LOSCHELDER

Newsletter Datenschutzrecht
Juni 2020

Sehr geehrte Damen und Herren,

am 25. Mai hat die DSGVO ihren zweiten Geburtstag gefeiert. Wir verschonen Sie mit Kalauern zu Kinderkrankheiten und Kinderschuhen und fassen Ihnen stattdessen in unserem ersten Beitrag die aus unserer Sicht wichtigsten Entwicklungen der ersten beiden Jahre zusammen.

In unserem zweiten Beitrag befassen wir uns mit der Cookie-Debatte, die mit der aktuellen BGH Entscheidung vom 28. Mai ein vorläufiges Ende gefunden hat. Unser dritter Beitrag befasst sich mit den fachlichen Anforderungen an einen Datenschutzbeauftragten. In unserem vierten Beitrag zeigen wir Ihnen die datenschutzrechtlichen Implikationen der Fahrtenbuchnutzung auf.

Und zu guter Letzt wollen wir Ihnen auch in diesem Monat die besonders interessanten Bußgeldfälle und einige Kuriositäten nicht vorenthalten.

Inhalt

Zwei Jahre DSGVO – (K)ein Grund zum Feiern?

Die DSGVO hat vor und mit ihrem Inkrafttreten im Mai 2018 für erheblichen Wirbel bei nahezu allen Unternehmen gesorgt. Nun, zwei Jahre später, hat die DSGVO mit der Corona-Krise auch ihren ersten Härtetest hinter sich, viele offene Punkte sind diskutiert und nur zu einem kleinen Teil geklärt. In unserem Beitrag dürfen wir Ihnen die Dauerbrenner im Unternehmensalltag zusammenfassen.

- **Bußgelder und Behördenaktivität**

Ja, es hat bisher ganz erhebliche (und öffentlichkeitswirksame) Bußgelder für Verstöße gegen die DSGVO gegeben. Diese richteten sich, soweit ersichtlich und bisher bekannt, ausschließlich gegen Unternehmen und nicht gegen Personen der Geschäftsleitung oder operativ verantwortliche Mitarbeiter (unter dem relevanten deutschen Ordnungswidrigkeitenrecht keine Selbst-verständlichkeit). Im Fokus der Behörden standen dabei eher eindeutige Fälle, zumeist solche, in denen Daten missbraucht oder nicht hinreichend geschützt wurden und so die Datensicherheit beeinträchtigt war. Die deutschen Datenschutzbehörden haben dabei mit ihrem so genannten Bußgeldbemessungskonzept eine streitbare Grundlage geschaffen, mit der sich Bußgelder tagessatzgenau berechnen lassen. Große gerichtliche Schlachten besonders strittiger Rechtsfragen hat es bisher nicht gegeben. Die Behörden konzentrieren sich auf solche Fälle, die sowohl in rechtlicher als auch in tatsächlicher Hinsicht eher eindeutig erscheinen und bei denen zumeist keine ernsthafte Gegenwehr zu erwarten ist.

Deutlich zugenommen hat die Aktivität der Behörden im Übrigen, insbesondere mit Blick auf der Verfolgung von Beschwerden Betroffener. Hierzu werden Unternehmen angehört und aufgefordert, Sachverhalte zu erläutern und letztlich zu kooperieren. Nach unserer Erfahrung lässt sich mit einer sachgerechten und risikoangemessenen Kommunikation in vielen Fällen Schlimmeres vermeiden.

Unternehmen sind gut beraten, die derzeit im Wesentlichen noch herrschende Zurückhaltung der Datenschutzbehörden nicht auf die leichte Schulter zu nehmen. Spätestens mit dem Abklingen der Corona-Krise und der weiteren personellen Aufstockung bei den

Behörden werden diese deutlich aktiver werden und sich auch alltäglicheren Fällen annehmen.

- **Verteilung von Verantwortlichkeiten**

Für die Praxis von ganz erheblicher Bedeutung ist die Frage nach der datenschutzrechtlichen Verantwortlichkeit. Denn nur das Unternehmen, das verantwortlich im Sinne des Gesetzes ist, muss sämtliche Anforderungen aus der DSGVO erfüllen und haftet bei Verstößen. Verantwortlich ist das Unternehmen, das über den Zweck und die Mittel der Datenverarbeitung entscheidet (Art. 4 Nr. 7 DSGVO). In zahlreichen Fällen bedarf dies einer genauen Überprüfung anhand der vertraglichen und technischen Gegebenheiten, insbesondere in Abgrenzung zur ansonsten ebenfalls weit verbreiteten Auftragsverarbeitung. Bei Kooperationen ist darüber hinaus stets zu prüfen, ob ein Fall der gemeinsamen Verantwortlichkeit gem. Art. 26 DSGVO vorliegt. Die sich daraus ergebenden Probleme sind längst nicht bei allen Unternehmen angekommen, sodass es aus unserer Sicht immer nötig ist, sogenannte „Datenschutzverträge", „DPA" oder Klauseln zum Datenschutz genau zu prüfen. In allen Fällen mit datenschutzrechtlicher Relevanz wird hier die entscheidende Weichenstellung vorgenommen. Hierbei ist nicht zu vergessen: Auch beim konzerninternen Datenaustausch müssen die Datenflüsse rechtlich geregelt sein, da auch hier, datenschutzrechtlich, ein Austausch zwischen zwei separaten Einheiten erfolgt.

- **Herstellerhaftung**

Nach allgemeiner Meinung ist die DSGVO nicht an Hersteller von IT-Systemen adressiert. Die Behörden nehmen also in der Regel keine Prüfung von Produkten vor, um diese zu verbieten oder zu „zertifizieren". Allein verantwortlich für den datenschutzkonformen Einsatz bleiben die Anwender, die die Software gegenüber ihren Kunden, Mitarbeitern, Geschäftspartnern etc. einsetzen. Nach den Vorstellungen der DSGVO wird der Markt das Problem nicht datenschutzkonform einsetzbarer Software lösen, indem diese irgendwann nicht mehr nachgefragt wird.

Dass dies jedenfalls derzeit nicht selbstverständlich ist, lässt sich an vielen Beispielen belegen. Dieser Regelungsansatz ist auch von Behördenseite bereits vielfach kritisiert worden. Die überwiegende

Anzahl der Unternehmen sind auf Fremdentwicklung angewiesen und haben nicht die Abnahme- oder Marktmacht, etwaige Funktionalitäten oder Vertragsbedingungen einzufordern. Sie müssen schlicht die Produkte beziehen, die sich am Markt finden. Vielerorts ist daher der Ruf nach einer datenschutzrechtlichen Herstellerverantwortlichkeit laut geworden. Ob und wann eine solche Verantwortlichkeit ins Gesetz kommt, ist derzeit allerdings noch völlig offen. Jedenfalls ist eine baldige Einführung von flächendeckenden Zertifizierungsmöglichkeiten zu erwarten.

Derzeit bleibt Anwendern indes nichts anderes übrig, als sich möglichst genau über die technischen Einzelheiten der eingesetzten Produkte zu informieren zu versichern und über eine sachgerechte Konfiguration eine Vereinbarkeit mit dem Datenschutz zu erreichen. Anbieter müssen ihre Produkte datenschutzkonform gestalten und transparent und verständlich erklären. Nur so entgehen sie einem entsprechenden (vertragsrechtlichen) Mängelrisiko, das sich im Ernstfall zu einem Bußgeldregress ausweiten kann.

- **Betroffeneninformation**

Von ganz erheblicher praktischer Bedeutung ist die Betroffeneninformation: Unternehmen sind nach Art. 13, 14 DSGVO verpflichtet, die Betroffenen zum Zeitpunkt der Datenerhebung bzw. bei Erhebung über Dritte spätestens mit Offenlegung über zahlreiche Einzelheiten der Verarbeitung zu informieren. Diese Pflicht gilt unabhängig von der eingesetzten Technik, der Anzahl der Betroffenen oder dem Zweck der Verarbeitung. Gerade im Außenauftritt müssen Unternehmen darauf achten, eine ordnungsgemäße Information der Betroffenen sicherzustellen, da dies ansonsten Anlass für Abmahnungen und Beschwerden bietet. Eine der meistverbreiteten Formen der Betroffeneninformation stellt sicherlich die Datenschutzerklärung auf Webseiten dar. Hier haben sich mittlerweile viele Standardformulierungen und Methoden eingebürgert, die jedenfalls bisher flächendeckend nicht von den Datenschutzbehörden als unzulässig betrachtet wurden. Eine hinreichende Information ist im Übrigen auch Grundvoraussetzung für die Einholung wirksamer Einwilligungen.

- **Datenpannen**

Den Jahresberichten der Datenschutzbehörden ist zu entnehmen, dass diese seit Mai 2018 mit einer Flut von Meldungen zu angeblichen Datenpannen zu kämpfen haben. Dies liegt zum einen an den gegenüber dem alten Datenschutzrecht deutlich erweiterten Meldepflichten. Zum anderen aber werden nicht zuletzt aufgrund der Bußgeldrisiken und unzureichenden Klärung der Begrifflichkeit oftmals auch solche Vorfälle gemeldet, die bei strikter Prüfung noch keine Verletzung des Schutzes personenbezogener Daten darstellen. In einem solchen Fall ist dies allerdings nicht geboten, worauf auch die Behörden zuletzt ganz deutlich hingewiesen haben. Richtig ist, dass in allen Risikofällen, in denen ein Bezug zum Datenschutz vorliegt, eine sachgerechte und vor allem zeitnahe Prüfung und Dokumentation stattfinden muss, um etwaige Verletzungen zu identifizieren, Verstöße schnellstmöglich abzustellen und um zu beurteilen, ob eine Meldepflicht vorliegt (innerhalb der ersten 72 Stunden).

Eine Pflicht, Vorfälle an die Behörde zu melden, liegt etwa dann nicht vor, wenn keine Verletzung des Schutzes personenbezogener Daten vorliegt (Verletzungserfolg) oder ein Risiko für die Betroffenen ausgeschlossen ist. Werden Daten also „nur“ unrechtmäßig verarbeitet, ohne dass es zu einer unberechtigten Veröffentlichung, Einsichtnahme oder Übermittlung kommt, kann gegebenenfalls schon eine Verletzung verneint werden. Kommen Daten abhanden, die aber derart sicher verschlüsselt sind, dass die Wahrscheinlichkeit einer Entschlüsselung und damit unberechtigten Kenntnisnahme gegen Null tendiert, kann gegebenenfalls das Risiko für die Betroffenen verneint werden. In jedem Fall ist es geboten, eine Einzelfallbeurteilung vorzunehmen (und zu dokumentieren). Gleiches gilt für eine Meldung an die Betroffenen, die nur dann notwendig ist, wenn ein hohes Risiko für die persönlichen Rechte der Betroffenen vorliegt. Hier geht es insbesondere um die Art der betroffenen Daten und die Frage danach, welche negativen Folgen aufgrund der Datenpanne eintreten können.

- **Sensitive Daten**

Sensitive Daten gemäß Art. 9 DSGVO, in der Praxis vor allem Gesundheitsdaten, stehen in jeglicher Hinsicht im Fokus der datenschutzrechtlichen Debatte. Auch außerhalb der Corona-Krise

stellt sich die Frage, unter welchen besonderen Bedingungen solche Daten verarbeitet oder gar nutzbar gemacht werden können. Die DSGVO ist äußerst streng und sieht als Grundsatz nur eine individuelle Einwilligung oder Verträge mit Angehörigen der Gesundheitsberufe als Erlaubnis vor. Die engen Ausnahmen, die insbesondere auf die medizinische Versorgung abzielen, sind daher sorgsam zu prüfen. Mit Blick auf die bestehenden Risiken kann festgestellt werden, dass die Behörden Fälle mit sensitiven Daten mit besonderer Härte verfolgen.

Dennoch wächst der Markt digitaler Gesundheitsanwendungen stetig. Zuletzt ist hier auch gesetzlich nachgesteuert worden: Gesundheits-Apps sind „auf Rezept" erstattungsfähig. Dies gilt indes nur, wenn sie u.a. datenschutzkonform ausgestaltet und vom Bundesinstitut für Arzneimittel und Medizinprodukte in eine Liste erstattungsfähiger digitaler Gesundheitsanwendungen aufgenommen wurden. Zu den Details erscheint in Kürze eine Abhandlung von uns in der Zeitschrift für Datenschutzrecht, die wir Ihnen bei Interesse gerne zukommen lassen.

- **Cookies**

Zum Dauerbrenner Cookies, Pixel und andere Tags in Online-Anwendungen dürfen wir auf unseren zweiten Beitrag verweisen.

- **Auskunftsersuchen**

Nach unserer Erfahrung haben sich Auskunftsersuchen nicht zum Dauerbrenner entwickelt. Zur Erinnerung: Betroffene haben stets das Recht, Auskunft von Unternehmen zu verlangen, ob und welche Daten über sie verarbeitet werden. Kurz nach Inkrafttreten der DSGVO haben viele Betroffene diese neue Möglichkeit genutzt, mittlerweile handelt es sich aber nach unserer Wahrnehmung um Einzelfälle, die dann aber im Detail anhand der derzeitigen Behördenpraxis zu beurteilen sind. Zunehmend werden Auskunftsersuchen „wesensfremd" im Rahmen von Gerichtsstreitigkeiten, gerne auch von ehemaligen Mitarbeitern, genutzt. Besondere Schwierigkeiten ergeben sich dann, wenn zahlreiche und praktisch kaum zusammenstellbare Datenbestände zu dem Antragsteller vorliegen oder wenn nicht mehr festgestellt werden kann, woher die Daten stammen. Es hat sich bewährt, jeden Einzelfall gesondert zu betrachten und auch anhand der Motive

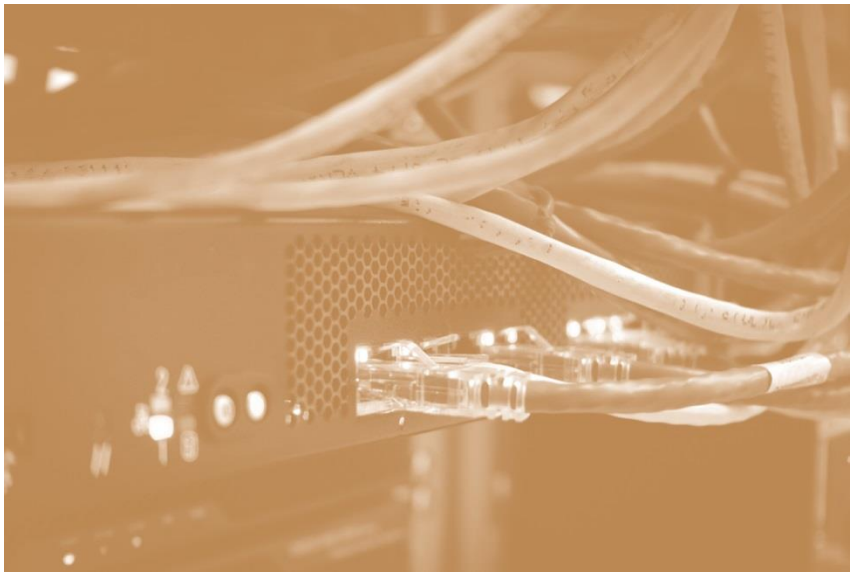
und Vorstellungen des Betroffenen eine sachgerechte und transparente Lösung zu finden.

- **Ausblick**

Die Sensibilisierung für den Datenschutz hat sich in der Bevölkerung, aber auch in Unternehmen massiv gesteigert. Kaum ein internes IT Projekt, eine Betriebsvereinbarung oder ein Compliance-Thema, das nicht den Datenschutz auf den Plan ruft. Gleichzeitig haben die meisten Unternehmen noch mit der Bürokratie zu kämpfen, welche die DSGVO unweigerlich mit sich bringt.

Mit großer Spannung dürfen die ersten Gerichtsentscheidungen zum deutschen Bußgeldbemessungskonzept erwartetet werden, ebenso wie mögliche Aufweichungen der gesetzlichen Vorschriften, gerade mit dem Blick auf die Verarbeitung von Gesundheitsdaten. Gleichzeitig sind Änderungen der DSGVO vorstellbar, vor allem im Bereich der Herstellerhaftung – dies aber angesichts der zurückhaltenden Zeichen aus Brüssel wohl eher lang- als kurzfristig.

Zu guter Letzt sollte nicht aus dem Blickfeld geraten, das mit fortschreitender Digitalisierung das Datenschutzrecht auch hilft: Etablierte Prozesse können genutzt werden, um neue Lösungen zügig zu implementieren. Datenschutz und auch die Nutzung nicht personenbezogener Daten können gewinnbringend für innovative Lösungen genutzt werden, im Rahmen von Datenanalysen wird Mehrwert für künftige Geschäftsstrategien generiert.



Cookies – a (never) ending story

Am 28. Mai 2020 hat der Bundesgerichtshof eine lang erwartete Entscheidung verkündet: Cookies dürfen, soweit nicht unbedingt erforderlich, nur mit Einwilligung verwendet werden. Gleiches gilt für Pixel, Tags, die Nutzung des Local Storage und ähnliches. Eine wirksame Einwilligung liegt dabei nur dann vor, wenn aktiv geklickt, gewischt oder markiert wurde. Das bloße „Weitersurfen" stellt keine wirksame Einwilligung dar. All dies hatte auch der EuGH schon im Oktober in der Rechtssache „planet49" verkündet. All dies ist letztlich seit bald 20 Jahren EU-rechtlich normiert. Neu ist, dass auch das deutsche Recht dies vorsieht. Und der Fokus ist erneut auf die Cookie-Praxis gerückt. Websitebetreiber sind daher spätestens jetzt gut beraten, ihre Cookie-Policy zu überprüfen und, soweit noch nicht erfolgt und einwilligungsbedürftige Cookies gesetzt werden, auf angepasste Consent Management Tools umzusteigen.

Mit dem BGH-Urteil vom 28.05.2020- I ZR 7/16 – Cookie Einwilligung II, von dem bisher nur die Pressemitteilung veröffentlicht ist, hat die Cookie-Saga vor den Gerichten nun einen (vorläufigen) Abschluss gefunden. Danach ist vor dem Einsatz von Cookies auf Websites (und jedem anderen Zugriff auf die Endgeräte der Nutzer) die Einholung einer ausdrücklichen, informierten Einwilligung erforderlich, wenn das Cookie bzw. der Zugriff nicht

„unbedingt erforderlich“ für die Bereitstellung der Website oder die Erbringung des jeweiligen Dienstes ist.

Eines vorweg: Was nun „unbedingt erforderlich“ ist, klärt der BGH nach dem bis jetzt bekannten Entscheidungsinhalt nicht abschließend. Hierüber kann mithin weiterhin gestritten werden.

Nun aber zurück zum Fall und seinen Auswirkungen für die Praxis:

- **Stein des Anstoßes**

Ausgangspunkt des Urteils war eine Klage des Verbraucherzentrale Bundesverbands (VZBV) gegen die Gestaltung eines Gewinnspiels auf der Website planet49. Für die Teilnahme am Gewinnspiel mussten die Nutzer nicht nur ihre Kontaktdaten angeben, sondern auch über die Nutzung dieser Daten durch Sponsoren und Kooperationspartner zur Werbung per Post, Telefon, Email und SMS und über die Verwendung von Marketing-Cookies entscheiden.

- **Rechtliches Hornissennest**

Mit der Klage lenkte der VZBV das Augenmerk auf eine langanhaltende Streitigkeit zum Umgang mit Cookies und Einwilligungen. Letztlich geht es um das Verhältnis des deutschen TMG und zur europäischen ePrivacy-RL. Diese schienen sich nach bisherigem Verständnis zu widersprechen in Bezug auf die Verwendung von Cookies: Das europäische Recht sieht deren Einsatz nur mit Einwilligung vor (Art. 5 Abs. 3 ePrivacy-RL), § 15 Abs. 3 TMG lässt dies für Werbe- und Marketingzwecke auch ohne Einwilligung zu, solange ein Widerspruchsrecht besteht. Seit dem 28. Mai 2020 wissen wir indes, dass hier ein Missverständnis vorliegt: Der BGH legt das nationale Recht richtlinienkonform aus. Heißt übersetzt: In der „korrekten“ Lesart verlangt auch § 15 Abs. 3 TMG eine aktive Nutzereinwilligung.

Dieser BGH-Entscheidung vom 28. Mai 2020 ist ein langwieriger Rechtsstreit vorausgegangen, in dem auch der EuGH eingebunden war (der BGH hatte diesem einige EU-rechtliche Fragen zur Vorabentscheidung vorgelegt). Der EuGH hatte in diesem Komplex am 1. Oktober 2019 entschieden (wir berichteten im Oktober 2019).

- **Was wurde entschieden?**

Der BGH-Entscheidung ist in Sachen Cookie-Einsatz (und ebenso jeder vergleichbare Zugriff auf Endgeräte von Nutzern, ganz unabhängig davon, ob dabei personenbezogene Daten verarbeitet werden oder nicht) dreierlei zu entnehmen:

1. Eine Einwilligung wird immer dann benötigt, wenn Cookies & Co. nicht „unbedingt erforderlich" sind für das Angebot eines Dienstes, auch nach deutschem Recht.
2. Eine Einwilligung ist nur dann wirksam abgegeben, wenn der Endnutzer aktiv handelt, z.B. eine Checkbox anklickt, bevor die Datenverarbeitung erfolgt oder das Cookie gesetzt wird. Eine voreingestellte Checkbox, die abgewählt werden kann, genügt dem ebenso wenig wie ein Hinweis „durch Weitersurfen willigen Sie ein".
3. Der Nutzer muss vor der Verarbeitung transparent über alle Vorgänge informiert werden.

Dogmatisch ist mit Spannung zu erwarten, wie genau der BGH seine Entscheidung begründen wird. Für die Praxis aber bedeutet diese Entscheidung, spätestens jetzt den Einsatz von Cookies und vergleichbaren Tools in den verantworteten Online-Anwendungen nochmals zu überprüfen und dokumentiert zu entscheiden, ob diese mit oder ohne Einwilligung eingesetzt werden, eine etwaige Einwilligung wirksam eingeholt wird und die Nutzer hinreichend transparent informiert werden. Werden durch die Tools personenbezogene Daten verarbeitet, droht ansonsten ein hohes Bußgeld unter der DSGVO. Das ePrivacy-Recht (TMG), welches ohne Personenbezug alleine anwendbar ist, entfaltet seine Schlagkraft dagegen eher über Abmahnungen von Wettbewerbern. Der Markt jedenfalls bietet eine große Anzahl an Tools, um Einwilligungen zu managen („Consent Management Tools"), die auch dort helfen, wo keine eigenen Anwendungen programmiert werden sollen.

Einen Gesamtüberblick mit aktualisierter Cookie-Ampel haben wir jüngst auch für die Werbewirtschaft verfasst. Die Kurzversion ist in der Printfassung der WA Medien erschienen, die Langversion finden Sie hier zum Nachlesen.

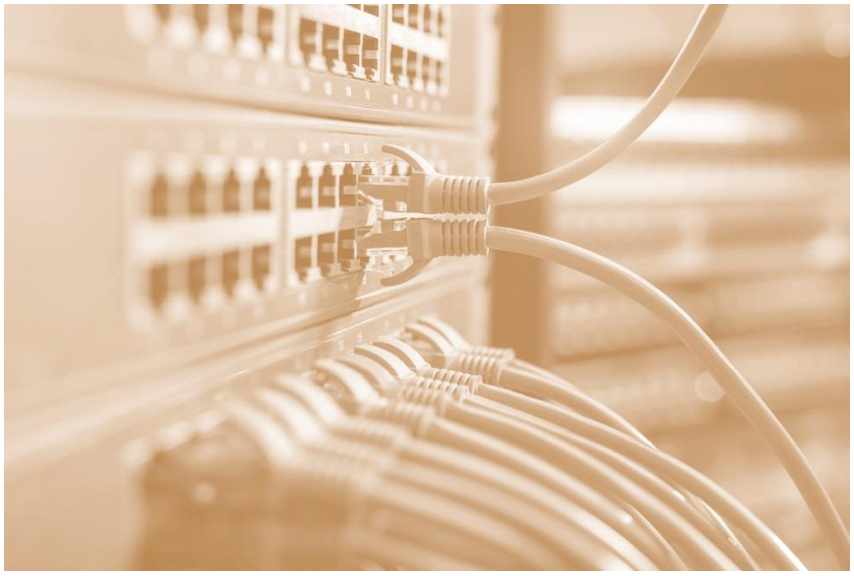
Zur fachlichen Qualifikation des Datenschutz-beauftragten

Schon vor der DSGVO bestand für eine Vielzahl deutscher und europäischer Unternehmen die Pflicht, einen Datenschutzbeauftragten zu bestellen. Dies muss nach aktueller Rechtlage in Deutschland immer dann geschehen, wenn mehr als 20 Personen im Unternehmen ständig mit der Verarbeitung von Daten beschäftigt sind, die Verarbeitung von Daten zur Kerntätigkeit des Unternehmens gehört oder besonders sensible Daten verarbeitet werden. Diese Position kann dann entweder extern besetzt werden oder aber mit einem Angestellten des eigenen Unternehmens. Dabei ist auf eine hinreichende fachliche Qualifikation zu achten. Fehlt sie, kann dies Grund für eine Abberufung oder Kündigung sein.

Entscheidet man sich für eine interne Lösung, so ist zu beachten, dass eine Abberufung von diesem Posten oder eine vollständige Kündigung nunmehr nur noch aus einem „wichtigen Grund“ erfolgen darf. Diese hohe Hürde ist erst dann überwunden, wenn dem Arbeitgeber unter Berücksichtigung aller Umstände und Interessen der Beteiligten ein weiterer Einsatz des Mitarbeiters als Datenschutzbeauftragter nicht mehr zugemutet werden kann. Ein solch wichtiger Grund liegt zum Beispiel vor, wenn der Datenschutzbeauftragte einen Geheimnisverrat begeht oder datenschutzrechtliche Kontrollpflichten dauerhaft verletzt.

In einem vom LAG Rostock zu entscheidenden Fall (LAG Rostock, Urt. v. 25.02.2020 - 5 Sa 108/19) stellte sich die Frage, ob eine Abberufung oder Kündigung auch dann erfolgen darf, wenn der Datenschutzbeauftragte nicht oder nicht mehr über die nötige fachliche Qualifikation verfügt. Das Gesetz setzt keine bestimmte Ausbildung oder näher bezeichnete Fachkenntnisse voraus. Das LAG Rostock führte aus, dass sich die erforderliche Sachkunde ganz nach der Größe des Unternehmens, dem Umfang der anfallenden Daten und eingesetzten IT-Verfahren und der Art der betroffenen Daten richtet. Hierzu solle ein Datenschutzbeauftragter Kenntnisse über Abläufe und Technik der Datenverarbeitung haben und natürlich entsprechendes Wissen im Datenschutzrecht haben. Dieses Wissen gilt es, in fortlaufenden Weiterbildungen zu erhalten. Zudem muss der Datenschutzbeauftragte auch „zuverlässig" sein. Das heißt, der Arbeitgeber muss darauf vertrauen können, dass er seinen Pflichten gewissenhaft nachkommen wird. Das LAG Rostock erkennt zur Feststellung der Unzuverlässigkeit auch Verdachtsmomente an, die nicht explizit datenschutzrechtlichen Bezug haben. So gilt auch als unzuverlässig, wer in anderer Tätigkeit für das Unternehmen zum Beispiel durch Unterschlagung, vorsätzliche Rufschädigung oder Tätlichkeiten gegen Kollegen auf sich aufmerksam gemacht hat. Entscheidend ist also, dass das nötige Vertrauen in den Datenschutzbeauftragten als Institut der Selbstkontrolle nicht mehr besteht.

Die Abberufung oder sogar Kündigung eines Datenschutzbeauftragten ist somit generell möglich. Jedenfalls bei einer Kündigung sind die Hürden indes sehr hoch. Ob ein solches Vorgehen zulässig ist, muss also genauestens geprüft werden, bevor Abberufung (unter erleichterten Voraussetzungen) oder Kündigung ausgesprochen werden.



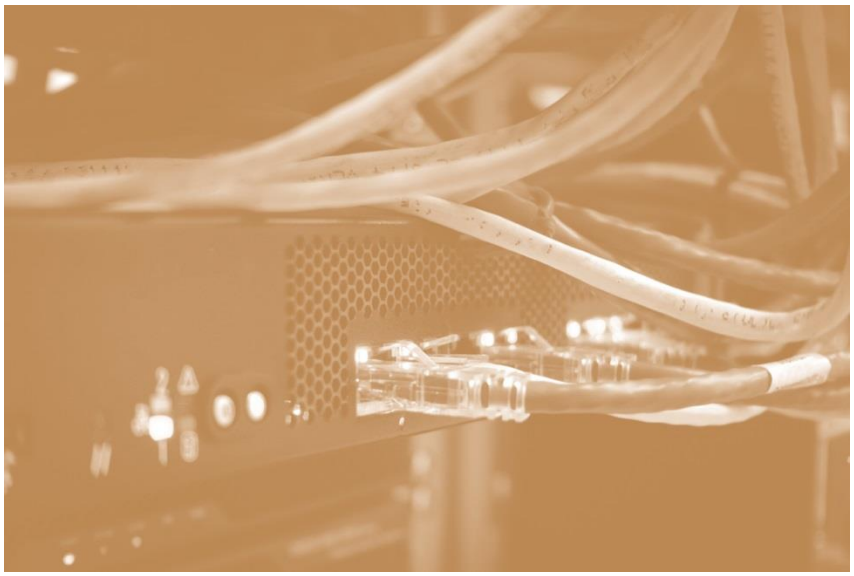
Fahrtenbuch und DSGVO

Das VG München hatte sich mit der Frage beschäftigen, ob die Verpflichtung zum Führen eines Fahrtenbuches und zum Vorzeigen der Aufzeichnungen bei der zuständigen Behörde rechtmäßig war. Dabei kam es gleich zweimal auf die datenschutzrechtliche Beurteilung an.

Im Oktober 2018 wurde das Firmenfahrzeug eines Unternehmens geblitzt. Bei der Befragung des Halters, auf den das KFZ zugelassen gewesen war, gab dieser zwar an, einen ehemaligen Mitarbeiter auf den Lichtbildern zu erkennen. Er weigerte sich jedoch unter Hinweis auf den Datenschutz, der Polizei die Personalien des Fahrers mitzuteilen. Die Behörde konterte mit der Verpflichtung, ein Fahrtenbuch zu führen. Dies war rechtens, wie nun auch das VG München bestätigte.

In datenschutzrechtlicher Hinsicht ist hervorzuheben, dass die Polizei ohne DSGVO-Verstoß entsprechende Informationen verlangen darf: Die DSGVO finde, so das Gericht, bei einer polizeilichen Ermittlung bereits keine Anwendung (Ausnahme nach Art. 2 Abs. 2 lit. d DSGVO), jedenfalls sei sie nach Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO erlaubt. Und auch der Halter sei zur Herausgabe personenbezogener Fahrerdaten befugt, da die Weitergabe der Personalien zur Erfüllung seiner rechtlichen

Mitwirkungspflicht bei der Feststellung des Fahrzeugführers erforderlich sei. Dies begründe ein „berechtigtes Interesse“ ohne überwiegende gegengewichtige Betroffeneninteressen nach Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO.



Zu guter Letzt: Geldbußen des Monats

Auch in diesem Monat gibt es wieder viel über Bußgelder und kuriose Fälle aus dem Ausland zu berichten.

- **Finnland**

Nicht nur der Bundesgerichtshof muss sich mit der Rechtmäßigkeit von Cookie-Bannern auseinandersetzen. Auch die finnische Datenschutzbehörde wurde aufgrund einer Beschwerde mit der Beurteilung eines Cookie-Banners beauftragt. Der Beschwerdeführer war der Ansicht, dass die Gestaltung des Banners die Verweigerung der Speicherung von Cookies erschwerte, die das die Website betreibende Unternehmen überwiegend zum Zweck personalisierter Werbung einsetzte.

Auf dem Cookie-Banner wurde der Nutzer darauf hingewiesen, dass er Cookies akzeptiere, wenn er die Webseite weiterhin

nutze. Dem Nutzer bot sich dann die Möglichkeit, zwischen den Buttons „OK“ und „weitere Informationen“ zu wählen. Ein Klick auf den letzteren Button führte allerdings nur zu der Datenschutzerklärung des Unternehmens. In dieser wird der Nutzer lediglich darauf hingewiesen, dass zum einen unerwünschte Cookies des Unternehmens durch Anpassung der Browser-Einstellungen und zum anderen unerwünschte Third-Party-Cookies durch Anpassung auf der Webseite des Drittanbieters blockiert werden können.

Die finnische Datenschutzbehörde kam zu dem Schluss, dass eine Einwilligung des Betroffenen unter diesen Umständen nicht freiwillig geschieht und ein solches Vorgehen nicht mit den Vorgaben aus Art. 4 Nr. 11 DSGVO zu vereinbaren ist. Sie wies darauf hin, dass eine Einwilligung zudem immer ein aktives Verhalten des Betroffenen voraussetze und ein Schweigen keine Einwilligung darstellen könne. Daneben bemängelte die Behörde, dass die Möglichkeit des Widerspruchs nicht vergleichbar einfach wie die Erteilung der Einwilligung ist. Von einem Bußgeld sah die Behörde in diesem Fall jedoch ab.

- **Niederlande**

Die niederländische Aufsichtsbehörde AP verhängte gegen ein Unternehmen ein Bußgeld in Höhe von 725.000 Euro wegen der Verletzung biometrischer Daten, indem es die Fingerabdrücke ihrer Angestellten verarbeitet.

Die Aufsichtsbehörde untersuchte, ob die Verarbeitung der Fingerabdrücke durch einen Grund aus Art. 6 Abs. 1 DSGVO gerechtfertigt gewesen sei. Allerdings fand die Behörde heraus, dass die Verarbeitung nicht zur Authentifizierung der Arbeitnehmer oder aus sonstigen Sicherheitsgründen erforderlich gewesen ist, sodass ein berechtigtes Interesse im Sinne des Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO nicht in Frage kam. Daneben hätte zwar eine ausdrückliche Einwilligung der Arbeitnehmer die Verarbeitung der Fingerabdrücke nach Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO erlaubt. Dem Unternehmen gelang es jedoch nicht, der Behörde das Vorliegen einer solchen Einwilligung zu beweisen, obwohl es dazu nach Art. 7 Abs. 1 DSGVO verpflichtet gewesen ist.

- **Belgien**

Nachdem ein Datenleck in einem belgischen Unternehmen bekannt geworden war, führte die belgische Aufsichtsbehörde – ohne dass das Leck durch Dritte an die Behörde herangetragen wurde – von Amts wegen die Überprüfung der Datenverarbeitungsprozesse in dem Unternehmen durch.

Das Unternehmen verlangte nach der Untersuchung die Löschung der Aufzeichnungen und stützte dies auf die vermeintliche Unzuständigkeit der Behörde.

Die Prozesskammer der belgischen Aufsichtsbehörde stellte im Rahmen ihrer Entscheidung neben den Verletzungen einiger Normen des belgischen Datenschutzrechts auch eine Verletzung des Art. 31 DSGVO fest, der den Verantwortlichen zur Zusammenarbeit mit der Aufsichtsbehörde verpflichtet.

Das Bußgeld in Höhe von 50.000 Euro verhängte die Kammer jedoch, weil im Zuge der Untersuchungen festgestellt wurde, dass kein Datenschutzbeauftragter in dem Unternehmen ernannt wurde, obwohl dies erforderlich gewesen ist.

- **Schweden**

Die schwedische Datenschutzbehörde verhängte gegen einen Gesundheits- und Ärzteausschuss ein Bußgeld in Höhe von 120.000 SEK (ungefähr 11.350 Euro) weil dieser sensible Patientendaten ohne rechtliche Grundlage auf seiner Webseite veröffentlichte.

Bei ihrer Untersuchung stellte die Datenschutzbehörde fest, dass der Ausschuss keine schriftlichen, sondern nur mündliche Verfahren zur Veröffentlichung von Dokumenten und (personenbezogenen) Daten auf der Webseite führte. Daraus schloss die Behörde, dass der Ausschuss keine angemessenen organisatorischen Maßnahmen ergriffen hatte, um sicherzustellen, dass personenbezogene Daten vor einer falschen Veröffentlichung auf der Webseite geschützt werden. Aus diesem Grund verpflichtete die Behörde den Ausschuss dazu, in Zukunft schriftliche Anweisungen für die Veröffentlichung auf der Webseite einzuführen und durch Verfahren sicherzustellen, dass die Veröffentlichung auch tatsächlich im Einklang mit den Anweisungen vorgenommen wird.

Daneben stellte die Behörde fest, dass es bei der untersuchten Veröffentlichung der sensiblen personenbezogenen Daten an einem ausreichenden Rechtsgrund fehlt.

Diese beiden datenschutzrechtlichen Verstöße brachten die Datenschutzbehörde zur Verhängung eines Bußgeldes in Höhe von umgerechnet rund 11.350 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

Claudia Willmer
+49(0)221 65065-337
claudia.willmer@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