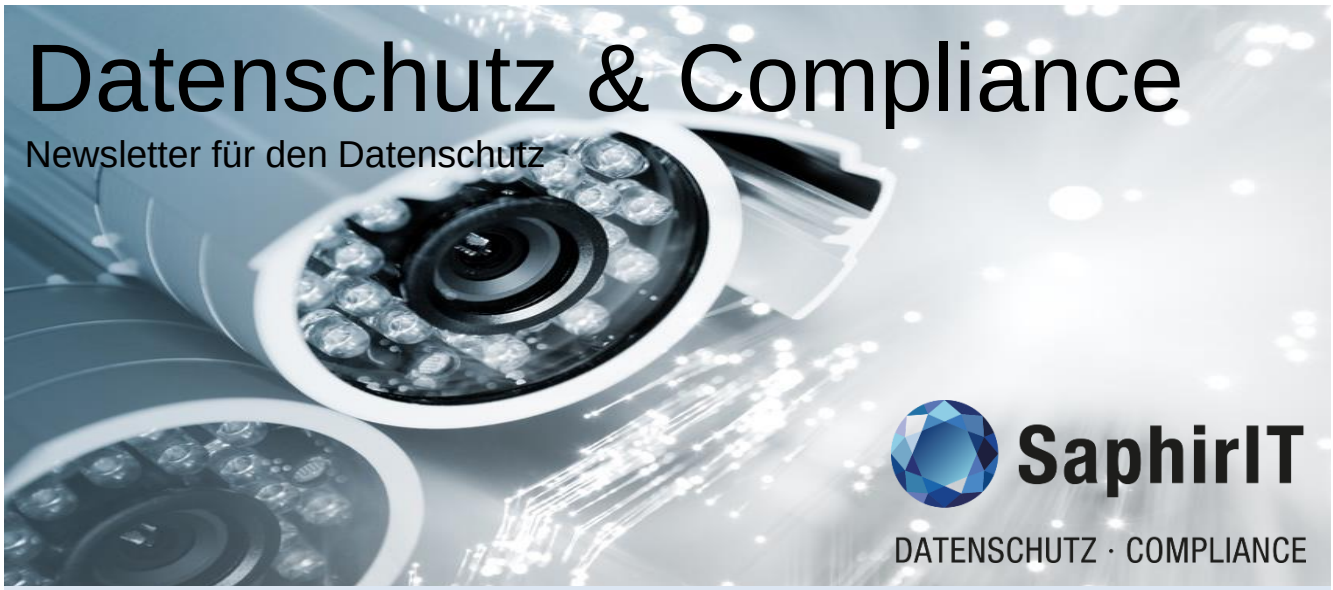

Ausgabe Oktober 2019 | Seite 133 - 136

INHALT

SEITE 133
Update: Datenschutzkonferenz veröffentlicht Berechnungsmodell für Bußgelder

SEITE 134
Datenschutzrechtliche Zulässigkeit von Führerscheinkopien durch den Arbeitgeber

SEITE 135
Schadensersatz nach der DSGVO nur bei konkretem Schadensnachweis

Sehr geehrte Damen und Herren,

hiermit übersenden wir Ihnen unseren Newsletter Oktober 2019.

Wie immer wünschen wir Ihnen viel Spaß bei der Lektüre. Bei Fragen oder Anmerkungen sprechen Sie uns gerne an.

Mit freundlichen Grüßen
Ihre SaphirIT GmbH

Update: Datenschutzkonferenz veröffentlicht Berechnungsmodell für Bußgelder

Bereits in unserem letzten Newsletter September 2019 (abrufbar unter: https://www.saphirit.de/newsletter-flyer.html) hatten wir über das Berechnungsmodell der Datenschutzkonferenz (DSK) berichtet.

Mit Pressemitteilung vom 16.10.2019 hat die DSK nun ihr „Konzept zur Zumessung von Geldbußen bei Verstößen gegen die DS-GVO durch Unternehmen“ vorgestellt.

Das Modell soll, so die DSK, bei der Bemessung von Geldbußen einen Beitrag zur Transparenz im Hinblick auf die Durchsetzung des Datenschutzrechts leisten. Verantwortlichen, wie auch Auftragsverarbeitern soll es möglich gemacht werden, die Entscheidungen der Aufsichtsbehörden nachzuvollziehen und sich in ihre Lage zu versetzen.

Anknüpfungspunkt des Berechnungsmodells ist, wie vom europäischen Gesetzgeber gewollt, der Umsatz eines Unternehmens. Wirk-

same verhältnismäßige und abschreckende Bußgelder sollen sichergestellt werden.

Abrufbar ist das Berechnungsmodell unter: https://www.datenschutzkonferenz-online.de/media/ah/20191016_bu%C3%9Fgeldkonzept.pdf

Datenschutzrechtliche Zulässigkeit von Führerscheinkopien durch den Arbeitgeber

Arbeitgeber sind dazu verpflichtet, wenn sie ihren Mitarbeitern ein Kfz zur Verfügung stellen, zu überprüfen, ob der Mitarbeiter die dafür notwendige Fahrerlaubnis besitzt. Falls der Arbeitgeber dem nicht nachkommt, kann er sich nach § 21 Abs. 1 Nr. 2 StVG strafbar machen.

Für den Fall, dass der Führerschein, oder ein anderes Ausweisdokument, wie Personalausweis oder Reisepass, kopiert wurden, gibt es immer wieder Fälle in denen Betroffene dies monierten und teils auch die Aufsichtsbehörde von diesem Vorgehen in Kenntnis setzten.

Die Erhebung der Daten auf einem Ausweisdokument stellt eine Datenverarbeitung im Sinne der Datenschutzgrundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG) dar (Art. 88 Abs. 1 DSGVO i.V.m. § 26 Abs. 1 BDSG).

Diese Rechtsgrundlage müsste dann auch das Kopieren von Ausweisdokumenten legitimieren.

Zu dieser Rechtsfrage haben sich bereits drei Aufsichtsbehörden in ihren Jahresberichten geäußert.

Die Bremer Landesbeauftragte für den Datenschutz hält eine Anfertigung von Kopien der Führerscheine nicht für erforderlich. Es reiche aus, sich bei jeder Kontrolle davon zu überzeugen, ob der betroffene Mitarbeiter einen gültigen Führerschein besitzt. Das Anfertigen einer Kopie stelle eine Doppelspeicherung dar und verstoße gegen den Grundsatz der Datensparsamkeit, der in der DSGVO verankert ist (vgl. 38. Jahresbericht der Landesbeauftragten für Datenschutz Bremen, 2015, Ziffer 11.2).

Der Hessische Landesdatenschutzbeauftragte sieht dies ein wenig anders und trägt vor, dass eine Kopie und die Ablage in der Personalakte „unter besonderen Umständen“ durchaus erforderlich seien. Auch wenn es sich hierbei um eine recht vage Aussage handelt und es in der Praxis häufig schwierig ist „besondere Umstände“ zu begründen, zeigt sie, dass die Anfertigung von Kopien durchaus auch möglich und gerechtfertigt sein können (44. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten, 2015, Ziffer 4.5.2).

Ungewöhnlich großmütig äußerte sich das Bayerische Landesamt für Datenschutz. Dieses trägt vor, der Führerschein beinhalte nur Informationen, die dem Arbeitgeber ohnehin schon vorlägen, sodass es vertretbar sei Ko-

pien des Führerscheins anzufertigen (6. Tätigkeitsbericht des Bayerischen Landesamtes für Datenschutzaufsicht für die Jahre 2013 und 2014, Ziffer 15.5).

Da die Ansichten der Aufsichtsbehörden in der Sache jedenfalls noch auseinandergehen ist zu empfehlen, wenn möglich auf das Kopieren von Ausweisdokumenten zu verzichten. Das regelmäßige (bspw. halbjährliche) Vorlegen des Ausweises und ein kurzer Vermerk sollten in den meisten Fällen dann ausreichen. Dennoch sollte im Einzelfall der Prozess einmal beleuchtet und bestenfalls niedergeschrieben werden, um Unklarheiten vorzubeugen.

Sollten Sie hierzu Fragen haben sprechen Sie uns gerne an um eine Lösung speziell für Ihr Unternehmen zu finden.

Schadensersatz nach der DSGVO nur bei konkretem Schadensnachweis

Das Amtsgericht Bochum (AG) hat mit Beschluss vom 11.03.2019 entschieden, dass es für einen Schadensersatz nach der Datenschutzgrundverordnung (DSGVO) eines konkreten Schadensnachweises bedarf. Die theoretische Möglichkeit eines Schadens reiche, so das AG, nicht aus.

Gemäß Art. 82 Abs. 1 DSGVO hat jede Person, der wegen eines Verstoßes gegen die DSGVO ein materieller oder immaterieller Schaden entstanden ist einen Anspruch auf Schadensersatz gegen den Verantwortlichen. Ein Verschulden seitens des Verantwortlichen ist dabei nicht nötig.

Der Antragsteller wurde von der Antragsgegnerin behördlich betreut. Der Vorwurf war eine Weitergabe von Daten ohne Einwilligung des Betreuten (Antragsteller).

Die Aufgaben der Betreuerin umfassten Vermögensangelegenheiten, Wohnungsangelegenheiten und die Vertretung gegenüber Behörden.

Eine Bestellungsurkunde diente als Ausweis. Seit Juni 2018 war die Betreuung aufgehoben.

Der Antragsteller trug vor, dass die Antragsgegnerin während der Betreuungszeit personenbezogene Daten an dessen Vermieter und an weitere Stellen herausgegeben habe.

Zudem sei die Bestellungsurkunde unverschlüsselt an den jetzigen Prozessbevollmächtigten übersandt worden.

Der Antragsteller machte einen Schadensersatz geltend.

Da die Betreuung auch den Aufgabenkreis der Wohnungsangelegenheiten umfasste, gehöre die Offenlegung der Betreuung unter Vorlage der Bestellungsurkunde wie auch die Weitergabe an andere Stellen zu den rechtlichen Verpflichtungen der Antragsgegnerin. Einer

Einwilligung nach Art. 6 DSGVO bedürfe es daher nicht, so das Gericht.

Die Übersendung der Bestellungsurkunde an den jetzigen Prozessbevollmächtigten sei aus denselben Gründen rechtmäßig. Lediglich die Versendung als unverschlüsselte E-Mail könne einen Verstoß gegen Art. 32 DSGVO darstellen. Es lägen aber keine Anhaltspunkte vor, dass personenbezogene Daten unbefugten Dritten tatsächlich bekannt geworden seien.

Die theoretische Möglichkeit reiche für die Geltendmachung eines Schadensersatzes nicht aus. Ein Schadensersatzanspruch besteht mithin nicht (AG Bochum, Beschluss v. 11.03.2019, Az. 65 C 485/18).

Kommt es zu einer Klage aufgrund eines möglichen Verstoßes gegen die DSGVO so muss zunächst der Kläger beweisen, dass ein Verstoß gegen die DSGVO tatsächlich vorliegt.

Meist dürfte dies für den Kläger leicht möglich sein, da der Verantwortliche umfassenden Informationspflichten unterliegt. Darüber hinaus muss der Kläger beweisen, dass er einen tatsächlichen Schaden erlitten hat, so das AG.

Die verantwortliche Stelle dagegen muss beweisen, dass sie alle Vorschriften der DSGVO eingehalten hat. In der Praxis stellt dies eines der größten Probleme dar. Verantwortliche sollten immer in der Lage sein einen ordnungsgemäßen Datenschutz nachweisen zu können. Dies dürfte aber nur dann zu erreichen sein, wenn den umfassenden Dokumentationspflichten nachgekommen wird. Ein vollständiges Datenschutzmanagementsystem ist hierbei die beste Möglichkeit sich gegen mögliche Klagen wehren zu können.

Sollten Sie bei sich im Unternehmen noch kein umfassendes Datenschutzmanagementsystem implementiert haben, sprechen Sie uns gerne an.

SaphirIT GmbH
Sutthauser Straße 285
49080 Osnabrück
Geschäftsführer
Amtsgericht Osnabrück

www.saphirit.de
USt-ID-Nr. DE268765300
Frank W. Stroot
HRB 20385

Oldenburgische Landesbank AG
IBAN DE29 2802 0050 5042 8200 00
BIC OLBODEH2XXX

Telefon 0541/60079296
Telefax 0541/60079297
datenschutz@saphirit.de