BRANDI
RECHTSANWÄLTE

VIDEOÜBERWACHUNG

Informationen zum Datenschutz I November 2023

Einleitung

Mit Hilfe von Videoüberwachungsmaßnahmen lassen sich Straftaten oder andere Rechtsverstöße wie Vandalismus oder Hausfriedensbruch aufklären. Das Hausrecht kann durchgesetzt und das allgemeine Sicherheitsgefühl gesteigert werden. Außerdem kann durch den Einsatz von sichtbaren Videokameras eine Abschreckungswirkung erzielt werden, die mögliche Täter von der Begehung von Straftaten abhalten und Mitarbeiter und Kunden vor Übergriffen schützen soll. Insbesondere aufgrund der zuvor genannten positiven Effekte erfreuen sich Maßnahmen zur Videoüberwachung bei Unternehmen großer Beliebtheit.

Gleichzeitig ist eine Videoüberwachung regelmäßig mit einem erheblichen Eingriff in das Persönlichkeitsrecht der Betroffenen verbunden, da deren Verhalten – jedenfalls bei Speicherung der Aufnahmen – dauerhaft erfasst wird und auch rückwirkend genau analysiert und ausgewertet werden kann. Die Eingriffsintensität ist dabei umso höher, je länger die Daten aufbewahrt werden und je umfangreichere Aufzeichnungen existieren. In diesem Kontext ist auch der von der Überwachung betroffene Personenkreis zu berücksichtigen. Eine Videoüberwachung gegenüber Kunden kann regelmäßig eher umgesetzt werden als gegenüber Mitarbeitern, da die Kunden üblicherweise frei entscheiden können, ob sie die Räumlichkeiten trotz des Umstands der Überwachung betreten möchten, während Mitarbeitern meist keine echte Wahlmöglichkeit zukommt. Videoüberwachungsmaßnahmen sind nach den datenschutzrechtlichen Bestimmungen deshalb nur zulässig, soweit die insoweit vorgesehenen Beschränkungen zum Schutz der Betroffenen eingehalten werden.

Allgemeine rechtliche Anforderungen

Die Datenschutz-Grundverordnung (DSGVO) enthält zwar keine unmittelbaren Regelungen für Maßnahmen zur Videoüberwachung, aber umfassende allgemeine Vorgaben, die bei der Verarbeitung personenbezogener Daten und dementsprechend auch im Rahmen einer Videoüberwachung zu beachten sind. Eine ausdrückliche Regelung für die Videoüberwachung öffentlich zugänglicher Räume findet sich demgegenüber in § 4 Bundesdatenschutzgesetz (BDSG). Unter Berücksichtigung der Wertungen aus Art. 6 Abs. 2 und 3 DSGVO findet die Vorschrift auf private Verantwortliche wie Unternehmen aber keine direkte Anwendung, da es insoweit auf nationaler Ebene an einer Regelungsbefugnis fehlt. Die in § 4 BDSG vorgesehenen Beschränkungen und Wertungen sind allerdings indirekt, etwa im Rahmen der allgemeinen datenschutzrechtlichen Interessenabwägung, zu berücksichtigen.

Eine Videoüberwachung liegt vor, wenn mit Hilfe optisch-elektronischer Einrichtungen personenbezogene Daten verarbeitet werden. Personenbezogene Daten werden mit den Kameras dann verarbeitet, wenn einzelne Personen auf den Bildern eindeutig zu erkennen sind oder die Aufnahmen Rückschlüsse auf die Identität des Gefilmten ermöglichen. Vom Begriff der Videoüberwachung werden dabei grundsätzlich sowohl die Videobeobachtung – die Live-Übertragung der Bilder auf einen Monitor – als auch die Videoaufzeichnung – die Speicherung von Aunahmen, die später ausgewertet werden können – umfasst. In technischer Hinsicht fallen nicht nur klassische Überwachungskameras unter den Begriff, sondern grundsätzlich alle Geräte, die für einen Überwachungszweck eingesetzt werden können. Hierzu gehören auch Webcams, Smartphones, Drohnen und Tür- oder Klingelkameras. Ist der Einsatz der Geräte nicht vorrangig mit einem Überwachungszweck verbunden, sondern zielt etwa darauf ab, die Anzahl von Kunden oder Besuchern, die das Unternehmensgebäude oder eine Filiale des Unternehmens betreten haben, zu ermitteln, werden gleichwohl Videoaufnahmen der Betroffenen angefertigt und die insoweit maßgeblichen datenschutzrechtlichen Bestimmungen müssen seitens des Unternehmens eingehalten werden.

Wie auch jede andere Datenverarbeitung, ist die Durchführung von Videoüberwachungsmaßnahmen nur zulässig, wenn sie auf eine Rechtsgrundlage gestützt werden kann. Regelmäßig wird insoweit das überwiegende berechtigte Interesse des Unternehmens i.S.v. Art. 6 Abs. 1 S. 1 lit. f) DSGVO herangezogen, auch wenn Videoüberwachungsmaßnahmen grundsätzlich auch durch die übrigen Rechtsgrundlagen des Art. 6 Abs. 1 S. 1 DSGVO gerechtfertigt werden können. § 4 Abs. 1 BDSG stellt ebenfalls darauf ab, dass eine Videoüberwachung unter anderem zulässig ist, wenn sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen Betroffener entgegenstehen.

Um zu ermitteln, ob im konkreten Fall ein überwiegendes berechtigtes Interesse des Unternehmens i.S.v. Art. 6 Abs. 1 S. 1 lit. f) DSGVO vorliegt, ist eine Interessenabwägung vorzunehmen. Hierbei sind die Interessen des Unternehmens an der Videoüberwachung gegen die Interessen der Betroffenen am Schutz ihrer Daten abzuwägen. Es muss insoweit ein legitimer Zweck für die Videoüberwachung vorliegen und diese muss geeignet, erforderlich und angemessen sein.

Als legitimer Zweck bzw. berechtigtes Interesse kommen insbesondere die Wahrnehmung und Durchsetzung des Hausrechts, der Eigentums- und Personenschutz sowie die Sicherung von Beweisen in Betracht. Das berechtigte Interesse muss in der Regel auf konkrete Tatsachen, wie etwa vorherige Vorfälle, gestützt werden können. Alleinige Befürchtungen oder eine vermeintlich abschreckende Wirkung reichen demgegenüber für sich genommen in der Regel nicht aus.

Geeignet ist die Videoüberwachung, wenn der seitens des Unternehmens verfolgte Zweck durch die Überwachung erreicht werden kann. Durch die Überwachung der kritischen Bereiche kann zumeist gewährleistet werden, dass relevante Ereignisse aufgenommen werden; außerdem können potentielle Täter abgeschreckt werden. Darüber hinaus ist die Videoüberwachung bei entsprechender Gestaltung in der Regel auch geeignet, um gleichwohl begangene Straftaten und andere Vorfälle aufzudecken.

Das Kriterium der Erforderlichkeit ist erfüllt, wenn es keine gleich geeigneten, milderen Mittel gibt. Eine Videoüberwachung kann etwa deshalb erforderlich sein, weil es allein durch eine bessere Absicherung des Geländes oder einen verstärkten Personaleinsatz nicht möglich ist, alle kritischen Bereiche jederzeit in gleicher Weise abzusichern. Die Speicherung von Aufnahmen kann darüber hinaus etwa notwendig sein, um Vorfälle nach Bekanntwerden aufklären und ahnden zu können. Im Rahmen der Erforderlichkeit ist zudem die konkrete Ausgestaltung der Videoüberwachung zu berücksichtigen. Es sollte insoweit etwa darauf geachtet werden, dass ausschließlich relevante Bereiche, soweit möglich anlassbezogen aufgezeichnet werden, nur wenige, dafür aber gut positionierte Kameras zum Einsatz kommen und bei Bedarf zusätzlich eine manuelle Einschränkung des Aufnahmebereichs, etwa durch Schwärzungen, erfolgt.

Im Rahmen der Angemessenheit ist schließlich zu prüfen, ob die Interessen der Betroffenen in ausreichendem Maße gewahrt werden. Hierbei sind die konkreten Umstände des Einzelfalls in den Blick zu nehmen. Ein wichtiger Baustein ist insoweit die umfassende Information der Betroffenen über die Videoüberwachung vor Betreten des überwachten Bereichs. Die Betroffenen sind außerdem davor zu schützen, dass sie über Gebühr in ihren Persönlichkeitsrechten durch eine konstante Videoüberwachung kontrolliert werden. Dies kann etwa durch eine Beschränkung der Erfassungsbereiche erreicht werden. Sind die Aufnahmen so detailliert, dass einzelne Personen und ihr Verhalten erkennbar sind, ist außerdem sicherzustellen, dass der Zugriff auf die Aufnahmen beschränkt wird, die Erkenntnisse nicht beliebig genutzt werden können und die Aufnahmen zeitnah gelöscht werden, soweit es zu keinem Vorfall gekommen ist. Zur Umsetzung kommen sowohl technische als auch organisatorische Maßnahmen wie Löschroutinen, Zugriffsbeschränkungen und Dokumentationspflichten in Betracht.

Werden besonders sensible Bereiche oder besonders schutzwürdige Personen, wie Beschäftigte oder Kinder, von der Videoüberwachung erfasst, gelten besonders strenge Maßstäbe für Interessenabwägung und Zulässigkeit der Videoüberwachung. In bestimmten Bereichen – Überwachung von Umkleiden, Sanitär- oder Pausenräumen – kann eine Videoüberwachung aufgrund der besonderen Schutzinteressen darüber hinaus auch grundsätzlich unzulässig sein.

Information der Betroffenen

Nach § 4 Abs. 2 BDSG sind der Umstand der Beobachtung und der Name und die Kontaktdaten des Verantwortlichen durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt erkennbar zu machen. Besteht die Möglichkeit, durch die Videoüberwachung erhobene Daten einer bestimmten Person zuzuordnen, besteht darüber hinaus gem. § 4 Abs. 4 BDSG regelmäßig die Pflicht, die betroffenen Personen entsprechend der Art. 13 und 14 DSGVO über die Datenverarbeitung zu informieren. Über den Umstand der Überwachung sowie den Namen und die Kontaktdaten des Verantwortlichen hinaus, sind insoweit zusätzlich insbesondere die Kontaktdaten des Datenschutzbeauftragten, die Zwecke und die Rechtsgrundlage für die Verarbeitung, die berechtigten Interessen des Verantwortlichen, die Empfänger der Daten und die Speicherdauer bereitzustellen. Außerdem müssen die Betroffenen über die ihnen in Bezug auf die Datenverarbeitung zustehenden Rechte informiert werden.

Um die Informationspflichten zu erfüllen, empfiehlt sich der Einsatz von Hinweisschildern, die den Betroffenen über den Umstand der Überwachung sowie die weiteren Pflichtinformationen in Kenntnis setzen. Es besteht insoweit die Möglichkeit, alle erforderlichen Informationen gesammelt über das Hinweisschild zur Verfügung zu stellen. Alternativ ist es auch zulässig, auf vorgelagerten Hinweisschildern zunächst nur die zentralen Informationen in zusammengefasster Form anzugeben und gleichzeitig darauf zu verweisen, dass weitergehende, vollständige Informationen – etwa in Form von Merkblättern – an gut zugänglicher Stelle zur Verfügung gestellt werden. Im letztgenannten Fall muss sodann auch darauf hingewiesen werden, wo diese von dem Betroffenen konkret eingesehen werden können. Sollen die weitergehenden Informationen online zur Verfügung gestellt werden, bietet es sich an, einen QR-Code abzubilden oder alternativ die Online-Adresse, unter der die Informationen abgerufen werden können, auf dem Hinweisschild abzubilden. Die in der Vergangenheit weit verbreitete Praxis, ausschließlich durch aussagekräftige Piktogramme auf die Videoüberwachung hinzuweisen, genügt demgegenüber nicht mehr. Bei der Gestaltung der Hinweisschilder können Unternehmen sich an den Empfehlungen und Mustern der Datenschutz-Aufsichtsbehörden orientieren.

Die Hinweisschilder sollten an allen Eingängen zum überwachten Bereich gut sichtbar angebracht werden. Eine Kenntlichmachung der einzelnen Erfassungsbereiche der jeweiligen Kameras ist hingegen nicht erforderlich, soweit allgemein auf die Videoüberwachung hingewiesen wird. Darf die Videoüberwachung ausnahmsweise verdeckt durchgeführt werden, sind die Informationen dem Betroffenen in der Regel nachträglich zu erteilen.

Sind auch Mitarbeiter des Unternehmens von der Videoüberwachung betroffen, kann es sinnvoll sein, über die allgemeinen Informationsmaterialien hinaus zusätzlich ein Merkblatt für interne Zwecke zu erstellen, mittels dessen die wesentlichen Aspekte, insbesondere die Maßnahmen zur Absicherung der Videoüberwachung, erläutert werden.

Speicherdauer

Nach § 4 Abs. 5 BDSG dürfen Videoaufzeichnungen solange aufbewahrt werden, wie es zur Erreichung des verfolgten Zwecks erforderlich ist und die Interessen der Betroffenen an der Löschung nicht überwiegen. Aus Art. 17 Abs. 1 DSGVO ergibt sich ebenfalls, dass personenbezogene Daten insbesondere dann zu löschen sind, wenn sie für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind. Für Videoaufzeichnungen gelten dementsprechend vom Grundsatz her die allgemeinen Maßstäbe zur Aufbewahrung und Archivierung von personenbezogenen Daten.

Die Landesbeauftragte für den Datenschutz Niedersachsen und der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz vertreten mit Blick auf Videoaufnahmen, die

der Beweissicherung dienen sollen, die sehr restriktive Auffassung, dass regelmäßig innerhalb von ein bis zwei Tagen geklärt werden könne, ob das Bildmaterial benötigt werde oder gelöscht werden könne, und gibt insoweit an, dass entsprechende Daten grundsätzlich nach 48 Stunden gelöscht werden sollten. In begründeten Ausnahmefällen könne aber auch eine längere Speicherdauer zulässig sein.

Das Bayrische Landesamt für Datenschutzaufsicht, die Datenschutzkonferenz und der Europäische Datenschutzausschuss halten demgegenüber eine Speicherdauer von 72 Stunden für grundsätzlich zulässig. Innerhalb von drei Tagen bzw. ein bis zwei Arbeitstagen könne regelmäßig geklärt werden, ob eine Sicherung des Materials erforderlich sei. Eine längere Speicherdauer könne nur mit entsprechender Begründung bei tatsächlichem Vorliegen außergewöhnlicher Umstände (z.B. zugriffsberechtigte Person ist nur alle 4 Tage „im Haus") akzeptiert werden. Eine verlängerte Speicherfrist könne darüber hinaus etwa auch bei mehrtätigen Feiertagen und in Urlaubszeiten, in denen der Geschäftsbetrieb ruht, zulässig sein. Gleiches gelte, wenn die Videoüberwachung nicht nur der Beweissicherung und dem Aufdecken von Straftaten, sondern darüber hinaus auch dazu diene, einen besonderen Sachverhalt, der sich über einen längeren Zeitraum erstreckt, nachzuvollziehen.

Das VG Hannover hat jüngst ebenfalls entschieden, dass der Betreiber einer Selbstbedienungs-Tankstelle Videoaufzeichnungen für maximal 72 Stunden speichern darf und die Aufnahmen anschließend unter Berücksichtigung der DSGVO zu löschen sind (wir berichteten im Juli 2023).

Um zu verhindern, dass Videoaufnahmen entgegen der Vorgaben zu Datenminierung und Speicherbegrenzung für einen zu langen Zeitraum aufbewahrt werden, bietet sich eine automatisierte periodische Löschung des Bildmaterials, etwa durch automatische Löschung oder Überschreibung der Aufnahmen in fest definierten Intervallen, an.

Dokumentation

Wie jeder andere Prozess, bei dem personenbezogene Daten verarbeitet werden, ist auch die Videoüberwachung in das nach Art. 30 DSGVO verpflichtend zu führende Verzeichnis der Verarbeitungstätigkeiten aufzunehmen. Innerhalb der technischen und organisatorischen Maßnahmen ist nach Art. 32 DSGVO außerdem zu dokumentieren, inwieweit ein dem besonderen Risiko der Videoüberwachung entsprechendes Schutzniveau eingehalten und die Rechte der Betroffenen gewahrt werden.

In Abhängigkeit von der Komplexität der Videoüberwachung kann es unter Berücksichtigung der für Unternehmen geltenden Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO sinnvoll sein, zusätzlich eine separate Dokumentation der Videoüberwachung zu erstellen, um die datenschutzkonforme Gestaltung sowie die Auseinandersetzung mit den widerstreitenden Interessen und den Risiken für die Betroffenen nachweisen zu können. In dieser können zum einen die technische Umsetzung sowie die organisatorischen Regelungen an zentraler Stelle dargestellt und festgehalten werden. Zum anderen kann im Rahmen der Dokumentation eine umfassende rechtliche Bewertung der Überwachungssituation erfolgen. Die Dokumentation sollte einer regelmäßigen Kontrolle unterzogen und bei Bedarf angepasst werden.

Hat die Videoüberwachung ein hohes Risiko für die Rechte und Freiheiten der Betroffenen zur Folge, ist zusätzlich eine Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO durchzuführen. Eine solche kann nach Erwägungsgrund 91 DSGVO jedenfalls dann geboten sein, wenn es sich um eine weiträumige Videoüberwachung öffentlich zugänglicher Bereiche handelt. In die Muss-Liste für Datenschutz-Folgenabschätzungen, die von der Datenschutzkonferenz, dem Zusammenschluss der Datenschutz-Aufsichtsbehörden des Bundes und der Länder, veröffentlicht wurde, ist der klassische Fall der Videoüberwachung allerdings zumindest bislang nicht aufgenommen worden, sodass nicht in jedem Fall eine Prüfung und Dokumentation i.S.v. Art. 35 DSGVO erfolgen muss. Die automatisierte Auswertung von Video- oder Audio-Aufnahmen zur Bewertung der Persönlichkeit der Betroffenen ist allerdings erfasst. Gleiches gilt für durch Videoüberwachung gewonnene Aufnahmen, die als biometrische Daten qualifiziert werden können.

Fazit

Aus datenschutzrechtlicher Perspektive bestehen aufgrund der hohen Eingriffsintensität mit Blick auf die Zulässigkeit einer Videoüberwachung hohe Anforderungen. Soweit die Überwachungsmaßnahmen nicht rechtlich zwingend vorgegeben sind, hat grundsätzlich eine umfassende Abwägung der widerstreitenden Interessen des Betreibers der Videoüberwachung und der Betroffenen zu erfolgen. Dies gilt in besonderem Maße, wenn besonders schutzbedürftige Personen wie Arbeitnehmer oder Kinder von der Überwachung betroffen sind. In bestimmten Bereichen kann sich eine Videoüberwachung auch grundsätzlich als unzulässig erweisen. Darüber hinaus sind außerdem die Anforderungen an Transparenz und Datensicherheit zu berücksichtigen. Insoweit sind eine umfassende Information der Betroffenen sowie eine entsprechende technische Gestaltung der Überwachungsmaßnahmen erforderlich.

Unternehmen, die eine Videoüberwachung durchführen wollen, sollten ihren Datenschutzbeauftragten aufgrund der Sensibilität des Themas und der besonderen Erfordernisse bereits in der Planungsphase aktiv einbeziehen. Hierdurch kann die Videoüberwachung von vornherein rechtskonform gestaltet und aufwendige, nachträgliche Anpassungen vermieden werden. Darüber hinaus kann auch das Risiko aufsichtsbehördlicher Maßnahmen verringert werden.

Christina Prowald/ Dr. Sebastian Meyer

Kontakt:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Christina Prowald
Wissenschaftliche Mitarbeiterin

T +49 521 96535 - 980
F +49 521 96535 - 113
M christina.prowald@brandi.net

Kontakt:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Dr. Sebastian Meyer, LL.M.
Rechtsanwalt und Notar mit Amtssitz in Bielefeld
Fachanwalt für Informationstechnologierecht (IT-Recht)
Datenschutzauditor (TÜV)

T +49 521 96535 - 812
F +49 521 96535 - 113
M sebastian.meyer@brandi.net