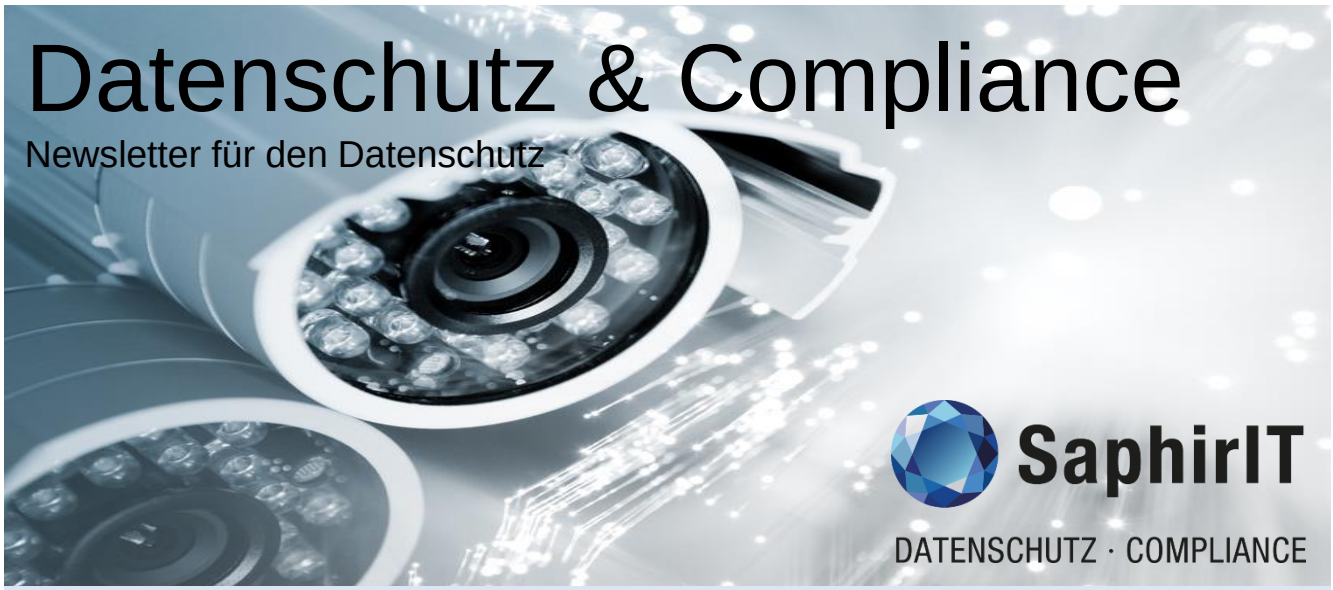

Ausgabe April 2021 | Seite 215 - 219

INHALT

Sehr geehrte Damen und Herren,

hiermit übersenden wir Ihnen unseren Newsletter April 2021.

Viel Spaß bei der Lektüre. Bei Fragen oder Anmerkungen sprechen Sie uns gerne an.

Mit freundlichen Grüßen
Ihre SaphirIT GmbH

Schmerzensgeld wegen unrechtmäßiger Datenweitergabe

In unserer letzten Ausgabe vom März 2021 hatten wir bereits darüber berichtet, dass die Verhängung von Schmerzensgeldern nach der Datenschutzgrundverordnung (DSGVO) bisher nicht einheitlich beantwortet wird (abrufbar unter. https://www.saphirit.de/newsletter-flyer.html).

Einige Gerichte sind der Auffassung die Kläger müssten, sofern sie Schmerzensgeld forderten, darstellen, was für ein konkreter Schaden ihnen entstanden ist.

Zur Frage wann und unter welchem Umständen den Schmerzensgeld nach der DSGVO geltend gemacht werden kann muss sich nun der Europäische Gerichtshof (EuGH) äußern und darstellen wie die Vorschriften der DSGVO auszulegen sind.

Unabhängig von dem Urteil, das wir Ihnen letzten Monat vorgestellt haben, hat das Amtsgericht Hildesheim einem Kläger Schmerzensgeld in Höhe von 800,00 EUR zugesprochen.

In dem Fall ging es um Folgendes:

Der Kläger erwarb von der Beklagten einen PC und speicherte, wie üblich, seine privaten Daten auf dem Betriebssystem.

Nach kurzer Zeit ließ sich der PC jedoch nicht mehr starten, weshalb der Kläger per E-Mail den Kaufvertrag widerrief.

Er erhielt daraufhin eine automatische Eingangsbestätigung, die unter anderem folgenden Passus enthielt:

„Weiterhin möchten wir Sie darauf hinweisen, dass bei Rückgabe von Geräten mit Speichermedien, der Urzustand wieder herzustellen ist. Die Löschung aufgespielter, vertraulicher und personenbezogener Daten liegt in Ihrer Verantwortung.“

Der Kläger übersandte daraufhin den PC an den Beklagten zurück, ohne seine Daten zu löschen, da ihm dies nicht möglich war, da der PC sich nicht starten ließ.

Vor dem Rückversand erhielt der Kläger noch folgenden Hinweis:

„Im Rahmen der Überprüfung bzw. Nachbesserung kann es zur Löschung der Daten auf dem Artikel kommen. Für einen Datenverlust übernehmen wir keine Haftung, es unterliegt vielmehr allein Ihrer Verantwortung für eine Datensicherung zu sorgen. Bitte beachten Sie, dass Sie verantwortlich sind das Gerät zurückzusetzen und ohne Passwörter zu übergeben oder uns alle erforderlichen Passwörter mitzuteilen.“

Der Beklagte nahm eine Wiederaufbereitung vor und versetzte den PC wieder in einen verkaufsfähigen Zustand.

Der PC wurde von der Beklagten daraufhin an den Zeugen H verkauft. Beim Einrichten seines PCs entdeckte dieser die Daten des Klägers auf dem Gerät. Die Daten umfassten Fotos, die Rechnung einer Autowerkstatt und die Steuererklärung des Klägers.

Die Daten waren bei der Wiederaufbereitung von den Mitarbeitern des Beklagten übersehen worden.

Der Beklagte war der Ansicht er habe nicht gegen die DSGVO verstoßen, da es Aufgabe des Klägers gewesen sei die Löschung der Daten vorzunehmen.

Das Amtsgericht Hildesheim hat jedoch zu Gunsten des Klägers entschieden. Der Kläger habe einen Anspruch auf Zahlung eines angemessenen Schmerzensgeldes nach Art. 82 Abs. 1, 2 DSGVO in Höhe von 800,00 EUR.

Gemäß Art. 82 Abs. 1 DSGVO hat jede Person, der wegen eines Verstoßes gegen die DSGVO ein Schaden entstanden ist (materiell oder immateriell) einen Anspruch auf Schadensersatz gegen den Verantwortlichen.

Das Amtsgericht sah hier einen Verstoß gegen die DSGVO.

„Die Beklagte hat vorliegend gegen die DSGVO verstoßen, da sie den von dem Kläger eingeschickten PC ohne dessen Einwilligung an den Zeugen H. veräußert und damit die auf dem PC befindlichen Daten einem Dritten zugänglich gemacht hat. Dies stellt eine nicht rechtmäßige Verarbeitung (Art. 4 Nr. 2 DSGVO) von Daten im Sinne des Artikel 6 Absatz 1 Satz 1 a) DSGVO dar.“

Der Beklagte habe sich durch den Hinweis, dass der Kläger vor Rücksendung des PCs alle Daten löschen sollte, auch nicht der Verantwortung entziehen können für eine rechtmäßige Datenverarbeitung nach der DSGVO zu sorgen. Dem Kläger sei durch die einhergehende Bloßstellung ein immaterieller Schaden entstanden. Auch die Höhe des Schmerzensgeldes von 800,00 EUR sei angemessen, da der Datenumfang nicht unerheblich gewesen sei (AG Hildesheim, Urt. v. 05.10.2020, Az. 43 C 145/19).

Hinweis: Auch wenn es sich momentan wohl noch sehr stark von Gericht zu Gericht unterscheiden kann, ob ein Schmerzensgeldanspruch zugesprochen wird oder nicht zeigt dieses Urteil, dass insbesondere die Implementierung von Lösch- und Kontrollprozessen sehr wichtig ist. Zudem zeigt das Urteil, dass auch ein Hinweis, dass alle Daten vom Betroffenen zu löschen sind, den Verantwortlichen nicht der Verantwortung entziehen.

Sollten Sie Hilfe bei der Erstellung eines Löschkonzeptes benötigen sprechen Sie uns gerne an.

Verdeckte Videoüberwachung am Arbeitsplatz

Eine verdeckte Videoüberwachung am Arbeitsplatz ist grundsätzlich umstritten und allenfalls unter sehr engen Voraussetzungen, insbesondere beim Verdacht des Vorliegens einer Straftat möglich. Das Landesarbeitsgericht Nürnberg (LAG) hat hierzu eine aktuelle Entscheidung gefällt.

Ein Lagermitarbeiter eines Unternehmens soll zwei Jägermeisterflaschen à 0,04l, in einem Bereich fern ab seines Arbeitsplatzes, entwendet haben. Der Arbeitgeber kündigte dem Arbeitnehmer daraufhin fristlos.

In diesem Bereich hatte der Arbeitgeber eine verdeckte Videoüberwachung installiert, da es in dem Bereich mehrfach zu Schwund im Spirituosenbereich gekommen sein soll.

Bei der Videoüberwachung handelt es sich um die Verarbeitung personenbezogener Daten. Grundsätzlich bedarf es daher zur rechtmäßi-

gen Verarbeitung einer Einwilligung der betroffenen Personen.

Das Bundesarbeitsgericht sieht allerdings in § 26 Abs. 1 S. 2 Bundesdatenschutzgesetz (BDSG) eine Ausnahme. Danach ist eine Verarbeitung personenbezogener Daten zur Aufdeckung von Straftaten innerhalb eines Beschäftigungsverhältnisses zulässig.

Voraussetzung dafür sind jedoch folgende Punkte:

- tatsächliche Anhaltspunkte für das Vorliegen einer Straftat
- mildere Ermittlungsmaßnahmen stehen nicht zur Verfügung und
- die Maßnahme ist verhältnismäßig

Der Europäische Gerichtshof für Menschenrechte geht in seiner Rechtsprechung davon aus, dass § 26 Abs. 1 S. 2 BDSG keine geeignete gesetzliche Grundlage für eine verdeckte Videoüberwachung darstellt.

Vielmehr liege darin ein Verstoß gegen das Transparenzgebot, da heimliche Maßnahmen nicht ausdrücklich in § 26 BDSG aufgeführt seien.

Im betreffenden Fall hatte das Arbeitsgericht Würzburg die Videoaufzeichnung sowie die gefertigten Screenshots für unverwertbar erklärt und der Kündigungsschutzklage des Arbeitnehmers stattgegeben.

Das LAG Nürnberg bestätigte nun das Urteil des ArbG Würzburg. Die verdeckte Videoüberwachung sei nicht verhältnismäßig gewesen, da nicht alle Maßnahmen zur Erforschung des Sachverhalts ausgeschöpft gewesen seien.

Das LAG führte hierzu aus: *„Hier konnte die Beklagte nicht zur Überzeugung des Gerichts darstellen, dass sie vor der Installation und Inbetriebnahme der Überwachungskamera andere, nicht in das Persönlichkeitsrecht der Arbeitnehmer eingreifende Mittel zur Aufklärung des Verdachtes des Diebstahles von Spirituosen ausgeschöpft hat und die Kameraüberwachung das praktisch einzig verbliebene Mittel zur Aufklärung der Täterschaft war.“*

Der Bundesgerichtshof (BGH) entschied in einem anderen Fall, entgegen der Auffassung des LAG, dass auch Zufallsfunde bei verdeckter Videoüberwachung verwertet werden könnten.

Der Einsatz von verdeckter Videoüberwachung ist in der Rechtsprechung umstritten und nicht einheitlich beantwortet.

Der Einsatz verdeckter Videoüberwachung kann nur die „Ultima Ratio“, also das letzte Mittel zur Aufklärung eines Verdachts einer Straftat sein darf. Sofern eine verdeckte Überwachung stattfindet muss diese möglichst wenig einschneidend für die Rechte der Mitarbeiter in zeitlicher und räumlicher Hinsicht sein.

Grundsätzlich sollten Unternehmen immer abwägen, ob eine verdeckte Überwachung tatsächlich notwendig ist und überprüfen welche anderen Schritte möglicherweise zu ergreifen sind, um bestimmte Sachverhalte aufzuklären. Es ist stets zu prüfen, ob ein milderes Mittel in Betracht kommt. Beispielsweise eine Taschenkontrolle oder ähnliche Maßnahmen, die weniger einschneidend sind (LAG Nürnberg, Urt. v. 08.12.2020, Az. 7 Sa 226/20).

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