LOSCHELDER

Newsletter Datenschutzrecht

August 2019

Inhalt

Angedrohte Bußgelder für Marriot International Ltd. und British Airways– Spätfolgen eines Unternehmenskaufs und unzureichender Datensicherheit

Datenschutzrechtliche „Altlasten" können Unternehmenskäufern auch nach Jahren teuer zu stehen kommen; dies zeigt ein kürzlich angekündigtes Bußgeld der britischen Datenschutzaufsichtsbehörde (ICO) in Höhe von £ 9.200.396. Die Hotelkette Marriot International Ltd. soll für eine Datenpanne von Starwood belangt werden, mit dem es im Jahre 2016 fusionierte. Betroffen sind 339 Millionen Gästedaten weltweit; 30 Millionen davon betreffen Kunden aus 31 Ländern des Europäischen Wirtschaftsraums. Der Vorwurf der Aufsichtsbehörde ist, Marriot International Ltd. habe beim Kauf von Starwood keine ausreichende Due Diligence durchgeführt und hätte seine IT besser schützen müssen. Und auch in einem weiteren UK-Fall droht ein ganz erhebliches Bußgeld von über 200 Mio. Euro – gegen British Airways, ebenfalls wegen fehlender Datensicherheit.

Im Fall Marriott International waren bereits 2014 personenbezogene Daten durch einen Cyber-Vorfall bei Starwood kompromittiert. Marriot International Ltd. bemerkte den Vorfall aber nicht im Rahmen des Unternehmenskaufs, sondern erst im Jahr 2018 und meldete ihn sodann im November 2018 der Aufsichtsbehörde. Das Bußgeld ist noch nicht final; das Unternehmen hat noch Gelegenheit, zu der Bußgeldhöhe Stellung zu nehmen. Die Ankündigung zeigt aber, in welcher Größenordnung eine Datenpanne dieses Ausmaßes bebußt und vor allem wie teuer eine nachlässige Daten-Due-Diligence werden kann. Auf die datenschutzrechtlichen Pflichten beim Asset-Deal und auf die Positionierung der Datenschutzkonferenz zu typischen Fallgruppen haben wir in unserem Juli-Newsletter hingewiesen.

Ebenfalls eine unzureichende Datensicherheit ist Grund für das von der ICO im Fall British Airways angekündigten Bußgelds: 2018 sollen dort Cyberkriminelle von rund 500.000 Kunden Kreditkarteninformationen inklusive CVV-Nummern (Sicherheitscodes) abgegriffen haben.

Gemeinsame Verantwortlichkeit beim Einsatz von Social Media-PlugIns

Am 29. Juli 2019 erließ der EuGH sein Urteil in der Sache Fashion ID (Rs. C-40/17). Wir hatten in unserem Januar-Newsletter bereits ausführlich über die Schlussanträge des Generalanwalts in dieser Sache berichtet. Der Websitebetreiber Fashion ID hatte den (damals noch verbreiteten) „Gefällt-mir"-Button von Facebook auf seiner Seite integriert. Der Button war als aktives PlugIn eingebunden, d.h. Nutzerdaten von Website-Besuchern (IP-Adresse, Webbrowser-Kennung, Cookies sowie Datum und Zeit des Aufrufs) wurden unabhängig davon an Facebook übermittelt, ob der Nutzer auf den „Gefällt mir"-Button klickt oder einen Facebook-Account hat. Der „Gefällt-mir"-Button ist mittlerweile zwar überholt, aber das Urteil dürfte auf die datenschutzrechtliche Beurteilung aktiver PlugIns von Drittanbietern generell übertragbar sein.

Der EuGH bestätigte den Generalanwalt darin, dass ein Website-Betreiber, der ein Social Media-PlugIn eines anderen Anbieters einbindet, datenschutzrechtlich verantwortlich ist, soweit der Websitebetreiber tatsächlich über die Zwecke und Mittel entscheidet. Er und der Anbieter des PlugIns sind gemeinsam Verantwortliche im Sinne von Art. 26 DSGVO. Das heißt am Beispiel des „Gefällt mir"-Buttons: Soweit der Websitebetreiber über das Erheben der in Rede stehenden Daten und deren Weitergabe durch Übermittlung tatsächlich entscheidet, ist er dafür mitverantwortlich, muss eine gesonderte Einwilligung einholen und den Nutzer eigens informieren. Für die anschließende Datenverarbeitung durch Facebook trägt der

Websitebetreiber hingegen keine Verantwortung. Bereits mit den Schlussanträgen haben wir empfohlen, die eigenen (Online-) Marketing-Maßnahmen nochmals daraufhin zu untersuchen, ob personenbezogene Daten von (potentiellen) Kunden an Drittunternehmen weitergeleitet werden und, wenn dies der Fall ist, ob hierfür eine Erlaubnis (oder ein Auftragsverarbeitungsvertrag) gegeben ist sowie eine hinreichend transparente und frühzeitige Information erfolgt.

Das bedeutet konkret, in den Datenschutzhinweisen der Website auf die eingebundenen Drittangebote hinzuweisen und über die damit in Zusammenhang stehenden Erhebungen und Übermittlungen zu informieren. Zudem gilt es bei der Nutzung aktiver PlugIns *vor* der Nutzung der Website den Betroffenen klar und unmissverständlich zu informieren. So könnte ein zusätzliches Banner oder Hinweis der Websitenutzung vorgeschaltet werden, um den Betroffene stets vor der Erhebung und Weitergabe seiner Daten über die Datenverarbeitung zu informieren. Sie darf zudem nur erfolgen, wenn der Benutzer auf „einverstanden" geklickt hat – das bloße „Übergehen" des Banners, das bloße Weitersurfen stellen keine Einwilligung dar.

Eine einfachere Websiteeinbindung kann durch sog. „Zwei-Klick-Systeme" oder die noch benutzerfreundlichere sog. „Shariff-Lösung" erfolgen. Bei Zwei-Klick-Systemen werden die Buttons auf der Website *deaktiviert* eingebunden und angezeigt; aktiviert werden sie erst durch einen Klick des Nutzers, mit einem zweiten Klick können dann Inhalte geteilt werden. Heise online beispielsweise bediente sich eines solchen Tools zur Einbindung des Gefällt-mir-Buttons und bietet diesen als open source an. Bei der ebenfalls von heise als open source angebotenen Shariff-Lösung entfällt ein Klick, weil die HTML-Links nicht über iframes eingebunden werden müssen. Dadurch wird eine Aktivierung der Buttons nicht erforderlich.

Der Landesbeauftragte für Datenschutz und Informationsfreiheit NRW hat angekündigt, dass die deutschen und europäischen Datenschutzaufsichtsbehörden in nächster Zeit noch prüfen und konkretisieren werden, was das Urteil nach ihrer Ansicht im Einzelfall für die Praxis bedeutet. Es bleibt abzuwarten.

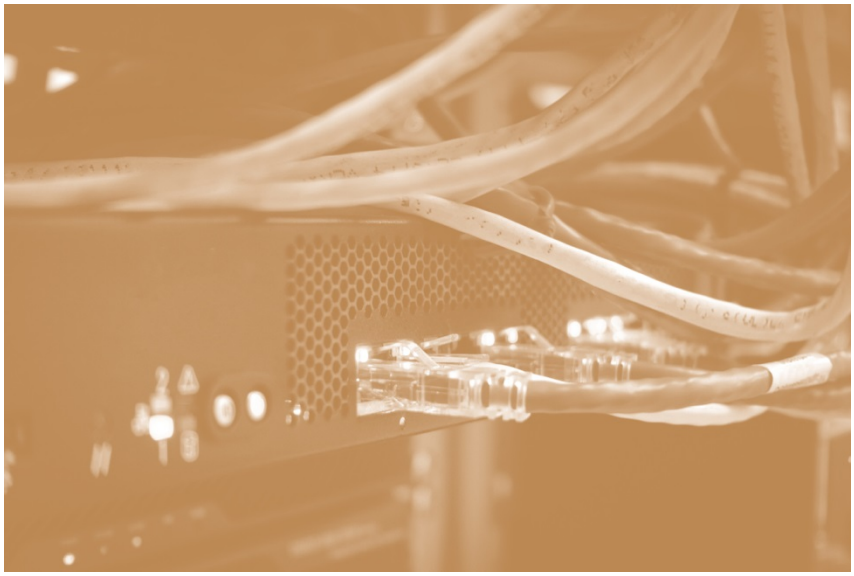
Gewinnspielteilnahme gegen Werbeeinwilligung zulässig

Das OLG Frankfurt hat in einem richtungsweisenden Urteil festgehalten, dass bei transparenter Gestaltung die Teilnahme an einem Gewinnspiel davon abhängig gemacht werden darf, dass der Teilnehmer in künftige E-Mail-Werbung einwilligt. Diese Verknüpfung war mit Inkrafttreten der DSGVO in Verruf geraten, da im neuen Datenschutzrecht ein strengeres „Kopplungsverbot" enthalten ist. Die Entscheidung des OLG Frankfurt hält nun überzeugend fest: Es gibt kein allumfassendes Kopplungsverbot. Dies eröffnet Gestaltungsoptionen.

Eine datenschutzrechtliche Einwilligung ist nur dann wirksam, wenn sie freiwillig erteilt wird. Die Kopplung an eine andere Leistung oder Vergünstigung kann der Freiwilligkeit einer Einwilligung entgegenstehen und ist daher grundsätzlich verboten (sog. „Kopplungsverbot"). In seiner Entscheidung vom 27.06.2019 hat das OLG Frankfurt (6 U 6/19) nun überzeugend festgehalten, dass Freiwilligkeit eine echte, freie Wahl des Betroffenen voraussetzt, die Einwilligung zu verweigern oder zu widerrufen, ohne Nachteile zu erleiden. Es dürfe kein Druck auf den Betroffenen ausgeübt werden. Zentral ist folgende Aussage: „Ein bloßes Anlocken durch Versprechen einer Vergünstigung, etwa - wie hier - einer Teilnahme an einem Gewinnspiel, reicht dafür aber nicht aus (…). Einer Freiwilligkeit steht … nicht entgegen, dass die Einwilligungserklärung mit der Teilnahme an einem Gewinnspiel verknüpft ist. Der Verbrau-

cher kann und muss selbst entscheiden, ob ihm die Teilnahme die Preisgabe seiner Daten „wert“ ist.“

Diese Entscheidung bestätigt, dass auch unter dem neuen Datenschutzrecht Gestaltungsspielräume bestehen und etwa besondere Vergünstigungen und Gewinnspielteilnahmen mit der Akzeptanz von Werbung verknüpft werden dürfen. Maßgeblicher Faktor für eine freiwillige Einwilligung in diesen Konstellationen – oder auch eine wirksame Erlaubnis über die Vertragserfüllung – ist stets eine transparente und hinreichend deutliche Information der Betroffenen.



Zwangsgeld in Höhe von 5.000 Euro für Auskunftsverweigerung gegenüber Behörde

Datenschutzrechtliche Informationsersuchen der Behörden müssen ernst genommen werden. Selten kommt es daher vor, dass Behörden mittels Repressionen gegen Unternehmen vorgehen müssen, um solche Ersuchen durchzusetzen. Anders in einem Fall, über den das Verwaltungsgericht Mainz kürzlich zu entscheiden hatte. Das VG Mainz bestätigte in seinem Urteil vom 09.05.2019 (Az.: 1 K 760/18.MZ.), dass eine Datenschutzbehörde ein Zwangsgeld in Höhe von 5.000 Euro androhen und festsetzen darf, wenn sich ein Verantwortlicher „beharrlich“ weigert, den behördlichen Fragebogen auszufüllen.

Die Klägerin war Betreiberin eines Tanzlokals und filmte im Außen- und Innenbereich ihres Lokals, insbesondere auch in den Separees,

mit der Begründung, vor der Begehung von Straftaten abschrecken zu wollen. In den Separees sei es häufiger zu strafrechtlich relevanten Handlungen gekommen. Nachdem die Betreiberin einem Informations- bzw. Auskunftsersuchen des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz hinsichtlich der Videoaufnahmegeräte nicht nachkam, drohte dieser zunächst ein Zwangsgeld in Höhe von 500 Euro und aufgrund der andauernden Weigerung schließlich ein Zwangsgeld in Höhe von 5.000 Euro an.

Das VG Mainz erachtete das Zwangsgeld als angemessen, weil sich die Betreiberin „beharrlich“ weigerte und möglicherweise Videoaufnahmen von sexuellen Handlungen gefertigt würden. Die Aufnahmen beträfen also potenziell sensible Daten. Darauf, dass die Vornahme sexueller Handlungen arbeitsvertraglich verboten sei, könne sich die Verantwortliche nicht zurückziehen, da offenbar faktisch sexuelle Handlungen vollzogen würden und es nicht auszuschließen sei, dass dies insoweit von der Klägerin geduldet wird.

Informations- bzw. Auskunftsersuchen dürfen also durch Zwangsgelder durchgesetzt werden auch empfindliche Höhen erreichen. Je sensibler die möglicherweise rechtswidrig verarbeiteten Daten sind und je länger die Auskunftsverweigerung andauert, desto höher darf das Zwangsgeld ausfallen. Bei der Beurteilung ist auf die tatsächliche Lage abzustellen.

Neues zum Auskunfts- und Berichtigungsanspruch

Ein interessantes Berufungsurteil zum Umfang und Zweck des Auskunftsanspruchs fällte das OLG Köln am 26. Juli 2019 (Az. 20 U 75/18). Der Kläger, ein Versicherungsnehmer der beklagten Versicherung, begehrte unter anderem Auskunft nach Art. 15 DSGVO. Nach seiner Ansicht umfasste sein Auskunftsrecht nicht nur seine Stammdaten, sondern auch etwaige auf seine Person bezogene Telefonprotokolle, interne Dokumentationen oder Vermerke. Er erhoffte sich, durch die Auskunft Informationen zu erlangen, die ihm die Durchsetzung seines ebenfalls gegen die Beklagte geltend gemachten Schadensersatzanspruches erleichterten. Das OLG bestätigte den Kläger in seiner Ansicht und widersprach damit der bisherigen Linie des LG Köln (Az.: 26 O 360/16 und 26 O 25/18). Das Auskunftsrecht umfasse auch interne Gesprächsvermerke und Telefonnotizen, in denen Aussagen eines Betroffenen oder Aussagen über den Betroffenen festgehalten werden. Die Auskunft konnte im konkreten Fall auch nicht mit dem Hinweis auf fehlende Suchmöglichkeiten oder fehlende wirtschaftliche Ressourcen verweigert werden. Das OVG Hamburg konkretisierte den Berichtigungsanspruch aus Art. 16 DSGVO (5 Bf 225/18.Z): Nach Namensänderung gibt dieser kein Recht auf auch rückwirkende Anpassung der Personalakte an den neuen Namen.

Die datenschutzrechtlichen Fragen waren in dem Verfahren vor dem OLG Köln nur ein Teilproblem, aber die Antworten des OLG sind äußerst aufschlussreich. Zur Verweigerung der Auskunft im konkret geltend gemachten Umfang berief sich die Beklagte unter anderem auf ihre Geschäftsgeheimnisse. Es verletze Geschäftsgeheimnisse, würde der Begriff des personenbezogenen Datums derart weit gefasst, dass davon auch interne Telefonprotokolle, Dokumentationen oder Vermerke mit personenbezogenen Inhalten umfasst würden. Zudem sei es der beklagten Versicherung als Großunternehmen, das einen umfangreichen Datenbestand verwalte, mit den ihr zur Verfügung stehenden Ressourcen wirtschaftlich unmöglich, Dateien auf personenbezogene Daten zu durchsuchen und zu speichern. Beide Argumente wies das OLG unmissverständlich zurück. Personenbezogene Telefonvermerke und Gesprächsnotizen seien ohne weiteres personenbezogene Daten im Sinne der DSGVO. Außerdem seien Daten, die der Betroffene selbst preisgegeben habe, im Verhältnis zum Betroffenen nicht schutzwürdig und vom Begriff des Geschäftsgeheimnisses nicht umfasst. Es sei überdies Aufgabe des Verantwortlichen, der sich der elektronischen Datenverarbeitung bedient, diese im Einklang mit den datenschutzrechtlichen

Anforderungen zu organisieren und sicherzustellen, dass den sich hieraus ergebenden Rechten Dritter Rechnung getragen wird.

Zum Berichtigungsanspruch nach Art. 16 DSGVO hielt das OVG Hamburg fest, dass die klagende Polizistin ihren Vornamen nicht rückwirkend in der Personalakte berichtigen lassen kann: Die Änderung des Vornamens wirkt ex nunc, nicht ex tunc. Daher ist der in früheren Vermerken und Eintragungen enthaltene frühere Vorname auch nicht unrichtig (geworden).

Leitlinien zur Videoüberwachung veröffentlicht

Der Europäische Datenschutzausschuss hat einen Leitfaden zu den datenschutzrechtlichen Grundsätzen der Nutzung von Videoaufnahmegeräten veröffentlicht (Guidelines 3/2019). Für die datenschutzrechtliche Beurteilung von Videoüberwachungssystemen auf Firmengelände bietet der Leitfaden interessante Hinweise; Überraschungen enthält er nicht.

Zunächst zur Erlaubnis für die Speicherung von Videoaufnahmen: Nach dem Leitfaden können Videoüberwachungssysteme auf dem Unternehmensgelände grundsätzlich nur auf den Erlaubnistatbestand des berechtigten Interesses gestützt werden, Art. 6 Abs. 1 lit. f DSGVO. Dieses muss – wie bei jeder Datenverarbeitung – im Einzelfall begründet werden. Hierfür ist nach dem Leitfaden keine drohende Gefahr des konkreten Unternehmens erforderlich. Ein rein prophylaktisches Interesse ist jedoch auch nicht berechtigt.

Beispielhaft sind als Gründe Vandalismus in der Nachbarschaft oder der besonders hohe Warenwert von z. B. Juwelierstücken genannt. Werden die Aufnahmen so gespeichert, dass die Gesichter irreversibel verzerrt werden, enthalten die Videoaufnahmen nach dem Leitfaden kein personenbezogenes Datum mehr („*Anonymisierung*").

Auch zur Speicherdauer finden sich Hinweise. Nach Ansicht des Europäischen Datenschutzausschusses ist eine Speicherung von Videoaufnahmen dann nicht mehr erforderlich, wenn feststeht, dass keine Straftat begangen wurde. Bei einem kleinen Geschäft beispielsweise wisse der Geschäftsinhaber in der Regel nach einem Tag, ob eine Straftat begangen wurde. Aufgrund des Wochenendes oder nach einer Straftat sei aber eventuell eine längere Speicherdauer angemessen. Es sind also stets angemessene Speicherdauern für den Einzelfall zu bestimmen, dokumentiert zu begründen und Löschprotokolle einzurichten.

Aufgrund der möglicherweise hohen Zahl von Betroffenen auf den Videos und der Sensibilität von Videoaufnahmen sei auch sicherzustellen, dass keine Aufnahmekopien unnötigen Umfangs herausgegeben werden. Vom Betroffenen müsse und dürfe etwa im Rahmen von Auskunftsverlangen gefordert werden, dass er sich klar identifiziert und konkretisiert, zu welchem Zeitpunkt er auf den Videoaufnahmen erscheint. Bei einem Einkaufszentrum beispielsweise, das 30.000 Personen täglich besuchen, sei ein Zeitraum von zwei Stunden anzugeben, in dem der Betroffene an der Videokamera vorbeigegangen ist.

Schließlich enthält der Leitfaden noch ein Beispiel für ein Hinweisschild. Bei der Angabe der Informationen sei auf zwei Ebenen zu arbeiten. Auf dem Schild seien nur die wichtigsten Informationen aufzunehmen, wie Angaben zum Verantwortlichen oder die Benennung des Erlaubnistatbestandes (Ebene 1). Auf die weiteren Datenschutzhinweise (Ebene 2), die anderorts abgelegt sind (z. B. unter einem Link abrufbar oder als Auslage an der Rezeption einsehbar), könne auf dem Schild hingewiesen werden.

Die Guidelines sind abrufbar unter:

https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201903_videosurveillance.pdf

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

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

Dr. Lucyne Ghazarian
+49 (0)221 65065-222
lucyne.ghazarian@loschelder.de

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

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