Datenschutzrechtliches für die Videoüberwachung

Vorsicht, Kamera!

Datenschutzrechtliche Schranken für die Videoüberwachung

Vor Eingängen oder auf Grundstücken, private Überwachungskameras sind allgegenwärtig. Und allzu oft verstößt deren Einsatz gegen den Datenschutz, wie eine große Zahl von Beschwerden und Bußgeldern belegt. Was gilt es zu beachten?

Von Holger Bleich und Joerg Heidrich

kompakt

- Kameras, die in den öffentlichen Raum gerichtet sind, erfassen personenbezogene Daten im DSGVO-Sinn.
- Betreiber müssen eine ausreichende Rechtsgrundlage vorweisen können und Transparenzpflichten erfüllen.
- Auch für den Betrieb von Türklingeln und Gegensprechanlagen mit Kamera gilt die DSGVO, weshalb sie schwer rechtskonform zu betreiben sind.

Als Dashcam, im Smartphone oder an Hauswänden zur Überwachung: Kameras sind im öffentlichen Raum allgegenwärtig. Sie lösen Bewegtbilder so gut auf, dass man Personen auch noch erkennen kann, wenn sie weit entfernt sind. Dabei sind die Kameras bisweilen so winzig, dass Hersteller sie nahezu unsichtbar in beliebige Geräte verbauen können.

Geraten Unbeteiligte unwissentlich ins Blickfeld einer Kamera, kann dies Rechte verletzen. Zum einen geht es ums Persönlichkeitsrecht, also den Anspruch auf Kontrolle übers eigene Bild. Zum anderen handelt es sich bei jeder Aufnahme von Menschen, die man auf den Bildern anhand beliebiger Merkmale identifizieren kann, um eine Erhebung personenbezogener Daten im datenschutzrechtlichen Sinn.

Die europäischen Datenschutz-Aufsichtsbehörden fassen deshalb den Begriff „Videoüberwachung“ sehr weit. In einer Orientierungshilfe (siehe ct.de/yq1q) definierte es die Datenschutzkonferenz (DSK) als gemeinsames Gremium der deutschen Behörden folgendermaßen: „Eine Videoüberwachung liegt vor, wenn mithilfe optisch-elektronischer Einrichtungen personenbezogene Daten verarbeitet werden. Von diesem Begriff werden nicht nur handelsübliche Überwachungskameras erfasst, sondern jegliche Geräte, die zur längerfristigen Beobachtung und somit für einen Überwachungszweck eingesetzt werden.“

Aus den Tätigkeitsberichten der Aufsichtsbehörden geht hervor, dass es in keinem anderen Bereich so viele Beschwerden von Privatleuten gibt wie dem der Videoüberwachung von öffentlichen Räumen. Und in diesem Bereich wurden europaweit seit Einführung der DSGVO auch mit großem Abstand die meisten Bußgelder verhängt.

Dabei kennt die DSGVO nicht einmal eine explizite Regelung für die Videoüberwachung. In den meisten Fällen greifen die Aufseher daher als potenzielle Rechtsgrundlage auf das sogenannte „berechtigte Interesse“ aus Art. 6 Abs. 1 f DSGVO zurück. Dessen Prüfung ist dreistufig aufgebaut.

Interesse berechtigt?

Zunächst muss eben dieses berechtigte Interesse auf der Seite des Kamerabetreibers vorliegen. Dies kann der Wunsch sein, das eigene Grundstück oder das Auto vor Diebstahl zu sichern, das Aufzeichnen von Straßenszenen bei Unfällen oder der

Sichtkontakt zur klingelnden Person vor der Wohnungstür.

Der geplante Einsatz muss zudem erforderlich sein, um den beabsichtigten Zweck zu erreichen. Insbesondere darf es keine andere, zumutbare Maßnahme geben, die erwartbar weniger stark in die Rechte der betroffenen Personen eingreift. So mag es im Interesse des Betreibers eines Supermarkts liegen, durch Videoüberwachung zu verhindern, dass nachts auf seinem Parkplatz geparkt wird. Erforderlich wäre dies aber nicht, da er auch eine Schranke anbringen könnte und damit weniger in die Rechte von Personen eingreifen würde.

Ein berechtigtes Interesse allein reicht allerdings nicht aus. Vielmehr ist nach DSGVO im dritten Schritt eine Abwägung zwischen dem Interesse des Kamerabetreibers mit den „Interessen oder Grundrechten und Grundfreiheiten der betroffenen Personen“ notwendig. Und deren Interessen überwiegen in vielen Fällen, wenn für die Videoüberwachung nicht sehr gute Gründe vorliegen. Diese können zum Beispiel bei der Überwachung besonders gefährlicher Anlagen oder gefährdeter Bereiche in Bankfilialen angenommen werden.

In den meisten Fällen wird die Abwägung aber nicht so eindeutig ausfallen. So stehen beispielsweise die Interessen eines Unternehmens, jenen Eingangsbereich zu überwachen, in dem es wiederholt zu Diebstählen kam, denen der Mitarbeiter gegenüber, nicht beim Kommen und Gehen überwacht zu werden.

In solchen Fällen kommt es dann auch darauf an, wie die Überwachung konkret gestaltet wird. Hierzu kann der Aufnahmewinkel und -bereich gehören, den die Kamera erfasst. Falls die Kamera nicht nur einen Livefeed liefert, sondern auch aufzeichnet, spielen außerdem Speicherfristen und Zugriffsbeschränkungen aufs Material eine Rolle.

Zudem ist rechtlich relevant, ob die Betroffenen eine Überwachung erwarten. Dies haben Aufsichtsbehörden und Gerichte in der Vergangenheit besonders für Orte wie

Tankstellen, Banken, Kaufhäuser oder den öffentlichen Nahverkehr als gegeben angesehen. Dagegen überwiegen die schutzwürdigen Interessen der Betroffenen meist an Orten wie Schwimmbädern, Innenbereichen von Hotels oder Restaurants, Sitzecken in Bäckereien, Schulen und natürlich Sanitäranlagen.

Wie unangenehm es werden kann, wenn Vorgaben nicht eingehalten werden, musste Anfang 2021 der Computerhändler notebooksbilliger.de erfahren [1]. Das Unternehmen hatte über mindestens zwei Jahre seine Beschäftigten per Video überwacht, ohne dass dafür eine Rechtsgrundlage vorlag. Erfasst hat er unter anderem Arbeitsplätze, Verkaufsräume, Lager und Aufenthaltsbereiche. Auch Kunden von notebooksbilliger.de waren von der unzulässigen Videoüberwachung betroffen, da einige Kameras auf Sitzgelegenheiten im Verkaufsraum gerichtet waren.

Die Argumentation des Händlers, dass es Ziel der installierten Videokameras gewesen sei, Straftaten zu verhindern und aufzuklären sowie den Warenfluss in den Lagern nachzuverfolgen, überzeugte die zuständige Datenschutzbehörde in Niedersachsen nicht. Allerdings ist der Fall noch vor Gericht und es ist offen, ob das hohe Bußgeld von 10,4 Millionen Euro für den Fall tatsächlich angemessen ist.

Transparenzanforderungen

Selbst wenn er eine valide Rechtsgrundlage für eine Videoüberwachung vorhält, kann der Verantwortliche immer noch viel falsch machen. Denn neben der Rechtmäßigkeit fordert die DSGVO auch die Transparenz der Verarbeitung: Aus Art. 12 und den nachfolgenden Vorschriften ergeben sich weitgehende Informationspflichten in Richtung der potenziell Betroffenen.

Der Verantwortliche muss ein Informationsschild anbringen, das bildlich durch ein Kamerasymbol auf die Beobachtung hinweist. Zusätzlich ist viel Text erforderlich: Es muss die Identität des Verantwortlichen angegeben sein, außerdem seine

Kontaktdaten und im Fall eines Unternehmens die des Datenschutzbeauftragten. Betroffene müssen über Zwecke und Rechtsgrundlagen der Videoüberwachung sowie die maximale Speicherdauer der Aufzeichnungen hingewiesen werden. All dies gehört schließlich auf ein möglichst großes Schild gedruckt und gut sichtbar ausgehängt.

Ein editierbares Muster der Datenschutzbehörden zeigt, wie ein rechtskonformer Hinweis auf Videoüberwachung aussehen muss (siehe ct.de/yq1q). *Quelle: LfDI Niedersachsen*

Noch weitergehende Informationspflichten, etwa obligatorische Angaben zu den Rechten auf Auskunft, Widerspruch, Löschung der Aufnahmen sowie auf die Beschwerdemöglichkeit bei der Datenschutzaufsichtsbehörde, dürfen ins Web ausgelagert werden. Es genügt, einen Link oder einen QR-Code anzugeben. Immerhin: Die Datenschutzbehörden bieten hierfür Vorlagen als PDF- oder Word-Dateien, die Sie für den eigenen Gebrauch anpassen können (siehe ct.de/yq1q).

Datenschutzfolgenabschätzung

Besteht durch einen technischen Prozess ein besonders hohes Risiko für die Privatsphäre von potenziell davon Betroffenen,

so hat der Verantwortliche laut DSGVO vorab eine sogenannte Datenschutzfolgenabschätzung durchzuführen. Es geht um eine verschriftlichte Risikoabschätzung unter datenschutzrechtlichen Gesichtspunkten. Eine solche Pflicht besteht nach Ansicht der DSK auch bei der Videoüberwachung, und zwar explizit dann, wenn die Verarbeitung ein „hohes Risiko für die Rechte und Freiheiten natürlicher Personen“ zur Folge hat (Art. 35 Abs. 1 DSGVO).

Das umfasst insbesondere Systeme, die unzählige Personen in einem öffentlichen Bereich erfassen. Hierzu zählen der DSK zufolge etwa Kameras in Sport-, Versammlungs- und Vergnügungsstätten, Bahnhöfen, Einkaufszentren und Parkräumen. Ausgenommen ist die Überwachung von privaten Bereichen, die nicht öffentlich zugänglich sind. Das gilt sowohl für Unternehmen als auch für Privatpersonen, die ihr eigenes Grundstück überwachen wollen.

Sofern letztere es schaffen, nur ihren eigenen privaten Bereich zu erfassen – und nicht den öffentlichen Raum oder den Garten des Nachbarn – findet die DSGVO ohnehin keine Anwendung. Denn das Gesetz gilt grundsätzlich nicht für die „Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten“. Allerdings wird diese Schwelle schnell gedankenlos überschritten, etwa bei der „Überwachung“ des öffentlichen Verkehrsraums mit Auto- oder Fahrrad-Dashcams – hier tangiert man immer die Rechte Dritter.

Videoüberwachung bei Autos

Vor allem Teslas „Wächtermodus“ hat dazu geführt, dass derzeit viel über 360-Grad-Kameraüberwachung moderner Fahrzeuge diskutiert wird. Diese geht weit über die Dashcam-Aufnahmeproblematik hinaus, zu der mittlerweile gefestigte Rechtssprechung existiert [2].

Aufsehen hat zuletzt ein Bußgeld erregt, das die niedersächsische Landesdatenschutzaufsicht Ende Juli dieses

Jahres verhängt hat: 1,1 Millionen Euro muss Volkswagen für Datenschutzverstöße während einiger Forschungsfahrten zahlen, bei denen Techniker die Funktionsfähigkeit eines Fahrassistenzsystems zur Vermeidung von Verkehrsunfällen getestet hatten. Kameras hatten das Verkehrsgeschehen rund um den Wagen zur Analyse von Fehlern aufgezeichnet.

Der Behörde fehlte eine Datenschutzfolgenabschätzung für das Vorhaben. Vor allem aber monierte sie, dass keine Magnetschilder mit einem Kamerasymbol und die weiteren vorgeschriebenen Informationen für alle Verkehrsteilnehmer vorhanden waren. Diese hätten darüber aufgeklärt werden müssen, wer die Verarbeitung zu welchem Zweck durchführt und wie lange die Daten gespeichert werden. Wie Betroffene die Informationen während einer Autobahnfahrt dem Schild am Testfahrzeug hätten entnehmen können, sagte die Behörde nicht. Volkswagen hat das Bußgeld akzeptiert.

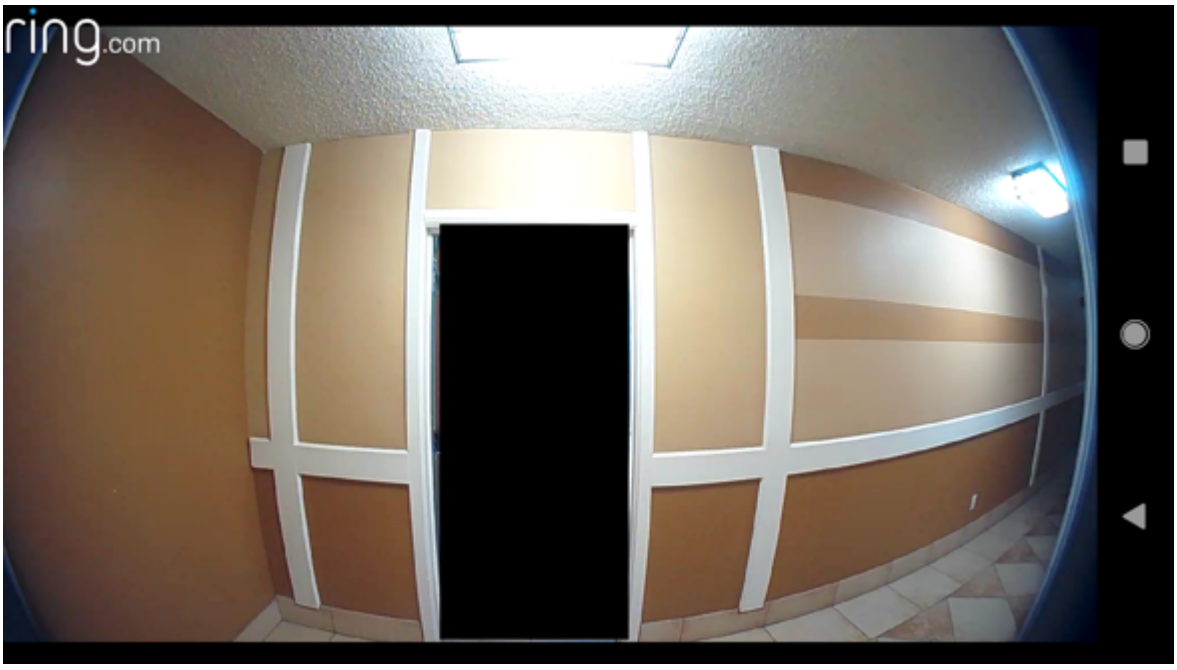
Doorbell-Cams

Ein weiteres datenschutzrechtliches Problem, das vor allem Privatleute betrifft, bilden vernetzte Wohnungs- und Haustürklingeln, die außerdem eine HD-Kamera enthalten. Weil diese Geräte insbesondere von Amazons Tochterfirma Ring bereits für unter 100 Euro zu haben und extrem leicht zu installieren sind, finden sie sich mittlerweile neben vielen Eingangstüren. Das eigentlich obligatorische Hinweisschild mit Kamerasymbol sucht man meist vergebens. Hier besteht akute Bußgeldgefahr, falls sich Nachbarn oder Passanten bei der zuständigen Datenschutzaufsicht beschweren.

Die Vorgaben der DSK sind unmissverständlich: Unbedenklich seien die Systeme nur dann, wenn sie keinen öffentlichen Raum erfassen und „eine Bildübertragung erst nach Betätigung der Klingel ermöglichen, eine dauerhafte Speicherung der Bildaufnahmen ausschließen, räumlich nicht mehr abbilden, als ein Blick durch einen Türspion gewähren würde, und wenn die Übertragung nach einigen Sekunden automatisch unterbricht“.

Fast alle Funktionen, die Ring in seinen Prospekten bewirbt, muss man demnach unbedingt abschalten – etwa die Aktivierung durch Bewegungsmelder oder via App und die dauerhafte Speicherung der Aufnahmen in der Amazon-Cloud. Ring beziehungsweise Amazon machen darauf an keiner Stelle aufmerksam, weshalb dies kaum einem begeisterten Anwender bewusst sein dürfte.

Immerhin findet sich in der Ring-App die Möglichkeit, zwei rechteckige „Privatsphärenbereiche“ im Blickfeld der Kamera definieren zu können. Diese Felder bleiben schwarz, und Ring garantiert, dass darin keine Aufzeichnung stattfindet. So kann man beispielsweise die Wohnungstür des Nachbarn oder den erfassten Teil des Gehwegs vorm Haus maskieren.



In der Ring-App lassen sich rechteckige Bereiche im Blickfeld von der Aufnahme ausschließen, etwa der Wohnungseingang gegenüber. *Bild: ring.com*

Während deutsche Datenschutzbehörden bislang nur vereinzelt Bußgelder wegen Video-Türklingeln an Privatleute aussprechen, sieht das etwa in Spanien ganz anders aus: Agencia Española de Protección de Datos verhängt jeden Monat derlei Bußgelder, meist zwischen 300 und 600 Euro. Es scheint nur eine Frage der Zeit, bis dieser Trend auch andere EU-Behörden erreicht. (*hob@ct.de*)

1. Literatur
2. Holger Bleich, Joerg Heidrich, Teure Überwachung, notebooksbilliger.de soll 10,4 Millionen Euro Bußgeld zahlen, c’t 4/2021, S. 164
3. Dr. Michael Koch, Vorsicht Datenschleudern!, Was beim Datenschutz im Auto zu beachten ist, c’t 1/2022, S. 28

DSK-Infos und editierbare Vorlagen: ct.de/yq1q