LOSCHELDER

Newsletter Datenschutzrecht
September 2020

Sehr geehrte Damen und Herren,

in den letzten Wochen waren viele von uns wohl mit der Nachbereitung und Aufbereitung der Folgen der BGH-Cookie-Entscheidung und dem EuGH-Urteil in Sachen Schrems II beschäftigt.

Zu beiden Themen schweigt unser Newsletter heute einmal, um Platz für andere brisante Themen zu schaffen: Videoüberwachung als Dauerbrenner, ein neues Gesetz am Horizont (Telemedien- und Telekommunikationsdatenschutz werden wenigstens national novelliert, wenn dies auf EU-Ebene nicht klappen will), Spannendes zur datenschutzrechtlichen Verantwortlichkeit bei Insolvenz und ein Update in Sachen Corona-Positionen der Aufsichtsbehörden.

Und zu guter Letzt haben wir natürlich auch in diesem Monat einige spannende Bußgeldfälle für Sie zusammengetragen.

Inhalt

DSK: Neues zur Videoüberwachung

Die Datenschutzkonferenz der Länder (DSK) konkretisiert in einer neuen Orientierungshilfe den zulässigen Rahmen einer datenschutzkonformen Videoüberwachung durch nicht-öffentliche Stellen. Zum ersten Mal beschäftigt sich die DSK darin mit Videoüberwachung in der Nachbarschaft und der datenschutzrechtlichen Bewertung von Tür- und Klingelkameras, Drohnen, Wildkameras sowie Dashcams. Die wichtigsten Punkte und Neuerungen finden Sie hier.

Über eine Videoüberwachung werden personenbezogene Daten verarbeitet, wenn einzelne Personen auf den Bildern zu erkennen sind oder die Aufnahmen aus anderen Gründen Rückschlüsse auf die Identität der Gefilmten ermöglichen. Wie bei jeder Verarbeitung personenbezogener Daten braucht es dann auch für die Videoüberwachung einer datenschutzrechtlichen Erlaubnis und dafür insbesondere einen vorher festgelegten Zweck: Es darf nicht „ins Blaue hinein" oder aus unpräzisen „Sicherheitsgründen" gefilmt werden. Eine dauerhafte und anlasslose Überwachung ist regelmäßig unzulässig.

Als Erlaubnisgrundlage hält die DSK zwar im Vergleich zu ihrem früheren Kurzpapier auch eine Einwilligung durch die gefilmte Person in größerem Umfang für möglich; jedoch dürfte es oft nicht praktikabel sein, von jeder gefilmten Person Einwilligungen nachweisbar einzuholen, erst recht nicht bei einer Überwachung des öffentlichen Raums. Daher ist nach Ansicht der DSK die Überwachung in den meisten Fällen nur dann erlaubt, wenn berechtigte Interessen des Überwachenden greifen und diesen keine gegenläufigen, überwiegenden Betroffeneninteressen entgegenstehen (Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO). Dies erfordert eine vorherige umfassende Interessenabwägung und die Dokumentation derselben. Daneben treffen den Verwender der Überwachungsanlagen die üblichen Pflichten der Datenverantwortlichen, wie die zeitliche Speicherbegrenzung (hier geht die DSK regelmäßig von 72 Stunden aus, während teilweise auch 48 Stunden als regelmäßige Obergrenze gesehen werden), die Information der Betroffenen oder die Implementierung angemessener technisch-organisatorischer Maßnahmen.

Was geht und was geht nicht?

Rechtssicher und aussagekräftig beurteilt werden kann stets nur der konkrete Einzelfall. Einige Tendenzen lassen sich der Orientierungshilfe für bestimmte Bereiche aber entnehmen, die wir nachfolgend zusammenfassen:

- **Aufnahmen im familiären Bereich**

Durch die sogenannte „Haushaltsausnahme" sind nach wie vor solche Videoaufnahmen datenschutzrechtlich uneingeschränkt zulässig, die im familiären Bereich, also ohne einen Zusammenhang zu einer beruflichen oder wirtschaftlichen Tätigkeit entstehen.

- **Überwachung am Arbeitsplatz**

Die Überwachung der Beschäftigten ist nur dann zulässig, wenn sichergestellt werden kann, dass ein kontrollfreier und unbeobachteter Arbeitsbereich verbleibt. Eine Überwachung eines nicht-öffentlich zugänglichen Bereichs soll nur dann zulässig sein, wenn dies erforderlich ist, um einen Bereich vor dem Eindringen Unberechtigter zu schützen, zur Überwachung der betrieblichen Abläufe oder damit der Arbeitgeber seinen Schutzpflichten ausreichend nachkommen kann; Arbeitsbereiche der Beschäftigten sind dabei aber so weit wie möglich auszublenden. Wird patrouillierendes Sicherheitspersonal von der Überwachung miterfasst, sind technisch-organisatorische Maßnahmen zu treffen, um den Eingriff in deren Rechte abzuschwächen. Eine totale Überwachung zum Zweck der Leistungskontrolle ist auch dann unzulässig, wenn die Arbeit eine persönliche Geschäftsführung oder -kontrolle erfordert. Gleiches gilt für die Überwachung der Pausenräume. Eine Überwachung zur Aufklärung einer Straftat ist nur dann zulässig, wenn sich bereits vor der Überwachung aus tatsächlichen Umständen ein konkreter Verdacht ergeben hat.

- **Überwachung in der privaten Nachbarschaft**

Bei einer Überwachung, die über die private Grundstücksgrenze hinausgeht, endet das Hausrecht des Hausherrn und beginnt der

Anwendungsbereich der DSGVO. Damit ist die anlasslose Überwachung öffentlich zugänglicher Bereiche ohne konkretes Überwachungsinteresse in den meisten Fällen unzulässig. Soweit sich die Überwachung auch auf das Grundstück eines Nachbarn erstreckt, kann dies für den Betreiber der Überwachungsanlage zusätzlich zivil- und sogar strafrechtliche Konsequenzen haben.

- **Überwachung in der Gastronomie**

In den meisten Fällen unzulässig ist die Überwachung in Ess- und Aufenthaltsbereichen sowie Café- und Gastronomieflächen in Bäckereien, Tankstellen, Hotels, etc., in denen sich Gäste aufhalten. Anders verhält es sich, wenn Lager- oder Tresorräume überwacht werden, da diese in der Regel nicht frei zugänglich sind. Dies gilt jedoch nur, soweit keine milderen Methoden zur Sicherung, wie z.B. eine Codekarte oder ein Passwort ausreichend in Betracht kommen.

- **Überwachung mithilfe von Dashcams**

Die Überwachung mithilfe von Dashcams soll nur in den Fällen zulässig sein, in denen technisch sichergestellt werden kann, dass der Einsatz nur kurzzeitig und anlassbezogen stattfindet. Weitere Informationen zur Verwendung von Dashcams hat die DSK in einem Positionspapier zusammengestellt.

- **Überwachung mithilfe Übersichtskameras und Webcams**

Der Einsatz von Übersichtskameras, die z.B. einen Überblick über die Verkehrs- oder Wetterlage geben sollen, ist nur dann zulässig, wenn auf ihren Aufnahmen Einzelpersonen und Fahrzeuge nur schemenhaft und Gebäude gar nicht erkennbar sind, was unter anderem durch die Positionierung der Kamera, fehlende Zoom-Funktion oder niedrige Bildauflösung erreicht werden kann. Zudem sollte die Übertragung des Bildes so eingestellt und der Zeitraum so gewählt sein, dass die Bilder keinen genauen Rückschluss über das Verhalten der gefilmten Personen zulassen. Gleiches soll für Webcam-Aufnahmen gelten, die ihre Aufnahmen in Echtzeit übertragen.

- **Überwachung mithilfe von Tür- und Klingelkameras**

Zulässig ist die Verwendung einer Anlage sein, die nur nach Betätigung der Klingel filmt, keine Speicherung zulässt und durch ihre Positionierung nur das Bild wiedergibt, das der Benutzer sonst auch mit einem Blick durch den Türspion erhalten würde. Eine dauerhafte und anlasslose Überwachung muss technisch ausgeschlossen sein. Ein System, das in Wohnbereichen sowohl als Überwachungs-, als auch als Tür- und Klingelkamera eingesetzt, d.h. durch Bewegung, manuell oder per Smartphone aktiviert werden kann (ggf. ein Pre-Recording einsetzt) und dabei den öffentlichen Raum erfasst, ist dagegen nur in den seltensten Fällen zulässig.

- **Überwachung mithilfe von Drohnen**

Gerade wenn es sich um Aufnahmen im öffentlichen Raum handelt, ist es wegen der Menge der damit erfassten personenbezogenen Daten und der oft unübersichtlichen Zahl der betroffenen Personen fast unmöglich, die Anforderungen der DSGVO einzuhalten. Dadurch und durch zusätzliche rechtliche Vorgaben, wie der Luftverkehrs-Verordnung, wird der zulässige örtliche Einsatzbereich von Kameradrohnen durch nicht-öffentliche Stellen erheblich eingeschränkt; im Haushaltsbereich aber – daran sei nochmals erinnert – greift die DSGVO nicht.

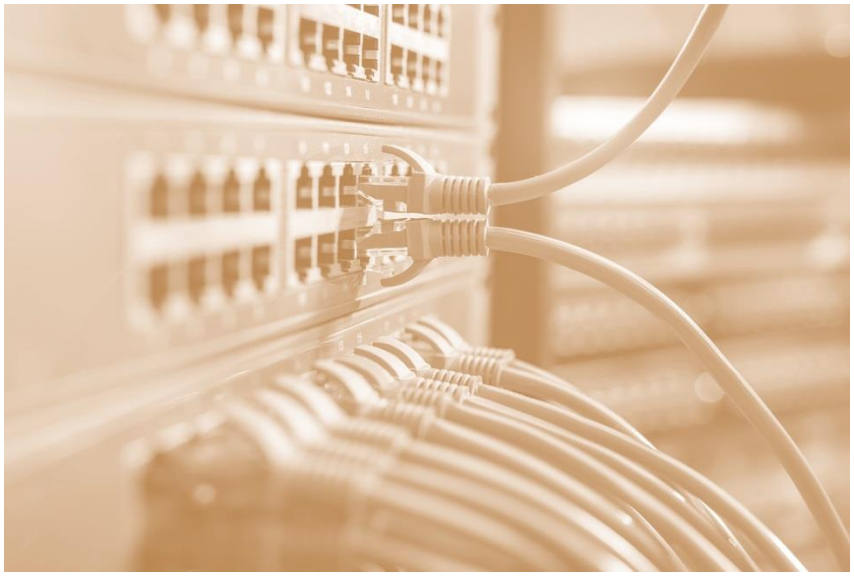
- **Überwachung mithilfe von Wildkameras**

Zulässig ist die Verwendung von Wildkameras nur, wenn die Aufnahme von Menschen äußerst unwahrscheinlich erscheint und vom Verwender mit allen zur Verfügung stehenden Mitteln ausgeschlossen wurde sowie das berechtigte Interesse des Verwenders mindestens gleichgewichtig zu gegenläufigen Betroffeneninteressen ist. Die Kamera ist technisch so einzustellen, dass keine Videosequenzen, sondern Einzelbilder mit einigen Sekunden Abstand aufgenommen werden. Wildkameras, die allein nachts zum Einsatz kommen sollen, sind tagsüber abzuschalten.

All dies gibt jeweils die Ansicht der Datenschutzaufsichtsbehörden wieder. Dies ist eine wertvolle Orientierungshilfe, steht einer abweichenden Bewertung im Einzelfall aber nicht entgegen. Es kann

sich daher lohnen, den konkreten Fall auch bei scheinbarer Unzulässigkeit nochmals genau zu analysieren.

In jedem Fall ist es wesentlich, über die Umstände und Zwecke hinreichend zu informieren: Videoüberwachungen sind großflächig anzukündigen, Muster dafür werden von den Aufsichtsbehörden teils sogar bereitgestellt. Regelmäßig ist eine zweistufige Information sinnvoll: Auf erster Ebene mit großem Piktogramm und ersten Basisinformationen bevor eine betroffene Person den überwachten Bereich betritt, an zentralem Ort dann auf zweiter Stufe sämtliche Detailinformationen. Hieran ändert sich mit der Orientierungshilfe nichts.



Aus zwei mach eins: Der Entwurf des TTDSG

Zu viele Köche verderben den Brei - diese alte Weisheit gilt auch für ein Übermaß an Gesetzen. Das hat nunmehr auch die Bundesregierung für das Zusammenspiel der datenschutzrechtlichen Regelungen des TMG und TKG mit der DSGVO beherzigt. Sie versucht daher aktuell mit einem neuen, konsolidierenden Gesetz Abhilfe zu schaffen: dem „TTDSG". Für dieses TTDSG liegt nun ein erster Referentenentwurf vor – wir stellen Ihnen den wesentlichen Inhalt und die Neuerungen vor.

Verwirrende Ausgangslage

Nach über zwei Jahren Anwendbarkeit der DSGVO müssen deutsche Anbietern von Telemedien und Telekommunikationsdiensten vor allem eines konstatieren: Verwirrung, Rechtsunsicherheit und enttäuschte Erwartungen. Die DSGVO, die den Umgang mit personenbezogenen Daten regelt, verdrängt in vielen, aber eben nicht allen Teilen die bestehenden nationalen Regelungen des TMG und TKG zum Umgang mit Daten in Telemedien und durch Telekommunikationsdienste. Nicht-personenbezogene Daten in diesen Kommunikationsdiensten unterliegen dagegen regelmäßig dem ePrivacy-Recht: Dieses aber ist entgegen der ursprünglichen Planung noch in alten Strukturen mit einer jahrzehnte alten EU-Richtlinie und nationalen Umsetzungsgesetzen gegossen. Der Plan, mit Inkrafttreten der DSGVO auch eine parallele und abgestimmte ePrivacy-Verordnung ins Rennen zu schicken, ist bekanntermaßen nachhaltig gescheitert. Bis heute liegt kein auch nur ansatzweise konsensfähiger Entwurf vor. In Einzelfällen ist oft unklar, welches Recht gilt, das ePrivacy-Recht ist oft alleine technisch überholt und zudem nicht „optimal" ins nationale Recht umgesetzt. Letzteres hat der Rechtsstreit „Planet49", der sein Ende mit der BGH-Entscheidung zum Umgang mit Cookies von Ende Mai diesen Jahres fand, eindrucksvoll gezeigt (wir berichteten ausführlich über die sogenannten Planet49-Urteile von EuGH und BGH in den Newslettern vom Oktober 2019 und Juni 2020).

Die Bundesregierung sieht verständlicherweise Handlungsbedarf, zumal die erhoffte Konsolidierung der ePrivacy-Verordnung aus Brüssel auf sich warten lässt. Ein einheitliches Gesetz soll die weiterhin anwendbaren Datenschutzregelungen des TMG und TKG zusammenfassen und mit den Anforderungen der DSGVO konsolidieren im neu zu schaffenden **TTDSG**. Für dieses Vorhaben liegt nun seit Mitte Juli ein erster Referentenentwurf (TTDSG-Entwurf) vor, der außer der Übernahme der bestehenden Datenschutzregelungen vor allem für den Anwendungsbereich des TMG und die zuständige Aufsicht einige Neuerungen vorsieht.

Aus drei mach eins

Als Kern des Problems sieht die Bundesregierung die Unsicherheiten, die durch die Verteilung der datenschutzrechtlichen Vorgaben über zwei Gesetze und eine EU-Verordnung – TKG, TMG

und DSGVO – entstehen. Durch die Übernahme der einschlägigen Datenschutzbestimmungen des TMG (§§ 11 – 15a TMG) und des TKG (§§ 88 – 107 TKG) soll mehr Klarheit geschaffen werden. Zudem soll für alle Datenschutzfragen nach dem Entwurf der Bundesbeauftragte für Datenschutz und Informationsfreiheit (BfDI) zuständig sein.

Während ein Großteil der Datenschutzbestimmungen des TKG bis auf wenige Umformulierungen im Wesentlichen unverändert übernommen werden, soll das TTDSG auch der Überarbeitung des TMG dienen. Dem Gesetz, das die ePrivacy-Richtlinie i.d.F. der RL 2002/58/EG umsetzen soll, wurde nicht nur durch die Planet49-Urteile erhebliche Mängel in der Umsetzung der europarechtlichen Vorgaben attestiert. Die Abgrenzung zur und Verschränkung mit der DSGVO ist bislang den Gesetzesanwendern überlassen.

Lehren der Planet49-Urteile

Die beachtenswerteste Änderung stellt deshalb die Überarbeitung des bisherigen § 15 Abs. 3 TMG dar. Zur Erinnerung: § 15 Abs. 3 TMG erlaubte den Einsatz von Cookies für Werbe- und Marktforschungszwecke nach herrschender Lesart bis Mai 2020 auch ohne Einwilligung („opt out“). Mit den EU-Vorgaben der ePrivacy-Richtlinie war dies kaum zu vereinbaren. Der BGH legte § 15 Abs. 3 TMG denn auch in seinem Urteil von Ende Mai 2020 innovativ dahingehend aus, dass dieser eine Einwilligung („opt in“) fordere. Offen bleibt danach aber weiterhin, wann genau eine Einwilligung notwendig ist: Dies ist immer dann der Fall, wenn der Endgerätezugriff nicht „unbedingt erforderlich“ ist, um einen Dienst anzubieten. Dies belässt Wertungs- und Diskussionsräume.

Diese Gemengelage bedenkend möchte der Entwurfsverfasser mit dem TTDSG klären, in welchen Fällen der Zugriff auf oder das Speicherung von Informationen auf den Endgeräten der Nutzer durch Cookies oder ähnliches auch ohne Einwilligung möglich ist. Im TTDSG-Entwurf bestimmt der § 9, dass für derartige Zugriffe auf Endgeräte grundsätzlich die Einwilligung der Nutzer erforderlich ist. Ausnahmen sollen gelten, wenn der Zugriff

- technisch erforderlich ist, um eine Kommunikation über ein elektronisches Kommunikationsnetz zu übermitteln, oder um Telemedien bereitzustellen, deren Inanspruchnahme vom Endnutzer gewünscht wird,

- vertraglich ausdrücklich vereinbart wurde, um bestimmte Dienstleistungen zu erbringen, oder
- zur Erfüllung gesetzlicher Verpflichtungen erforderlich ist.

Die materiellen Anforderungen, die an die Einwilligung gestellt werden, entsprechen denen aus der DSGVO.

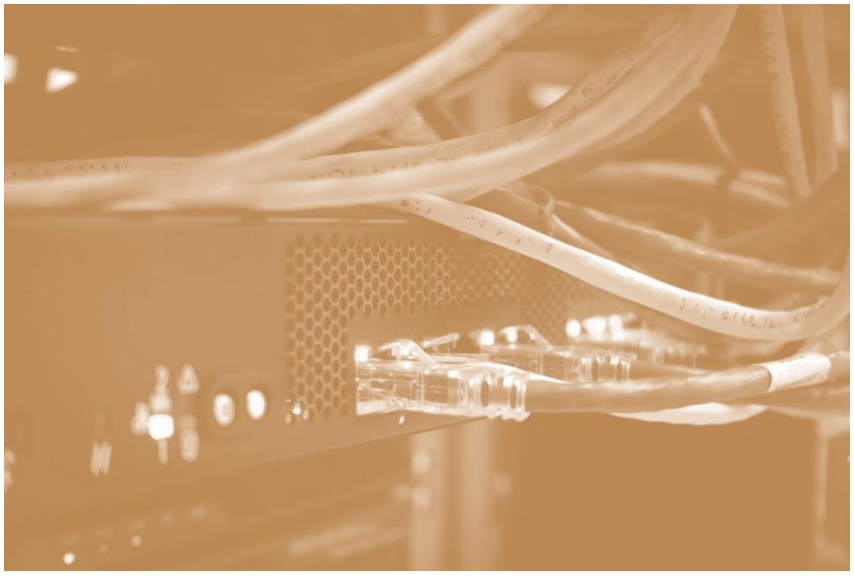
Erweiterung des Anwendungsbereichs und Vorgreifen auf ePrivacy-Verordnung

Darüber hinaus sollen durch das TTDSG zukünftig auch sogenannte Over-the-Top-Telekommunikationsdienste (OTT-Dienste) erfasst sein. Zu diesen gehören etwa Anwendungen für Internet-Telefonie, Sofortnachrichten (Messaging) oder webgestützte Email-Angebote.

Mit Regelungen wie dieser möchte der Entwurfsverfasser auch national Fakten schaffen: Da die dringend notwendige Überarbeitung der e-Privacy-Richtlinie als Verordnung seit Jahren am Brüsseler Gesetzgebungsprozess scheitert – über den letzten Entwurf berichteten wir im Newsletter vom November 2019 – will der nationale Entwurfsverfasser bei der Schaffung des TTDSG die Gelegenheit wahrnehmen und selbst nationale Regelungen treffen, die aus gescheiterten Entwürfen der ePrivacy-Verordnung stammen.

Laufender Gesetzgebungsprozess

Da der vorliegende TTDSG-Entwurf nicht nur erst die Fassung eines „Referententwurfs" hat, sondern zudem aus dem Bundesministerium für Wirtschaft und Energie lediglich inoffiziell durchgestoßen wurde, ist es durchaus möglich, dass er noch einige Änderungen erfährt, bevor er als Gesetzesinitiative in den Bundestag eingebracht wird. Inhaltlich regen sich schon erste Zweifel, ob etwa § 9 TTDSG-Entwurf tatsächlich die Anforderungen der ePrivacy-Richtlinie erfüllt. Sollte dies nicht der Fall sein, droht eine Wiederholung der Planet49-Saga. Aber da der Entwurf aller Wahrscheinlichkeit nach noch einige Überarbeitungsrunden vor sich hat, bleibt die Hoffnung auf eine gute und belastbare Lösung bestehen. Über die weiteren Entwicklungen werden wir berichten.



Kein Datenschutz für Patientendaten?

Das VG Hamburg hatte sich in diesem Monat mit Fragen der datenschutzrechtlichen Verantwortlichkeit zu befassen, wenn das ursprünglich Verantwortliche Unternehmen insolvenzbedingt nicht mehr in Anspruch genommen werden kann. Heraus kam eine ebenso folgenreiche wie hoch diskutierte Entscheidung.

Der Sachverhalt: Im Jahr 2011 meldete die Betreibergesellschaft einer Klinik in der Stadt Büren – eine Tochtergesellschaft der Marseille Klinken – Insolvenz an, in deren Folge das Grundstück an den Eigentümer – eine andere Tochtergesellschaft der Marseille Kliniken – zurückgegeben wurde. Seitdem steht die Klinik leer, in ihr lagern aber ungesichert tausende Gesundheitsdaten ehemaliger Patienten. Nachdem im Mai 2020 medienwirksam über die stillliegende Klinik und den darin gelagerten Akten berichtet wurde, versuchten zahlreiche Unbefugte, sich Zutritt zu der Klinik und den Akten zu verschaffen. Neben zahlreichen angeordneten Sicherheitsmaßnahmen verlangte die Hamburger Datenschutzaufsicht zuletzt von der Schwestergesellschaft, die Patientenakten in datenschutzkonformer Weise zu lagern.

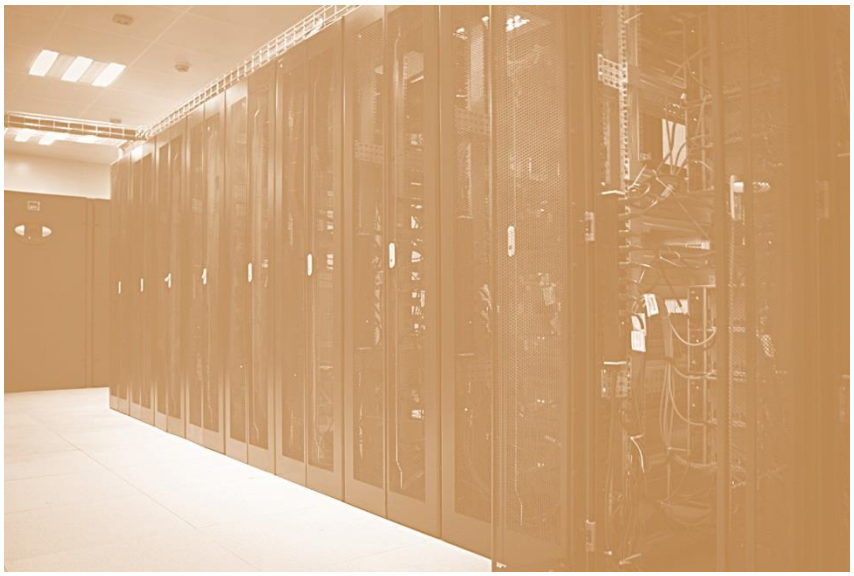
Das VG Hamburg lehnte dies indes im daraufhin eingeleiteten Verfahren ab. Aus seiner Sicht sei die Schwestergesellschaft zu keinem Zeitpunkt datenschutzrechtlich in Erscheinung getreten. Durch das Zurücklassen der Patientenakten sei das

Schwesterunternehmen nicht automatisch verantwortlich für die Daten geworden. Das bloße „Weiterlagern“ ohne Zustandsveränderung durch die Schwestergesellschaft reicht aus Sicht des Gerichts nicht aus, um eine eigene Verarbeitung der Daten darzustellen, die für die Verantwortlichkeit notwendig ist.

Diese Entscheidung des Gerichts hat nicht zuletzt für die betroffenen Patienten erhebliche Folgen: ohne datenschutzrechtlichen Verantwortlichen können diese keine datenschutzrechtlichen Ansprüche geltend machen, ohne datenschutzrechtlich Verantwortlichen obliegt es niemandem, für einen angemessenen Schutz der sensitiven Daten Sorge zu tragen. Konkret bedeutet dies, dass sie von der Schwestergesellschaft weder Einsicht in die Akten noch ihre Löschung verlangen oder die Einhaltung angemessener Maßnahmen zur Datensicherung durchsetzen können.

Es werden denn auch bereits erhebliche Bedenken an der Richtigkeit der Entscheidung geäußert: es wird – berechtigterweise – die Frage gestellt, ob durch gesellschaftsrechtliche Betriebsaufspaltungen die datenschutzrechtliche Verantwortlichkeit vollständig auf nur einen Rechtsträger verlagert werden darf, ohne dass Mutter-, Tochter- oder Schwesterunternehmen im Falle der Insolvenz die datenschutzrechtlichen Pflichten treffen und so sämtliche datenschutzrechtliche Einflussmöglichkeiten der Betroffenen auf ihre Daten verloren gehen, zumal das Eigentum am Grundstück ebenfalls übergegangen ist.

Mit dieser Frage wird sich in der nächsten Zeit das Hamburger OVG befassen müssen. Bis zur Entscheidung des OVG bleibt es spannend.



Datenschutz und Corona: Neues aus Brüssel und Deutschland zu Temperaturkontrollen

Eingangskontrollen mit Temperaturmessungen sind auch in europäischen Behörden Alltag geworden. Wie Fiebermessungen in der Behördenpraxis datenschutzkonform sein können, hat der Europäische Datenschutzbeauftragte (EDPS) in einer Stellungnahme dargelegt. Auch die deutsche Datenschutzkonferenz (DSK) hat sich mit dem Thema jüngst intensiv befasst und am 10.09.2020 ein neues Papier dazu veröffentlicht, konkret (nur) in Bezug auf den Einsatz von Wärmebildkameras. Welche Anforderungen der EDPS und die DSK aufstellen und welche Bedeutung dies für private Betriebe hat, haben wir in diesem Beitrag für Sie zusammengefasst.

Zunehmend wird das Homeoffice wieder gegen die angestammten Büros getauscht. Dies ist zu diesen Zeiten natürlich nicht ohne Einhaltung gewisser Infektionsschutzmaßnahmen möglich, die zugleich dem Arbeitsschutz dienen. Ein besonderer Fokus liegt dabei seit Beginn der Corona-Pandemie auf Eingangskontrollen mit Temperaturmessungen. Da dies auch in europäischen Behörden gängige Praxis geworden ist, hat der Europäische Datenschutzbeauftragte (EDPS – nicht zu verwechseln mit dem Europäischen Datenschutzausschuss „EDSA“, in dem die nationalen Datenschutzaufsichtsbehörden vertreten sind) jüngst in einer Stellungnahme dargelegt, wie solche Temperaturmessungen

datenschutzkonform ausgestaltet werden können. Die DSK und damit die deutschen Datenschutzaufsichtsbehörden sehen dies – so viel sei vorweggenommen – ausweislich ihres neuen Papiers vom 10.09.2020 deutlich strenger (für Wärmebildkameras):

DSGVO überhaupt anwendbar?

Nach überzeugender Ansicht des EDPS stellen Temperaturkontrollen nur dann eine Verarbeitung personenbezogener Daten dar, wenn das Ergebnis in irgendeiner Art und Weise gesammelt, gespeichert oder auf sonstige Weise in einem Ablagesystem verarbeitet wird. Wird nur (manuell) die Temperatur gemessen ohne dass das Ergebnis irgendwo vermerkt wird, liegt keine Datenverarbeitung vor. Dies ist im EU-Umfeld wegen der Bestimmung des sachlichen Anwendungsbereiches in Art. 2 Abs. 1 DSGVO stringent: Die DSGVO gilt danach nur für die automatisierte Datenverarbeitung sowie im nicht-automatisierten Bereich, wenn die Daten in einem Dateisystem gespeichert werden sollen. „Unsystematische" manuelle Momentaufnahmen fallen nicht darunter. **Aber Vorsicht**: § 26 Abs. 7 BDSG erweitert den Anwendungsbereich des Datenschutzrechts im Beschäftigtenverhältnis auf die manuelle, nicht-automatisierte Verarbeitung von Daten, die nicht in Dateisystemen gespeichert werden sollen. Die EDPS-Auffassung ist daher nicht ohne weiteres auf Arbeitsverhältnisse im Anwendungsbereich des BDSG übertragbar.

Erlaubnisgrund und Grenzen

Jedenfalls für die EU-Behörden geht der EDPS weiter davon aus, dass die Datenverarbeitung bei manuellen Messungen zum Schutz der Mitarbeiter vor Infektionen durch eine Personalordnung und andere Personalanordnungen gerechtfertigt sein kann. Rein automatisierte Temperaturchecks sollen hingegen nur auf freiwilliger Basis zulässig sein.

Der EDPS hat denn auch eine Reihe von Maßnahmen vorgestellt, die für datenschutzkonforme Temperaturmessungen zu beachten seien, wenn denn eine Speicherung erfolgen sollte: Dazu gehört, dass die Messergebnisse tatsächlich nur zur Einlasskontrolle genutzt werden dürfen, in einem getrennten IT-System zu speichern sind und nicht mit einer Identitätskontrolle zu verknüpfen sind. Daneben könne u.U. ein sinnvolles System zur Überprüfung der Messergebnisse,

Weiterleitung an Covid-19 Teststellen und Krankschreibungen entwickelt werden.

DSK zu automatischen Temperaturmessungen

Auch die Datenschutzkonferenz (DSK) hat sich mit dem Thema der automatischen Temperaturmessungen durch Wärmebildkameras befasst. In einen Anfang September veröffentlichten Beschluss, legt dieser Zusammenschluss deutscher Datenschutzaufsichtsbehörden dar, dass er **quasi keine datenschutzkonforme Anwendungskonstellation** erkennen kann. Die von dem EDPS für grundsätzlich möglich gehaltene Rechtfertigung über eine Einwilligung lehnt die DSK sowohl im Beschäftigungskontext wie auch für den Besuch von Behörden oder sonstigen öffentlichen Gebäuden ab. Wenn der Zugang zu einem Gebäude von der Zustimmung in automatisiertes Fiebermessen abhängig gemacht wird, sei diese in der Regel nicht freiwillig im Sinne des Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO, so die Position der DSK.

Auch in der übrigen Beurteilung gibt die DSK strenge Maßstäbe vor: Da mit der Temperaturmessung Informationen über mögliche Erkrankungen erhoben werden, handele es sich bei den Ergebnissen um Gesundheitsdaten, die nach Art. 9 Abs. 1 DSGVO besonderen Schutz genießen. Entsprechend finden auch die Erlaubnisgrundlagen des Art. 9 Abs. 2 DSGVO Anwendung – mit der Folge, dass etwa der Arbeitsvertrag keine Grundlage für eine automatisierte Temperaturmessung als Voraussetzung für den Zutritt ins Bürogebäude bieten könne.

Immerhin: In Einzelfällen könnten Zugangskontrollen an Bürogebäuden durch automatisiertes Fiebermessen möglich sein. Dann jedoch nur als Teil einer konkreten anlassbezogenen Arbeitsfähigkeitsprüfung, die wiederum strengen datenschutzrechtlichen Vorgaben unterliegt. Die tägliche Kontrolle aller Mitarbeiter zum generellen Infektionsschutz sei von dieser Ausnahme jedenfalls nicht erfasst. Nach diesen engen Maßstäben dürften automatisierte Temperaturkontrollen in Betrieben in den Augen der DSK nur in wenigen Fällen zulässig sein.

Sowieso hält die DSK automatisierte Temperaturmessungen in der Regel nicht für erforderlich. Erstens sei das Temperaturmessen nur mäßig aussagekräftig, wenn es um die Ermittlung einer tatsächlichen Infektion gehe, und zweitens gebe es mildere Mittel zur Vermeidung

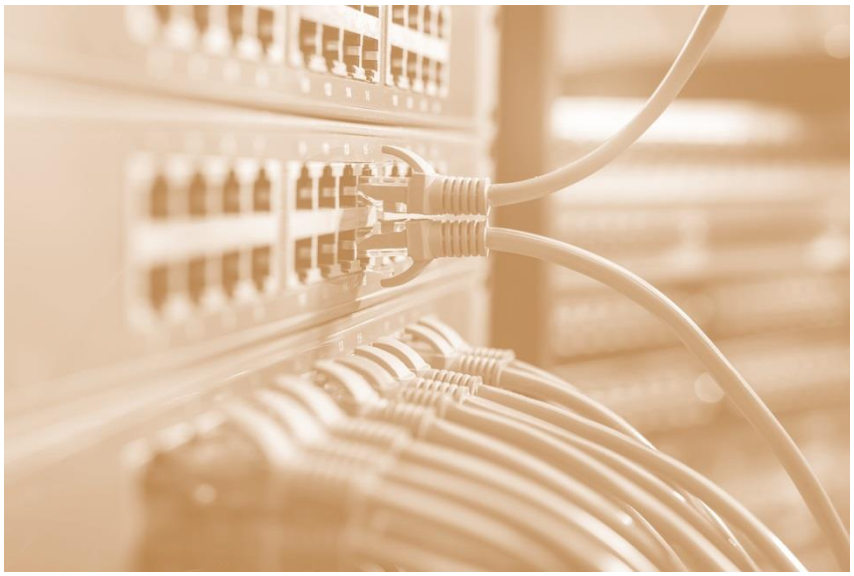
von Infektionen und zum Schutz von Beschäftigten – Abstandsregeln und Alltagsmasken etwa. Bei der Frage des Zugangs zu öffentlichen Gebäuden wie Bahnhöfen oder Verwaltungsgebäude würde der Infektionsschutzes deshalb aller Wahrscheinlichkeit nach nicht die Interessen der Betroffenen überwiegen können. Da auch sonst keine Erlaubnisgrundlage einschlägig sei, können nach Ansicht der DSK automatisierte Temperaturchecks vor öffentlichen Gebäuden nicht datenschutzkonform durchgeführt werden.

Fazit

Auch wenn die Einschätzung des EDPS speziell nur die Temperaturmessung in EU-Behörden betrifft, hat sie dennoch Signalwirkung für die Beurteilung der Praxis in privaten Betriebe (unter Beachtung der Erweiterung des Anwendungsbereiches in § 26 BDSG). Dabei deckt sich die EDPS-Beurteilung zu nichtautomatisierten Temperaturmessungen im Wesentlichen mit denen der deutschen Datenschutzbehörden, die wir im Überblick in unseren Newslettern von April und Mai zusammengefasst haben.

Die DSK beurteilt dies indes ungleich strenger, allerdings konkret nur in Bezug auf Wärmekameras. Ihrer Auffassung nach dürften diese in der überwiegenden Zahl der Fälle weder in privaten Betrieben noch in öffentlichen Gebäuden zulässig sein.

Die unterschiedlichen Auffassungen zeigen, dass das Thema diskussionswürdig ist und die Rechtslage keinesfalls eindeutig. Die spezifischen Aussagen der DSK zu Wärmebildkameras verdeutlichen überdies, dass bei der Zulässigkeitsprüfung die eingesetzte Technik ebenso im Detail zu betrachten ist, wie die geplanten Abläufe.



Zu guter Letzt

Zu guter Letzt gibt es auch in diesem Monat wieder interessante Entscheidungen, zuvörderst ausländischer Datenschutzbehörden, die zu Bußgeldern für die Verantwortlichen führten.

- **Belgien**

In Belgien geriet das Telekommunikationsunternehmen Proximus unter die Lupe der Datenschutzbehörde, nachdem ein Betroffener darauf hinwies, dass das Unternehmen seiner Bitte, seine personenbezogenen Daten nicht mehr in dem – von Proximus herausgegebenen – (Telefon-)Verzeichnis zu veröffentlichen, nicht nachgekommen sei. Das Untätigbleiben des Unternehmens führte nicht nur dazu, dass die personenbezogenen Daten weiterhin in dem Proximus-Verzeichnis und auch in ähnlichen Verzeichnissen anderer Herausgeber veröffentlicht wurden, sondern aus Sicht der Datenschutzbehörde auch zu empfindlichen datenschutzrechtlichen Verstößen. Nach ihrer Auffassung hat das Unternehmen durch das Unterbleiben der Löschung seine datenschutzrechtlichen Verpflichtungen aus Art. 5, 6, 7 und 24 DSGVO nicht angemessen erfüllt. Zudem stellte die Behörde fest, das Proximus die Betroffenen nicht ausreichend transparent über die Verarbeitung ihrer personenbezogenen Daten informiert hatte, sodass zusätzlich ein Verstoß gegen die Informationspflicht aus Art. 12, 13 DSGVO vorgelegen hat. Aus diesem Grund verhängte die Datenschutzbehörde ein Bußgeld in Höhe von 20.000 Euro.

- **Dänemark**

Die dänische Datenschutzbehörde hat gegen eine Hotelgruppe nicht nur ein Bußgeld in Höhe von umgerechnet 148.000 Euro verhängt, sondern diese auch bei der Polizei angezeigt. Grund dafür war, dass die Hotelgruppe noch über 500.000 Kundendaten verfügte, deren Löschfrist bereits mehrere Jahre verstrichen war. Die Datenschutzbehörde sah in der überlangen Aufbewahrung einen Verstoß gegen den Grundsatz der Speicherbegrenzung aus Art. 5 Abs. 1 lit. e DSGVO.

Im Jahr 2018 unterstützte das dänische Unternehmen PrivatBo einen Wohnungsfonds bei einem beabsichtigten Verkauf von drei Immobilien. Bei dieser Gelegenheit stellte PrivatBo Material für die fraglichen Objekte zur Verfügung, das auf insgesamt 424 USB-Sticks an die Bewohner der Objekte verteilt wurde. PrivatBo war sich jedoch nicht bewusst, dass einige der Dokumente persönliche Informationen vertraulicher Art enthielten, die nicht hätten weitergegeben werden dürfen. Aus Sicht der dänischen Datenschutzbehörde hätte PrivatBo die USB-Sticks vor ihrer Weitergabe auf derart vertrauliche Daten kontrollieren müssen. Aus Sicht der Behörde ist die fahrlässige Weitergabe der Daten auf eine mangelhafte Errichtung geeigneter technischer und organisatorischer Sicherheitsmaßnahmen zurückzuführen. Dies stellt einen Verstoß gegen Art. 32 DSGVO dar, der Verantwortliche zur Errichtung solcher Sicherheitsmaßnahmen verpflichtet. Weil die Weitergabe der Daten allerdings unabsichtlich geschah, verhängte die Behörde ein Bußgeld in Höhe von umgerechnet ca. 20.000 Euro und verzichtete auf strafrechtliche Schritte.

- **Italien**

Am fleißigsten waren in diesem Monat die italienischen Datenschutzbehörden, die vor allem mit datenschutzrechtlichen Fragen rund um das Angestelltenverhältnis zu tun hatten:

  - Zunächst ahndete die Behörde den unbefugten Zugriff des Arbeitgebers auf die Browser-Historie des Geschäftscomputers eines Angestellten. Zwar war dem Verantwortlichen der Zugriff durch die Kenntnis von Passwörtern grundsätzlich möglich, allerdings wurde der Betroffene aus Sicht der Datenschutzbehörde im Vorfeld nicht ausreichend über eine entsprechende

Kontrolle informiert. Dieser Verstoß gegen die Informationspflicht, die eine ausführliche Aufklärung über die Verarbeitung personenbezogener Daten (hier Informationen aus der Browser-Historie) führte zu einem Bußgeld in Höhe von 10.000 Euro.

- Zudem ahndete die Behörde in zwei Fällen einen Verstoß gegen die Informationspflicht: Zum einen wurde es einem ehemaligen Mitarbeiter die Bitten nach Einblick in sein E-Mail-Konto und Löschung des Kontos verwehrt. Aus der behördlichen Überprüfung ergab sich zudem, dass E-Mails während des Urlaubs der Angestellten automatisch an das Konto des Managers weitergeleitet wurden. Somit lag nicht nur ein Verstoß gegen die Informationspflicht aus Art. 12 und 15 DSGVO, sondern auch ein Verstoß gegen den Grundsatz der Rechtmäßigkeit. Dieses Verhalten ahndete die Behörde mit einem Bußgeld in Höhe von 15.000 Euro.

In einem weiteren Fall konnte ein Unternehmen dem Wunsch eines ehemaligen Mitarbeiters auf Einsicht in seine personenbezogenen Daten nicht nachkommen, da es weder über die Daten in Papierform noch auf seiner Datenbank verfügte. Die Datenschutzbehörde rügte dieses Verhalten, da ein Verantwortlicher dem Betroffenen jederzeit Einsicht in die von ihm verarbeiteten Daten gewähren können muss. Auch in diesem Fall verstieß das Unternehmen gegen seine Informationspflicht aus Art. 12 und 15 DSGVO, was die Behörde mit einem Bußgeld in Höhe von 3.000 Euro belegte.

- Daneben ahndete die Behörde in zwei Fällen die rechtswidrige Verarbeitung personenbezogener Daten: Zum einen hatte eine italienische Stadtverwaltung im Rahmen einer Pressemitteilung personenbezogene Daten einiger Angestellten ohne deren Wissen an insgesamt vier Zeitungen weitergegeben, die diese veröffentlichten. Die Datenschutzbehörde verneinte die Erforderlichkeit der Veröffentlichung der personenbezogenen Daten im Rahmen der Pressemitteilung, sodass keiner der Rechtfertigungsgründe des Art. 6 DSGVO vorlag. Die Behörde verhängte in diesem Zusammenhang ein Bußgeld in Höhe von 2.000 Euro.

Außerdem wurde einem Stadtrat ein Bußgeld in Höhe von 2.000 Euro auferlegt, weil dieser auf seiner Website personenbezogene Daten veröffentlichte. Die Datenschutzbehörde stellte nicht nur fest, dass die Veröffentlichung ohne rechtlichen Grund nach Art. 6 DSGVO geschah, sondern auch, dass die Veröffentlichung mehrere Jahre andauerte, was die Frist von 15 Tagen, die nach italienischem Recht aus Transparenzzwecken erforderlich ist, ganz erheblich überschritt.

- **Niederlande**

Wegen eines Verstoßes gegen die Informationspflicht hat die niederländische Datenschutzbehörde gegen das Nationale Kreditregister ein beachtliches Bußgeld in Höhe von 830.000 Euro erlassen. Sanktioniert wurde dadurch die Praxis des Kreditregisters, Betroffenen die Kopie ihrer Daten postalisch nur gegen eine Gebühr zukommen zu lassen. Aus Sicht der Behörde muss die Einsicht in die personenbezogenen Daten für jeden Betroffenen einfach, ohne Hindernisse und vor allem nach Ablauf einer angemessenen Frist auch wiederholt möglich sein, da nur so der Betroffene ausreichend über die Verarbeitung seiner Daten aufgeklärt werden kann. Die Höhe des Bußgeldes kann damit begründet werden, dass das Nationale Kreditregister nicht bloß die Information unterließ, sondern der Information zusätzliche Hindernisse in den Weg legte, was den Betroffenen erheblich von der Durchsetzung seiner datenschutzrechtlichen Rechte abschrecken könnte.

- **Norwegen**

In Norwegen wurde gegen die Verwaltung der Kommune Rælingen ein Bußgeld in Höhe von 47.500 Euro auferlegt. Grund dafür war, dass die Kommune die App „Slowbie“ zum Versenden gesundheitsbezogener persönlicher Daten zwischen der Schule und den Heimen der Kinder bereits zu einem Zeitpunkt in Betrieb genommen wurde, zu dem die erforderlichen Risiko- und Datenschutzfolgenabschätzungen und -tests noch nicht abgeschlossen waren. Da es so die Sicherheit der besonders sensiblen Gesundheitsdaten nicht ausreichend genug gewährleistet werden konnte, sah sich die Behörde zur Verhängung eines Bußgeldes gezwungen.

Daneben hat das norwegische Straßenverkehrsamt Videoüberwachungsmaterial zu anderen, als den ursprünglich

vorgesehenen Zwecken verarbeitet und länger als nötig aufbewahrt. Diese Verstöße gegen den Grundsatz der Zweckbindung und der Speicherbegrenzung nach Art. 5 Abs. 1 Buchstabe b und e DSGVO belegte die Datenschutzbehörde mit einem Bußgeld in Höhe von 38.000 Euro.

- **Polen**

In Polen verhängte die Datenschutzbehörde ein Bußgeld in Höhe von umgerechnet 25.000 Euro gegen den staatlichen Generalvermessungsingenieur, der mit Landräten Verträge über die Weitergabe von personenbezogenen Daten aus den Grund- und Eigentumsregistern abschloss. Dabei wusste er, dass es zu einer solchen Weitergabe an der erforderlichen Rechtsgrundlage fehlte. Die Behörde erkannte in diesem vorsätzlich rechtswidrigen Verhalten einen gravierenden Verstoß gegen den Grundsatz der Rechtmäßigkeit und Treu und Glauben nach Art. 5 DSGVO.

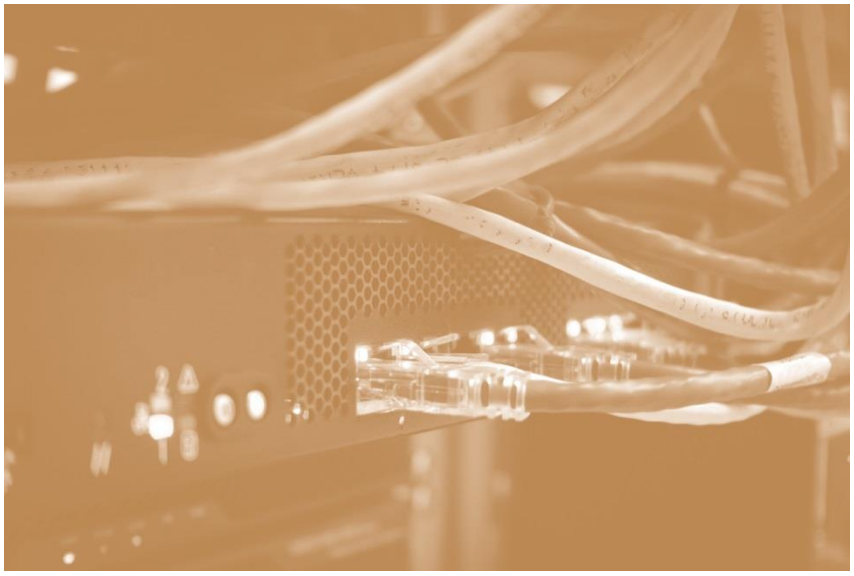
- **Spanien**

Die Datenschutzbehörde verhängte auch in diesem Monat ein Bußgeld gegen ein Telekommunikationsunternehmen: in diesem Fall gegen Vodafone Spanien in Höhe von 75.000 Euro. Vodafone hatte die Handynummer eines ehemaligen Kunden, der seinen Vertrag mit Vodafone bereits im Jahr 2015 kündigte, weiterhin zu Werbezwecken benutzt. Zwar erklärte Vodafone, wegen der einfach zu merkenden Nummer würde diese intern als „Dummy-Nummer“ verwendet. Davon zeigte sich die Datenschutzbehörde allerdings unbeeindruckt und erkannte weiterhin die Rechtswidrigkeit der Datenverarbeitung.

Außerdem untersuchte die Datenschutzbehörde einen in Spanien publik gewordenen Fall, in dem ein Arzt verdächtigt wurde, Patientendaten zum Zwecke der politischen Wahlwerbung zu missbrauchen. Die Behörde stellte fest, dass der Arzt, der einer politischen Partei nahestand, tatsächlich gezielt Wahlwerbung an Patientenadressen sendete. Auch in diesem Fall liegt ein Verstoß gegen den Grundsatz der Zweckbindung aus Art. 5 Abs. 1 Buchstabe b DSGVO vor, den die Behörde ein Bußgeld in Höhe von 5.000 Euro ahndete.

- **Ungarn**

Die Herausgeber des Forbes-Magazin wurde in Ungarn mit zwei Bußgeldern von – umgerechnet – insgesamt 12.500 Euro belegt. Damit ahndete die Behörde den Umstand, dass das Magazin im Januar und September 2019 gleich zweimal die 50 reichsten Ungarn auflistete, ohne diese vorab über die Ergebnisse des Vergleichs und zudem über ihre datenschutzrechtlichen Rechte zu informieren. Die Verarbeitung war bereits deswegen rechtswidrig, weil die Behörde kein überwiegendes Interesse an der Veröffentlichung feststellen konnte. Daneben traten zahlreiche Verstöße gegen die Informationspflichten des Verantwortlichen. Die Behörde ordnete bereits nach dem ersten Verstoß nachdrücklich an, dass Betroffene vor der Verarbeitung über sämtliche Aspekte der Verarbeitung und mögliche Interessen Dritter an der Verarbeitung informiert werden müsse. Dies hielt die Herausgeber jedoch nicht davon ab, im Rahmen der September-Ausgabe erneut in gleicher Weise gegen das Datenschutzrecht zu verstoßen.



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

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

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

Claudia Willmer
+49(0)221 65065-337
claudia.willmer@loschelder.de

Impressum

LOSCHELDER RECHTSANWÄLTE
Partnerschaftsgesellschaft mbB
Konrad-Adenauer-Ufer 11
50668 Köln

Tel. +49 (0)221 65065-0, Fax +49 (0)221 65065-110
info@loschelder.de
www.loschelder.de