

Datenschutz & Compliance

Newsletter für den Datenschutz



SaphirIT

DATENSCHUTZ · COMPLIANCE

Ausgabe Oktober 2017 | Seite 33-37

INHALT

SEITE 33

BAG: Überwachung eines Mitarbeiters durch Detektiv zulässig

SEITE 35

Datenweitergabe in die USA: EuGH muss erneut über Standardvertragsklauseln entscheiden

SEITE 36

Geldbuße wegen Dashcam Einsatz im Auto

Sehr geehrte Damen und Herren,

hiermit übersenden wir Ihnen unseren aktuellen Newsletter Oktober 2017.

Wir wünschen Ihnen viel Spaß bei der Lektüre.

Mit freundlichen Grüßen
Ihre SaphirIT GmbH

BAG: Überwachung eines Mitarbeiters durch Detektiv zulässig

- Nachweisbarkeit eines Fehlverhaltens des Arbeitnehmers -

Das Bundesarbeitsgericht (BAG) entschied, dass die Überwachung eines Mitarbeiters durch den Arbeitgeber unter Zuhilfenahme eines Detektivs bei Vorliegen eines begründeten Verdachts einer schwerwiegenden Pflichtverletzung datenschutzrechtlich nicht zu beanstanden ist.

Ausgangspunkt war die Kündigung durch einen Arbeitgeber aufgrund eines Fehlverhaltens des

Arbeitnehmers. Dieses Fehlverhalten galt es nachzuweisen.

Der besagte Arbeitnehmer war seit ca. 40 Jahren im Betrieb seines Arbeitgebers beschäftigt. Im Jahr 2013 eröffneten die Söhne des Arbeitnehmers einen eigenen Betrieb, welcher in derselben Branche wie der Arbeitgeber tätig war.

Ab 2014 kam es jedoch vermehrt dazu, dass der Arbeitnehmer arbeitsunfähig krankgeschrieben war. 2015 dann konnte er überhaupt nicht mehr arbeiten.

Der Arbeitgeber bekam im Laufe der Zeit zufällig Kenntnis von einer E-Mail des Unternehmens der Söhne. In dieser E-Mail warben diese mit der 38-jährigen Berufserfahrung ihres Vaters. Der Arbeitgeber erlangte folglich den Verdacht, dass sein Arbeitnehmer die Krankheiten nur vortäuschte, um wettbewerbswidrig für das andere Unternehmen tätig sein zu können.

Der Arbeitgeber beauftragte in Folge dieses Verdachts einen Detektiv mit der Observation seines Arbeitnehmers. Der Verdacht erhärtete sich aufgrund dieser Ermittlungen. Daraufhin kündigte der Arbeitgeber dem Arbeitnehmer außerordentlich fristlos.

Der gegen die Kündigung klagende Arbeitnehmer war der Auffassung, dass die gesammelten Beweise ihn in seinem Recht auf Datenschutz verletzen, weshalb sie nicht gegen ihn verwertbar seien. Außerdem sei er ohnehin tatsächlich krank gewesen und habe nicht wettbewerbswidrig gehandelt. Das Gericht hatte somit zu klären, ob und inwiefern dem Arbeitnehmer ein Fehlverhalten nachgewiesen werden konnte.

§ 32 Bundesdatenschutzgesetz (BDSG) dient als eigenständige Norm für den Datenschutz im Beschäftigungsverhältnis. Demnach dürfen personenbezogene Daten des Arbeitnehmers nur insoweit erhoben, verarbeitet oder genutzt

werden, wenn diese Daten für die Begründung, Durchführung oder Beendigung des Arbeitsverhältnisses notwendig sind. Nach § 32 Abs. 1 Satz 2 BDSG ist es aber ferner zulässig, personenbezogene Daten zu erheben, wenn dies zur Aufdeckung von Straftaten notwendig ist. Dies ist aber nur der Fall, wenn tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat und eine Erhebung, Verarbeitung oder Nutzung der Daten nicht unverhältnismäßig erscheint.

Die Vorinstanz stützte sich auf den klaren Wortlaut des § 32 BDSG welcher eine Straftat verlangt und kam zu dem Ergebnis, dass es sich im vorliegenden Fall nicht um eine Straftat, sondern lediglich um eine Treupflichtverletzung gehandelt habe. § 32 Abs. 1 Satz 2 BDSG komme somit nicht zur Anwendung. In einem solchen Fall könne dann auch nicht ersatzweise auf § 32 Abs. 1 Satz 1 BDSG zurückgegriffen werden, weshalb das Gericht die Datenerhebung durch den Detektiv im Ergebnis für rechtswidrig hielt.

Das BAG vertrat diese Auffassung nicht. Die Tatsache, dass hier eine mögliche schwerwiegende Treupflichtverletzung keine Straftat darstelle schließe den Rückgriff auf § 32 Abs. 1 S. 1 BDSG nicht aus. Vielmehr ginge es im Wortlaut des Absatzes 1 Satz 1 ausdrücklich um die Beendigung von Beschäftigungsverhältnissen. Dennoch sei wie auch bei Abs. 1 S. 2 ein Eingriff nur unter Abwägung der beiderseitigen Interessen nach dem Grundsatz der Verhältnismäßigkeit erlaubt.

Ausschlaggebend sei hier, dass ein konkreter Verdacht einer schwerwiegenden Pflichtverletzung gegeben sei und dieser auch nicht mit einem milderem Mittel hätte beseitigt werden können. Das BAG kam folglich zu dem Ergebnis, dass der Eingriff in die Persönlichkeitsrechte des Arbeitnehmers hinter dem Interesse des Arbeitgebers zur Aufklärung einer schwer-

wiegenden kündigungsbegründenden Pflichtverletzung zurückbliebe. Die Kündigung des Arbeitgebers sei demnach nicht nur rechtmäßig, sondern auch aus datenschutzrechtlicher Sicht nicht zu beanstanden (BAG Ur. v. 29.07.2017, Az. 2 AZR 597/16).

Datenweitergabe in die USA:

EuGH muss erneut über Standardvertragsklauseln entscheiden

Der Oberste irische Gerichtshof vertritt nach einer Klage seiner Datenschutzbehörden die Auffassung, dass die Weitergabe privater Daten durch Facebook gegen EU-Datenschutzrecht verstoßen könnte. Über diese Weitergabe privater Kundendaten auf Basis von Standardvertragsklauseln in die USA hat nun der Europäische Gerichtshof (EuGH) zu entscheiden.

Das erste Mal ins Rollen gebracht wurde das Verfahren 2015, als der österreichische Jurist Max Schrems, in seinem ersten Verfahren gegen die Weitergabe von Daten durch Facebook-Irland erreichte, dass das Safe-Harbour Abkommen gekippt wurde (siehe unser Sonderrundbrief vom Oktober 2015).

Nach Ansicht der irischen Datenschutzbehörden verstoßen die momentan geltenden Standardvertragsklauseln bei der Weitergabe von Daten gegen EU-Datenschutzrecht. Dieser Auffassung hat sich der irische Gerichtshof angeschlossen. Die irischen Richter wollen die von der EU Kommission zugelassenen Stan-

dardvertragsklauseln vom EuGH überprüfen lassen.

Nicht nur Facebook, sondern auch viele andere Unternehmen haben nach Annullierung des Safe-Harbour Abkommens und nicht auch zuletzt wegen der immer wieder aufkommenden Diskussion am Nachfolgeabkommen „Privacy Shield“, ihren Datentransfer in die USA mit Hilfe genau dieser Standardvertragsklauseln möglich gemacht. Für viele Unternehmen war und ist dies die einzig praktisch nutzbare Alternative.

Nach der Entscheidung über das Safe-Harbour Abkommen hatte Schrems die irische Datenschutzbehörde aufgefordert, die Weitergabe von Daten in die USA zu stoppen. Es bestünde nämlich keine ausreichend sichere Rechtsgrundlage, die einen angemessenen Schutz gewährleisten könne. Facebook Irland habe unter Safe-Harbour den US Behörden sensible Daten praktisch auf dem Silbertablett präsentiert.

Schrems hatte gefordert, die irische Datenschutzbehörde hätte von der in den Standardvertragsklauseln enthaltenen „Notfall-Regelung“ Gebrauch machen müssen. Diese Regelung erlaube Datenschützern den Datentransfer einseitig zu stoppen. Hiergegen zog die irische Datenschutzbehörde jedoch mit der Begründung vor Gericht, dass eine einseitige Anwendung des Stopps gegen Facebook gegen den Gleichbehandlungsgrundsatz verstoße. Da die zuständige irische Richterin die Bedenken an der Erlaubnis eines Datentransfers auf Basis der Standardvertragsklauseln teilt, stimmte sie, mit der Begründung eine einheitliche Anwendung der von der EU Kommission

genehmigten Transfers sei in der Gemeinschaft sehr wichtig, der Vorlage beim EuGH zu.

Einem sicheren Datentransfer in die USA ist nicht erst seit dieser Vorlage eine besonders wichtige Bedeutung zuzumessen. Es bleibt abzuwarten, wie der EuGH zu den Standardvertragsklauseln entscheiden wird. Denn diese Entscheidung wird nicht nur Facebook Irland, sondern auch sämtliche Unternehmen die ihren Datentransfer momentan via Standardvertragsklauseln regeln, treffen.

Geldbuße wegen Dashcam-Einsatz im Auto

- Anlassloses Filmen geparkter Fahrzeuge verletzt Recht auf informationelle Selbstbestimmung -

Das Amtsgericht München entschied mit Urteil vom 09.08.2017, dass das anlasslose Filmen von anderen geparkten Fahrzeugen durch eine im Fahrzeug platzierte Dashcam eine unbefugte Erhebung und Bereithaltung von personenbezogenen Daten darstellt. Es werde damit gegen das Bundesdatenschutzgesetz (BDSG) verstoßen.

Die zu einem Bußgeld von 150,00 EUR verurteilte 52-jährige Frau, wollte der Polizei mit den gewonnenen Aufnahmen helfen, eine mögliche Beschädigung ihres Fahrzeuges aufzudecken. Platziert hatte sie die Kameras sowohl vorne, als auch hinten in ihrem Fahrzeug. Durch die Kameras wurde jedoch nicht nur ihr PKW, sondern auch der hinter dem Fahrzeug befind-

liche öffentliche Verkehrsraum aufgenommen. Während der Zeit der Aufnahmen zwischen 13:00 und 16:00 Uhr wurden mindestens auch drei andere Fahrzeuge durch die Kameras aufgenommen. Da ein anders Auto tatsächlich ihr Auto streifte, wollte die Dame die Aufnahmen der Polizei als Beweismittel vorlegen.

Daraufhin wurde jedoch ein Bußgeldverfahren gegen die Frau eingeleitet und ein Bußgeldbescheid wurde ihr zugestellt. Sie legte mit der Begründung, es seien keine anderen Menschen, insbesondere Gesichter anderer Fahrer, durch die Kameras aufgenommen worden und bei Kennzeichen handele es sich nicht um schützenswerte Informationen, Einspruch ein. Es sei ihr lediglich darauf angekommen poten-

tielle Täter einer möglichen Sachbeschädigung zu überführen.

Das Gericht vertrat die Auffassung, dass das Recht der Gefilmten auf informationelle Selbstbestimmung überwiege und das Interesse am Aufdecken einer Straftat dahinter zurückstehen müsse. Es liege ein schwerwiegender Eingriff in das Recht auf informationelle Selbstbestimmung durch das anlasslose Filmen vor.

Es ginge nach Ansicht des Gerichts nicht, dass 80 Millionen Bundesbürger mit Kameras herumlaufen würden, um möglicherweise irgendwelche strafbaren Situationen aufnehmen zu können. Gerade die im vorliegenden Fall permanente Überwachung des öffentlichen Raumes durch eine Privatbürgerin sei nicht zulässig, da Unbeteiligte nicht selbst bestimmen könnten, wann und wo sie sich aufhielten, ohne, dass unbeteiligte Personen dies dokumentierten und bei Behörden verwenden würden.

Die Frage ob von Dashcams aufgenommene Videoaufnahmen verwendet werden dürfen bzw. überhaupt Aufnahmen getätigt werden dürfen beschäftigt die Gerichte in den letzten

Jahren zunehmend. Die Rechtsprechung dazu ist dabei nicht immer unbedingt einheitlich.

So hatten wir in unserem letzten Newsletter September 2017, einen Fall des Oberlandesgerichts (OLG) Nürnberg geschildert, welches entschieden hatte, dass unter bestimmten Voraussetzungen Dashcam Aufnahmen in einem Zivilprozess verwendet werden dürfen. Das OLG Stuttgart entschied in einem ähnlichen Fall, bei dem es um die Aufklärung eines Verkehrsunfalls ging auch, dass die Aufnahmen verwertbar seien. Das Landgericht Rottweil dagegen hatte die Nutzung des Materials in der Vorinstanz nicht zugelassen.

Generell kann nach momentaner Rechtslage nur davor gewarnt werden das Verkehrsgeschehen auf eigene Faust mit Kameras aufzunehmen. Auch die Bundesdatenschutzbeauftragte Andrea Voßhoff warnte ausdrücklich davor solche Aufnahmen zu tätigen, da dies datenschutzrechtlich grundsätzlich nicht zulässig sei (AG München, Urt. v. 09.08.2017, Az. 1112 OWi 300 JS 121012/17).

Falls Sie unseren Newsletter in Zukunft nicht mehr erhalten möchten, schicken Sie bitte eine kurze E-Mail an info@saphirit.de

SaphirIT GmbH
Sutthäuser 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

