammenhang mit anderen Personen teilt. Die Gesundheit ist etwas Höchstpersönliches und damit der eigenen Intimsphäre zuzuordnen. Wird eine Person zu ihrem Gesundheitszustand gefragt, muss sie deswegen auf eine solche Frage nicht antworten. Insbesondere besteht auch keine Aufklärungspflicht zwischen Vertragsparteien, sobald bei einer Partei bzw. ihren Mitarbeitern das Allgemeine Persönlichkeitsrecht betroffen ist.

Ob jenseits einer freiwilligen Einwilligungslösung auch andere gesetzliche Erlaubnisgründe die Datenverarbeitung tragen könnten, ist zweifelhaft. Dies gilt insbesondere für die Abfrage von Gesundheitsdaten wie die Frage nach erhöhter Temperatur, Fieber oder Atemnot. Eine Solche ist nur unter den engen Voraussetzungen der Art. 9 DSGVO, § 22 BDSG zulässig. Eine Rechtfertigung wegen einer Meldepflicht scheidet dabei bei fast allen Unternehmen aus – namentlich meldepflichtig sind nach dem Infektionsschutzgesetz, vereinfacht zusammengefasst, nur Angehörige von Gesundheitsberufen und Gemeinschaftseinrichtungen wie Kindertagesstätten. Eine Erfassung aus Gründen der öffentlichen Gesundheit und Vermeidung einer weiteren Verbreitung schließlich dürfte unter den aktuellen Gegebenheiten auch kaum zu bejahen sein, soweit sich Unternehmen hierauf berufen können. Ändern könnte sich dies aber etwa, wenn weiterreichende behördliche Vorgaben erlassen werden würden. Um zu vermeiden, dass man in den Anwendungsbereich der DSGVO gelangt, sollten sich Unternehmen daher aktuell für eine rechtssichere Lösung auf mündliche Konversationen oder auf Ausfüllzettel, die anschließend weggeworfen werden, beschränken.

Abfragen nach vergangenen Reisen dagegen könnten noch als allgemeine personenbezogene Daten und nicht als Gesundheitsdaten einzuordnen sein. Diese können dann unter erleichterten Voraussetzungen gem. Art. 6 DSGVO erhoben werden. Hier könnte je nach Gegebenheiten im Einzelfall eher diskutiert werden, ob aus überwiegenden berechtigten

Unternehmensinteressen heraus eine auch namentliche Erhebung und Speicherung zulässig ist, wenn bei später notwendigen Betriebsschließungen etwa Schadensersatzansprüche gegen das verursachende Unternehmen geprüft werden sollen. Ganz abstrakt dürfen derartige Schadensersatzansprüche aber nicht sein; dann würden auch sie keine Datenverarbeitung erlauben.

Insgesamt sind daher Unternehmen gut beraten, bei Zutrittskontrollen auf ein möglichst hohes Maß an Freiwilligkeit zu setzen und einen Ausschluss von Personen zu vollziehen, wenn deutliche Umstände für eine konkrete Gefahr sprechen und die vertraglichen Haftungs- und Folgerisiken als gering einzustufen sind.

Zur Rolle des Datenschutzrechts bei vertraglichen und gesetzlichen Auskunftsansprüchen

„Das dürfen wir aus datenschutzrechtlichen Gründen nicht." „Dem steht die DSGVO entgegen." Solche knappen, pauschalen und oftmals vorgeschobenen Antworten erhalten Unternehmen seit Inkrafttreten der DSGVO immer öfter, wenn sie versuchen, bei Schuldnern gesetzliche oder vertragliche Auskunftsansprüche geltend zu machen. Auch der Bundesgerichtshof (BGH) hatte kürzlich darüber zu befinden, inwieweit die vertragliche Zweckbindung und die potentielle Gefahr eines Datenmissbrauchs einem Auskunftsanspruch entgegenstehen können.

Der vom BGH zu entscheidende und in seinen Details komplizierte Fall war gesellschaftsrechtlich eingekleidet. Im Wesentlichen ging es darum, unter welchen Voraussetzungen ein Treugeber-Gesellschafter die Kontaktdaten seiner Mitgesellschafter erhalten kann, um eine außerordentliche Gesellschafterversammlung einzuberufen. Die in Anspruch genommene Treuhandgesellschaft wollte die Kontaktdaten nur herausgeben, wenn der Treugeber im Gegenzug eine Sicherungszahlung von 10.000 Euro leistete und sich verpflichtete, die Kosten etwaiger Klagen und datenschutzrechtlicher Bußgeldverfahren zu übernehmen. Die Treuhandgesellschaft argumentierte mit einem zu befürchtenden Missbrauch der Daten sowie mit der Zweckbindung der Verarbeitung gemäß dem Treuhandvertrag.

Der BGH stellt in seinem Beschluss vom 19.11.2019 (Az. BGH II ZR 263/ 18) klar, dass die Gefahr deines Datenmissbrauchs nur dann dem Auskunftsrecht des Gesellschafters entgegenstünde, wenn es für diese konkrete Anhaltspunkte gebe. Ferner erachtete der BGH die beanspruchte Datenübermittlung auch mit den Gesellschafterverträgen als vereinbar und kam im konkreten Fall zu dem Ergebnis, dass die ausdrückliche Nennung nur einiger Verarbeitungsvorgänge im Vertrag nicht automatisch ausschließe, dass weitere Verarbeitungsvorgänge danach nicht mitzuteilen seien, solange keine Zweckentfremdung vorliege. Gleichwohl wurde die Möglichkeit, Auskunftsansprüche nur gegen die Übernahme des (datenschutzrechtlichen) Haftungsrisikos zu erfüllen, vom BGH nicht pauschal ausgeschlossen.

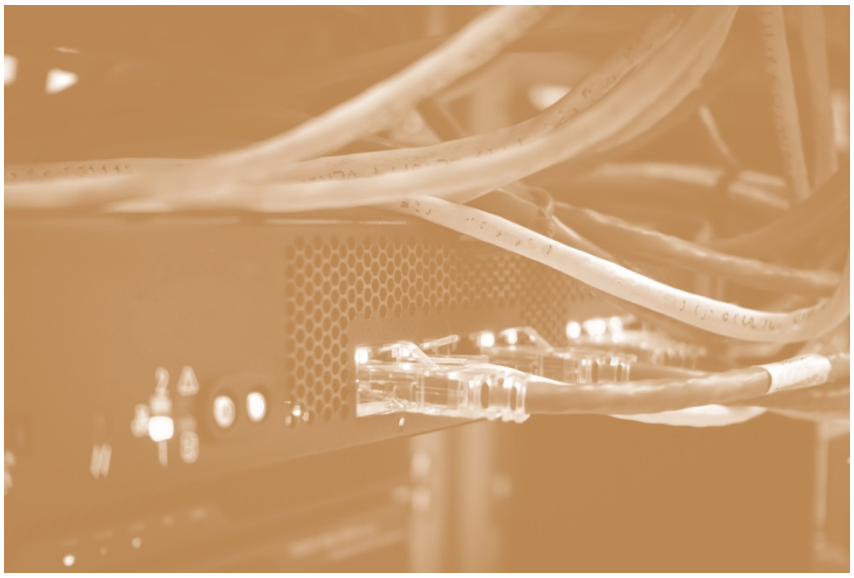
Die in dem Urteil behandelten Probleme sind äußerst praxisrelevant. Zu oft passiert es, dass Auskunftsansprüche zu pauschal gestellt bzw. zu pauschal mit fadenscheinigen Argumenten abgewehrt werden. Beides verspricht in der Praxis keinen Erfolg. Unternehmen müssen daher das Datenschutzrecht stets mit dem richtigen Augenmaß würdigen und in die eigene Argumentation einfließen lassen.

- **Durchsetzung von Auskunftsansprüchen**: Unternehmen sollten stets die Inhalte und den Umfang der gewünschten Auskunft ermitteln. Reicht eine anonymisierte Auskunft aus und können Namen und weitere Details geschwärzt werden, sollte dies dem Schuldner vorgeschlagen werden. Auf diesem Wege schneidet man bereits früh datenschutzrechtliche Abwehrargumente ab. Soll die Auskunft hingegen auch

personenbezogene Daten enthalten, muss die Anspruchsgrundlage (Vertrag oder Gesetz) ermittelt werden. In der Regel ergibt sich bereits hieraus auch die datenschutzrechtliche Erlaubnis zur Übermittlung. Sollte dies im Ausnahmefall nicht so sein, können immer noch die zahlreichen weiteren Erlaubnistatbestände der DSGVO und insbesondere die gesetzlich normierte Zweckänderung weiterhelfen. Gläubiger eines Auskunftsanspruchs tun allerdings grundsätzlich gut daran, diese Gesichtspunkte zwar mitzudenken, aber nicht von Anfang zu thematisieren, sondern die Reaktion des Schluderns abzuwarten.

- **Abwehr gegen Auskunftsansprüche**: Unternehmen, die sich Auskunftsansprüchen ausgesetzt sehen, sollten darauf verzichten, diese pauschal mit dem Datenschutzrecht „erschlagen" zu wollen. Vielmehr ist in einem solchen Fall sorgsam zu prüfen und zu argumentieren, ob bzw. dass es rechtlich unter keinem Gesichtspunkt möglich ist, die Auskunft zu erteilen. In bestimmten Fällen mag sich herausstellen, dass eine Datenübermittlung nur mit einem gewissen Rechts- und damit Bußgeldrestrisiko möglich ist. In solchen Fällen mag man darüber nachdenken, dem Datenempfänger im Innenverhältnis das Bußgeldrisiko über eine vertragliche Vereinbarung aufzuerlegen. Ob und wie eine solche Regelung allerdings rechtlich und auch vertraglich zulässig gestaltet werden kann, ist im Einzelfall sorgfältig zu prüfen, um keine weiteren Risiken zu schaffen.

In beiden Fällen kann das Datenschutzrecht also nützlich, kreativ und zielführend eingesetzt werden. Das erfordert jedoch eine sorgsame Beurteilung der Sachlage und der Erlaubnistatbestände, damit das Datenschutzrecht nicht zur „lame duck" verkommt.



Aktuelles zum Datenverkehr und KI im EU-Binnenmarkt

Was in Sachen „Data“ in den nächsten Monaten aus Brüssel zu erwarten ist, konkretisierte die neue EU-Kommission im vergangenen Monat. Auch in der Vergangenheit hat die Europäische Kommission verschiedene Schritte unternommen, um die Entwicklung der Datennutzung im EU-Binnenmarkt voranzutreiben. Neben der DSGVO zählen hierzu auch die Verordnung über den freien Verkehr nicht personenbezogener Daten, der Cybersecurity-Act, die Open Data-Richtlinie oder auch die Digitale-Inhalte-Richtlinie. Seit kurzem wird auch die künftige ePrivacy-Verordnung wieder intensiver diskutiert, nachdem der letzte Entwurf im Herbst 2019 gescheitert war.

Im Februar stellte die (neue) EU-Kommission ihre Strategie für die Entwicklung rund um das Thema „Data“ der nächsten Monate vor. Diese beinhaltet neben dem Vorschlag eines „Rechtsakts über Daten“ und eines Aktionsplans für europäische Demokratie auch die Überprüfung der Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (kurz: eIDAS-VO) und die Stärkung der Cybersicherheit durch die Entwicklung einer gemeinsamen europäischen Cyber-Einheit. Mit diesen Vorhaben möchte die EU-Kommission ihre drei Hauptziele weiterverfolgen, die sie sich für die nächsten fünf Jahre in Sachen „Data“ auferlegt hat:

- Technologie soll für jeden Einzelnen zugänglich sein und bestmöglich für ihn funktionieren,
- Schaffung und Sicherung einer fairen und global wettbewerbsfähigen Wirtschaft sowie
- Einer offenen, demokratischen und nachhaltigen Gesellschaft.

Für die Erreichung dieser Ziele setzt die EU-Kommission stark auf den Einsatz künstlicher Intelligenz: Die neue Kommissionspräsidentin Ursula von der Leyen hat in ihren politischen Leitlinien auf die Notwendigkeit der Weiterentwicklung der digitalen Möglichkeiten aufmerksam gemacht. Sie kündigte damals an, sich mit einer Debatte über menschliche und ethische künstliche Intelligenz und den Einsatz von Big Data zur Schaffung von Wohlstand für Gesellschaften und Unternehmen zeitnah zu befassen.

In diesem Zusammenhang hat die EU-Kommission im Februar ein White Paper veröffentlicht. Dieses baut inhaltlich auf einem Expertengutachten aus dem Jahr 2019 auf, das sich mit Ethikfragen zum Thema „künstliche Intelligenz" befasste. Mit dem White Paper legt die Kommission einen Vorschlag vor, nach dem die Entwicklung künstlicher Intelligenz vor allem auf Qualität und Vertrauen basieren soll:

- **Qualität:** Es soll künftig einen echten Binnenmarkt für Daten geben. Es soll möglich werden, Daten – solange sie keinen Personenbezug aufweisen – sektorübergreifend Unternehmen, Forschern, öffentlichen Verwaltungen, aber auch Privatleuten zur Verfügung zu stellen. Der durch den Austausch entstehende Datenpool soll Entwicklungsprozesse in Forschung, Wirtschaft und auch im gesellschaftlichen Zusammenleben beschleunigen und weitere Innovationen ermöglichen. Die so gewonnenen Datensätze sollen eine hochwertige Grundlage bilden für die Entwicklung künstlicher Intelligenz für viele verschiedene Bereiche.

- **Vertrauen:** Der Einsatz künstlicher Intelligenz soll nicht zulasten der öffentlichen Ordnung und Sicherheit gehen; vielmehr sollen auch weiterhin strenge EU-Vorschriften zum Verbraucherschutz, zur Bekämpfung unlauterer Geschäftspraktiken sowie zum Schutz personenbezogener Daten und der Privatsphäre gelten. Außerdem sollen für

> komplexe Bereiche, wie Gesundheit, Polizeiarbeit und Transport der Rechtsrahmen für eine transparente, rückführbare und durch Menschenhand kontrollierte Datenverarbeitung geschaffen werden. Mittel für die Sicherstellung dieser Anforderungen sollen behördliche Tests und Zertifizierungen sein.

Die EU-Kommission will zudem Anreize setzen, damit zukünftig auch mittlere und kleinere Unternehmen auf den Einsatz künstlicher Intelligenz setzen.

Das White Paper steht nun bis Mitte Mai zur öffentlichen Konsultation bereit. Es bleibt also bis dahin abzuwarten, wie die Kommission die Rahmenbedingungen für den Ausbau künstlich intelligenter Geräte konkret ausgestalten wird.

Parallel hat die Diskussion zur ePrivacy-Verordnung Fortgang gefunden. Nachdem der letzte Entwurf im November 2019 endgültig gescheitert war, wurde vielfach bezweifelt, welche Einigung überhaupt möglich wäre. Der neue EU-Digitalkommissar Thierry Breton schlug im Dezember 2019 eine komplette Neuausrichtung der Verhandlungen vor. Zentral sind die Fragen um die Ausgestaltung des Einsatzes von Cookies und vergleichbaren files und tags. Vor allem liegen die Ansichten darüber, welche Ausnahmen es zu einer allgemeinen Einwilligungslösung geben soll, weit auseinander.

Frischen Wind sollen nun das neue Jahr und die neue Besetzung in Rat und Kommission bringen. Eingeleitet hat dies ein Anfang Februar vom Ratspräsidenten veröffentlichtes Non-Paper, das die Möglichkeit der Streichung der entscheidenden, umstrittenen Norm über die Nutzung von Cookies zur Erfassung von Endnutzerdaten (Art. 8 gescheiterter ePrivacy-Verordnungsentwurf) in den Raum wirft. In diesen Bereichen könnte sowieso grundsätzlich auf die DSGVO zurückgegriffen werden. Dieser strikte Ansatz ist bislang aber nicht umgesetzt; Ende Februar und Anfang März wurden vielmehr offizielle Überarbeitungsvorschläge veröffentlicht und diskutiert, die eine Cookie-Verwendung auch ohne Einwilligung in verschiedenen Fallgestaltungen erlauben wollen, etwa bei berechtigten Verwendungsinteressen ähnlich dem aus der DSGVO bekannten Abwägungstatbestand der „berechtigten Interessen“. Und auch eine weiterreichende Zulässigkeit der Cookie-Nutzung für Analysezwecke ist weiterhin vorgesehen. Vorgesehen sind aber

strenge prozedurale Voraussetzungen und Sicherheitspflichten: Es kann etwa u.a. Rücksprache mit der Aufsichtsbehörde zu halten sein, die Endnutzer sind über die Datenverarbeitung zu informieren und die erlangten Daten dürfen wohl nur in anonymisierter Form an Dritte weitergegeben werden. Wir werden den weiteren Fortgang beobachten und Sie auf dem Laufenden halten.

Zu guter Letzt: Geldbußen und Kuriositäten des Monats

In Sachen Geldbußen und anderen lebensnahen Gegebenheiten gibt es auch diesmal Spannendes zu berichten.

Jahrelang war es ein Mantra der Datensicherheit: Wechseln Sie ihre Passwörter regelmäßig! Das Bundesamt für Sicherheit in der Informationstechnik sieht das mittlerweile (und nun auch offiziell) anders. Im IT-Grundschutz heißt es künftig zum Passwortwechsel: „Reine zeitgesteuerte Wechsel SOLLTEN vermieden werden." Voraussetzung ist, dass das IT-System Möglichkeiten enthält, um die Kompromittierung von Passwörtern zu erkennen. Unternehmen können und sollen die Vorgaben des BSI bei der Implementierung der angemessenen technischen und organisatorischen Maßnahmen gem. Art. 32 DSGVO berücksichtigen.

Neue berichtenswerte Bußgeldfälle gab es zuletzt insbesondere in anderen EU-Mitgliedstaaten:

- **Spanien die Erste**

  Die spanische Datenschutzaufsichtsbehörde AEPD hat der spanischen Airline Iberia ein Bußgeld in Höhe von 20.000 Euro auferlegt. Ein Kunde forderte das Unternehmen im Jahre 2019 dazu auf, seine personenbezogenen Daten, die er dem Unternehmen im Hinblick auf ein Treueprogramm zur Verfügung stellte, zu löschen. Obwohl die Löschung von Seiten Iberia Airlines bestätigt wurde, erhielt der Kunde weiterhin Werbenachrichten per E-Mail.

  Die spanische Datenschutzaufsichtsbehörde sah in dem wiederholten Zusenden der Werbenachrichten einen Verstoß gegen Art. 6 DSGVO. Da die Airline in der Vergangenheit schon mehrmals mit einem solchen Verhalten aufgefallen sei, erkannte die Behörde darin sogar ein vorsätzliches Handeln, was sie mit einem Bußgeld in Höhe von 20.000 Euro belegte.

- **Spanien die Zweite**

  Daneben hat die AEPD Vodafone Spanien ein Bußgeld in Höhe von 120.000 Euro auferlegt. Kurz nachdem ein Kunde einen Vertrag mit Vodafone abgeschlossen hatte, bemerkte dieser, dass er aus Versehen die Daten seines Sohnes angegeben hatte. Vodafone reagierte jedoch nicht auf die Bitte des Vaters, die Daten entsprechend zu ändern, und ließ den Vertrag für weitere 13 Monate mit den Daten des Sohnes laufen.

  Nach der Auffassung der AEPD war die Verarbeitung der personenbezogenen Daten des Sohnes rechtswidrig. Weder der Vater – schon wegen der unbewussten Angabe der Daten – noch der Sohn haben in die Verarbeitung wirksam eingewilligt.

  Zudem speicherte Vodafone die Daten des Sohnes in einer Datenbank, in denen Verzugsschuldner aufgelistet wurden, ohne zuvor die dafür vorgesehene Zeit abzuwarten.

  Die beide Verarbeitungen stellten zusammen nach Auffassung der Behörde einen schwerwiegenden Verstoß gegen Art. 6, Art. 5 DSGVO dar, den die Aufsichtsbehörde mit einem Bußgeld in Höhe von 120.000 Euro belegte.

- **Polen**

  Auch bei unseren polnischen Nachbarn verhängte die Datenschutzaufsichtsbehörde OUDO ein Bußgeld in Höhe von umgerechnet rund 4.700 Euro gegen eine Danziger Grundschule. Diese nutzte biometrische Daten von insgesamt 680 Schülern, um die Bezahlung des Kantinenessens zu verifizieren. Zwar geschah diese Verarbeitung auf Grundlage der Einwilligung der Eltern. Allerdings handelt es sich bei den biometrischen Daten um besonders sensible, bei denen eine Einwilligung für die Verarbeitung nicht ausreicht, wenn ein Gesetz die Einwilligung verbietet. In Polen war jedoch genau dies der Fall. Dadurch, dass in der Schule auch alternative Möglichkeiten zur Verifizierung angeboten wurden, konnte die Verarbeitung der biometrischen Daten auch nicht wegen ihrer Erforderlichkeit gerechtfertigt werden.

  Die polnische Datenschutzaufsichtsbehörde erachtete die Verarbeitung deswegen als rechtswidrig und ahndete sie mit einem Bußgeld in Höhe von knapp 5.000 Euro.

Für alle weiteren Fragen rund um das Datenschutzrecht stehen Ihnen gerne zur Verfügung

Dr. Kristina Schreiber
+49(0)221 65065-337
kristina.schreiber@loschelder.de

Dr. Simon Kohm
+49(0)221 65065-200
simon.kohm@loschelder.de

Impressum

LOSCHELDER RECHTSANWÄLTE
Partnerschaftsgesellschaft mbB
Konrad-Adenauer-Ufer 11
50668 Köln

Tel. +49 (0)221 65065-0, Fax +49 (0)221 65065-110
info@loschelder.de
www.loschelder.de