Videosicherheitssysteme

Datenschutzrechtliche Hinweise für Errichter, Planer und Betreiber

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 Videoüberwachung im Unternehmen nicht entziehen können.

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

Allgemeines

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 neuen 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 Ver-

arbeitung 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 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 (vgl. Absatz 1 b. bis e.).

Interessenabwägung:
Die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen 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 Videoüberwachung anzuwenden sind, enthält die DS-GVO nicht. Aus diesem Grunde hat der deutsche Gesetzgeber in § 4 des neuen Bundesdatenschutzgesetzes Regeln zum Einsatz von Videosicherheitssystemen aufgestellt, die dem bisherigen § 6 b BDSG weitergehend entsprechen. Auch wenn die Datenschutzbehörden Zweifel haben, ob der Gesetzgeber hierzu ermächtigt war (es fehlt eine Öffnungsklausel in der DS-GVO), sind diese Regelungen geltendes Recht in Deutschland.

Videosicherheitssysteme in öffentlich zugänglichen Räumen

Gemäß § 4 BDSG n.F. ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) zulässig, soweit sie zur Wahrnehmung des Hausrechtes oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen (vgl. Abs. 1).

Die Vorschrift gilt also für Räume, die dem öffentlichen Verkehr gewidmet sind oder nach dem erkennbaren Willen des Berechtigten von jedermann genutzt oder betreten

werden können. Davon umfasst ist z. B. die Außenüberwachung und Zutrittskontrolle, die Überwachung von Verkaufsräumlichkeiten und Schalterräumen sowie die Überwachung von Parkplätzen, Tiefgaragen, Hotelfoyers und ähnlichen Flächen, die von jedermann betreten werden können. Davon abzugrenzen ist die Videoüberwachung von Büro- und Geschäftsräumen, umfriedeten gewerblichen Anlagen, Lagern und Produktionsstätten etc., deren Zulässigkeit an den allgemeinen Grundsätzen der DS-GVO (insbesondere Art. 6) und gegebenenfalls den Regeln des Beschäftigtendatenschutzes zu messen ist.

Interessenabwägung

Als berechtigte Interessen des Betreibers sind grundsätzlich die Wahrnehmung des Hausrechtes, der Schutz vor Überfällen, Diebstahl oder Vandalismus, der Schutz von Mitarbeitern und Kunden, die Beweissicherung sowie der Perimeterschutz anerkannt. Dabei muss die Maßnahme zur Zweckerfüllung geeignet sein und darf auch nur zur Erfüllung des genannten Zwecks eingesetzt werden. Des Weiteren muss der Betreiber nach dem Grundsatz der Erforderlichkeit stets prüfen, ob es keine milderen Mittel gibt, die den gleichen Zweck erfüllen aber weniger in die Rechte der Betroffenen eingreifen, wie z. B. die Beschränkung der Überwachung auf bestimmte Schwerpunkte bzw. bestimmte Zeiträume oder die Verpixelung von „private zones".
Zur Erforderlichkeit gehört auch, dass eine hinreichend konkrete Gefahr besteht (z. B. belegt durch Vorfälle aus der nahen Vergangenheit). Schließlich muss die Überwachung verhältnismäßig sein, was durch Abwägung zwischen den schutzwürdigen Interessen der Betroffenen (insbesondere Persönlichkeitsrecht) einerseits und den anzuerkennenden Zwecken des Betreibers andererseits zu entscheiden ist. In der Intimsphäre (z. B. Sanitärräume, Umkleidekabinen) und der Privatsphäre (z. B. Gasträume, in denen Kommunikation bzw. soziale Interaktion stattfindet) darf grundsätzlich keine Videoüberwachung stattfinden. In der sogenannten Sozial-/Geschäftssphäre hingegen sind Eingriffe in Persönlichkeitsrechte unvermeidbar; sie sind insbesondere dann zu dulden, wenn Personen eher beiläufig oder nur kurzfristig in überwachte Zonen geraten (z. B. Schalterräume, Parkplätze, Tankstellen, Verkaufsflächen).

Dabei hat der Gesetzgeber in März 2017 durch das „Videoüberwachungsverbesserungsgesetz" neue Abwägungsvorgaben eingebracht, die auch in den neuen § 4 Abs. 1 Satz 2 BDSG n.F. übernommen wurden. Danach gilt bei der Videoüberwachung von öffentlich zugänglichen großflächigen Anlagen (z. B. Sport-, Versammlungs- und Vergnügungsstätten, Einkaufszentren oder Parkplätzen) oder von Fahrzeugen und öffentlich zugänglichen großflächigen Einrichtungen des öffentlichen Schienen-, Schiffs- und Busverkehrs der Schutz von Leben, Gesundheit oder Freiheit von dort aufhältigen Personen als ein besonders wichtiges Interesse. Der Betreiber kann sich also auch auf diese Gründe berufen, wenn die von ihm betriebene Videoüberwachung in den gesetzlich genannten Bereichen stattfindet. Im Übrigen ist auch nach Art. 6 Absatz 1 f der DS-GVO die Berücksichtigung von „Drittinteressen" künftig zulässig.

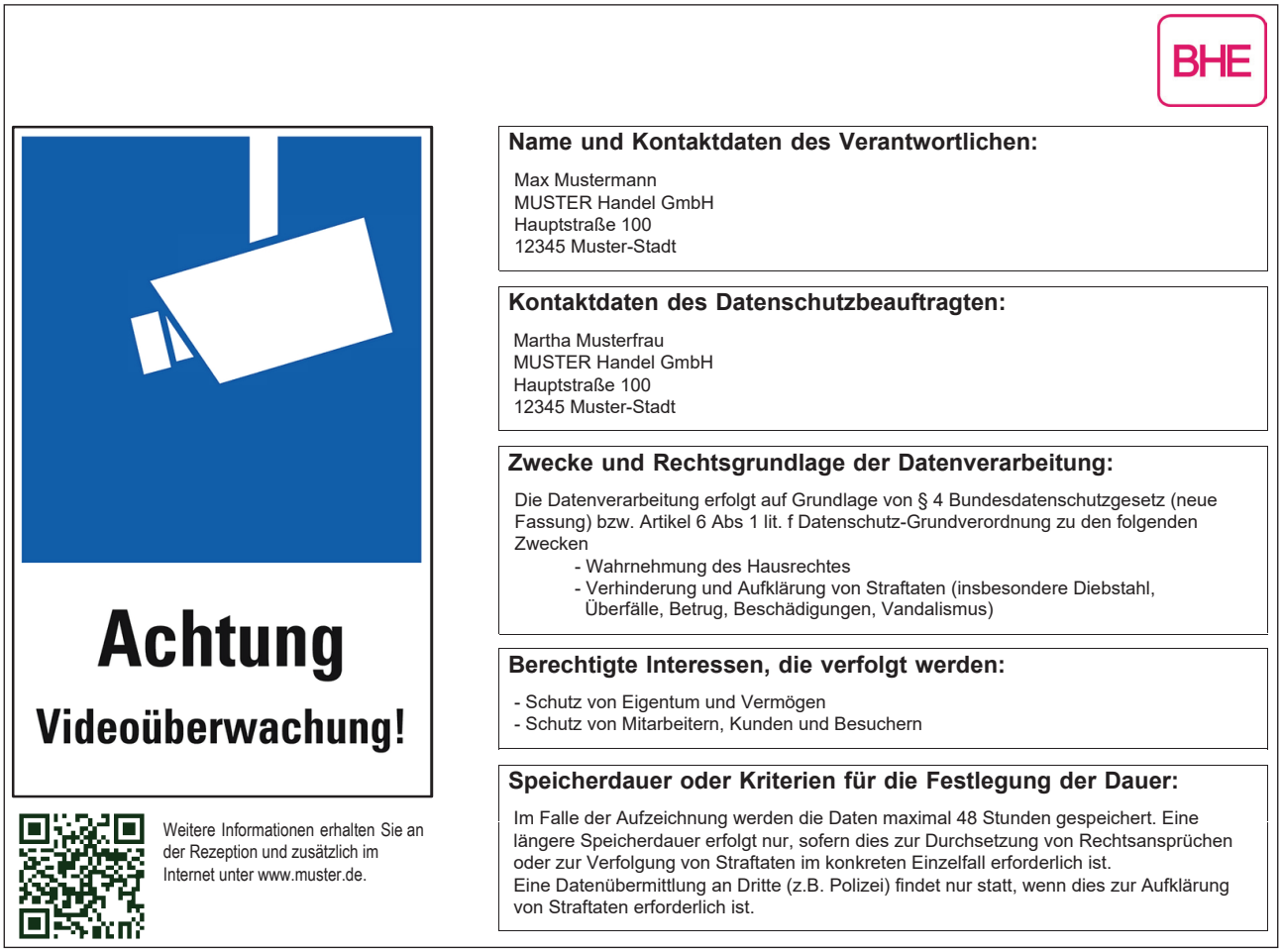
Kennzeichnung

Gemäß § 4 Abs. 2 BDSG n.F. sind der Umstand der Beobachtung und der Name und die Kontaktdaten der Verantwortlichen durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt erkennbar zu machen. Dies hat in der Regel durch Schilder zu erfolgen, deren Botschaft von den Betroffenen wahrgenommen werden kann, bevor sie in den Erfassungsbereich einer Kamera geraten. Das Schild muss nach Auffassung der Daten-

schutzbehörden jedoch noch weitere Informationen enthalten, die den Betroffenen gemäß Artikel 13 DS-GVO „zum Zeitpunkt der Erhebung der Daten“ mitzuteilen sind. Dies umfasst z. B. die Namen und Kontaktdaten des Verantwortlichen, gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten, die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, die berechtigten Interessen die verfolgt werden sowie die Speicherdauer oder Kriterien für die Festlegung der Dauer.

Die Datenschutzbeauftragten der Länder haben sich mittlerweile auf ein bundeseinheitliches Muster geeinigt. Das Muster samt näheren Informationen sowie eine Bestellmöglichkeit DS-GVO-konformer Aufkleber finden Sie unter www.bhe.de/video-hinweisschild.

Muster-Hinweisschild nach DS-GVO



Speicherung, Verwertung und Löschung

Nicht nur das reine Monitoring (geregelt in § 4 Abs. 1 BDSG n.F.), sondern auch die Speicherung oder Verwertung der erhobenen Bilddaten unterliegt den Grundsätzen der Zweckmäßigkeit, Erforderlichkeit und Verhältnismäßigkeit (vgl. § 4 Abs. 3 BDSG n.F.). Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen (vgl. § 4 Abs. 5 BDSG n.F.). Hier hat der Betreiber im Rahmen der von ihm anzustellenden Datenschutz-Folgenabschätzung (s. u.) für jeden Einzelfall zu prüfen, wie lange die Bilddaten unbedingt zur Erreichung der Zwecke (z. B. Beweissicherung) aufbewahrt werden müssen.

Weitere datenschutzrechtliche Pflichten

Bevor ein Videosicherheitssystem installiert und betrieben wird, hat das Unternehmen i.d.R. im Rahmen einer „Datenschutz-Folgenabschätzung“ gemäß Artikel 35 DS-GVO zu prüfen, welche Risiken für die Rechte und Freiheit natürlicher Personen damit verbunden sind und welche technischen organisatorischen Maßnahmen (sog. TOMs) zu ergreifen sind, um den Schutz der erhobenen Bilddaten sicherzustellen. Dies ergibt sich aus Artikel 35 Abs. 3 c DS-GVO, wonach bei einer systematischen umfangreichen Überwachung öffentlich zugänglicher Bereiche grundsätzlich eine Datenschutz-Folgenabschätzung durchzuführen ist, weil durch solche Überwachungsmaßnahmen regelmäßig in besonderer Form in die Rechte und Freiheiten natürlicher Personen eingegriffen wird. Welche Maßnahmen zum Zwecke der Datensicherheit erhoben werden sollten, ergibt sich aus Artikel 32 DS-GVO (Datensicherheit) und Artikel 25 DS-GVO (Datensparsamkeit). Darüber hinaus sind sämtliche Verarbeitungstätigkeiten - insbesondere solche, die einer Datenschutz-Folgenabschätzung unterliegen - sowie die zum Schutz ergriffenen Maßnahmen in einem Verarbeitungsverzeichnis gemäß Artikel 30 DS-GVO aufzuführen, das dem Unternehmen als Beleg dafür dient, dass die datenschutzrechtlichen Pflichten eingehalten werden. Ein solches Verfahrensverzeichnis sollte vom betrieblichen Datenschutzbeauftragten erstellt werden, der gemäß § 38 Abs. 1 BDSG n.F. vom Unternehmen unabhängig von der Zahl seiner Mitarbeiter zu bestellen ist, wenn Verarbeitungen stattfinden, die einer Datenschutz-Folgenabschätzung unterliegen, was bei der systematischen und umfangreichen Durchführung von Videoüberwachungsmaßnahmen im öffentlich-zugänglichen Bereichen (s.o.) grundsätzlich der Fall ist! Das Unternehmen muss darüber hinaus gemäß Artikel 37 Abs. 7 DS-GVO die Kontaktdaten des Datenschutzbeauftragten veröffentlichen und diese Daten auch der Aufsichtsbehörde mitteilen.

Sanktionen

Die Verletzung der genannten datenschutzrechtlichen Pflichten kann von den zuständigen Aufsichtsbehörden (das sind die Landesdatenschutzbeauftragten) künftig 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 künftig 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 künftig möglich (vgl. Artikel 80 DS-GVO), sodass derartige Ansprüche auch gebündelt durch Interessenverbände geltend gemacht werden können.

Auftragsverarbeitung

Solche Sanktionen und Haftungsgefahren können nicht nur den Betreiber einer Videoüberwachungsmaßnahme 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 Parame-

trierung 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 Wartungsverträgen werden die Parteien künftig wohl auch einen gesonderten Vertrag über 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.

Videoüberwachung im Arbeitsumfeld

Da sich die Beschäftigten einer Videoüberwachung im Arbeitsumfeld kaum entziehen können, sind an die Zulässigkeit besonders hohe Anforderungen zu stellen. Soweit sich die Arbeitnehmer mit derartigen Maßnahmen nicht ausdrücklich einverstanden erklärt haben oder eine legitimierende Kollektivvereinbarung vorliegt, muss sich die Zulässigkeit derartiger Maßnahmen an den hierzu in der DS-GVO und dem BDSG n.F. aufgestellten Grundsätzen messen lassen.

Einwilligung

Erfolgt die Videoüberwachung von Beschäftigten auf der Grundlage einer Einwilligung, so sind gemäß § 26 Abs. 2 BDSG n.F. für die Beurteilung der Freiwilligkeit insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Personen sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen.

Freiwilligkeit kann danach vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen (z. B. bei konkreten Bedrohungslagen). Die Einwilligung bedarf in der Regel der Schriftform, wobei der Arbeitgeber die beschäftigte Person zuvor entsprechend den Vorgaben des Artikel 7 Abs. 3 DS-GVO über die Zwecke der Datenverarbeitung und über ihr Widerrufsrecht aufzuklären hat. Denn eine solche Einwilligung kann jederzeit widerrufen werden, allerdings nur mit Wirkung für die Zukunft (vgl. Art. 7 Abs. 3 DS-GVO).

Datenschutzrechtliche Erlaubnistatbestände

Fehlt es an einer Einwilligung, so ist die Datenerhebung im Beschäftigungsverhältnis gemäß § 26 Abs. 1 Satz 1 BDSG n.F. nur dann zulässig, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses, für dessen Durchführung oder für dessen Beendigung erforderlich ist. Diese Regelung entspricht fast wortgleich dem bisherigen § 32 Abs. 1 BDSG, und lässt Raum für die Anwendung im Einzelfall. Nach bisheriger Auslegung dürften Videoüberwachungslösungen zulässig sein, die der Zutrittskontrolle, der Sicherheit der Beschäftigten und den schützenswerten Interessen des Verantwortlichen dienen, wenn den Arbeitnehmern ausreichende Rückzugsmöglichkeiten eingeräumt werden und die Maßnahme auch sonst verhältnismäßig ist. Nach ständiger Rechtsprechung des Bundesarbeits-

gerichtes darf die Überwachung beispielsweise nicht anlasslos und flächendeckend erfolgen, weil damit ein unzumutbarer Anpassungs- und Überwachungsdruck ausgeübt wird. Verstöße hiergegen können Schadensersatz- und Unterlassungsansprüche der Arbeitnehmer auslösen (s. o.).

Nur ausnahmsweise ist auch die verdeckte Überwachung eines Mitarbeiters erlaubt, wenn die strengen Voraussetzungen des § 26 Abs. 1 Satz BDSG n.F. eingehalten werden. Danach müssen zu dokumentierende tatsächliche Anhaltspunkte den konkreten Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat. Des Weiteren dürfen Art und Ausmaß der Überwachungsmaßnahme im Hinblick auf den Anlass nicht unverhältnismäßig sein und es dürfen die schutzwürdigen Interessen der betroffenen Person nicht überwiegen. Diese Regelung entspricht der ständigen Rechtsprechung des Bundesarbeitsgerichtes, das dem Arbeitgeber im Falle einer „Notwehrlage" auch die verdeckte Datenerhebung gestattet. Nach einer jüngsten Entscheidung des BAG soll dabei für die Ergreifung der Maßnahmen ein einfacher Verdacht im Sinne eines Anfangsverdachtes ausreichen, der über vage Anhaltspunkte und bloßen Mutmaßungen hinausgeht. Auch soll die Verwertung eines „Zufallsfundes" aus einer gerechtfertigten verdeckten Videoüberwachung möglich sein, wenn statt der verdächtigten Person ein anderer Mitarbeiter auf frischer Tat ertappt wird.

Kollektivvereinbarungen

Gemäß § 26 Abs. 6 BDSG n.F. bleiben die Beteiligungsrechte der Interessenvertretung der Beschäftigten durch die datenschutzrechtlichen Regelungen unberührt. Damit ist gemeint, dass neben dem Datenschutz auch das kollektive Arbeitsrecht zu beachten ist, wonach die Erfassung personenbezogener Daten von Mitarbeitern der Mitbestimmung unterliegt. Dies erstreckt sich gemäß § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz auf die Einführung und Anwendung technischer Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen.

Diese Mitbestimmungsrechte sollen aber nicht der Verhinderung von Videoüberwachungsmaßnahmen dienen, sondern nur der angemessenen, die Interessen beider Seiten berücksichtigenden Ausgestaltung der Maßnahmen. Dies erfolgt in der Regel im Wege von Betriebsvereinbarungen, die von der Unternehmensleitung mit den Vertretern der Beschäftigten (Betriebsrat) ausgehandelt und sodann schriftlich niedergelegt werden. Dabei sollte mit dem Betriebsrat über folgende Punkte eine Einigung getroffen werden:

- Zweckbestimmung der Kontrollmaßnahme
- Art und Weise des Systems, technische Parameter
- Zugangs- und Zugriffsberechtigungen
- Auswertung der Daten (z. B. Vieraugenprinzip)
- Speicherung, Löschung
- Nutzung und Weitergabe von Daten
- Regelmäßige Überprüfung der Erforderlichkeit der Maßnahmen

Haben die Parteien eine solche Betriebsvereinbarung getroffen, so sind die danach ausgeführten Videoüberwachungsmaßnahmen auch in datenschutzrechtlicher Hinsicht zulässig. Dies ergibt sich aus § 26 Abs.

4 BDSG n.F., wonach die Verarbeitung personenbezogener Daten von Beschäftigten (einschließlich besonderer Kategorien personenbezogener Daten) für Zwecke des Beschäftigungsverhältnisses auf der Grundlage von Kollektivvereinbarungen zulässig sind.

Verfügt das Unternehmen jedoch über keinen Betriebsrat (z.B. weil es nicht die dafür erforderliche Betriebsgröße aufweist), so sollte der Arbeitgeber frühzeitig – d. h. zu Planungsbeginn – die betroffenen Mitarbeiter über die Einführung und Anwendung der Videoüberwachungsanlage aufklären und dabei deutlich machen, dass die Überwachung nicht der Verhaltens- und/oder Leistungskontrolle dient. Einwilligungserklärungen der Mitarbeiter sind nur in Ausnahmefällen einzuholen, weil der Arbeitgeber beim Widerruf einer Einwilligung in Rechtfertigungsnot kommen könnte. Vielmehr sollte der Arbeitgeber den Mitarbeitern die Gründe für die Überwachung, die vorgenommene Interessenabwägung und die Maßnahmen zum Schutze der erhobenen Daten transparent darlegen und all dies unter Berufung auf die einschlägigen Erlaubnistatbestände in seinem Verfahrensverzeichnis (und einer i.d.R. durchzuführenden Datenschutz-Folgenabschätzung) beweiskräftig protokollieren. Auf diese Weise ist der Arbeitgeber gegen arbeitsrechtliche Einsprüche und Schadensersatzforderungen der Mitarbeiter, aber auch gegen aufsichtsbehördlichen Verfahren erst einmal gewappnet.

Bewertung und Ausblick

Auch wenn mit der DS-GVO viele in Deutschland seit langem geltende Regeln und Pflichten wiederholt und weiterentwickelt werden, herrscht in Bezug auf deren künftige Auslegung und Anwendung große Unsicherheit.

Das liegt u.a. daran, dass bei der Bewertung des europäischen Rechts das Verständnis der Behörden und Gerichte aller Mitgliedstaaten zu berücksichtigen ist, das sich noch entwickeln muss. Zwar haben sich die deutschen Aufsichtsbehörden mit der Herausgabe des DSK-Kurzpapiers Nr. 15 „Videoüberwachung nach der Datenschutz-Grundverordnung“ zwischenzeitlich eine einheitliche Meinung gebildet und damit einer gewissen Selbstbindung unterworfen.

Noch gibt es aber keine auf europäischer Ebene entwickelten Leitlinien zur Videoüberwachung, die die Vollzugspraxis der europäischen Aufsichtsbehörden binden würden. Den deutschen Betreibern von Videoüberwachung kann deshalb die jetzige Phase der Unsicherheit nicht erspart werden, zumal die Aufsichtsbehörden die vom Deutschen Bundestag in § 4 BDSG n.F. verabschiedeten Regelungen zur Videoüberwachung beharrlich ignorieren. So lässt sich derzeit nur noch hoffen, dass die Gerichte in zu entscheidenden Streitfällen die „Leitplanken“ definieren, innerhalb derer eine Videoüberwachung künftig in Deutschland zulässig ist.

BHE e.V. **Feldstr. 28** **66904 Brücken** **Telefon: 06386 9214-0** **Telefax: 06386 9214-99** **Internet: www.bhe.de** **E-Mail: info@bhe.de**