Luther.

Newsletter IP/IT

2. Ausgabe 2020

Inhalt

„Black-Friday“ – Bundespatentgericht trifft Entscheidung zur Wortmarke

Das Bundespatentgericht hat entschieden, dass die Wortmarke „Black Friday“ nur für einzelne Dienstleistungen im Bereich Werbung und Handel mit Elektro- und Elektronikwaren zu löschen sei. Im Übrigen hat das Gericht die vollständige Löschung der Wortmarke durch das Deutsche Patent- und Markenamt aufgehoben.

Beschluss vom 26. September 2019, Az. 30 W (pat) 26/18

Hintergrund

Der Black Friday gilt nicht ohne Grund als einer der umsatzstärksten Tage im Jahr. Am Tag nach Thanksgiving locken viele Geschäfte und Online Shops mit extremen Rabattaktionen und generieren dadurch einen Umsatz in Milliardenhöhe. Seit 2013 genießt ein Unternehmen aus Hongkong, die Super Union Holdings Ltd., für eine Vielzahl von Waren und Dienstleistungen Schutz für die Wortmarke „Black Friday“.

Nachdem verschiedene Unternehmen beim Deutschen Patent und Markenamt (DPMA) darauf drängten, die Wortmarke aus dem Register zu löschen, gab das DPMA den entsprechenden Löschungsanträgen im Jahr 2018 statt und ordnete die vollständige Löschung der Marke an. Nach Ansicht des DPMA habe der Eintragung der angegriffenen Marke sowohl im Anmelde- als auch im Entscheidungszeitpunkt das Schutzhindernis der fehlenden Unterscheidungskraft entgegengestanden. Weitergehende Hintergrundinformationen zum mit dem Black Friday verbundenen Markenrechtsstreit finden Sie in unserem Blogbeitrag vom 29. Oktober 2019. Gegen die Entscheidung des DPMA hat die Markeninhaberin Beschwerde eingelegt.

Die Entscheidung

Nunmehr hat der 30. Senat des Bundespatentgerichts entschieden, dass die vollständige Löschung der Marke durch

das Deutsche Patent- und Markenamt zwar aufgehoben, die Löschung jedoch für einzelne Werbedienstleistungen und den Handel mit Elektro- und Elektronikwaren bestätigt werden sollte. Das Bundespatentgericht folgte dabei im Wesentlichen der Argumentation der Markeninhaberin, nach der der Name „Black Friday“ im Zeitpunkt der Markenanmeldung für den Durchschnittsverbraucher in Deutschland als Tag des Börsencrashs 1929, nicht aber im Zusammenhang mit Rabattaktionen, bekannt war. Dabei setzte sich das Bundespatentgericht ausführlich mit den von den Antragstellern vorgelegten Unterlagen auseinander, stellte jedoch im Ergebnis fest, dass eine Gesamtschau der im Verfahren vorgelegten Unterlagen nicht dazu führe von einer Prägung des Verkehrsverständnisses dahingehend auszugehen, dass der inländische Durchschnittsverbraucher den Begriff „Black Friday“ bereits im Anmeldezeitpunkt (2013) als Schlagwort für eine Rabattaktion verstanden habe.

Zu einem anderen Ergebnis kam das Gericht jedoch im Bereich des Handels mit Elektro- und Elektronikwaren sowie für bestimmte Werbedienstleistungen in Klasse 35. Das Bundespatentgericht stützte sich bei der Entscheidung insbesondere auf die Tatsache, dass es insofern schon vor der Markenanmeldung auf dem deutschen Markt verschiedene Aktionen gab. In diesen Bereichen sei es daher aus der Perspektive des Anmeldezeitpunktes vernünftigerweise zu erwarten gewesen, dass sich der Begriff „Black Friday“ im Sinne einer Rabattaktion etablieren könne. Aus diesem Grund sprach sich das Gericht für ein schon im Anmeldezeitpunkt bestehendes zukünftiges Freihaltebedürfnis nach § 8 Abs. 2 Nr. 2 Markengesetz aus und ordnete für diese Dienstleistungen die Löschung der Marke an.

Das Bundespatentgericht hat die Rechtsbeschwerde zugelassen.

Unser Kommentar

Es bleibt nunmehr abzuwarten, ob die Parteien Beschwerde beim Bundesgerichtshof einreichen. Unabhängig davon, wird die Thematik auch an anderer Stelle verfolgt. So verhandelt das Landgericht Düsseldorf im Hauptsacheverfahren über die Abmahnung des Portals Black-Friday.de durch die Markeninhaberin. Zudem wurde beim Landgericht Berlin Klage auf Löschung der Marke wegen Nichtbenutzung eingereicht. Bis zur endgültigen Klärung des Rechtsstreits ist Händlern zu empfehlen, den Begriff für die relevanten Waren und Dienstleistungen nicht ohne Lizenz zu nutzen. Es ist davon auszugehen, dass die Markeninhaberin die Wortmarke auch künftig verteidigen wird.

Google Analytics: Statistik- und Analyse-Tools für Webseiten

Statistik- und Analyse-Tools für Webseiten sind immer wieder Gegenstand der datenschutzrechtlichen Diskussion. Insbesondere die Zuordnung der Verantwortlichkeit für die Datenverarbeitung ist unklar und oft abhängig von der Verwendung und den Einstellungen des jeweiligen Tools. Google Analytics steht dabei als eine der am weitesten verbreiteten Anwendungen oft im Fokus.

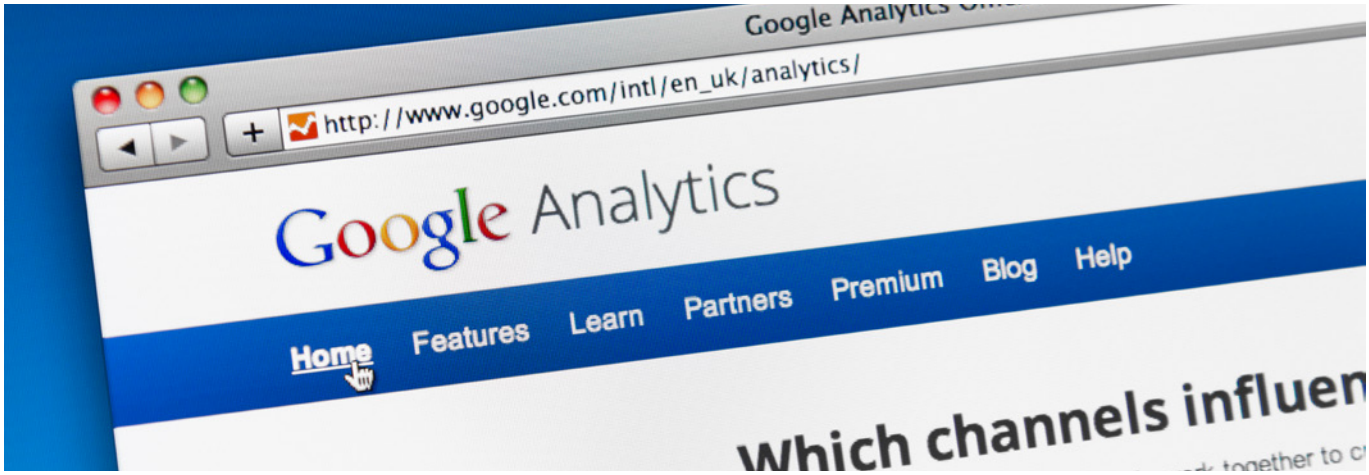
Hintergrund

Trackingtools sind aus dem digitalen Zeitalter nicht mehr wegzudenken. Oft wird das Onlineverhalten flächendeckend und URL-übergreifend gespeichert, analysiert und vermarktet. Unangefochtener Marktführer auf dem Gebiet ist Google Analytics. Laut einer Statistik des W3Techs-Consortiums verwenden heute ca. 54 % aller Websites weltweit die Services des kalifornischen Technologieunternehmens aus Mountain View. Aber auch abseits reiner Online-Auftritte entscheiden sich immer mehr Unternehmen zu einer Implementierung von Google Analytics.

Google Analytics – ein mächtiges Tool, aber auch transparent?

Über ein in Echtzeit aktualisiertes Dashboard können detaillierte Auswertungen über verschiedenste Parameter von Besuchern (Benutzern) abgerufen und darauf basierende Rückschlüsse auf deren Verhaltensweisen zusammengestellt werden. Sie sollen es dem Betreiber ermöglichen, seinen Webauftritt (sein Produkt) an die Bedürfnisse oder gar Wünsche seiner „Audience“ anzupassen, während die betroffenen Personen meist selbst nicht wissen, was sie sich davon genau erhoffen. Es mag sogar einige in der Audience geben, die sich gar nichts Bestimmtes wünschen, doch auch ihr Nutzerverhalten gibt aus Sicht des Services Anlass, das eigene Angebot zu überdenken und es weiter zu optimieren.

Mit Hilfe von Variablen wie der geografischen Herkunft oder anderer sozioökonomischer Parameter der getrackten Perso-



nen (z.B. deren Geschlecht, die Zugehörigkeit zu einer bestimmten Altersklasse, etc.), werden Ergebnisse graphisch aufbereitet und in anschaulicher Art und Weise dargestellt. Das Problem: Der Betreiber einer Website oder das Unternehmen, das Tools wie Google Analytics in seinen Produkten einsetzt, hat regelmäßig keinerlei Kenntnis darüber, was über die Erbringung der vom Provider angebotenen, ihm manchmal mehr, manchmal weniger bekannten, Services hinaus mit den Daten geschieht, die von den betroffenen Personen gesammelt werden.

Joint-Controllership

Bei der Einrichtung von Google Analytics ist zunächst die von der Google LLC dargebotene Auftragsverarbeitungsvereinbarung in ihrer jeweils aktuellen und sich beinahe monatlich ändernden Fassung sowie die Nutzungsbedingungen zu akzeptieren. Nur dem aufmerksamen Betrachter fällt überhaupt auf, dass Google seit einiger Zeit in den voreingestellten Standardeinstellungen des Vertragsprozesses eine Vereinbarung on top abzeichnen lässt, die den Namen „Measurement Controller-Controller Data Protection Terms“ trägt. Diese Terms regeln eine Art gemeinsame Verantwortlichkeit der Akteure. Jedoch nicht für Google Analytics insgesamt, sondern nur für einen Teilbereich der Daten, die innerhalb der Services übertragen und verarbeitet werden. Diese Daten werden als „shared data“ bezeichnet. Die dahinterliegende „Datenfreigabeeinstellung“ soll laut Definition eine Einstellung sein, „*die der Kunde über die Benutzeroberfläche der Messdienste aktiviert hat und die es Google und dessen Zweigunternehmen ermöglicht, personenbezogene Daten zur Verbesserung der Produkte und Dienstleistungen von Google bzw. des jeweiligen Unternehmens einzusetzen*“. Um welche Daten es sich im Einzelnen tatsächlich handelt, wird weder innerhalb der Terms, noch an irgendeiner anderen Stelle näher beschrieben.

Die jetzige Vorgehensweise von Google ist also sicher eine Reaktion auf die Urteile des EuGH zu Facebook-Fanpages und FashionID, mit denen erneut deutlich wurde, dass der Gewährleistung eines wirksamen und umfassenden Schutzes personenbezogener Daten von natürlichen Personen in der EU höchste Priorität zukommen soll. Nach den Entscheidungen dürften an die gemeinsame Festlegung von Zwecken und Mitteln der Datenverarbeitung keine allzu hohen Anforderungen zu stellen sein. Eine detaillierte Kenntnis über die Verarbeitungstätigkeit des jeweils anderen oder das Vorliegen eines gemeinsamen Zwecks ist wohl ebenfalls nicht erforderlich, um die gemeinsame Verantwortlichkeit zu begründen.

Unser Kommentar

Vor diesem Hintergrund könnte die Einbindung von Tracking- und Analysetools durchaus als ein Fall von § 26 Abs. 1 DSGVO anzusehen sein, für den es den Abschluss einer entsprechenden Vereinbarung zwischen den Akteuren bedarf. Auf lange Sicht wird es nicht ausreichen, dass Anbieter entsprechender Tools dem Websitebetreiber bzw. Produktinhaber eine Vereinbarung anbieten, die sich vor allem durch ihre Inhaltslosigkeit auszeichnet und die nicht einmal eindeutig regelt, für welche Daten sie überhaupt anwendbar ist. Es wird eine detailliertere Auseinandersetzung mit den Anforderungen an derartige Vereinbarungen erforderlich werden. Einen ersten Schritt in diese Richtung hat der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg im Mai 2019 mit der Veröffentlichung eines Musters für eine Vereinbarung über die gemeinsame Verantwortlichkeit getan. Damit kann natürlich nur eine erste Orientierung gegeben werden, die sich insbesondere für einfache Fälle anbietet. Gerade in komplexen Konstellationen mit mehreren Akteuren und Drittstaatentransfer wie im Falle von Google Analytics wird sich zeigen müssen, welche Inhalte tatsächlich erforderlich sind.

Rückzug der öffentlichen Stellen aus den sozialen Medien?

Der Landesbeauftragte für Datenschutz und Informationsfreiheit des Landes Baden-Württemberg, Stefan Brink, hat Ende Januar seinen vergleichsweise reichweitenstarken Twitter-Account wegen Datenschutzbedenken gelöscht. Öffentliche Stellen und Unternehmen sollten daher ihre Nutzung von Social Media auf den Prüfstand stellen.

Hintergrund

Die meisten öffentlichen Stellen nutzen mittlerweile ausgiebig das Angebot sozialer Netzwerke, sodass Facebook, Twitter und Co. zu einem wesentlich Informationskanal für sie geworden sind. In Anbetracht dessen, dass viele Nutzer soziale Netzwerke verwenden, um sich sowohl beruflich, als auch privat zu informieren, stellen diese eine kostengünstige und schnelle Möglichkeit dar, eine enorme Bandbreite an Nutzern zu erreichen. Mit den Vorteilen gehen jedoch gleichzeitig auch rechtliche Fallstricke einher.

Durch die noch junge Datenschutzgrundverordnung (DSGVO) herrscht bei vielen noch Unsicherheit darüber, wie die rechtlichen Anforderungen konkret umgesetzt werden müssen. Dies insbesondere im Hinblick auf die Nutzung sozialer Medien. Je nach Konzeption, Plattformlösung, Geschäftsmodell, einer ggf. kommerziellen Verwertung von Nutzungsdaten sowie Sitz des Plattformbetreibers, gelten unterschiedliche Anforderungen.

Zwar gibt es einige wenige höchstrichterliche Entscheidungen, die grundlegende Anforderungen festsetzen, die praktische Umsetzung bleibt jedoch weitestgehend unberührt, so dass weiterhin Unklarheiten darüber bestehen, wie es „richtig“ geht – und das gilt nicht nur für private Unternehmen, sondern auch für öffentliche Stellen.

Die Kollision von Theorie und Praxis

Betreibt ein privatwirtschaftliches Unternehmen oder eine öffentliche Stelle einen Account, so kommt es zur Verarbeitung

von Nutzerdaten durch den Account-Inhaber, wie auch durch den Plattformbetreiber. Der EuGH stellte in seiner Entscheidung (C-210/16) daher fest, dass der Betrieb einer Facebook-Fanpage zu einer gemeinsamen Verantwortlichkeit zwischen dem Fanpage-Betreiber und dem Plattformbetreiber Facebook im Sinne des § 26 DSGVO führt. Dieses Urteil bestätigte das Bundesverwaltungsgericht für das deutsche Recht im Oktober 2019 (BVerwGE 6 C 15.18). Da Facebook durch den Betrieb der Fanpage die Möglichkeit erhalte, auf dem Endgerät des Fanpage-Besuchers Cookies zu platzieren, sei es Facebook unbeschränkt möglich, personenbezogene Daten der Fanpage-Besucher zu verarbeiten. Da der Fanpage-Betreiber ebenfalls von der Datenverarbeitung profitiere, etwa indem ihm eine Statistik mit den ausgewerteten Ergebnissen zur Verfügung gestellt wird, um seine Fanpage optimieren zu können, bestehe auch ein nach Art. 26 DSGVO erforderlicher gemeinsamer Zweck.

Die Mitverantwortlichkeit hat zur Folge, dass den Fanpage-Betreiber – gemeinsam mit Facebook – die Pflichten der DSGVO vollumfänglich treffen. Doch ist eine Erfüllung der datenschutzrechtlichen Anforderungen in diesen Fällen in der Praxis tatsächlich umsetzbar? Die nachfolgenden Beispiele sollen die Diskrepanzen von Theorie und Praxis verdeutlichen:

1. Gesetzliche Rechtsgrundlage

Der LfDI Rheinland-Pfalz (LfDI) geht in seinem Handlungsrahmen für die Nutzung von Social Media durch öffentliche Stellen davon aus, dass der Betrieb einer Facebook-Fanpage nur unter bestimmten Voraussetzungen als datenschutzkonform angesehen werden kann. In dem Leitfaden geht der LfDI dabei auf verschiedene Punkte ein. Unter anderem wird die Frage erörtert, ob für die Datenverarbeitung beim Betreiben einer Fanpage überhaupt eine Rechtsgrundlage vorhanden ist. Der LfDI geht schließlich davon aus, dass sich die öffentlichen Stellen nicht auf Art. 6 Abs. 1 S. 1 lit. e) DSGVO und ihre Öffentlichkeitsarbeit berufen können, sondern allein eine Einwilligung des Nutzers im Sinne von Art. 6 Abs. 1 S. 1 lit. a) DSGVO in Betracht komme.

2. Einwilligung durch den Nutzer

Bei der Frage nach dem Vorliegen einer wirksamen Einwilligung differenziert der LfDI zunächst zwischen registrierten und nicht registrierten Nutzern. Bei den registrierten Nutzern lasse sich eine Einwilligung durch die Anmeldung bei dem sozialen Netzwerk und die Zustimmung zu den Nutzungsbedingungen fingieren. Allerdings sei dabei entscheidend, dass die entsprechenden Nutzungsbedingungen diejenigen Informationen enthalten, die zur Einhaltung der Informationspflichten nach der DSGVO erforderlich sind und die Nutzungsbedingungen auch sonst den Grundsätzen der DSGVO genügen. Gerade mit Blick auf das Transparenzgebot dürfte dies jedoch häufig fraglich sein.

Bei nicht registrierten Nutzern erfolgt zunächst keinerlei Zustimmung beim Aufruf der Webseite, sodass eine gesonderte Einwilligungserklärung eingeholt werden muss. Wird eine solche nicht eingeholt und ist der Besuch der Fanpage dennoch möglich, ist nach Auffassung des LfDI die Datenverarbeitung rechtswidrig und der Betrieb der Fanpage somit nicht datenschutzkonform.

Der Fanpage-Betreiber hat jedoch in der Regel keine Möglichkeit, die technischen Voraussetzungen der Plattform anzupassen, um auf diese Weise die erforderlichen Einwilligungserklärungen einzuholen. Zudem fehlt dem Betreiber schlichtweg der Einfluss auf die vom Plattformbetreiber gegenüber dem Nutzer gestellten Nutzungsbedingungen.

3. Joint-Controller-Vereinbarung

Sind zwei oder mehr Parteien für die Datenverarbeitungsprozesse gemeinsam verantwortlich, so ist der Abschluss einer Joint-Controller-Vereinbarung gemäß Art. 26 DSGVO zwingend – fehlt es an dieser Vereinbarung, ist die Datenverarbeitung rechtswidrig. Der EuGH hat im Fall von Facebook entschieden, dass es sich beim Plattformbetreiben und den jeweiligen Fanpage-Betreibern um gemeinsame Verantwortliche im Sinne der DSGVO handelt (die zu den Facebook-Fanpages dargestellte Problematik lässt sich grundsätzlich auch auf andere Social Media-Angebote übertragen, wird hier aber zunächst weiter anhand von Facebook erläutert).

Facebook stellte den Fanpage-Betreibern seinerzeit eine Informationen zur Datenverarbeitung („Insights“) zur Verfügung, mit der die rechtlichen Anforderungen erfüllt sein sollten. Nach Auffassung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) sind diese Informationen jedoch gerade nicht ausreichend, um den Anforderungen der DSGVO zu genügen. Auch nach einer Beanstandung durch die DSK und eine daraufhin erfolgte Überarbeitung der Vereinbarung sind noch immer nicht alle Fragen der DSK umfassend geklärt. Für den Fanpage-Betreiber bedeutet dies, dass er die fehlenden Informationen letztlich bei Facebook einholen und eine Vereinbarung gemäß Art. 26 DSGVO schließen muss.

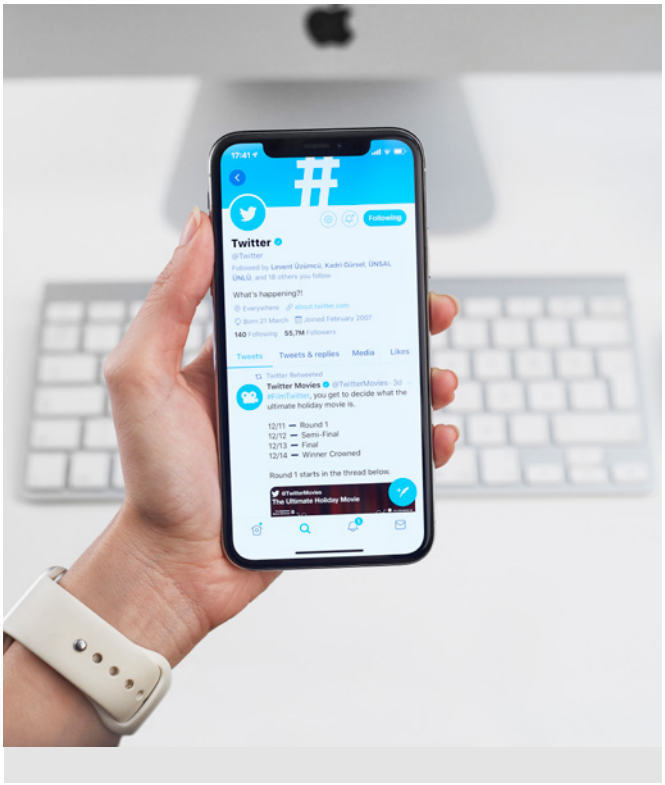
Aufgrund der fehlenden Kooperationsbereitschaft von Facebook ist der Abschluss einer individuellen Vereinbarung aktuell allerdings sehr unwahrscheinlich, weswegen ein datenschutzkonformer Betrieb von Facebook-Fanpages wohl weiterhin nicht möglich sein wird.

Aufgabe des amtlichen Twitter-Accounts des LfDI Baden-Württemberg

Wie wir bereits vor kurzem berichtet haben, kam der Landesbeauftragte für Datenschutz und Informationsfreiheit (LfDI) Baden-Württemberg, Stefan Brink, aufgrund datenschutzrechtlichen Bedenken zu dem Entschluss, seinen amtlichen Twitter-Account zum 31. Januar 2020 aufzugeben. Seiner Auffassung nach gelten für den Betrieb eines Twitter-Accounts ähnliche Voraussetzungen wie bei einer Facebook-Fanpage: Twitter Inc. bilde umfassende Profile durch Tracking und werte das Verhalten seiner Nutzer und übrigen Twitter-Leser aus, was einen erheblichen Eingriff in die informationelle Selbstbestimmung der Betroffenen bedeute. Der Nutzer könne das Tracking und Analysieren seiner Follower bei Twitter auch nicht unterbinden. Daher komme es auch in dieser Konstellation zu einer Mitverantwortlichkeit zwischen Account-Inhaber und Netzwerkbetreiber. Allerdings gibt es keine Joint-Controller-Vereinbarung im Sinne von Art. 26 DSGVO zwischen dem Inhaber des Accounts und Twitter. Nach vergeblichen Verhandlungen mit Twitter über eine entsprechende Vereinbarung verwirklichte der LfDI Baden-Württemberg sein Vorhaben, gab seinen Account auf und kündigte darüber hinaus an, auch von anderen öffentlichen Stellen offiziell zu fordern, ihre Social Media-Accounts zu deaktivieren. Der LfDI Baden-Württemberg betont jedoch, dass er nicht bezwecke, die Kommunikation zwischen Behörden und Bürgern bzw. Unternehmen und Kunden zu unterbinden. Vielmehr wolle er mittelbar Druck auf die in der Regel im Ausland sitzenden Plattformbetreiber ausüben, gegenüber denen die deutschen Aufsichtsbehörden aufgrund ihres Sitzes keine unmittelbaren Anordnungen erlassen können.

Unser Kommentar

Die Entscheidung des LfDI Baden-Württemberg, seinen Twitter-Account zu löschen, basiert letztlich auf dem Grundsatz der rechtsstaatlichen Bindung von Behörden. Behörden sind als vollziehende Gewalt nach Art. 20 Abs. 3 Grundgesetz an Recht und Gesetz gebunden und stehen aufgrund ihrer gesellschaftlichen Vorbildfunktion in einer besonderen Verantwortung. Daher sollte eine Nutzung von sozialen Netzwerken von Behörden erst dann in Betracht gezogen werden, wenn dies auch rechtskonform möglich ist. Somit ist der Entschluss des LfDI Baden-Württemberg, Twitter im Rahmen seiner Vorbildfunktion nicht weiter zu nutzen, zu begrüßen; ebenso seine Ankündigung, ein solches Vorgehen auch von anderen öffentliche Stellen zu fordern.



Auch private Unternehmen sollten bereits über Alternativen und Möglichkeiten nachdenken, die sozialen Medien rechtskonform zu nutzen. Denn die datenschutzrechtlichen Anforderungen für öffentliche Stellen lassen sich auch auf privatwirtschaftliche Unternehmen übertragen. Daher ist auch für sie aktuell ein datenschutzkonformer Betrieb in den meisten Fällen nicht möglich. Ob die Aufsichtsbehörden sich künftig einzelne Unternehmen oder öffentliche Stellen vornehmen, oder umfassend in einer „großen Aufräumaktion“ tätig werden, bleibt abzuwarten. Es gilt jedoch der Grundsatz „keine Gleichheit im Unrecht“, was bedeutet, dass sich (einzelne) Unternehmen und/oder Stellen im Falle einer behördlichen Überprüfung nicht darauf berufen können, dass andere Unternehmen und/oder öffentliche Stellen ebenfalls rechtswidrig handeln. Ein Grund mehr, sich frühzeitig mit dem Thema zu befassen.

Besonders spannend wird letztlich die Frage sein, ob sich durch den schrittweisen Rückzug der Unternehmen und öffentlichen Stellen die großen Plattformbetreiber nun doch in Richtung DSGVO-Konformität bewegen lassen.

Homeoffice – Datenschutzrechtliche Vorgaben

Nicht zuletzt durch das Coronavirus verlagern sich berufliche Tätigkeiten zunehmend in das Homeoffice. Das entbindet Arbeitgeber und Arbeitnehmer jedoch nicht davon, gesetzliche Vorgaben wie den Datenschutz zu beachten, auch wenn die Umsetzung zuweilen schwierig erscheinen mag.

Hintergrund

Die Verlegung der Arbeit außerhalb der Betriebsstätte birgt datenschutzrechtliche Risiken, welche Unternehmen mit entsprechenden Sicherheitsvorkehrungen minimieren können und sollten. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie verschiedene Aufsichtsbehörden haben bereits entsprechende Vorkehrungen für das sichere Arbeiten von Zuhause aus empfohlen. Diese und weitere Tipps sollen im Folgenden als eine erste Handreichung für Unternehmen dienen.

Sicherheitsmaßnahmen im Homeoffice

Bei der Arbeit im Homeoffice sollten grundsätzlich die gleichen Sicherheitsanforderungen wie am Arbeitsplatz im Büro erfüllt werden. Soweit vom heimischen Schreibtisch aus personenbezogene Daten verarbeitet werden, gelten daher die datenschutzrechtlichen Vorgaben der Datenschutzgrundverordnung (DSGVO) wie auch am Arbeitsplatz im Büro. Dies gilt insbesondere für die Pflicht, angemessene technische und organisatorische Maßnahmen (Art. 32 DSGVO) zu treffen, um so Datenschutzverstöße zu verhindern. Diese Pflicht trifft zunächst das Unternehmen, das die technischen Voraussetzungen (etwa in Form der Einrichtung eines Virtual Private Network) zu schaffen hat und Mitarbeitern entsprechende Verhaltensregelungen an die Hand geben muss. Neben klaren Regelungen diesbezüglich ist es wichtig, dass diese auch an alle betroffenen Mitarbeiter kommuniziert werden.

IT-Sicherheit

- Es sollte sichergestellt werden, dass für die Arbeit im Homeoffice ausschließlich die vom Arbeitgeber bereitgestellte Hard- sowie Software genutzt wird, soweit nicht spezielle Bring-Your-Own-Device Regelungen gelten. Dies gilt nicht nur für den genutzten PC/Laptop, sondern auch für die Speicherung von Arbeitsergebnissen auf Festplatten, USB-Speichern oder anderen Datenspeichern.
- Daten sollten grundsätzlich in den Verzeichnissen/Ordnern von Servern bzw. zentralen IT-Systemen des Unternehmens gespeichert werden, um weiterhin Archivierungs- und Dokumentationsanforderungen (z. B. aus der DSGVO, den GoBD oder dem GeschGehG) nachzukommen. Soweit Ausnahmen hiervon zugelassen werden, etwa wenn eine Internet-Anbindung an die zentralen IT-Systeme und damit eine Speicherung auf den IT-Systemen nicht möglich ist, ist jedenfalls sicherzustellen, dass die Daten auf den verwendeten Datenträgern verschlüsselt (inkl. Ablageverschlüsselung) gespeichert werden.
- Mobile Geräte (Laptops, Smartphones sowie Tablets) sollten auf aktuellem Stand sein (auf Updates achten!); dies gilt insbesondere auch für Virenschutzsoftware und Firewalls. Diesbezüglich sollten die Mitarbeiter aufgefordert werden, ihre Geräte regelmäßig an das Firmennetzwerk anzuschließen und Aktualisierungshinweise der IT-Abteilung zu berücksichtigen.
- Der PC sollte so eingerichtet werden, dass dieser durch ein Kabel oder ein verschlüsseltes WLAN mit dem Internet verbunden ist.
- Sonstige drahtlose Schnittstellen (wie z.B. Bluetooth) sollten deaktiviert werden.
- Sollten (Video-) Konferenzsysteme oder -plattformen ge-

nutzt werden, ist sicherzustellen, dass es sich um einen von der IT-Abteilung freigegebenen Dienst handelt. Zahlreiche auf dem Markt befindliche Konferenzsysteme erheben in unzulässiger Weise Nutzerdaten, wie z. B. Standortdaten, und/oder zeichnen die Kommunikation ohne entsprechende Einwilligung der Teilnehmer auf.

Clean Desk Policy

Neben der IT-Sicherheit sollte ferner gewährleistet sein, dass auch auf dem privaten Schreibtisch der Schutz von geschäftlichen Daten höchste Priorität hat. Auch hier sollte das Sicherheitsniveau aus dem Büro aufrecht erhalten werden. Der Arbeitsplatz sollte daher insbesondere so organisiert werden, dass sich private und betriebliche Daten nicht vermischen.

- Es sollte sichergestellt werden, dass der Bildschirm nicht durch andere eingesehen werden kann. Darüber hinaus sollten automatische Bildschirmsperren mit Passwortschutz sowie Sichtschutzfolien verwendet werden.
- Es sollten keine Papierdokumente, USB-Sticks, Datenträger, etc. bei Verlassen des Schreibtischs offen liegen gelassen, sondern in verschließbaren Behältnissen aufbewahrt werden.
- Beim Verlassen des Arbeitsplatzes sollte darauf geachtet werden, dass Türen geschlossen sind, sodass eine unbefugte Kenntnisnahme, ein Verlust oder eine Veränderung von Daten verhindert wird.

Kommunikation

- Es sollten eindeutige Kommunikationswege und Kontaktstellen für Mitarbeiter sichergestellt werden. So können diese sicher sein, dass die Daten und Informationen in den richtigen Händen landen.
- Auch ein Datenverlust im Homeoffice kann eine meldepflichtige Datenschutzverletzung beinhalten. Mitarbeiter sollten daher mit ihren Pflichten zur Benachrichtigung der zuständigen Stellen im Unternehmen für den Fall einer Datenschutzverletzung vertraut sein, damit das Unternehmen seinen gesetzlichen Meldepflichten nachkommen kann. Andernfalls drohen erhebliche Geldbußen durch die Datenschutz-Aufsichtsbehörden.
- Da der betriebliche Einsatz von Messenger-Diensten besonderen datenschutzrechtlichen Vorgaben unterliegt, denen „gängige" Messenger-Dienste aus dem privaten Bereich nicht oder nur bedingt entsprechen, sollten Messenger-Dienste zur Kommunikation grundsätzlich vermieden werden. Wird ein solcher Dienst dennoch eingesetzt, sollte zumindest darauf geachtet werden, dass keine vertraulichen Unternehmensinformationen ausgetauscht werden. Auch sollten einige Sicherheitsstandards, wie eine Ende-zu-Ende-Verschlüsselung, gewährleistet sein.
- Von der Nutzung privater Mobiltelefone oder privater E-Mail Accounts für die betriebliche Kommunikation oder sonstige betriebliche Zwecke sollte abgesehen werden.
- Sofern im Homeoffice zu betrieblichen Zwecken telefoniert werden muss, sollten andere Personen im Haushalt keine Kenntnis von den Inhalten der Telefonate nehmen können.

Drucken und Entsorgen

- Ausdrucke betrieblicher Dokumente sollten grundsätzlich nicht im Homeoffice erfolgen. Sollte dies für die Erledigung von betriebsbedingten Aufgaben zwingend erforderlich sein, sollte darauf geachtet werden, dass die Dokumente unverzüglich aus dem Drucker entnommen werden, damit andere Personen im Haushalt keine Kenntnis dieser Daten nehmen können. Sofern über VPN im Firmennetz gearbeitet wird, ist sicherzustellen, dass keine Druckaufträge auf Drucker in den Firmengebäuden abgeschickt werden. Im Fall eines zwingenden Ausdrucks sollte dafür Sorge getragen werden, dass die ausgedruckten Informationen auch vor Ort geeignet vernichtet werden können (Aktenvernichter/Datentonnen).
- Betriebliche Papierdokumente sollten nicht mit dem privaten Papiermüll entsorgt werden. Sofern er nicht vorschriftsmäßig vernichtet werden kann, sollte Papiermüll gesammelt und verschlossen gelagert werden. Sobald dies möglich ist, sollte der Papiermüll sodann im Büro nach den geltenden Regeln entsorgt werden.

Besondere Kategorien personenbezogener Daten, Auftragsverarbeitungsvereinbarungen und Drittstaatentransfer

- Zugang zu besonderen Kategorien personenbezogener Daten (z. B. Gesundheitsdaten) sollte nur mit PIN und hardwarebasiertem Vertrauensanker (Zwei-Faktor-Authentifizierung) erfolgen.
- Unternehmen, die Leistungen als Auftragsverarbeiter für andere ausführen, sollten sicherstellen, dass die Auftragsverarbeitungsvereinbarungen keine Restriktionen in Bezug auf die Arbeit im Homeoffice beinhalten.
- Für Homeoffice Aktivitäten in Ländern außerhalb des Europäischen Wirtschaftsraums (EWR), die sich auf Daten von Unternehmen innerhalb des EWR beziehen, sind ggf. die weitergehenden Vorgaben der Art. 44 ff. DSGVO zu erfüllen.

Gesetz zum Abkommen über ein Einheitliches Patentgericht ist nichtig

Das Bundesverfassungsgericht (BVerfG) hat das Zustimmungsgesetz zum Einheitlichen Patentgericht für nichtig erklärt, ein Einheitliches Patentgericht in der EU ist damit vorerst in weite Ferne gerückt.

BVerfG, Beschluss vom 13. Februar 2020, Az. 2 BvR 739/17

Hintergrund

Das BVerfG ist der Ansicht, dass das Zustimmungsgesetz nicht mit Art. 23 Abs. 1 S. 3 i.V.m. Art. 79 Abs. 2 Grundgesetz (GG) vereinbar ist, da es nicht mit der notwendigen absoluten Zweidrittelmehrheit beschlossen wurde. Die entsprechende Sitzung erfolgte lediglich mit ca. 35 Abgeordneten. Die zeitnahe Einführung eines Einheitlichen Patentgerichts ist somit vom Tisch. Zudem könnte dieser Beschluss einen erheblichen Einfluss auf das politische Handeln bei der europäischen Integration haben.

Die Idee eines Einheitspatentes, also die Schaffung eines einheitlichen Patentschutzes für das Gebiet der EG/EU, wird bereits seit Ende der 1950er Jahre diskutiert. Mit dem Beschluss des BVerfG wurde diese – nicht enden wollende – Geschichte um ein weiteres Kapitel ergänzt. Das Zustimmungsgesetz zum Übereinkommen über ein Einheitliches Patentgericht (EPGÜ-ZustG) wurde im März 2017 einstimmig angenommen. Anschließend erhob ein Düsseldorfer Rechtsanwalt Verfassungsbeschwerde gegen dieses Gesetz, worauf es – auf Grund einer informellen Bitte des BVerfG – nicht vom kurz zuvor ernannten Bundespräsidenten Frank-Walter Steinmeier unterzeichnet wurde.

Bereits wenige Wochen vor dieser Entscheidung hatte die britische Regierung angekündigt, nicht mehr am Einheitlichen Patentgericht festhalten zu wollen. Diese Mitteilung kam trotz des „Brexit“ überraschend, da man bisher davon ausgegangen war, dass an der geschlossenen Ratifizierung festgehalten wird. Weiter Informationen hierzu finden Sie bei den Kollegen von JUVE.

Dabei bietet ein Einheitspatent den großen Vorteil eines zentralisierten Verfahren, mit dem europäischen Patentamt als zentraler Anlaufstelle. Durch ein Einheitliches Patentgericht würden zudem parallele und oft kostenintensive Rechtsstreitigkeiten in mehreren Ländern vermieden. Somit besteht insbesondere bei Erfindern ein großes Bedürfnis, dass das Einheitliche Patentgericht am Ende der „Story“ überlebt.

Die Entscheidung

Die am 20. März 2020 veröffentlichte Entscheidung wurde nur weniger Tage vorher angekündigt und bereits lange herbeigesehnt. Das BVerfG hat das Zustimmungsgesetz zum Einheitlichen Patentgericht für nichtig erklärt, und damit – vorerst – Klarheit geschaffen. Dabei hat das Gericht die Entscheidung auf das nicht ausreichende Quorum gestützt, während die anderen Beschwerdepunkte des Beschwerdeführers weniger beachtet wurden. Demnach hat die Einführung des Einheitliche Patentgerichts Verfassungsrelevanz und stellt eine funktional äquivalente Regelung zu einer Änderung der EU-Verträge dar. Bei einer Übertragung von Hoheitsrechten im Kontext der Europäischen Union – wie es das BVerfG hier annimmt – bedarf es einer Zweidrittelmehrheit, welche hier unstreitig nicht vorlag.

Dabei ist diese Ansicht der Verfassungsrichter selbst im Zweiten Senat nicht unumstritten. So führten drei Verfassungsrichter in einem Minderheitsvotum u. a. an, dass nun bei jeder Kompetenzübertragung im Anwendungsbereich des Art. 23 Abs. 1 GG vom Bundestag und Bundesrat eine Zweidrittelmehrheit angestrebt werden könnte, um sich weniger Risiken auszusetzen. Dies könnte dazu führen, dass politische Prozesse im Bereich der europäischen Integration erschwert werden. Besonders Interessant ist dabei die Tatsache, dass sich die drei Verfassungsrichter mit der kürzesten bisherigen Amtszeit für das Minderheitsvotum zusammengeschlossen haben. Dies könnte bereits jetzt auf eine künftige Änderung in der Rechtsprechung hindeuten.

Den gesamten Beschluss - Az. 2 BvR 739/17 - des Zweiten Senates vom 13. Februar 2020 finden Sie auf der Internetpräsenz des BVerfG zum Nachlesen.

Nächste Schritte bis zum Einheitlichen Patentgericht

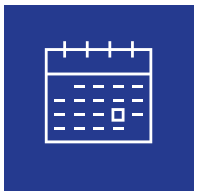
Dem Bundestag steht es nun frei, erneut mit der notwendigen Zweidrittelmehrheit über das Gesetz abzustimmen. Auch wenn entsprechende Prognosen schwierig sind, erscheint das Erreichen der gewünschten Mehrheit, auf Grund der damals einstimmigen Abstimmung, als durchaus realistisch. Jedoch kommt der Beschluss zu einem – aus der Sicht der Befürworter des Einheitlichen Patentgerichts – denkbar ungünstigen Zeitpunkt, bei dem der Zusammenschluss von einer solchen großen Personenanzahl schwierig bis unmöglich, und die Politik in vielen Bereichen gefordert ist. Es bleibt wohl noch ein langer und steiniger Weg, bis es zum Einheitlichen Patentgericht kommt.

Unser Kommentar

Es bleibt nun abzuwarten, ob bzw. wann der Bundestag für ein erneute Abstimmung zum Zustimmungsgesetz für das Einheitliche Patentgericht tagt. So bleibt es vorerst der Wunsch einiger Befürworter, dass dieses Vorhaben nicht insgesamt scheitert. Denn der einheitliche Schutz im Patentrecht stellt eine hervorragende Chance und Vereinfachung für Erfinder und Unternehmen dar, und ist somit längst überfällig. Die Entscheidung der britischen Regierung gegen ein Einheitliches Patentgericht verstärkt insgesamt die Zweifel an der entsprechenden zeitnahen Durchsetzung, da somit ein wichtiger „Partner“ weggefallen ist.

Spannend bleibt, wie sich der Bundestag zukünftig im Bereich der europäischen Integration verhalten wird. Hier bleibt zu hoffen, dass sich die Befürchtungen aus dem Minderheitsvotum nicht bestätigen. Denn eine absoluteZweidrittelmehrheit zu erreichen ist derzeit wohl schwerer als je zuvor und könnte somit zu einer Behinderung der Politik führen.

Veranstaltungen, Veröffentlichungen und Blog



Eine Übersicht mit unseren Veranstaltungen finden Sie hier.

Eine Liste unserer aktuellen Veröffentlichungen finden Sie hier.

Unseren Blog 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: MR.Cole_Photographer/Getty Images: Seite 1; yudhistirama/ iStockphoto: Seite 3; franckreporter/iStockphoto: Seite 5; pressureUA/ iStockphoto: Seite 6; bombuscreative/ iStockphoto: Seite 8; kimberrywood/iStockphoto: Seite 9; Bits and Splits /Adobestock: Seite 11

Haftungsausschluss

Obgleich dieser Newsletter sorgfältig erstellt wurde, wird keine Haftung für Fehler oder Auslassungen übernommen. Die Informationen dieses Newsletters stellen keinen anwaltlichen oder steuerlichen Rechtsrat dar und ersetzen keine auf den Einzelfall bezogene anwaltliche oder steuerliche Beratung. Hierfür stehen unsere Ansprechpartner an den einzelnen Standorten zur Verfügung.

Aus Gründen der besseren Lesbarkeit verzichten wir auf die gleichzeitige Verwendung geschlechterspezifischer Sprachformen. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter. Die verkürzte Sprachform hat nur redaktionelle Gründe und beinhaltet keine Wertung.

Luther.

Bangkok, Berlin, Brüssel, Delhi-Gurugram, Düsseldorf, Essen, Frankfurt a. M., Hamburg, Hannover, Jakarta, Köln, Kuala Lumpur, Leipzig, London, Luxemburg, München, Shanghai, Singapur, Stuttgart, Yangon

Weitere Informationen finden Sie unter
www.luther-lawfirm.com
www.luther-services.com

JUVE AWARDS 2019
Kanzlei des Jahres