16. Rechtliche Fragen zur Videosicherheit

16.1 Allgemeines

Die Videosicherheit wird in Deutschland häufig als Reizthema wahrgenommen. Einerseits hat das Sicherheitsbedürfnis bei den Bundesbürgern eine sehr hohe Bedeutung, andererseits sehen insbesondere Datenschützer Risiken bzgl. der bei der Videosicherheit gesammelten Daten.

Nachfolgend wird versucht, den aktuellen Stand der rechtlichen Regelungen bzw. Zulässigkeiten darzustellen. Zu beachten ist hierbei, dass es keine umfassende gesetzliche Regelung zur Videosicherheit gibt, vielmehr sind entsprechende Festlegungen aus verschiedenen Rechtsquellen abzuleiten. Ferner ist zu beachten, dass die juristische Aufarbeitung des Themas erst seit wenigen Jahren erfolgt. Die nachfolgenden Hinweise stellen daher keine Anleitung dar, nach der eine Unbedenklichkeitsbescheinigung ausgestellt werden kann.

16.2 Rechtliche Grundlagen

16.2.1 Datenschutzrecht

Videosicherheitssysteme werden von Unternehmen seit langem zur Wahrnehmung des Hausrechtes und zum Schutz von Rechtsgütern sowie zu Zwecken der Beweissicherung eingesetzt. Beim Betrieb der Anlagen werden personenbezogene, bildhafte Aufenthalts- und Bewegungsdaten erzeugt. Weil die abgebildeten Personen in der Regel bestimmbar sind, wirft dies Fragen des Datenschutzes auf, die von den Betreibern ebenso zu berücksichtigen sind, wie die Rechte von Mitarbeitern, die sich einer Videosicherheit im Unternehmen nicht entziehen können.

Nachfolgend werden die wichtigsten Rechtsgrundlagen dargestellt, die von Unternehmen beim Einsatz von Videosicherheitssystemen zu beachten sind. Dabei stehen die Regelungen der seit dem 25.05.2018 in Deutschland unmittelbar geltenden EU-Datenschutzgrundverordnung (DS-GVO) sowie der ebenfalls seit dem 25.05.2018 geltenden Neufassung des Bundesdatenschutzgesetzes (BDSG) im Mittelpunkt. Die im Folgenden dargestellten Ausführungen sind Ergebnis einer gewissenhaften Auslegung dieser Vorschriften und hierzu erhältlichen Informationsmaterialien. Sie erfolgen jedoch ohne Gewähr und können eine rechtliche Beratung im Einzelfall nicht ersetzen.

16.2.2 Personenbezogene Daten

Beim Einsatz von Videosicherheitssystemen werden personenbezogene Daten in automatisierter Form erhoben, verarbeitet und genutzt. Derartige Daten stehen unter dem Schutz der DS-GVO, die als EU-Verordnung direkt in Deutschland Anwendung findet. Daneben gelten die Vorschriften des neugefassten Bundesdatenschutzgesetzes, mit dem die zahlreichen Öffnungsklauseln der DS-GVO ausgefüllt wurden. Letztlich geht es um den Schutz von verfassungsrechtlich garantierten Persönlichkeitsrechten, aus denen das Bundesverfassungsgericht das Grundrecht auf informationelle Selbstbestimmung abgeleitet hat.

Unter „personenbezogene Daten“ versteht die DS-GVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (vgl. Artikel 4 Nr. 1). Als „Verarbeitung“ definiert die DS-GVO jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang im Zusammenhang mit personenbezogenen Daten, wie z. B. das Erheben, das Erfassen, das Ordnen, die Speicherung, das Auslesen, die Offenlegung durch Übermittlung, das Löschen oder die Vernichtung (vgl.

Artikel 4 Nr. 2). Adressat der Vorschriften über den Datenschutz ist der sogenannte „Verantwortliche“, d. h. die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (vgl. Artikel 4 Nr. 7). Verantwortlich sind damit auch Unternehmen, die Videosicherheitssysteme aus den o. a. Gründen betreiben und dabei personenbezogene Daten von Besuchern, Kunden, Dienstleistern und Arbeitnehmern erheben und verarbeiten.

Jegliche Verarbeitung personenbezogener Daten unterliegt den Grundsätzen des Artikel 5 DS-GVO, wonach Daten nur auf rechtmäßige Weise und für festgelegte, eindeutige und legitime Zwecke erhoben werden dürfen (Grundsätze der Rechtmäßigkeit und Zweckbindung), wobei die Erhebung auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein muss (Grundsatz der Datenminimierung). Vor allen Dingen aber gilt der Grundsatz der Rechtmäßigkeit aus Artikel 6 DS-GVO, wonach eine Verarbeitung nur dann zulässig ist, wenn bestimmte Bedingungen erfüllt sind (Verbot mit Erlaubnisvorbehalt). Diese Bedingungen lassen sich in drei Gruppen zusammenfassen:

Einwilligung:

Die betroffene Person ist mit der Vereinbarung ausdrücklich einverstanden (vgl. Absatz 1 a.)

Erlaubnis:

Die Verarbeitung ist in gesetzlich genannten Fällen (vgl. Absätze 1b bis e) erlaubt, z.B.:

- zur Erfüllung eines Vertrages,
- zur Erfüllung einer rechtlichen Verpflichtung,
- zum Schutz lebenswichtiger Interessen der betroffenen Person,
- zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder
- in Ausübung öffentlicher Gewalt

Interessenabwägung:

Die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen (Absatz 1 f.).

Der verantwortliche Betreiber muss in jedem Einzelfall prüfen, ob er sich auf einen dieser Tatbestände stützen kann. Konkrete Hilfestellungen, wie diese Grundsätze im Falle einer Videosicherheit anzuwenden sind, enthält die DS-GVO nicht. Aus diesem Grund hat der deutsche Gesetzgeber in § 4 des neuen Bundesdatenschutzgesetzes Regeln zum Einsatz von Videosicherheitssystemen aufgestellt, die dem bisherigen § 6 b BDSG weitergehend entsprechen. Mangels einer entsprechenden Öffnungsklausel in der DS-GVO werden diese Regelungen aber von den deutschen Datenschutzbehörden und Gerichten für unbeachtlich gehalten. Man wird jedoch die bisherige Rechtsprechung zu § 6b BDSG als Auslegungshilfe bei der Beurteilung konkreter Fälle heranziehen können, da sich die Tatbestände (insbesondere zur Interessenabwägung) sehr ähneln.

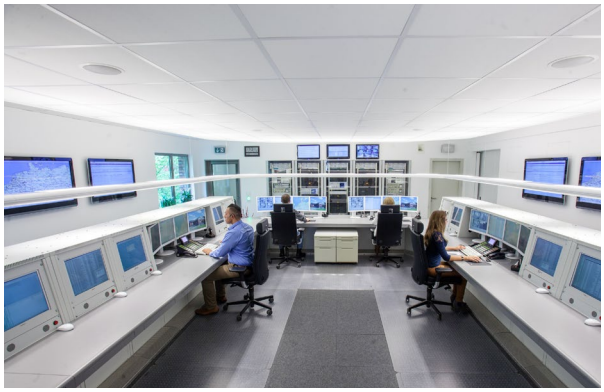
Außerdem haben die Datenschutzbehörden mittlerweile ausführliche Informationsschriften herausgegeben (s.u. 16.2.5.), an denen sich Errichter und Betreiber von Videosicherheitsanlagen orientieren können.

16.2.3 Sanktionen

Die Verletzung der genannten datenschutzrechtlichen Pflichten kann von den zuständigen Aufsichtsbehörden (das sind die Landesdatenschutzbeauftragten) mit hohen Bußgeldern belegt werden. So kann z. B. bei der Nichtdurchführung einer Datenschutz-Folgenabschätzung oder bei einem fehlenden Verfahrensverzeichnis eine Geldbuße von bis zu 10. Mio. Euro oder im Falle eines Unternehmens

von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt werden. Verstöße gegen die Grundsätze der Datenverarbeitung oder die Zulässigkeitsvoraussetzungen aus Artikel 5 und Artikel 6 DS-GVO können sogar Geldbußen von bis zu 20 Mio. Euro und im Falle eines Unternehmens von bis zu 4 % Prozent des gesamten weltweit erzielten Jahresumsatzes auslösen. Darüber hinaus können die Betroffenen Schadensersatzansprüche gegen den Verantwortlichen geltend machen, wenn sie aufgrund eines Verstoßes gegen die DS-GVO einen materiellen oder immateriellen Schaden erlitten haben (vgl. Artikel 32 DS-GVO). Auch Verbandsklagen sind möglich (vgl. Artikel 80 DS-GVO), sodass derartige Ansprüche auch gebündelt durch Interessenverbände geltend gemacht werden können.

16.2.4 Auftragsverarbeitung



Solche Sanktionen und Haftungsgefahren können nicht nur den Betreiber einer Videosicherheitsmaßnahme als originär Verantwortlichen treffen, sondern auch alle Dienstleister, die den Betreiber dabei unterstützen und in diesem Zusammenhang an der Verarbeitung der durch die Überwachung erhobenen Bilddaten mitwirken (sog. Auftragsverarbeiter i.S.v. Art. 28 DS-GVO). Das betrifft in erster Linie Leitstellen, auf die Überwachungsbilder aufgeschaltet werden. Aber auch die regelmäßige Wartung und Parametrierung einer Videoanlage ist nach Auffassung der Datenschutzbehörden Auftragsverarbeitung, wenn der Dienstleister dabei die Notwendigkeit oder die bloße Möglichkeit des Zugriffs auf personenbezogene Bilddaten hat.

In solchen Fällen hat der Verantwortliche den Auftragsverarbeiter vertraglich zu verpflichten, bei der Verarbeitung der personenbezogenen Daten die gleiche datenschutzrechtliche Sorgfalt anzuwenden, die dem Verantwortlichen selbst obliegt. Einzelheiten hierzu sind in Art. 28 DS-GVO geregelt, der den Parteien eines solchen Vertragsverhältnisses umfangreiche Auflagen macht. Bei laufenden Instandhaltungsverträgen werden die Parteien künftig wohl auch einen gesonderten Vertrag über die Auftragsverarbeitung schließen müssen. Ob dies auch für den Fall der einmaligen Planung, Errichtung und Inbetriebnahme einer Überwachungsanlage gilt, die vom Errichter nicht weiter betreut wird, ist im jeweiligen Einzelfall zu prüfen.

16.2.5 Ausblick

Auch wenn mit der DS-GVO viele in Deutschland seit längerem geltende Regeln und Pflichten wiederholt und weiterentwickelt wurden, herrschte nach deren Inkrafttreten im Mai 2018 in Bezug auf deren Auslegung und Anwendung große Unsicherheit. Das galt insbesondere für den Bereich der Bilddatenverarbeitung, die in der DS-GVO keine ausdrückliche Erwähnung findet, sondern unter die allgemein formulierten Grundsätze und Zulässigkeitstatbestände der Artikel 5 und 6 subsummiert werden muss. Zwischenzeitlich hat sich die Aufregung jedoch ein wenig gelegt, zumal sowohl auf europäischer als auch auf nationaler Ebene mittlerweile Informationsschriften und Leitlinien der Datenschutzbehörden vorliegen, in denen die Rechte und Pflichten von Betreibern beim Einsatz von Videosicherheitssystemen näher erläutert werden.

So hat der Europäische Datenschutzausschuss Anfang 2020 das Dokument „Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte“ herausgegeben, in der diese Form der Datenverarbeitung aus europäischer Perspektive besprochen wird. Besonders hervorzuheben ist aber die „Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen“, die im Sommer 2020 von der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (kurz: DSK) herausgegeben wurde.

Auf eine verlässliche höchstrichterliche Rechtsprechung wird man hingegen noch ein wenig warten müssen, weil die Mühlen der Justiz bekanntlich langsam mahlen. Gleichwohl liegen bereits Urteile des Bundesarbeitsgerichtes (BAG) und des Bundesverwaltungsgerichtes (BVerwG) vor, die zwar

noch zur alten Rechtslage ergangen sind, in denen aber bereits auf die neuen Vorschriften Bezug genommen wird. So hat das BVerwG in einem Urteil vom 27.03.2019 darauf hingewiesen, dass der neue § 4 BDSG keine Anwendung finden kann, weil Deutschland zum Erlass einer solchen Regelung wegen des vorrangigen europäischen Rechts nicht ermächtigt war. Das BAG hat in einer Entscheidung vom 23.08.2018 deutlich gemacht, dass die Auswertung von monatelang zurückliegenden Aufzeichnungen eines Arbeitgebers über die Veruntreuung von Geldern durch Mitarbeiter auch nach den Vorschriften der DS-GVO zulässig sein dürfte. Ansonsten wird man auch die Rechtsprechung anderer EU-Mitgliedstaaten sowie des Europäischen Gerichtshofs beobachten müssen, weil es sich bei der DS-GVO um ein europäisches Gesetz handelt, das europaweit einheitlich ausgelegt werden soll.

16.2.6 Persönlichkeitsrechte

Letztlich werden mit dem Datenschutz die Grundrechte und Grundfreiheiten natürlicher Personen geschützt (siehe Art. 1 Abs. 2 DS-GVO). Diese Persönlichkeitsrechte sind in der Grundrechte-Charta der EU (insbesondere Art. 8) sowie in den Artikeln 1 und 2 des Grundgesetzes verfassungsrechtlich garantiert. Das Bundesverfassungsgericht hat daraus in seinem Volkszählungsurteil aus dem Jahr 1983 das „Grundrecht auf informationelle Selbstbestimmung“ abgeleitet. Der Schutz von Persönlichkeitsrechten ist darüber hinaus in zahlreichen Gesetzen geregelt, z.B. im Arbeitsrecht oder im Zivilrecht.

Die dauerhafte Überwachung eines Arbeitsplatzes durch eine Kamera kann als Eingriff in das allgemeine Persönlichkeitsrecht gewertet werden. Gemäß Art. 28 DS-GVO können bereits fahrlässige Verletzungen einen Anspruch auf Ersatz des immateriellen Schadens (Schmerzensgeld) auslösen. Darüber hinaus besteht ein Beseitigungs- bzw. Unterlassungsanspruch nach § 1004 BGB.

Letzteres hat zur Folge, dass die weitere Videosicherheit nicht mehr erfolgen darf (Unterlassung) bzw. gespeicherte Bilder vernichtet werden müssen (Beseitigung). Einen Schadenersatz kann ein Arbeitnehmer jedoch i.d.R. nur geltend machen, wenn er den Arbeitgeber zuvor erfolglos auf Unterlassung in Anspruch genommen hat.

Zu unterscheiden ist, von wem die Videosicherheit initiiert wird:

- die von Behörden veranlasste Videosicherheit öffentlicher Straßen, Plätze u. Ä. – hier spricht man üblicherweise von der Videosicherheit im „öffentlichen Raum“
- die von Gewerbebetrieben bzw. vergleichbaren Stellen veranlasste Überwachung auf eigenem Grund und Boden
- die private Videosicherheit zum Schutz der eigenen Wohnung/des Hauses und/oder des Grundstücks

Nachfolgend wird ausschließlich auf die von Gewerbebetrieben veranlasste Videosicherheit eingegangen. Der Schwerpunkt liegt auf einer datenschutzrechtlichen Betrachtung.

16.3 Datenschutzrechtliche Zulässigkeit von Videosicherheitssystemen

Videosicherheitssysteme und die Voraussetzungen für deren Zulässigkeit werden in der DS-GVO nicht ausdrücklich erwähnt. Erklären sich die Betroffenen mit einer Videoüberwachung nicht ausdrücklich einverstanden (was nur selten umfassend gelingt), oder liegt keine Betriebsvereinbarung vor, welche die Überwachung im Unternehmen erlaubt (s.u. Beschäftigtendatenschutz), dann müssen die Voraussetzungen der Generalklausel in Art. 6 Abs. 1 f DS-GVO gegeben sein. Danach ist eine (Bild)-Datenverarbeitung zulässig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen und wenn im Rahmen der Verarbeitung die Grundvoraussetzungen von Art. 5 DS-GVO (Zweckmäßigkeit, Transparenz, Datensparsamkeit etc.) erfüllt sind.

Auf die Vorgaben deutscher Vorschriften zur Videosicherheit kommt es nach Auffassung der Datenschutzbehörden und Gerichte hingegen nicht an, weil die DS-GVO den Mitgliedstaaten keine Kompetenz zur Regelung derartiger Einzelsachverhalte einräumt. Insofern hat sich auch die Differenzierung