Luther.

Newsletter IP/IT

DSGVO: Office 365, Bußgeld-Katalog, Cookies & Co.

4. Ausgabe 2019

Inhalt

Datenschutzkonformer Einsatz von Microsoft Office 365

Hintergrund

Der Einsatz von Microsoft Produkten (angefangen bei Windows 10, über klassische Anwendungen wie Word, Excel und Powerpoint bis hin zu modernen Working-Tools wie Skype und Teams) wurde bisher von den Datenschutzaufsichtsbehörden sehr kritisch gesehen. Insbesondere die von den einzelnen Anwendungen erhobenen diagnostischen Daten (sog. Telemetriedaten) sowie Daten aus den "Connected Services" (Rechtschreibprüfung, Übersetzungsmodul, etc.) und die weitere Verarbeitung und Auswertung dieser Daten durch Microsoft selbst und sogar durch Dritte werden als nicht datenschutzkonform angesehen.

Vorreiter Niederlande und technische Änderungen von Microsoft

Die Aufsichtsbehörden in den Niederlanden haben für den flächendeckenden Einsatz von Office 365 in der gesamten Verwaltung sogenannte Datenschutzfolgenabschätzungen (DSFA) nach Art. 35 DSGVO durchgeführt. In der ersten DSFA, die Anfang des Jahres veröffentlicht wurde, wurden noch erhebliche datenschutzrechtliche Risiken festgestellt. Danach waren weitreichende Änderungen am Produkt notwendig, um es im Einklang mit der Datenschutzgrundverordnung (DSGVO) nutzen zu können. Die Niederlande und Microsoft verhandelten hiernach intensiv miteinander, schlussendlich machte Microsoft diverse Zugeständnisse: es wurden einige (technische) Änderungen vorgenommen, um den Datenfluss bei Verwendung von Office 365 auf ein datenschutzkonformes Maß zu begrenzen. Eine erneute Einschätzung ergab, dass der Einsatz von Office 365 aufgrund der vorgenommenen Änderungen geringere Risiken mit sich bringt.

Sonderrolle mobile Version und Office Online

Zu beachten ist allerdings, dass derzeit weder die mobilen Versionen der Office-Apps, die per Apple App Store bzw. Google Play Store, noch die Dienste von Office Online ausreichend datenschutzkonform betrieben werden können. Von einer Benutzung dieser Dienste sollte daher gegebenenfalls abgesehen werden, solange es hierzu keine Anpassungen seitens Microsoft oder eine neue Einschätzung gibt.

Akuter Handlungsbedarf

Gerade mit Blick auf die mit dem neuen Bußgeldmodell zu erwartende deutliche Erhöhung von Strafen für Datenschutzverstöße sollten Unternehmen den Einsatz von Office 365 und Windows 10 kritisch hinterfragen und auf eine sichere Basis stellen. Dies erfordert die Auseinandersetzung mit den technischen Neuerungen und die Implementierung entsprechender (auch organisatorischer und vertraglicher) Maßnahmen.

Gerne stehen wir Ihnen bei der Einführung von Microsoft Office 365 mit unseren Experten zur Seite. Durch unsere umfassende Erfahrung und Expertise im Datenschutz und IT-Recht können wir Sie umfassend beraten. Nehmen Sie hierzu einfach jederzeit Kontakt mit uns auf.

Checkliste zur Einführung von Microsoft Office 365

√	**Datenschutzfolgenabschätzung** Führen Sie eine Datenschutzfolgenabschätzung durch, um die im Unternehmen bestehenden oder potentielle Risiken im Umgang mit Windows 10 und Office 365 zu identifizieren und zu dokumentieren.
√	**Besonderheiten bei technischer Ausgestaltung** Es müssen organisatorische und technische Änderungen im Zusammenhang mit den Microsoft-Produkten vorgenommen werden (u. a. Updates auf aktuellere Versionen für datenschutzrelevante Einstellmöglichkeiten; Einführung zusätzlicher Verschlüsselung). Diese Änderungen und Einstellungen müssen ebenfalls in der Datenschutzfolgenabschätzung dokumentiert werden. Übrigens muss auch die Entscheidung gegen die Durchführung einer Datenschutzfolgenabschätzung oder einzelner Maßnahmen muss begründet dokumentiert werden.
√	**Vertragsgestaltung** Die Verträge mit Microsoft müssen überprüft und gegebenenfalls neu verhandelt werden. Denn die Neubewertung von Office 365 und Windows 10 basiert auch auf der Änderung vertraglicher Regelungen. Die Erfolgsaussichten hierfür sind abhängig von der Größe des Unternehmens, mit den Ergebnissen aus den Niederlanden und dem zunehmenden Druck der Aufsichtsbehörden in der EU bestehen jedoch gewichtige Argumente für (Nach)Verhandlungen.
√	**Änderungen bei Datenschutzverträgen** Die Verantwortlichkeiten in Bezug auf den Datenschutz müssen geprüft und gegebenenfalls festgelegt werden. Es ist derzeit unklar, ob Microsoft als Auftragsverarbeiter oder sogar als gemeinsamer Verantwortlicher mit dem jeweiligen Unternehmen tätig wird. Jedenfalls ist der Abschluss einer entsprechenden Vereinbarung erforderlich.
√	**Drittstaatentransfer** Die Übermittlung von Daten in Drittländer außerhalb der EU (insbesondere die USA) muss abgesichert werden. Microsoft ist zwar nach dem Privacy-Shield zertifiziert und bietet auch EU-Standard-Vertragsklauseln an, die eine Übermittlung zulässig machen würden. Diese Instrumente werden derzeit jedoch durch den europäischen Gerichtshof (EuGH) geprüft und können gegebenenfalls für ungültig erklärt werden. Eine Lösung könnte künftig die Nutzung der neuen Deutschland-Cloud von Microsoft sein.
√	**Betrieblicher Datenschutz** Mitarbeiter müssen in den Datenschutzhinweisen auf den Einsatz von Microsoft-Produkten und die Folgen hingewiesen werden. Interne Datenschutzrichtlinien müssen angepasst, Mitarbeiter gegebenenfalls entsprechend geschult werden.
√	**Betriebsvereinbarungen** Sofern ein Betriebsrat vorhanden ist, muss der Einsatz von Microsoft-Produkten mit diesem abgestimmt und eine entsprechende Betriebsvereinbarung abgeschlossen werden. Sofern bestimmte Dienste nicht deaktiviert werden können, müssen entsprechende Dienstanweisungen zur Nichtbenutzung erlassen werden.
√	**Schutz von Geschäftsgeheimnissen** Es bietet sich an, beim „Upgrade“ auf Microsoft Office 365 auch dem Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) Beachtung zu schenken, das seit April 2019 in Kraft ist. Microsoft bietet zahlreiche Funktionalitäten, die Teil eines Schutzkonzeptes für Geschäftsgeheimnisse sein können.

Neues Bußgeldmodell der deutschen Datenschutzbehörden – Höhere Strafen zu erwarten

Am 16. Oktober 2019 haben die deutschen Datenschutzaufsichtsbehörden das neue Modell zur Berechnung von Bußgeldern bei Verstößen gegen die Datenschutzgrundverordnung (DSGVO) durch Unternehmen veröffentlicht. Das Abstimmungsgremium der deutschen Datenschutzbehörden, die Datenschutzkonferenz (DSK), hat ein Konzept entwickelt, um eine einheitlichere und nachvollziehbarere Bußgeldverhängung in Deutschland zu ermöglichen.

Hintergrund

In der Vergangenheit haben sich die deutschen Behörden bei der Verhängung von Bußgeldern wegen Datenschutzverstößen sehr zurückhaltend verhalten, häufig galt das Gebot „Kooperation vor Strafe“. Dadurch sollten Unternehmen angeleitet werden, die DSGVO zu akzeptieren und aus eigenem Antrieb datenschutzkonforme Prozess einzuführen, anstatt lediglich das Risiko eines Bußgeldes als Anlass für einen stärkeren Datenschutz zu sehen. Andere EU-Länder haben jedoch von dem Bußgeldrahmen, den die DSGVO ermöglicht, bereits umfassend Gebrauch gemacht. So hat in diesem Jahr die britische Datenschutzbehörde ICO bereits Bußgelder in Höhe von 200 Millionen Euro gegen die Fluggesellschaft British Airways und 100 Millionen Euro gegen die Hotelkette Marriott angekündigt. Schon zuvor forderte die Aufsichtsbehörde in Frankreich von Google ein Bußgeld über 50 Millionen Euro. Durch das neue Bußgeldmodell werden sich deutschen Bußgelder der Praxis aus Frankreich und Großbritannien annähern und damit deutlich höher ausfallen als bisher. Die öffentlichkeitswirksamen Mitteilungen aus Berlin über die Bußgelder gegen Delivery Hero (in Höhe von ca. 200.000,00 €) und in voraussichtlich zweistelliger Millionenhöhe gegen ein noch unbekanntes Unternehmen dürften nur der Anfang sein (eine Übersicht deutscher und europäischer Bußgelder finden Sie in unserem Bußgeldatlas).

Ziel des neuen Bußgeldmodells ist es, den Datenschutz-aufsichtsbehörden eine einheitliche Methode zur Verfügung zu stellen, die eine systematische, transparente und nachvollziehbare Form der Bemessung von Geldbußen bei Datenschutzverstößen von Unternehmen ermöglicht. Die sich daraus ergebenden höheren Strafen sollen gleichzeitig abschreckend wirken und die Umsetzung bzw. Beachtung des Datenschutzes sicherstellen. Die neue Berechnungsgrundlage ist dabei von nun an für alle deutschen Datenschutz-aufsichtsbehörden verbindlich. Das Modell entfaltet allerdings keine Bindungswirkung gegenüber Gerichten und Europäischen Behörden. Es besteht jedoch die Möglichkeit, dass sich das deutsche Modell (zumindest teilweise) auch auf europäischer Ebene etablieren wird. Denn die Festlegung auf ein Berechnungsmodell oder gar die Vorstellung eines selbst entwickelten Berechnungsmodells durch das Abstimmungsgremium der europäischen Datenschutzbehörden steht noch aus. Die DSK hat aber bereits angekündigt, dass ein solches Konzept bei Inkrafttreten das nun geltende Modell verdrängen würde

Die Berechnungsweise nach dem neuen Bußgeldmodell

Das neue Modell zur Bußgeldbemessung orientiert sich im Wesentlichen an den Vorgaben des Art. 83 DSGVO und unterteilt sich in fünf Schritte:

1. Zunächst wird das verantwortliche Unternehmen in eine Größenklasse kategorisiert, die sich nach dem weltweit erzielten Jahresumsatz des vorangegangen Geschäftsjahres des Unternehmens richtet.

2. Anschließend wird der mittleren Jahresumsatz der jeweiligen Untergruppe (Kleinstunternehmen, kleine und mittlere Unternehmen oder Großunternehmen), in die das Unternehmen eingeordnet wurde, bestimmt.

3. Auf dieser Grundlage wird der wirtschaftliche Grundwert ermittelt: die Behörden errechnen einen sog. „Tagessatz“ indem sie den weltweiten Vorjahresumsatz des Unternehmens durch 360 teilen.

4. Anschließend wird der Verstoß mithilfe tatbezogener Einzelfallumstände einem bestimmten Schweregrad zugeordnet und mit einem entsprechenden Faktor multipliziert.

5. Zuletzt erfolgt eine Anpassung des Grundwertes anhand aller sonstigen, bisher nicht berücksichtigten Umstände des Einzelfalls. Dabei müssen alle für und gegen das verantwortliche Unternehmen sprechende täterbezogene sowie sonstige Umstände berücksichtigt werden.

Folgen des neuen Berechnungsmodells

Das neue Berechnungsmodell wurde bereits durch einzelne Behörden getestet, die konsequente, deutschlandweite Anwendung dürfte in den nächsten Monaten intensiviert werden. Gravierende Rechtsunsicherheiten können sich dabei aus dem erheblichen Spielraum der Aufsichtsbehörden bei der Bewertung der Umstände des jeweiligen Einzelfalls ergeben. So steht es weiterhin im Ermessen der Behörde, einen Verstoß einem Schweregrad zuzuordnen.

Die transparentere Bußgeldberechnung kann aber auch Vorteile für Unternehmen haben: sie können nun im Fall von Verstößen gemeinsam mit Datenschutzbeauftragten und Risikomanagern zu erwartende Bußgelder deutlich präziser als bisher bestimmen. Eine genaue Berechnung ist jedoch weiterhin nicht möglich. Auch sieht die DSGVO grundsätzlich keine Ermäßigung bei mehreren Datenschutzverstößen vor. Die Aufsichtsbehörden beabsichtigen daher, jeden Verstoß individuell zu bewerten und den Gesamtbetrag aus der Summe der einzelnen Bußgelder zu bestimmen. Das mag zunächst für die Annahme von sehr hohen Bußgeldern sprechen. Es besteht aber auch die Möglichkeit, dass der so bestimmte Betrag aufgrund der individuellen Umstände geringer ausfällt als die Gesamtsumme der für jeden einzelnen Verstoß ermittelten Bußgelder.

Worauf Unternehmen nun achten sollten

Noch mehr als bisher gilt der Grundsatz „Vorsorge statt Nachsorge“. Unternehmen sollten das neue Berechnungsmodell zum Anlass nehmen, ihre Datenschutzorganisation kritisch zu hinterfragen. Durch eine durchdachte und an der DSGVO orientierte Datenschutzorganisation können Bußgelder in Millionenhöhe am effektivsten vermieden werden.

Doch auch wenn bereits eine Untersuchung wegen eines Datenschutzvorfalls läuft und die Verhängung eines Bußgeldes konkret droht, bestehen noch Möglichkeiten, dieses zu reduzieren. Insbesondere eine umfassende und transparente Kooperation und Kommunikation mit den Aufsichtsbehörden dürfte wohlwollend aufgenommen werden und gegebenenfalls mildernd in die Berechnung einfließen. Im Ernstfall besteht zudem immer die Möglichkeit, noch gerichtlich gegen das Bußgeld vorzugehen. Dies dürfte insbesondere dann sinnvoll sein, wenn die Berechnung des Bußgelds anhand des Modells zu erheblichen finanziellen Nachteilen führt, z. B. wenn das am Umsatz bemessene Bußgeld nicht im Verhältnis zum Gewinn eines Unternehmens steht. Mangels Bindungswirkung des Modells können die Gerichte die Höhe des Bußgeldes im Verfahren jedoch selbst bestimmen und den Betrag gegebenenfalls den Umständen entsprechend anpassen.

Das endgültige Aus für „Opt-Out“ bei Cookies – EuGH schafft Klarheit

Website-Betreiber müssen bei der Einholung von Einwilligungen ihrer Nutzer zur Datenverarbeitung (z. B. im Rahmen von Cookies, Tracking oder Werbung) zukünftig immer das sog. „Opt-In“-Verfahren beachten. Das bedeutet insbesondere, dass eine Einwilligung aktiv erfolgen muss, indem der Nutzer eine Schaltfläche anklickt oder ein Häkchen zur Bestätigung setzt. Bisher war es umstritten, ob nicht auch eine vorausgefüllte, aber abwählbare Zustimmung ausreicht, das sog. „Opt-Out“. Darüber hinaus hat der EuGH auch die Anforderungen an die Information des Nutzers bei der Einholung einer Einwilligung konkretisiert. Website-Betreiber sind nun angehalten, diese Vorgaben umsetzen.

■ EuGH, Urt. v. vom 01.10.2019, C 673/17

Hintergrund

Nahezu jedes Unternehmen holt Einwilligungen der Nutzer zur Datenverarbeitung auf seiner Website ein. Vom Anbieten von nützlichen Funktionen (z. B. Warenkörben beim Online-Shopping) über statistische Analyse bis hin zum Marketing (z. B. individualisierte Werbung) werden Einwilligungen für eine Vielzahl von Funktionen genutzt. Mal sind sog. „Cookie-Banner“, die zur Einholung von Einwilligungen eingesetzt werden, dezent am Bildschirmrand platziert, mal füllen sie (häufig unzulässig) den halben oder gar den ganzen Bildschirm aus. Immer häufiger werden auch Consent-Manager genutzt, die eine datenschutzkonforme Einholung und Dokumentation von Einwilligungen sicherstellen sollen. In vielen Fällen ist die Einwilligung jedoch „vorausgefüllt“ und muss vom Nutzer abgewählt werden, wenn er eine Verarbeitung seiner Daten vermeiden möchte.

Ob diese Einwilligung tatsächlich aktiv und freiwillig erfolgt und somit den Anforderungen der DSGVO genügt, war bisher umstritten: die eher strengen deutschen Aufsichtsbehörden verneinten dies in der Regel, Unternehmen und Wirtschaftsanwälte waren eher der Meinung, dass (zumindest in bestimmten Fällen) diese „Opt-Out“-Lösung ausreichend sei. Eine klarstellende höchstrichterliche Entscheidung existierte bisher nicht.

Die Vorlage

Der nun vom EuGH entschiedene Fall basiert auf einer Anfrage des deutschen Bundesgerichtshofs (BGH) und richtet sich teilweise nach altem Recht zum Datenschutz. Der BGH stellte in seinen Fragen jedoch bereits stets auch auf die DSGVO ab, sodass die Entscheidung des EuGH auf die Lage nach der DSGVO übertragbar sein dürfte. Der BGH wollte vom EuGH unter anderem wissen, ob

- eine wirksame Einwilligung vorliegt, wenn ein vorhandenes Kästchen zur Cookie-Setzung bereits angekreuzt ist und
- inwiefern der Nutzer durch den Seitenbetreiber bezüglich der Verwendung von Cookies aufzuklären ist und ob hierzu auch die Zugriffsmöglichkeit von Dritten auf die Cookies sowie die Funktionsdauer gehört.

Diesen Fragen liegt ein Streit zwischen dem Gewinnspielbetreiber Planet49 und dem Bundesverband der Verbraucherzentralen und Verbraucherverbände (vzbz) zugrunde. Letzterer hatte gegen die Vorgehensweise von Planet49 im Rahmen der Teilnahme an einem Online-Gewinnspiel geklagt, bei welcher ebenfalls Cookie-Banner eingesetzt wurden. Neben der – nicht vorausgefüllten – Einwilligung zum Erhalt von Werbung fand sich auf der Website eine bereits vorausgefüllte, abwählbare Formulierung zur Zustimmung des Setzens von Cookies. In der damit lediglich gegebenen „Opt-Out“-Möglichkeit sah der vzbz einen Verstoß gegen datenschutzrechtliche Vorschriften, insbesondere gegen Regelungen der Datenschutzrichtlinie für elektronische Kommunikation (RL 2002/58/EG, auch „ePrivacy-Richtlinie“), deren relevante Vorgaben in Deutschland insbesondere im Telemediengesetz (TMG) zu finden sind..

Die Entscheidung

Am 01. Oktober 2019 entschied der EuGH (C 673/17), dass die „Opt-Out“-Lösung nicht den Anforderungen an eine wirksamen

Einwilligung genügt. Im Ergebnis schloss sich der EuGH mit seiner Entscheidung den Empfehlungen des Generalanwalts Maciej Szpunar in dessen Schlussanträgen vom 21. März 2019 an.

Von einer aktiven Einwilligung, wie es die ePrivacy-Richtlinie vorsehe, könne bei einem vorausgefüllten Einwilligungsfeld nicht die Rede sein. Anders als etwa das Setzen eines Hakens handle es sich hierbei nicht um eine aktive Handlung, sondern vielmehr um eine Duldung. Hierdurch könne nicht nachvollzogen werden, dass der Nutzer aktiv zugestimmt habe. Darüber hinaus fehle es der Einwilligung an der notwendigen Informiertheit. Zur Teilnahme am Gewinnspiel war die Einwilligung zu Cookies/Werbung zwar nicht Voraussetzung – der Nutzer wurde hierüber jedoch nicht explizit informiert, sodass die Annahme einer Verknüpfung nahe lag.

Zur zweiten Frage stellt der EuGH fest, dass den Website-Betreiber die Pflicht treffe, den Nutzer auch über die Dauer der Cookies sowie über die Zugriffsmöglichkeiten Dritter auf diese zu informieren. Dies folge aus dem Erfordernis, den Nutzer „klar und umfassend zu informieren". Anderenfalls könne dieser nicht, wie erforderlich, in „Kenntnis der Sachlage" in die Datenverarbeitung einwilligen. Hierbei dürfe man von einem „normal informierten, verständigen Nutzer" ausgehen. Von diesem dürfe jedoch wegen der technischen Komplexität hinsichtlich der Funktionsweise von Cookies kein höherer Kenntnisstand erwartet werden.

Darüber hinaus verpflichtet die Richtlinie einen Unternehmer aber auch dazu, den Verbrauchern ein Kommunikationsmittel zur Verfügung zu stellen, das eine direkte und effiziente Kommunikation gewährleistet, wobei der Unternehmer bezüglicher der Wahl des Mittels grundsätzlich frei ist. Die Einhaltung dieser Kriterien des Kommunikationsmittels, obliegt insoweit der Überprüfung durch die nationalen Gerichte. Der Gerichtshof hat lediglich angedeutet, dass der Umstand, dass eine Telefonnummer erst nach einer Reihe von Klicks erreichbar ist, nicht gegen eine klare und verständliche Weise im vorliegenden Fall spricht.

Cookies nur noch mit Einwilligung?

Bemerkenswert an der Entscheidung ist, dass der EuGH auf die Zulässigkeit der Cookies lediglich im Lichte der ePrivacy-Richtlinie eingeht, als mögliche Rechtsgrundlage jedoch nicht Art. 6 DSGVO heranzieht. Denn die Richtlinie ist in Deutschland nicht unmittelbar anwendbar. Vielmehr wurde sie (allerdings nur unzureichend) in nationales Recht umgesetzt. Nach deutschem Recht wäre das Setzen von Cookies erlaubt und dem Nutzer stünde bloß ein Widerspruchsrecht zu.

Die deutschen Datenschutzaufsichtsbehörden sind jedoch bisher davon ausgegangen, dass allein die DSGVO Anwendung findet. Die einschlägigen nationalen Vorschriften des Telemediengesetzes (TMG), durch welches die ePrivacy-Richtlinie umgesetzt werden sollte, seien durch Einführung der DSGVO nicht mehr anwendbar. Daher müsse sich die Rechtslage allein nach der DSGVO beurteilen, sodass hiernach auch das „berechtigte Interesse" als Rechtsgrundlage in Frage käme. Die Richtlinie verlangt hingegen eine ausdrückliche Einwilligung.

Wäre tatsächlich die ePrivacy-Richtlinie als speziellere Regelung vorrangig, könnten sich Unternehmen künftig bei der Datenverarbeitung nur noch auf eine Einwilligung berufen, die den Anforderungen des EuGH entsprechen. Das „berechtigte Interesse" im Sinne von Art. 6 Abs. 1 lit. f) DSGVO wäre dann nicht mehr als Legitimation denkbar.

Unser Kommentar

Die Entscheidung des EuGH macht deutlich, dass bei dem Betrieb einer Website der Schutz personenbezogener Daten sowie eine transparente Datenverarbeitung von großer Bedeutung sind. Website-Betreiber müssen nun darauf achten, die Einholung von Einwilligungen datenschutzkonform auszugestalten. Ein „Opt-Out"-Verfahren reicht nicht mehr aus. Auch die Annahme einer „stillschweigenden" Einwilligung durch Weiternutzen der Website ist nicht mehr zulässig. Vielmehr müssen Einwilligungen durch den Nutzer aktiv und informiert erteilt werden.

Eine Möglichkeit, um diesen Anforderungen gerecht zu werden, ist der Einsatz von Consent-Managern. Über diese werden alle verwendeten Cookies erfasst und häufig kategorisiert zusammengeführt (funktionale Cookies, Marketing-Cookies, Analyse-Cookies, etc.), um eine übersichtliche und vereinfachte Verwaltung zu erreichen. Für Website-Betreiber besteht der Vorteil, dass Einwilligungen datenschutzkonform eingeholt und dokumentiert werden können sowie dass keine eigene Lösung entwickelt werden muss. Nutzer der Website hingegen können unmittelbar und transparent erkennen, welche Cookies bzw. welche Kategorien eingesetzt werden und dann aktiv in diese einwilligen. Vor dem Einsatz dieser Tools sollte jedoch stets eine genaue datenschutzrechtliche Prüfung der Umsetzung durchgeführt werden. So müssen unter anderem entsprechende Auftragsverarbeitungsverträge mit dem Anbieter des Consent-Managers abgeschlossen werden. Ebenso muss sowohl über Cookies als auch den Einsatz eines Consent-Managers in der Datenschutzerklärung informiert werden.

Es bleibt zudem abzuwarten, ob und wie die Frage eines generellen Einwilligungserfordernisses bei der Verwendung von Cookies von den Gerichten und den Aufsichtsbehörden beantwortet wird. Bis

dahin wäre es sogar vertretbar, auch weiterhin in eng umgrenzten Fällen (z. B. bei sehr datenschutzfreundlich einsetzbaren Analysetools wie Matomo) den Einsatz von Cookies auf überwiegende berechtigte Interessen zu stützen. Mit der ePrivacy-Verordnung könnte sich diese Frage jedoch erledigen. Diese hat insbesondere den Einsatz von Cookies im Blick und wird derzeit von der EU verhandelt, jedoch voraussichtlich 2020 oder sogar erst 2021 verabschiedet. Wer zwischenzeitlich in jedem Fall datenschutzkonform agieren möchte, sollte für alle Cookies, die nicht technisch erforderlich sind, Einwilligungen einholen.

Müssen Facebook-Fanpages künftig deaktiviert werden?

Seit fast sieben Jahren läuft das Verfahren um die datenschutzrechtliche Zulässigkeit des Betriebes von Facebook-Fanpages. Das Bundesverwaltungsgericht (BVerwG) hat dazu nun entschieden, dass die Anordnung einer Datenschutzaufsichtsbehörde mit dem Inhalt, eine Facebook-Fanpage zu deaktivieren, rechtmäßig sein kann.

■ BVerwG, Urteil v. 11. September 2019, Az. 6 C 15/18

Hintergrund

Viele Unternehmen nutzen eine Facebook-Fanpage für ihre Marketing- und Vertriebstätigkeiten. Eine Fanpage ist ein spezielles Benutzerkonto, welches der Präsentation und Werbung eines Unternehmens dienen kann. Aufgrund der enormen Reichweite von Facebook und Co. ist dies eine vielversprechende Alternative zu traditionellen Werbe- und Präsentationswegen. Eine für den Betreiber besonders attraktive Funktion ist dabei „Facebook-Insights“, die ihm kostenfrei zur Verfügung gestellt wird, allerdings auch nicht abdingbar ist. Dem Betreiber werden hierüber Statistiken über Nutzerdaten zur Verfügung gestellt,

die Facebook zuvor mit Hilfe der Fanpage (durch das Setzen von Cookies bei dem Besuch der Fanpage) erhebt. Diese Daten kann der Betreiber zu Marktforschungs- oder Werbezwecken nutzen.

Eine solche Fanpage betrieb auch die Wirtschaftsakademie Schleswig-Holstein (WSH). Das Unabhängige Landeszentrum für Datenschutz (ULD) hatte in ihrer Funktion als Aufsichtsbehörde für den Datenschutz in Schleswig-Holstein gegenüber der WSH eine Anordnung erlassen, die Facebook-Fanpage zu deaktivieren. Grund dafür war unter anderem, dass ein Widerspruch eines Nutzers der Fanpage gegen die Datenverarbeitung gegenüber der WSH erfolglos bleibe, da die WSH keine technische Einwirkungsmöglichkeit auf die Datenverarbeitungsprozesse von Facebook habe. Gegen diesen Bescheid ging die WSH gerichtlich vor.

Vorinstanzliche Entscheidung

In den Vorinstanzen (VG Schleswig, 8 A 14/12; OVG Schleswig, 4 LB 20/13) hatte die Klage Erfolg. Das Schleswig-Holsteinische Oberverwaltungsgericht (OVG) lehnte eine datenschutzrechtliche Verantwortlichkeit der WSH ab, da für sie kein Zugriff auf die erhobenen Daten bestehe. Gegen dieses Urteil ging die Aufsichtsbehörde wiederum in Revision. Das BVerwG legte dem Europäischen Gerichtshof (EuGH) im Rahmen eines Vorabentscheidungsverfahrens die Frage vor, ob der Betreiber einer Facebook-Fanpage für die Datenverarbeitung durch Facebook mitverantwortlich sei.

Der EuGH stellte schließlich fest, dass eine gemeinsame Verantwortlichkeit im Sinne der Datenschutzgrundverordnung (DSGVO) zwischen dem Betreiber der Facebook-Fanpage und Facebook selbst vorliegt. Denn durch den Betrieb der Seite entstehe für Facebook die Möglichkeit, die Daten der Nutzer zu erheben. Zudem könne der Seitenbetreiber mittels Parametrierung mitentscheiden, welche Daten welcher Personen analysiert werden. Dadurch sei er maßgeblich an der Entscheidung über Zwecke und Mittel der Datenverarbeitung beteiligt, sodass die Voraussetzungen für eine gemeinsame Verantwortlichkeit nach Art. 26 DSGVO vorliegen.

Die Entscheidung

Nachdem der EuGH die gemeinsame Verantwortlichkeit feststellte, wurde der Rechtsstreit an das BVerwG zurückverwiesen. Dieses entschied auf Grundlage der bindenden Entscheidung des EuGH, dass die Aufforderung zur Deaktivierung der Facebook-Fanpage rechtmäßig sein kann, soweit „*die von Facebook zur Verfügung gestellte digitale Infrastruktur schwerwiegende datenschutzrechtliche Mängel aufweist*“.

Außerdem stelle das BVerwG fest, dass es zulässig ist, den Seitenbetreiber (statt Facebook) in die Pflicht zu nehmen, einen datenschutzkonformen Zustand herzustellen. Denn die Auswahl desjenigen, an den die Anordnung gerichtet werde, stehe im Ermessen der Aufsichtsbehörde; dabei müsse sie sich vom Gedanken der Effektivität leiten lassen. Da es Facebook an Kooperationsbereitschaft fehle und ein Vorgehen gegen Facebook daher mit „*erheblichen tatsächlichen und rechtlichen Unsicherheit verbunden*“ sei, könne die Aufsichtsbehörde effektiver gegen den Betreiber der Fanpage vorgehen.

Daher hob das BVerwG das vorherige Urteil auf und verwies den Rechtsstreit an das OVG zurück. Dieses hat nun zu prüfen, ob die Datenverarbeitungsvorgänge, die im Rahmen der Fanpage-Nutzung stattfinden, tatsächlich rechtswidrig sind.

Unser Kommentar

Schon das Urteil des EuGH vom 5. Juni 2018 (C-210/16) sorgte für Aufsehen: die gemeinsame Verantwortlichkeit von Facebook und dem Betreiber der Facebook-Fanpage bedeutet, dass auch den Seitenbetreiber die Pflichten der DSGVO treffen, wie etwa Informationspflichten nach Art. 13 ff. DSGVO. Daraus folgt, dass auch der Betreiber verpflichtet ist, Datenschutzhinweise auf der Fanpage für die Nutzer zur Verfügung zu stellen.

Weder EuGH noch BVerwG haben festgestellt, dass der Betrieb einer Facebook-Fanpage per se datenschutzwidrig ist. Die Datenschutzaufsichtsbehörden scheinen jedoch von einer grundsätzlichen Datenschutzwidrigkeit auszugehen, denn es fehle bereits an einer Vereinbarung im Sinne von Art. 26 DSGVO zwischen dem Seitenbetreiber und Facebook. Die von Facebook in den Nutzungsbedingungen integrierte Vereinbarung reiche nicht aus. Solange Facebook nicht nachbessere, sei eine datenschutzkonforme Nutzung nicht möglich. Darüber hinaus fehle es an der erforderlichen Transparenz bei der Datenverarbeitung durch Facebook.

Gegenüber Unternehmen könnte die Vorgehensweise des ULD dabei eine starke Benachteiligung darstellen, insbesondere, wenn sie auch durch andere Aufsichtsbehörden übernommen wird: diejenigen Unternehmen, die ihre Fanpage deaktivieren müssen, sind weniger visibel am Markt bzw. gegenüber Verbrauchern und verlieren eine interaktive Kommunikations- und

Austauschmöglichkeit mit Kunden und Interessenten. Es ist zudem sehr unwahrscheinlich, dass die (ohnehin schon am Rande der Überlastung arbeitenden) Aufsichtsbehörden gegen alle Fanpage-Betreiber entsprechende Anordnungen erlassen (alleine die Aufsichtsbehörde in NRW ist für ca. 750.000 Unternehmen sowie Teile der öffentliche Hand zuständig). Dies

könnte dazu führen, dass manche Unternehmen ihre Fanpage deaktivieren müssen, andere jedoch ihre Fanpage weiterbetreiben. Zudem besteht das Risiko, dass die Entscheidung auch auf andere „Fanpages“ oder Unternehmensseiten, z. B. Xing oder LinkedIn, übertragen wird. Denn auch dort werden vom Betreiber des Netzwerkes Daten erhoben, gesammelt und verarbeitet sowie dem jeweiligen Unternehmen aufbereitet zur Verfügung gestellt.

Aus diesen Gründen erscheint das Vorgehen gegen Unternehmen kritisch, auch wenn für Behörden grundsätzlich die Möglichkeit besteht, gegen diese unter dem Gesichtspunkt der Effektivität vorzugehen. Wie aber bereits die Verhandlungen der Niederlande mit Microsoft über den datenschutzkonformen Einsatz von Windows 10 und Office365 zeigen, dürfte auch ein Vorgehen gegen die „Big Player“ der IT-Industrie durchaus Erfolg versprechen. Die DSGVO gibt hierfür sowohl eine Rechtsgrundlage als auch Instrumente zur Durchsetzung von Maßnahmen an die Hand. Neben Anordnungen gegenüber Facebook besteht auch die Möglichkeit von hohen Bußgeldern – insbesondere mit dem von den deutschen Behörden entwickelten und mittlerweile in Anwendung befindlichen Bußgeldberechnungsschema. Die potentiell enorme Höhe der Bußgelder könnte Facebook zu einem Handeln zwingen, ohne die Fanpage-Betreiber zu belasten.

Sollte das OVG jedoch die Ansicht der Aufsichtsbehörden teilen, wäre die Konsequenz, dass in dem gesamten Geltungsbereich der DSGVO der Betrieb von Facebook-Fanpages eingestellt werden müsste, sobald eine entsprechende Anordnung zur Deaktivierung durch eine Aufsichtsbehörde ergeht.

Nichtsdestotrotz sollten Unternehmen und Personen, die eine Facebook-Fanpage betreiben, diese nicht sofort deaktivieren. Aufgrund der noch nicht abschließend geklärten Rechtslage dürfte ein Weiterbetrieb noch keine direkten Bußgelder nach sich ziehen. Erreicht jedoch den Seitenbetreiber die Anordnung einer Aufsichtsbehörde, eine Fanpage zu deaktivieren, sollte diese Anweisung unverzüglich befolgt werden.

Keine „belanglosen“ Daten mehr? – Auch Gesprächs- und Telefonnotizen sind personenbezogene Daten

Ein aktuelles Urteil des OLG Köln (OLG Köln, Urt. v. 25.07.2019 – 20 U 75/18) beschäftigt sich mit der Reichweite des Auskunftsanspruchs des Art. 15 der Datenschutzgrundverordnung (DSGVO) und der Auslegung des Begriffs des personenbezogenen Datums. Laut der Entscheidung müssen alle personenbezogenen Daten, auch elektronisch gespeicherte Gesprächs- und Telefonnotizen, die Personenbezug aufweisen, herausgegeben werden. Allerdings wies das Gericht auch darauf hin, dass der datenschutzrechtliche Auskunftsanspruch nicht dazu diene, Schadensersatzansprüche durchsetzbar zu machen, die nicht unmittelbar mit dem Recht auf informationelle Selbstbestimmung zusammenhängen.

■ OLG Köln, 25.07.2019 – 20 U /5/18

Hintergrund

Die Parteien stritten um Leistungen aus einem Versicherungsverhältnis. Im Rahmen dessen machte der Kläger einen Auskunftsanspruch über seine personenbezogenen Daten, die durch das Versicherungsunternehmen verarbeitet wurden, geltend. Diese Daten wollte er dann auch im Prozess nutzen. Der Kläger stützte seinen Auskunftsanspruch auf § 34 BDSG, da zu dem Zeitpunkt, in dem das Verfahren in erster Instanz (LG Köln,

Urt. v. 9.4.2018 – 26 O 360/16) rechtshängig wurde, die DSGVO noch nicht in Kraft getreten war.

Die Entscheidung

Das OLG Köln hatte nun zu entscheiden, wieweit der Auskunftsanspruch nach Art. 15 DSGVO in diesem konkreten Fall reicht. Denn auch wenn im Zeitpunkt der erstinstanzlichen Entscheidung die DSGVO noch nicht in Kraft getreten war, hat das Berufungsgericht bei seiner Entscheidung das geltende Recht, im Falle einer Rechtsänderung also das neue Recht der DSGVO, anzuwenden.

Die Klage hatte hinsichtlich des Auskunftsanspruchs Erfolg. Das Gericht stellte zunächst dar, welche Informationen im Allgemeinen unter den Begriff der „personenbezogenen Daten“ fallen: sowohl *Identifikationsmerkmale* (Name, Anschrift, Geburtsdatum, etc.), *äußere Merkmale* (z.B. Geschlecht, Augenfarbe, Größe, Gewicht), *innere Zustände* (wie Meinungen, Motive, Wünsche, Überzeugungen und Werturteile) als auch *sachliche Informationen* (Vermögens- und Eigentumsverhältnisse, Kommunikations- und Vertragsbeziehungen, sonstige Beziehungen der betroffenen Person zu Dritten und ihrer Umwelt) seien erfasst. Darüber hinaus umfasse der Begriff aber auch solche Aussagen, die eine *subjektive und/oder objektive Einschätzung zu einer Person* liefern.

Zu diesen Informationen zählen nach Auffassung des Gerichts auch elektronisch gespeicherte Vermerke zu Telefonaten sowie Gesprächsnotizen. Denn in diesen Vermerken seien Aussagen des Klägers selbst sowie Aussagen über ihn festgehalten worden. Das Gericht ist der Ansicht, dass es durch die Entwicklung der Informationstechnologie mit ihren umfassenden Verarbeitungs- und Verknüpfungsmöglichkeiten „*keine belanglosen Daten*“ mehr gebe.

Die Einwände des Versicherungsunternehmens konnten das Gericht nicht überzeugen. Einerseits sah es im konkreten Fall keine Verletzung von Geschäftsgeheimnissen, da die eigenen Angaben des Klägers gegenüber seiner Versicherung schon nicht als Geschäftsgeheimnis im Verhältnis zwischen den Parteien zu qualifizieren und daher nicht schutzbedürftig seien. Andererseits lehnte es den Einwand ab, dass es einem Großunternehmen wirtschaftlich unmöglich sei, alle Dateien auf Personenbezug zu durchzusuchen und zu sichern. Ein Unternehmen müsse dafür Sorge tragen, dass die verwendete elektronische Datenverarbeitung im Einklang mit der Rechtsordnung organisiert und insbesondere datenschutzkonform sei, sodass den Rechten Dritter Rechnung getragen werde.

Zudem lehnte das Gericht das Begehren des Klägers auf eine Teilentscheidung über den Auskunftsanspruch – getrennt vom Schadensersatzanspruch - ab. Das Vorgehen des Klägers im Prozess über Art. 15 DSGVO sei eine unzulässige Ausforschung, da der Kläger die Beklagte auch vor der Einleitung eines Gerichtsverfahrens auf Auskunft hätte in Anspruch nehmen können. Der Auskunftsanspruch sei ein Instrument, das betroffenen Person helfe, ihre Ansprüche nach der DSGVO – wie etwa die Rechte auf Berichtigung oder Löschung nach Art. 16 und 17 DSGVO – geltend machen zu können. Er sei jedoch nicht speziell dazu geschaffen worden, Schadensersatzansprüche, die nichts mit dem Recht auf informationelle Selbstbestimmung zu tun haben, durchsetzbar zu machen. Eine Umkehr der Beweislast nach dem deutschen Zivilprozessrecht - der Anspruchsteller muss in der Regel die für ihn günstigen Tatsachen darlegen und beweisen – durch die DSGVO sei hier nicht gegeben. Die Entdeckung von Anhaltspunkten für das Bestehen eines Anspruches sei vielmehr nur ein „Nebeneffekt“.

Unser Kommentar

Seit Inkrafttreten der DSGVO kommt es häufiger dazu, dass innerhalb von Prozessen der datenschutzrechtliche Auskunftsanspruch nach Art. 15 DSGVO geltend gemacht wird. Bezüglich der Reichweite dieses Anspruchs besteht jedoch noch große Rechtsunsicherheit. Es obliegt daher zurzeit den Gerichten, den Umfang anhand von Einzelfällen zu konkretisieren. Der Auskunftsanspruch wird dabei in der Regel extensiv ausgelegt, um den umfassenden Schutz von natürlichen Personen (das Hauptziel der DSGVO) zu gewährleisten. Für die Betroffenen ist dies von großem Vorteil, um Eingriffe in ihre informationelle Selbstbestimmung zu erkennen und dagegen vorgehen zu können. Allerdings ergibt sich daraus auch ein Missbrauchsrisiko, was offenbar auch das OLG Köln erkannt hat. Daher ist zu begrüßen, dass es in seiner Entscheidung darauf hingewiesen hat, dass der Auskunftsanspruch gerade nicht dazu dient, eine Beweiserleichterung im Zivilprozess zu schaffen.

Für Unternehmen können sich (trotz dieser Einschränkung) aus einem weitreichenden Auskunftsanspruch ebenfalls erhebliche Probleme ergeben, da in der Praxis häufig noch keine Prozesse implementiert sind, die alle relevanten Daten für die Erfüllung eines Auskunftsanspruchs „auf Knopfdruck“ verfügbar machen. Ein Rückzug auf eine Unzumutbarkeit der Implementierung solcher Systeme und Prozesse erscheint angesichts des Urteils des OLG Köln nur schwer möglich. Gegebenenfalls kann aber eine Auskunft berechtigt verweigert werden nach Art. 15 Abs. 4 DSGVO. Hiernach kann die Herausgabe von Kopien verweigert werden, soweit Geschäftsgeheimnisse oder berechtigte Interessen Dritter entgegenstehen. Allerdings muss der Verantwortliche nachweisen, dass diese Interessen betroffen sind, zudem wird das Vorliegen von berechtigten Interessen regelmäßig nicht dazu führen, dass

die Auskunft vollständig verweigert werden kann. Vielmehr dürfte in diesen Fällen eine aufwendige Identifikation und Schwärzung der betroffenen Dokumente erforderlich sein.

Kommt ein Unternehmen der Verpflichtung zur Auskunft nicht oder nur unzureichend nach, können hohe Bußgelder und Schadensersatzansprüche des Betroffenen die Folge sein. Unternehmen sollten daher unbedingt Maßnahmen treffen, um DSGVO-konform zu agieren. Diesbezüglich empfiehlt sich die Einführung von Systemen und Prozessen, durch welche personenbezogene Daten, die Gegenstand einer Verarbeitung sind, identifiziert, abgerufen und gegebenenfalls geschwärzt werden können. Dadurch kann einem Auskunftsersuchen angemessen und zeitnah Rechnung getragen werden.

Veranstaltungen, IP/IT Blog und Veröffentlichungen

Eine Übersicht mit unseren Veranstaltungen finden Sie hier

Unseren IP/IT Blog finden Sie hier

Eine Liste unserer aktuellen Veröffentlichungen finden Sie hier

Impressum

Verleger: Luther Rechtsanwaltsgesellschaft mbH
Anna-Schneider-Steig 22, 50678 Köln, Telefon +49 221 9937 0
Telefax +49 221 9937 110, contact@luther-lawfirm.com
V.i.S.d.P.: Dr. Michael Rath, Partner
Luther Rechtsanwaltsgesellschaft mbH, Anna-Schneider-Steig 22
50678 Köln, Telefon +49 221 9937 25795
michael.rath@luther-lawfirm.com

Bildnachweis: Fabrika/Fotolia: Seite 1; Marilyn Nieves/iStockphoto: Seite 3; Brandon Laufenberg/iStock: Seite 9; 123ducu/iStockphoto: Seite 10

Haftungsausschluss

Die Luther Rechtsanwaltsgesellschaft mbH berät in allen Bereichen des Wirtschaftsrechts. Zu den Mandanten zählen mittelständische und große Unternehmen sowie die öffentliche Hand.

Berlin, Brüssel, Düsseldorf, Essen, Frankfurt a. M., Hamburg, Hannover, Köln, Leipzig,
London, Luxemburg, München, Shanghai, Singapur, Stuttgart, Yangon

Luther Corporate Services: Delhi-Gurugram, Kuala Lumpur, Shanghai, Singapur, Yangon

Ihren Ansprechpartner finden Sie auf www.luther-lawfirm.com.

Auf den Punkt. Luther.