Luther.

Newsletter IP/IT

2. Ausgabe 2021

Inhalt

Unzulässige Videoüberwachung – LfD Niedersachsen verhängt Bußgeld von mehr als EUR 10 Mio. gegen notebooksbilliger.de

Videoüberwachung am Arbeitsplatz und in Geschäftsräumen muss gut geplant und datenschutzkonform ausgestaltet sein. Anderenfalls drohen Untersuchungen und Beanstandungen der Datenschutzaufsichtsbehörden. Im schlimmsten Fall können sogar erhebliche Bußgelder verhängt werden.

Hintergrund

Die Landesbeauftragte für den Datenschutz (LfD) Niedersachsen, Barbara Thiel, gab mit einer Pressemitteilung vom 8. Januar 2021 bekannt, dass sie gegen die Betreiberin des Elektronik-Handels notebooksbilliger.de ein Bußgeld in Höhe von EUR 10,4 Mio. verhängt hat. Dabei handelt es sich um das bisher höchste Bußgeld, das die niedersächsische Datenschutzbehörde wegen Verstößen gegen die Datenschutz-Grundverordnung (DSGVO) ausgesprochen hat.

Die Entscheidung

Die Datenschutzbehörde begründete ihre Entscheidung mit schwerwiegenden Verstößen im Zusammenhang mit der Videoüberwachung, die der Elektronik-Händler in seinem Unternehmen durchgeführt hatte. Dabei seien seine Beschäftigten in einem Zeitraum von mindestens zwei Jahren unrechtmäßig per Video überwacht worden. Auch Kunden seien von der rechtswidrigen Videoüberwachung in Verkaufsräumen des Elektronik-Händlers betroffen gewesen, der auch eigene Ladegeschäfte betreibt. Inzwischen habe das Unternehmen die Videoüberwachung aber rechtmäßig ausgestaltet.

notebooksbilliger.de hatte sich darauf berufen, mit der Videoüberwachung allgemein Diebstähle verhindern und aufklären zu wollen. Die Datenschutzbehörde bemängelte daran jedoch insbesondere, dass die Überwachung der Beschäftigten ohne einen konkreten Anlass erfolgt sei und eine Speicherung der Aufzeichnungen für bis zu 60 Tage deutlich über das erforderliche Maß hinausgehe. Die Videoüberwachung sei daher zur systematischen Leistungsüberwachung der Beschäftigten ge-

eignet gewesen. Auch die Überwachung von Sitzbereichen in Ladengeschäften des Elektronik-Händlers, in denen Kunden sich typischerweise länger aufhalten, sei nicht verhältnismäßig gewesen.

notebooksbilliger.de hat gegen die Entscheidung der LfD Niedersachsen bereits Einspruch eingelegt. Der Elektronik-Händler kritisiert, die Datenschutzbehörde habe den Sachverhalt nicht ausreichend ermittelt, etwa durch eine Begutachtung der betreffenden Kameras vor Ort. Zudem sei das Bußgeld in Relation zu der Schwere des Verstoßes unverhältnismäßig hoch. Das Unternehmen hält den Bescheid daher für nicht rechtmäßig.

Unser Kommentar

Das Bußgeld der LfD Niedersachsen zeigt, dass die Datenschutzbehörden inzwischen auch wegen vermeintlich geringerer Verstöße gegen die DSGVO empfindliche Bußgelder verhängen. Auch wenn eine Videoüberwachung insbesondere im Versandhandel und in der Logistikbranche zum Standard gehört, müssen Verantwortliche den Einsatz jeder einzelnen Videokamera daher genauestens prüfen. Dabei können auch Details wie die Ausrichtung der jeweiligen Kamera oder die Speicherfrist der Aufzeichnungen Auswirkungen auf die Rechtmäßigkeit des gesamten Verfahrens haben. Unternehmen, die Überwachungskameras in ihren Geschäftsräumen nutzen, sollten daher regelmäßig überprüfen, ob ihr Verfahren den aktuellen Anforderungen der Datenschutzbehörden an die Rechtmäßigkeit der Videoüberwachung genügt.

Insbesondere die Speicherdauer der Aufzeichnungen ist dabei genau zu prüfen. So sollte auch bei einer Überwachung zur Verhinderung und Aufdeckung von Straftaten sorgfältig abgewogen werden, wie lange die Aufzeichnung für den Verarbeitungszweck tatsächlich gesichert werden müssen. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) geht in ihrer „Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen“ vom 17. Juli 2020 (abrufbar unter: https://www.datenschutzkonferenz-online.de/media/oh/20200903_oh_vü_dsk.pdf) davon aus, dass Videoaufzeichnungen in der Regel nach Ablauf von nur 72 Stunden zu löschen sind, wenn sich innerhalb dieses Zeitraums keine Anhaltspunkte ergeben, die eine darüber hinausgehende Speicherung rechtfertigen. Verantwortliche wären damit verpflichtet, das aufgezeichnete Material innerhalb von 72 Stunden zu sichten, und dürften nur bei Hinweisen auf eine Straftat von einer Löschung absehen.

Fraglich ist in diesem Zusammenhang aber, ob die Rechte und Freiheiten der Beschäftigten durch eine regelmäßige gründliche Sichtung des aufgenommenen Materials nicht schwerer beeinträchtigt werden, als durch eine längere Speicherung von Aufzeichnungen, die jedoch erst bei einem konkreten Anlass gesichtet werden. Selbiges gilt hinsichtlich der Ansicht der LfD Niedersachsen, Verantwortliche müssten vor der Durchführung einer Videoüberwachung zur Verhinderung von Straftaten zunächst weniger einschneidende Mittel wie bspw. stichprobenartige Taschenkontrollen prüfen. Denn viele Beschäftigte dürften sich durch eine Durchsuchung ihrer privaten Habseligkeiten stärker beeinträchtigt fühlen als von einer Überwachung des Arbeitsbereiches per Videokamera.

Kritisch zu betrachten ist in diesem Fall auch die Höhe des verhängten Bußgelds. Es ist davon auszugehen, dass die niedersächsische Datenschutzbehörde bei der Bestimmung der Bußgeldhöhe das Bußgeldmodell angewandt hat, auf welches sich die Mitglieder der DSK verständigt haben. Dieses steht jedoch wegen seiner vergleichsweise schematischen und den Einzelfall nicht ausreichend berücksichtigenden Ausgestaltung in der Kritik. In der jüngeren Vergangenheit haben daher diverse Gerichte entsprechende DSGVO-Bußgelder erheblich reduziert oder vollständig für unwirksam erklärt (mehr dazu im folgenden Beitrag).

Bußgelder und Anordnungen der Datenschutzaufsichtsbehörden – lohnt sich ein (gerichtliches) Vorgehen?

Bußgeldbescheide und behördliche Anordnungen können erhebliche Risiken für die Betriebsabläufe und die Geschäftstätigkeit eines Unternehmens darstellen – müssen und sollten aber nicht ohne Weiteres hingenommen werden. Aktuelle Verfahren zeigen, dass die Erfolgschancen für ein (gerichtliches) Vorgehen aussichtsreich sein können.

Hintergrund

Millionenbußgelder für große Unternehmen wie 1&1, Deutsche Wohnen oder notebooksbilliger.de (mehr dazu im vorherigen Beitrag) sowie strenge Anordnungen (wie zum Beispiel die angedrohte Untersagung von Datentransfers zwischen Facebook und WhatsApp) sind im Datenschutz inzwischen keine Seltenheit mehr und können erhebliche Risiken für Unternehmen darstellen. Idealerweise wird einem Verfahren der Behörden dadurch vorgebeugt, dass die datenschutzrechtlichen Vorgaben beachtet und entsprechend umgesetzt werden. Bei aller Vorsicht kann es dennoch immer zu Datenschutzverstößen kommen, Risiken lassen sich nie vollständig negieren – so sind IT-Systeme niemals hundertprozentig sicher und auch der Faktor Mensch spielt eine zentrale Rolle für effektiven Datenschutz (oder für dessen Fehlen). Was also tun, falls man einen Bußgeldbescheid oder eine andere Anordnung (beispielsweise zur Untersagung der Nutzung einer bestimmten Software) erhält?

Falsch wäre es, einen Bescheid schlichtweg zu ignorieren oder ohne weitere Prüfung das Bußgeld zu bezahlen oder die Anordnung zu befolgen. Stattdessen gilt es, Ruhe zu bewahren und die korrekte Vorgehensweise abzuwägen und auszuwählen. Diverse Verfahren gegen bereits öffentlichkeitswirksam verhängte Bescheide zeigen, dass ein Bußgeld oder eine Anordnung nicht einfach hingenommen werden muss, sondern dass sich eine (gerichtliche) Vorgehensweise oftmals lohnen kann.

Deutsche Datenschutzaufsichtsbehörden werden strenger

Die gesetzlichen Rahmenbedingungen für Bußgelder nach der DSGVO erscheinen zunächst klar: nach Art. 83 DSGVO dürfen Bußgelder – abhängig vom Verstoß – bis zu EUR 20 Mio. oder bis zu 4 % des Umsatzes des vorherigen Geschäftsjahres des gesamten Konzerns umfassen. Nach Art. 58 DSGVO dürfen die Aufsichtsbehörden zudem Anweisungen, Untersagungen oder andere Anordnungen gegenüber datenverarbeitenden Unternehmen erlassen.

Die deutschen Aufsichtsbehörden verfolgten zunächst jedoch ihren bisherigen Kurs weiter, der die Kooperation mit Unternehmen in den Vordergrund stellte statt deren Sanktionierung. Drei Jahre nach Inkrafttreten der DSGVO sehen die Aufsichtsbehörden aber immer weniger Gründe dafür, Verstöße gegen die DSGVO nicht zu ahnden. Denn Unternehmen hatten ausreichend Zeit, DSGVO-konforme Prozesse zu etablieren. Auch wenn der Kooperationsgedanke weiterhin vorhanden zu sein scheint (bei den meisten in Deutschland verhangenen

Bußgeldern scheinen vorher „informelle“ Verwaltungsverfahren und/oder eine Diskussion zwischen Unternehmen und Behörden über die betroffene Datenverarbeitung stattgefunden zu haben), verhängen deutsche Datenschutzaufsichten nun ebenfalls schneller und strenger Bußgelder oder Anordnungen. Dabei orientieren sie sich an dem von ihnen für die DSGVO entwickelten Bußgeldberechnungsmodell.

Bußgelder werden von den Gerichten einkassiert

Die über dieses Modell zustande gekommenen Bußgelder werden von den Gerichten aber inzwischen reduziert oder vollständig für unwirksam erklärt. Zwar laufen einige Bußgeldverfahren noch weiter, es zeigt sich jedoch bereits deutlich, dass ein (gerichtliches) Vorgehen gegen Entscheidungen der Datenschutzaufsichtsbehörden sinnvoll sein kann. Denn die Gerichte sind nicht an diese Entscheidungen gebunden und haben einen hohen eigenen Ermessensspielraum bei der Festsetzung des Bußgelds, der seine Grenzen letztlich nur in der DSGVO findet:

- Die Höhe des Bußgelds erheblich verringern konnte 1&1: Von dem ursprünglichen Bußgeld von ca. EUR 9,5 Mio. sind nach dem Gerichtsverfahren vor dem LG Bonn lediglich zehn Prozent, knapp EUR 900.0000, übrig geblieben. Laut Gericht stehe das Bußgeld nicht im Verhältnis zur Schwere des Verstoßes. Das Unternehmen hatte Adressdaten eines Kunden an jemand Drittes herausgegeben, die diese Person dann zum Stalking des Kunden nutzte. Die Datenschutzaufsicht bemängelte insbesondere eine unzureichende Identifikation und Absicherung der Herausgabe von Kundendaten; jahrelang reichte hierfür die Angabe des Namens und des Geburtsdatums aus. Das Gericht ließ diese Argumentation jedoch nur bedingt gelten: Bei vorangegangenen Überprüfungen durch die Aufsichtsbehörde sei das Verfahren des Kommunikationsanbieters nie kritisiert worden. Auch habe es keine offiziellen Leitlinien zu Authentifizierungsverfahren bei Kommunikationsanbietern gegeben, an denen sich 1&1 habe orientieren können. Nicht zuletzt beschränkte sich der Datenschutzverstoß auf einen Vorfall und eine Privatperson, auf den das Unternehmen nach Kenntnis umgehend reagierte und sein Authentifizierungsverfahren umgestellt und mit einer PIN abgesichert hat sowie sich gegenüber der Datenschutzaufsichtsbehörde kooperativ zeigte.

- Für gänzlich unwirksam erklärte das LG Berlin Mitte Februar 2021 das Bußgeld in Höhe von gut EUR 14,5 Mio. gegen die Deutsche Wohnen. Dem Unternehmen wurden (trotz Warnung und Abmahnung der Aufsicht) von der Behörde diverse Verstöße gegen Lösch- und Archivierungspflichten bezüglich Mieterdaten vorgeworfen. Allerdings machte die Aufsicht keine Angaben zu den einzelnen Verstößen der Mitarbeiter des Unternehmens, die aber laut Gericht für eine Zurechnung des Verschuldens zum Unternehmen und damit für ein wirksames Bußgeld erforderlich gewesen wären. Denn bei der Verhängung von Bußgeldern sei deutsches Recht zu beachten, auch wenn die europäische DSGVO die Grundlage bilde – und nach deutschem Recht bedarf es für wirksame Bußgelder gegen Unternehmen grundsätzlich der Feststellung und Zurechnung des Verschuldens. Im Gegensatz dazu hatte das LG Bonn es im Verfahren gegen 1&1 als ausreichend angesehen, dass lediglich ein Verstoß gegen die DSGVO festgestellt worden sei, einzelne Verstöße von Mitarbeitern müssten hingegen nicht festgestellt werden. Gegen den Beschluss des LG Berlin hat die Behörde in Zusammenarbeit mit der zuständigen Staatsanwaltschaft inzwischen Beschwerde eingelegt, sodass abzuwarten bleibt, ob die Gerichte gegebenenfalls auch noch zur Höhe des Bußgelds Stellung nehmen.

Was ist zu tun bei einem Bescheid der Aufsichtsbehörden?

Die Verfahren zeigen: Ein offizieller Bescheid der Datenschutzaufsichtsbehörden ist kein Grund zur Panik. Vielmehr sollte er durch Datenschutzexperten (zum Beispiel den internen oder externen Datenschutzbeauftragten) sorgfältig geprüft und die weitere Vorgehensweise mit Bedacht abgewogen und gewählt werden. Was vermieden werden sollte: den Bescheid zu ignorieren und gar nicht zu reagieren oder lediglich pauschal zu antworten.

Anzuraten ist daher grundsätzlich die umfassende Kooperation mit der Behörde, auch wenn man gesetzlich nicht unmittelbar dazu verpflichtet ist. Denn selbst wenn eine solche Kooperation noch nicht direkt zum Einlenken der Behörde führen mag, dürfte die Bereitschaft zur Zusammenarbeit jedoch bei der Bußgeldbemessung, spätestens jedoch bei der Entscheidung des Gerichts als mildernder Umstand zu berücksichtigen sein. Dies gilt umso mehr, je früher mit der Behörde kooperiert wird – hier sollten nicht erst ein Bußgeldbescheid abgewartet, sondern auch bereits die (informellen) Anfragen und Rügen der Behörde ernst genommen und entsprechend beantwortet werden. Es versteht sich von selbst, dass der Verstoß umgehend beendet und im Fall einer Meldepflicht den Behörden entsprechend mitgeteilt werden sollte.

Sofern ein Vorgehen gegen das Bußgeld als sinnvoll erachtet wird, zum Beispiel wenn der Bescheid Fehler enthält oder die Situation nicht korrekt beurteilt wurde, sollte sodann fristgemäß Einspruch gegen den Bescheid (als Vorstufe zur gerichtlichen Prüfung) eingelegt werden. Dadurch wird die Behörde gezwungen, sich nochmals mit dem Verfahren und den Argumenten des sanktionierten Unternehmens zu beschäftigen.

Gerichtliches Vorgehen als weitere Eskalationsstufe

Hält die Behörde an dem Bußgeld fest, besteht die Möglichkeit, das Verfahren vor den Gerichten weiterzuführen. Dies ist zwar mit zusätzlichem Aufwand und weiteren Kosten verbunden, es existieren im Datenschutzrecht aber (noch) so viele offene Fragen, die Ansatzpunkte für eine erfolgreiche Verteidigung bieten können, dass eine weitere Eskalation sinnvoll und erfolgsversprechend sein kann.

So sind, wie man an den Entscheidungen des LG Bonn und des LG Berlin sehen kann, die Anforderungen an den Nachweis von Verstößen und deren Zurechnung zu einem Unternehmen nicht abschließend geklärt. Auch wird das derzeitige Bußgeldberechnungsmodell der Aufsichten regelmäßig als zu schematisch kritisiert, da sich eine pauschale Bewertung von Verstößen und Bußgeldern nach deutschem Recht grundsätzlich verbietet. Vielmehr müssen Behörden stets den Einzelfall umfassend berücksichtigen und bewerten, so beispielsweise auch das Verhältnis von Umsatz, Bußgeld und Gewinn. Denn die DSGVO stellt für die Berechnung eines Bußgelds zwar ausschließlich auf den Umsatz eines Unternehmens ab, es erscheint jedoch zumindest angreifbar, wenn ohne Rücksicht auf die konkreten finanziellen Verhältnisse sehr hohe Bußgelder gegen Unternehmen mit höherem Umsatz, aber vergleichsweise geringem Gewinn festgesetzt werden. Es bleibt abzuwarten, ob und wie sich die bereits angekündigte Anpassung des Bußgeldberechnungsmodells hierauf auswirkt.

Darüber hinaus besteht immer die Möglichkeit, dass die Datenschutzaufsichtsbehörde von einem unzutreffenden Sachverhalt ausgeht. Dies kann an fehlenden oder unvollständigen Informationen durch das Unternehmen, aber auch an einem falschen oder fehlenden Verständnis der übermittelten Informationen seitens der Behörde liegen. Nicht zuletzt sind die deutschen Datenschutzaufsichten in ihrem Verständnis des Datenschutzes oft auch strenger als es tatsächlich im Gesetz angelegt ist. Insofern hilft ein genaues Verständnis der Anforderungen des Datenschutzrechts, Argumentations- und Abwehrlinien gegen die Behörde und vor Gericht weiter zu stärken.

Influencer Marketing und die Kennzeichnungspflichten

Die Rechtslage hinsichtlich der Kennzeichnungspflichten beim Influencer-Marketing ist unübersichtlich, da eine zunehmende Anzahl von (teilweise widersprüchlichen) gerichtlichen Urteilen beachtet werden muss und die bestehenden gesetzlichen Regelungen nicht für diese neue Form des Marketings geschaffen wurden. Eine Gesetzesreform soll nun etwas Klarheit schaffen.

Hintergrund

Das Influencer Marketing liegt voll im Trend. In einer aktuellen Studie des Bundesverbands Digitale Wirtschaft aus dem März 2020 gab jeder fünfte Befragte an, sich von Influencern online beim Kauf beeinflussen zu lassen (vgl. https://www.bvdw.org/veroeffentlichungen/studien-marktzahlen/detail/artikel/mehr-als-jeder-fuenfte-verkaeufe-durch-influencer-marketing-neh-

men-laut-bvdw-studie-2020-nochmal-zu-1/). Influencer gelten als authentisch und glaubwürdig, da sie sich ihren Followern gegenüber als Privatpersonen präsentieren und sich damit ideal als Markenbotschafter für Werbekooperationen mit Unternehmen eignen. Die Absatzförderung läuft über die verschiedenen sozialen Netzwerke wie Instagram, Youtube, Twitch und TikTok. Dabei kennzeichnen Influencer längst nicht alle Posts, in denen fremde Produkte und Dienstleistungen präsentiert werden, als Werbung. Daher kam es zu mehreren aufsehenerregenden Fällen, in denen Influencer von Verbraucherverbänden wie dem Verband Sozialer Wettbewerb verklagt wurden. Die Rechtsunsicherheit bei Influencern ist groß, da die Gerichte die Frage der Kennzeichnungspflichtigkeit beim Influencer Marketing sehr unterschiedlich beurteilen. Mehr Rechtsklarheit soll nun ein neuer "Influencer-Paragraph" im Gesetz zur Stärkung des Verbraucherschutzes im Wettbewerbs- und Gewerberecht bringen, welches das Bundeskabinett am 20. Januar 2021 verabschiedet hat (siehe https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/DE/Staerkung_Verbraucherschutz_Wettbewerbs-_und_Gewerberecht.html).

Aktuelle Rechtslage

Ob Influencer ihre Posts in den sozialen Netzwerken als Werbung kennzeichnen müssen, beurteilt sich nach dem hierfür einschlägigen „Influencer-Paragraph" § 5a Abs. 6 des Gesetzes gegen den unlauteren Wettbewerb (UWG). Danach handelt unlauter, wer den kommerziellen Zweck einer geschäftlichen Handlung nicht kenntlich macht, sofern sich dieser nicht unmittelbar aus den Umständen ergibt, und das Nichtkenntlichmachen geeignet ist, den Verbraucher zu einer geschäftlichen Entscheidung zu veranlassen, die er andernfalls nicht getroffen hätte. Immer wieder posten oder vertaggen Influencer in ihren Posts auf die Instagram-Accounts von den Markenherstellern, deren Produkte diese tragen oder deren Dienstleistungen sie in sonstiger Weise ihren Followern präsentieren, ohne hierfür von dem Markenhersteller ein Entgelt oder eine sonstige Gegenleistung zu erhalten. Eine fehlende Gegenleistung schließt jedoch nicht zweifelsfrei das Vorliegen eines kommerziellen Zwecks aus. Vielmehr greifen einige Gerichte auf Indizien zurück, die zusammengenommen entweder dafür sprechen, die Instagram-Posts als redaktionelle Beiträge zu beurteilen, bei denen die Information der Follower im Vordergrund steht oder bei denen der werbende Charakter im Vordergrund steht, so wie zuletzt auch das Oberlandesgericht Köln (OLG Köln, Urteil vom 19.02.2021 – 6 U 103/20, vgl. OLG Köln, Urteil vom 19.02.2021 - 6 U 103/20 - openJur). Andere Gerichte wie das Oberlandesgericht Hamburg nehmen keine Werbekennzeichnungspflicht an, wenn ein followerstarker Influencer auf Instagram in seinen Posts auf Instagram-Accounts fremder Markenhersteller verlinkt, da den Followern der kommerzielle Zweck der Posting-Aktivitäten nach Ansicht der Hamburger Richter durchaus bewusst sei. Diese Rechtsunsicherheit führt dazu, dass Influencer ihre Posts auch dann als Werbung kennzeichnen, wenn diese sich die Produkte selbst gekauft haben und in dem Posts mit einem Tap Tag, also einem Link im anklickbaren Post selbst, auf den Instagram-Accounts des Herstellers verlinken.

Zukünftige Rechtslage

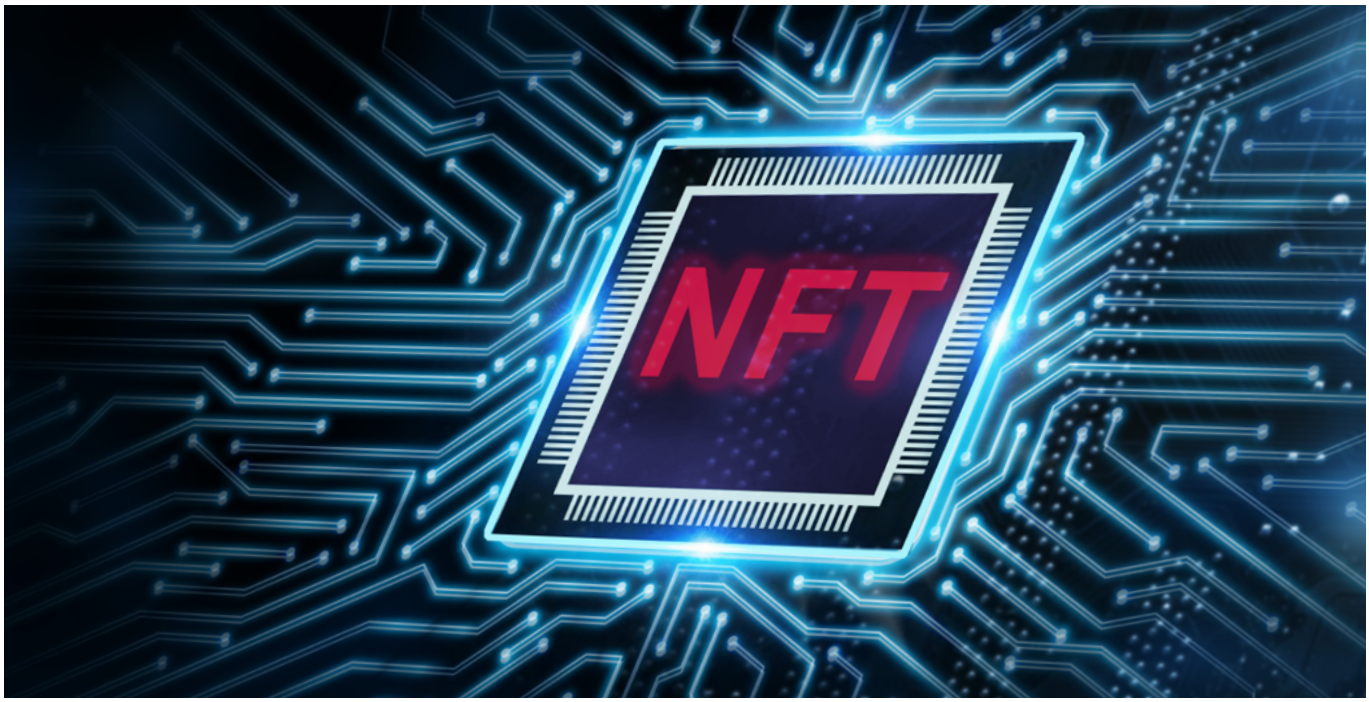
Aktuell liegt dem BGH eine Revision des Verbands Sozialer Wettbewerb vor, nachdem das Oberlandesgericht München eine verbotene Schleichwerbung der Influencerin Cathy Hummels mangels Vorliegens einer geschäftlichen Handlung im Sinne von § 2 Abs. 1 Nr. 1 UWG verneinte. Es wird mit Spannung erwartet, wie sich der BGH in Sachen Kennzeichnungspflichten für Influencer positionieren wird.

Auch in gesetzgeberischer Sicht sind Neuerungen zu beobachten, die zu mehr Rechtsklarheit für Influencer führen sollen. So befindet sich aktuell das Gesetz zur Stärkung des Verbraucherschutzes im Wettbewerbs- und Gewerberecht im laufenden Gesetzgebungsverfahren. Laut diesem Gesetz wird der lauterkeitsrechtliche § 5a Abs. 6 UWG durch den neuen "Influencer-Paragraphen" § 5a Abs. 4 UWG ersetzt. Danach soll ein kommerzieller Zweck bei einer Handlung zugunsten eines fremden Unternehmers nicht vorliegen, wenn der Handelnde kein Entgelt oder keine ähnliche Gegenleistung für die Handlung von dem fremden Unternehmer erhält oder sich versprechen lässt. Erhält der Influencer eine direkte Gegenleistung oder eine ähnliche Gegenleistung (beispielsweise Provisionen, Produkte, Pressereisen, die Stellung von Ausrüstung oder Kostenübernahmen), müssen Tap Tags in Posts mit dem Hashtag #Werbung oder #Anzeige gekennzeichnet werden.

Sollte das Gesetz in seiner aktuellen Form verabschiedet werden, müssen Influencer in Zukunft nicht mehr solche Posts auf Social Media als Werbung kennzeichnen, in denen sie die selbst erworbenen Produkte und Dienstleistungen fremder Markenhersteller ihren Followern präsentieren und keine Gegenleistung hierfür erhalten bzw. keine Gegenleistung versprochen bekommen haben. Das Gesetzgebungsverfahren sowie die Rechtsprechung sollten daher von Influencern weiterhin genauestens beobachtet werden, um das Risiko für Verstöße gegen rechtliche Vorgaben zur Werbung zu verringern und so idealerweise Abmahnungen und Gerichtsverfahren zu vermeiden.

NFTs – was sind das und wenn ja, wie viele?

Ähnlich zu Kryptowährungen wie Bitcoin oder Ethereum - und doch anders: NFT zur Übertragung von Rechten an digitalen Inhalten sind derzeit in aller Munde. Ohne begleitende rechtliche Regelungen kommen sie aber nicht aus.



Hintergrund

Was haben der Twitter-Gründer Jack Dorsey, die amerikanische Profibasketballliga NBA, die Band Kings of Leon und der Digitalkünstler Beeple gemein? NFTs oder Non-Fungible Tokens. Mit diesen noch relativ neuen digitalen Tokens können gerade digitale Inhalte und die Rechte daran über die Blockchain übertragen werden, wobei jeder Token einzigartig ist und stellvertretend für einen „digitalen Gegenstand“ steht.

Dorsey hat vor kurzem seinen ersten Tweet für USD 2,5 Mio. per NFT versteigert und die NBA betreibt mit Top Shot eine Plattform, in der man wichtige Momente der NBA-Geschichte in der Form von kurzen Video-Clips wie digitale Sammelkarten per NFT „besitzen“ kann. Die Kings of Leon haben ihr letztes Album per NFT verkauft und Beeple hat mit der Versteigerung einer Collage aus 5.000 Fotos bei Christies für knapp USD 70 Mio. diverse Rekorde gebrochen.

Was sind NFTs?

NFTs stellen eine Asset-Klasse aus dem Bereich der Kryptowährungen dar oder besser gesagt der Blockchain-Technologie, wobei der englische Ausdruck *fungible* für „vertretbar“, „austauschbar“ oder „ersetzbar“ steht und die NFT insbesondere von den „normalen“ Kryptowährungen abgrenzen soll. Bei diesen „normalen“ Kryptowährungen, zum Beispiel den Bitcoins, ist jeder Coin gleich. Wie bei einer traditionellen Währung ist es bei der Nutzung und Bezahlung mit Bitcoin egal, mit welchem konkreten Coin bezahlt wird oder welcher konkrete Coin übertragen wird. NFTs sind im Gegensatz dazu einzigartig und werden deshalb genutzt, um die „Inhaberschaft“ bestimmter Assets mit einen einzigartigen NFT zu verbinden und dadurch einer Person zuzuweisen. Das kann beispielsweise funktionieren, indem – vereinfacht ausgedrückt – in dem einzelnen NFT das Asset verlinkt ist, welches übertragen werden soll (zum Beispiel der erste Tweet von Jack Dorsey). Dieser NFT wird über eine Blockchain-Transaktion dann von den Verkäufern oder den Auktionatoren an die Käufer übertragen. Das kann sogar auch als sogenannter Smart Contract geschehen, welcher die Transaktion nach der Zah-

lung des Kaufpreises automatisiert auslöst und den NFT überträgt. Käufer haben diesen NFT dann in ihrer Wallet und können damit nachweisen, dass sie die „Inhaber“ eines bestimmten Assets sind. Doch mit diesen Smart Contracts ist noch mehr möglich: beispielsweise können sie so programmiert werden, dass Künstler nicht nur beim ersten Verkauf den Verkaufspreis erhalten, sondern an jedem weiteren Verkauf prozentual am Verkauf mitverdienen. Das funktioniert zumindest dann automatisch, wenn der Kaufpreis in einer Kryptowährung bezahlt wird, die auf der gleichen Blockchain „lebt“, wie der NFT.

NFTs benötigen begleitende rechtliche Regelungen

Aus rechtlicher Sicht ist dabei zu beachten, dass die Rechtslage in den meisten Fällen jedoch nicht durch den NFT bestimmt wird, sondern abseits der jeweiligen Blockchain gesondert geregelt werden muss. In den genannten Beispielsfällen geht es jeweils um die Übertragung von digitalen Inhalten (digitale Kunstwerke, Video-Clips, Tweets), sodass sich die Frage stellt, was genau in rechtlicher Hinsicht hier übertragen werden soll. Im Fall des Albums der Kings of Leon erhält man mit dem NFT zum Beispiel das Recht auf einen Download des Albums inklusive eines besonderen Albumcovers. Bei NBA Top Shots erlangt man nach den AGB lediglich die „Inhaberschaft“ hinsichtlich des NFTs und die Lizenz, den „gekauften“ Moment in der App anzusehen und weiterzuverkaufen, zu tauschen oder zu verschenken. Das bedeutet also nicht, dass einem dieser „Moment“ (gemeint ist der Video-Clip) auch wirklich gehört, man kann zum Beispiel anderen nicht verbieten, den gleichen Video-Clip auf YouTube hochzuladen. In den Fällen von Beeple und Jack Dorsey wurde vermutlich zwischen Verkäufer und Käufer in einem Lizenzvertrag vereinbart, was es bedeutet einen Tweet oder ein digitales Kunstwerk zu „besitzen“. Der NFT dient in diesem Verhältnis lediglich als Dokumentation der Rechteübertragung, die über eine „normale“ urheberrechtliche Lizenz abseits der Blockchain stattfindet. Auch die automatische Beteiligung der Künstler an weiteren Verkäufen muss in einem Vertrag abseits der Blockchain rechtlich geregelt werden. Lediglich die tatsächliche Durchsetzung dieser rechtlichen Verpflichtung funktioniert dann automatisiert per Smart Contract auf der Blockchain.

Unser Kommentar

Vorteil der Nutzung von NFTs ist die in der Blockchain-Technologie begründete Fälschungssicherheit. Allerdings kann man durchaus in Frage stellen, ob für die oben genannten Einsatzszenarien eine fälschungssichere Blockchain tatsächlich erforderlich ist. Deutlicher Nachteil der Blockchain ist der enorme Energieverbrauch, den gerade Blockchains wie Bitcoin und Ethereum verursachen. Zwar ist der Energieverbrauch einer einzelnen Transaktion natürlich nicht gleichzusetzen mit dem Energieverbrauch des Gesamtsystems und die beispielsweise von NBA Top Shots eingesetzte Blockchain der Flow-Technologie hat wohl einen deutlich niedrigeren Energieverbrauch als viele bekannte Kryptowährungen. Dennoch sollte man sich die Frage stellen, ob der zweifelhafte Nutzen von NFTs auch einen vergleichsweise niedrigen Energieverbrauch im Jahre 2021 rechtfertigen kann. Zudem ist stets zu beachten, dass NFTs in der Regel nicht für sich alleine stehen und daher begleitende rechtliche Regelungen in Form von traditionellen Verträgen benötigen, um Lizenz-, Schutz- und Verwertungsrechte und die weiteren rechtlichen Rahmenbedingungen eindeutig zu regeln.

Hamburgischer Beauftragte für Datenschutz und Informationsfreiheit (HamBfDI) – Zulässigkeit der Herabsetzung des Schutzniveaus von technisch-organisatorischen Maßnahmen (TOM)

Kann mit der Einwilligung der betroffenen Person zu deren Nachteil von datenschutzrechtlichen Vorgaben abgewichen werden? Laut dem HamBfDI sei dies zumindest für die Herabsetzung von technisch-organisatorischen Maßnahmen möglich.

Hintergrund

Wie der HamBfDI kürzlich in einem Vermerk mitteilte, können betroffene Personen wirksam in die Herabsetzung des Schutzniveaus beziehungsweise technisch-organisatorischer Maßnahmen (TOM), die die Verarbeitung ihrer personenbezogenen Daten betreffen, wirksam einwilligen. Dies ist allerdings nur dann zulässig, wenn der Verantwortliche die nach Art. 32 DSGVO geforderten Schutzmaßnahmen grundsätzlich vorhält und der betroffenen Person auf Verlangen zur Verfügung stellt, ohne dass der betroffenen Person dadurch Nachteile entstehen.

Die Frage, ob betroffene Personen mittels einer Einwilligung wirksam auf an sich datenschutzrechtlich vorgeschriebene Anforderungen an die Sicherheit der Verarbeitung verzichten können, ist bereits unter Geltung des § 9 BDSG-alt streitig gewesen und wurde häufig am Beispiel der Möglichkeit einer Einwilligung in die nur transportverschlüsselte (bei Übermittlung besonders sensibler oder einem Berufsgeheimnis unterliegender Daten) oder gar unverschlüsselte E-Mail-Kommunikation diskutiert. Kernpunkt ist die Frage, ob die datenschutzrechtlichen Vorgaben zur Disposition der betroffenen Person stehen.

Der HamBfDI bejaht dies im Ergebnis, auch wenn er die Erwägungen derer, die sich gegen eine Disponibilität eines Mindeststandards aussprechen, als berechtigt erachtet.

Abdingbarkeit des Systemdatenschutzes?

Ein Argument gegen die Möglichkeit, in die Reduzierung von Sicherheitsstandards einzuwilligen: für die Etablierung europäischer Mindeststandards, wie sie die DSGVO schaffen solle, dürften die Vorgaben des Art. 32 DSGVO nicht durch Vereinbarungen mit den betroffenen Personen unterlaufen werden. Es wird befürchtet, dass der Systemdatenschutz dabei aufgrund wirtschaftlicher Erwägungen auf ein minimales Niveau reduziert wird, wenn den Nutzern von Angeboten mit sogenannten „lock-

in Effekten“ (z. B. Soziale Netzwerke) eine entsprechende Einwilligung abgerungen wird - diese widerspräche auch den Geboten von Privacy by Default und Privacy by Design.

Gleichwohl ist der HambBfDI der Meinung, dass betroffenen Person nicht gegen ihren Willen beziehungsweise gegen ihre ausdrückliche Ablehnung (und gegebenenfalls zu ihrem Nachteil) ein Schutzniveau aufgezwängt werden dürfe. Zudem müsse die Antwort auf die Frage der Abdingbarkeit des Systemdatenschutzes differenziert erfolgen.

Unterscheidung zwischen betroffener Person und Verantwortlichem notwendig

Für den Verantwortlichen oder Auftragsverarbeiter sei Art. 32 DSGVO zwingendes Recht und enthalte verbindliche Regeln, da Art. 32 DSGVO eine Pflicht zur Implementierung angemessener Maßnahmen enthält. Dem Verantwortlichen oder Auftragsverarbeiter selbst werde keine Entscheidungsbefugnis darüber einräumt, ob er diese Pflicht umsetze.

Etwas anderes gelte jedoch im Verhältnis zur betroffenen Person: Primäres Schutzgut der DSGVO sei das Grundrecht auf Datenschutz (Art. 8 GrCH). Dieses stehe grundsätzlich zur Disposition ihres Trägers, also der betroffenen Person. Der HamBfDI zeigt in einem Erst-recht-Schluss auf, dass das Recht der betroffene Person, beispielsweise in die Veröffentlichung von unvorteilhaften oder sexualisierten Aufnahmen im Internet einzuwilligen, zwangsläufig auch das Recht beinhalte, einen unsicheren Übermittlungsweg für die Übersendung derartiger Aufnahmen zu wählen. Ob eine solche Einwilligung im Sinne der Person oder im Sinne des Datenschutzes sei, spiele keine Rolle, solange die Einwilligung freiwillig erfolgte. Damit seien die Schutzmaßnahmen bei der Verarbeitung der eigenen personenbezogenen Daten durch die betroffene Person abdingbar.

Art. 32 DSGVO verfolge dabei in erster Linie den Schutz der betroffenen Person und erst in zweiter Linie das Regelungsziel, ein einheitliches Niveau der Datensicherheit bei der Verarbeitung personenbezogener Daten zu schaffen. Dieses sekundäre Ziel werde auch dann erreicht, wenn ein Verzicht auf bestimmte Maßnahmen durch die betroffene Person zugelassen wird, die Regelung gegenüber dem Verantwortlichen jedoch verbindliche Anforderungen zur Schaffung eines angemessenen Standards der Datensicherheit im Allgemeinen stellt.

Der HamBfDI erläutert zudem, dass sich nichts anders aus Art. 6 und 7 DSGVO ergebe. Denn diese Normen beschränkten die grundsätzlich unbeschränkte Dispositionsfreiheit der betroffenen Person nur in Bezug auf das „Ob“ (indem dem Verantwortlichen die Verarbeitung der personenbezogenen Daten der betroffenen Person erlaubt werde) und nicht in Bezug auf das „Wie“. Da eine Regelung über eine Beschränkung der Dispositionsfreiheit über das „Wie“ fehle, blieben die genannten Artikel 6 und 7 DSGVO in Bezug auf das „Wie“ unbeschränkt.

Pflicht zur Schaffung Art. 32 DSGVO-konformer Datensicherheitsstandards

Aus Art. 25 DSGVO folgt die Pflicht des Verantwortlichen, unabhängig von der konkreten Verarbeitung aufgrund einer typisierenden Betrachtung der von ihm durchgeführten Verarbeitungen angemessene Schutzmaßnahmen zu ergreifen.

Zentrale Aussage des HamBfDI ist, dass die betroffene Person eine freie Entscheidung über einen Verzicht der Einhaltung der Vorgaben des Art. 32 DSGVO nur dann treffen kann, wenn die nach Art. 32 DSGVO erforderlichen TOMs durch den Verantwortlichen zumindest vorgehalten werden:

„Daher kann sich ein Verantwortlicher, der eine Verarbeitung durchführt, die die Übermittlung sensibler Daten erfordert, nicht darauf zurückziehen, dass er schon grundsätzlich keine sichere Übermittlung gewährleisten kann und dem Betroffenen eine pauschale Einwilligung dazu abringen. Vielmehr hat er eine sichere Übermittlungsform bereits zum Zeitpunkt der Auswahl der Mittel für die Verarbeitung vorzuhalten. Dies schließt nicht aus, dass der Betroffene in Bezug auf eine konkrete, ihn betreffende Verarbeitung darin einwilligen kann, dass die konkrete Maßnahme ohne das nach Art. 32 DSGVO erforderliche Schutzniveau durchgeführt wird, vorausgesetzt, dass der Verantwortliche dieses grundsätzlich gewährleisten kann.“

Anforderungen an die Einwilligung

Die Einwilligung in die Absenkung von TOM müsse den Anforderungen von Art. 7 analog DSGVO genügen. Die analoge Rechtsanwendung des HamBfDI folgt daraus, dass für die Einwilligung in das „Wie“ der Datenverarbeitung die gleichen Maßstäbe wie für die Einwilligung in das „Ob“ der Einwilligung gelten müssten (für die Art. 7 DSGVO unmittelbar gilt).

Insbesondere müsse die Einwilligung auch freiwillig erteilt werden – das setze jedoch voraus, dass für die betroffene Person eine angemessene sichere alternative Datenverarbeitung existiert, die nicht mit unzumutbaren Nachteilen verbunden ist. Unzumutbar könne zum Beispiel eine unangemessene Verlängerung der Bearbeitungsdauer oder das Entstehen von Bearbeitungskosten sein.

Eine Unzumutbarkeit kann sich aber auch schon daraus ergeben, dass Betroffene dauerhaft gezwungen sind, den aufwändigeren, zeitintensiveren und aufgrund von Druck- und Versandkosten kostenintensiveren Weg der schriftlichen Kommunikation zu wählen, weil keine sichere digitale Abwicklung ermöglicht wird. Der Verantwortliche hat deshalb von vornherein Sorge dafür zu tragen, dass auf konkret definierte und absehbare Zeit auch Möglichkeiten der sicheren digitalen Abwicklung eröffnet werden, die frei von diesen Nachteilen sind.

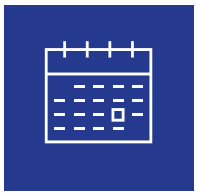
Unser Kommentar

Die Ablehnung der paternalistisch wirkenden Auffassung, die betroffene Person könne nicht wirksam in der Herabsetzung datenschutzrechtlicher Mindeststandards einwilligen, überzeugt. Das Datenschutzrecht schafft kein Recht, die betroffene Person vor sich selbst zu schützen.

Richtig ist aber auch, dass die Wirksamkeit einer Einwilligung der betroffenen Person eine echte Wahlmöglichkeit lassen muss (zum Beispiel die sichere Übermittlung auf dem Postweg anstelle der Übermittlung mittels einer unverschlüsselten E-Mail) und sie nicht faktisch zur Einwilligung gezwungen wird muss, um den ihr angebotenen Service des Verantwortlichen zu nutzen (keine „Friss oder stirb“-Situation).

Verantwortliche sollten daher grundsätzlich geeignete technisch-organisatorische Maßnahmen treffen, um beispielsweise im Hinblick auf die Kommunikation per E-Mail gar nicht erst auf die Einwilligung ihrer Kunden in die unverschlüsselte Kommunikation angewiesen zu sein. Stattdessen sollten sichere Wege geschaffen werden, dem Kunden Unterlagen zur Verfügung zu stellen (etwa mittels der Einrichtung von zugangsgeschützten Webportalen).

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; ismagilov/iStockphoto: Seite 3; stevanovic igor/Adobe Stock: Seite 5; MclittleStock/Adobe Stock: Seite 7; putilov_denis/Adobe Stock: Seite 9; BillionPhotos.com/Adobe Stock: 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 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