Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen[1]

Stand: 17. Juli 2020

Redaktion: Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg

[1] Unter dem Begriff der „nicht-öffentliche Stellen" sind natürliche Personen, juristische Personen des Privatrechts unabhängig von ihrer Rechtsform und der Art ihrer Betätigung, z. B. eingetragene Vereine, Genossenschaften, Kapital- und Personengesellschaften des Privatrechts (z. B. GmbH, AG, OHG, KG, GmbH und Co. KG, GbR), und andere privatrechtlich organisierte Personenvereinigungen (z. B. Genossenschaften, nichteingetragene Vereine, Gewerkschaften, Parteien, Berufsverbände, Gruppierungen ohne Rechtspersönlichkeit) zu verstehen.

Inhalt

1. Videoüberwachung

Jeder Mensch hat das Recht, sich in der Öffentlichkeit frei zu bewegen, ohne dass sein Verhalten permanent mit einer Kamera beobachtet oder aufgezeichnet wird. Im Alltag ist Videoüberwachung dennoch weit verbreitet. Täglich greift diese Form der Datenverarbeitung in das Recht auf informationelle Selbstbestimmung von Personen ein, ohne dass die Mehrzahl dafür einen Anlass gegeben hat. Mit großer Streubreite wird aufgezeichnet, zu welcher Uhrzeit, an welchem Tag, in welchem Zustand, mit welchem Erscheinungsbild, wie lange und an welchem Ort sich ein Betroffener aufhält, wie er diesen Bereich nutzt, wie er sich dort verhält und ob er allein oder in Begleitung ist. Bereits eine einfache Überwachungsanlage verarbeitet in erheblichem Umfang personenbezogene Daten, ohne dass der Großteil der erfassten Informationen für den Überwachenden je eine Rolle spielt.

Videoüberwachungsanlagen werden in großer Zahl eingesetzt. Das Risiko, dass damit die Rechte von Betroffenen verletzt werden, hat sich in den vergangenen Jahren deutlich erhöht. Grund dafür sind die geringen Anschaffungskosten und die verbesserte Qualität der Technik. Moderne Kameras zeigen Bilder in höchster Auflösung. In Echtzeit können diese in der ganzen Welt eingesehen und fast unbegrenzt gespeichert werden. Mehr als ein Smartphone oder Tablet braucht es oft nicht. Dabei werden Kameras nicht nur zur Sicherheit eingesetzt. Kameras erfassen und verarbeiten Daten von Personen, um personalisierte Werbung anzuzeigen oder Produkte zielgruppengenau anzubieten. Softwaregesteuerte Videotechnik vermisst in der Öffentlichkeit Gesichtszüge und Gefühlsregungen von Personen oder verfolgt das Bewegungs- oder Einkaufsverhalten von Kunden. Die erfassten Informationen werden in Sekundenbruchteilen ausgewertet und vervielfältigt. Der Betroffene hat kaum Einfluss auf eine solche Erfassung und erfährt selten, was mit den Aufnahmen geschieht.

Eine dauerhafte und anlasslose Videoüberwachung in der Öffentlichkeit greift erheblich in die Grundrechte von Personen ein. Daraus folgt, dass der Betreiber einer Videoanlage verpflichtet ist, eine Reihe gesetzlicher Voraussetzungen zu beachten. Diese Orientierungshilfe informiert Privatpersonen und Unternehmen, welche Rechtsgrundlagen angewendet werden und welche gesetzlichen Voraussetzungen für Videobeobachtungen oder -überwachungen jeweils gelten. Formvorschriften und Dokumentationspflichten werden erläutert, Beispiele zur Umsetzung der Transparenzpflichten sind beigefügt. Anhand einer Checkliste können Verantwortliche und Datenschutzbeauftragte kontrollieren, ob sie bei der Einrichtung einer Videoüberwachung alle wesentlichen Prüfungsschritte einhalten.

1.1. Begriff der Videoüberwachung

Eine Videoüberwachung liegt vor, wenn mit Hilfe 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. Eine Videoüberwachung kann daher vorliegen, wenn z. B. mit Webcams, Smartphones, Dashcams, Drohnen, Wildkameras sowie Tür- und Klingelkameras gefilmt wird. Auch wenn beim Einsatz dieser Geräte keine „Videoüberwachung“ im oben definierten Sinne stattfindet und zunächst kein Überwachungszweck verfolgt wird, richtet sich die Zulässigkeit der Datenverarbeitung nach den Vorschriften der Datenschutz-Grundverordnung (DS-GVO). Dies gilt nicht, wenn es sich um eine Datenverarbeitung zu ausschließlich persönlichen oder familiären Zwecken handelt oder wenn gar keine personenbezogenen Daten verarbeitet werden. Es kommt hierbei immer auf den Einzelfall an. Unerheblich ist, ob eine Kamera fest montiert oder frei beweglich ist. Der Begriff der Videoüberwachung umfasst sowohl die Video*beobachtung*,[2] bei der eine Live-Übertragung der Bilder auf einen Monitor erfolgt, als auch die Video*aufzeichnung*, bei der Aufnahmen gespeichert und später ausgelesen werden können.

Personenbezogene Daten werden mit Kameras verarbeitet, wenn einzelne Personen auf den Bildern eindeutig zu erkennen sind oder die Aufnahmen Rückschlüsse auf die Identität des Gefilmten ermöglichen. Personen können regelmäßig identifiziert werden, wenn Gesichtszüge erkennbar abgebildet sind. Auch aus den Begleitumständen einer Aufnahme kann sich ein Bezug zu einer bestimmten Person ergeben. Beispielsweise durch ein bestimmtes Körperbild, mitgeführte Gegenstände, besondere oder einzigartige Verhaltensweisen oder durch eine Kombination entsprechender Informationen (Ort, Datum, Zeit, Verhalten, etc.).

Bereits die Aufnahme einer Person greift in deren Recht auf informationelle Selbstbestimmung ein. Ab diesem Zeitpunkt kann der Betroffene nicht mehr kontrollieren, was im weiteren Verlauf mit seinen personenbezogenen Daten geschieht. Entsprechend liegt eine personenbezogene Aufnahme auch dann vor, wenn bereits bei der Aufnahme mit technischen Mitteln einzelne Personen oder Bereiche unkenntlich gemacht werden (Schwärzen, Verpixeln, etc.), dies im Nachhinein aber wieder aufgehoben werden kann. Gleiches gilt, wenn der Betreiber die Videoaufzeichnungen später ungesehen löscht (Speicherung auf Vorrat) oder wenn Videokameras nur im Bedarfs- oder Alarmfall aufzeichnen.

---

[2] Vgl. BVerwG, Urteil vom 27.03.2019 – 6 C 2.18, Rn.15 ff.

1.2. Haushaltsausnahme

Das Datenschutzrecht wird nicht auf Videoaufnahmen angewendet, die von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten und somit ohne Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit vorgenommen werden.[3] Dies ist beispielsweise bei Urlaubs- oder Freizeitaufnahmen zum Zweck der privaten Erinnerung der Fall. Demgegenüber stellt der Betrieb eines Kamerasystems an einem Einfamilienhaus zum Zweck des Schutzes des Eigentums, der Gesundheit und des Lebens der Besitzer des Hauses, das auch den öffentlichen Raum überwacht, keine Datenverarbeitung dar, die zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten vorgenommen wird.[4] Gleiches gilt für eine Veröffentlichung im Internet, bei der die Daten einer unbegrenzten Zahl von Personen zugänglich gemacht werden.[5]

1.3. Attrappen

Kamera-Attrappen verarbeiten keine personenbezogenen Daten. Daher werden die Vorschriften der DS-GVO und des Bundesdatenschutzgesetzes (BDSG) nicht angewendet. Zwar gelten die Hinweispflichten und andere datenschutzrechtliche Vorgaben für Attrappen nicht, allerdings erwecken Kamera-Attrappen den Eindruck, dass tatsächlich Daten von Personen verarbeitet werden und eine Überwachung stattfindet. Zweck einer Kamera-Attrappe ist es, das Verhalten von Menschen in eine gewünschte Richtung zu lenken. Obwohl tatsächlich niemand gefilmt wird, erzeugen täuschend echte Kameragehäuse einen sogenannten Überwachungsdruck. Müssen Dritte eine Überwachung objektiv ernsthaft befürchten, kann der erzeugte Verhaltensdruck für eine Verletzung der Persönlichkeitsrechte ausreichen.[6] Wer eine Attrappe zur Verhaltenssteuerung Dritter einsetzt, muss damit rechnen, dass zivilrechtliche Abwehransprüche (bspw. auf Unterlassen oder Schadensersatz) gegen ihn oder sie geltend gemacht werden.

---

[3] Vgl. Art. 2 Absatz 2 Buchstabe c und Erwägungsgrund 18 Satz 1 DS-GVO.
[4] Vgl. EuGH, Urteil vom 11.12.2014 – in der Rechtssache C-212/13, Rn. 33. Weitere Beispiele finden sich in der Leitlinie 3/2019 „Processing of personal data by means of video surveillance“ vom 29. Januar 2020 (nachfolgend: *Leitlinie*), Ziff. 2.3, Abrufbar unter: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf.
[5] Vgl. EuGH, Urteil vom 06.11.2003 – in der Rechtssache C-101/01, Rn. 47.
[6] Vgl. BGH, Urteil vom 16.03.2010 – VI ZR 176/09, Rn. 13; LG Berlin, Urteil vom 14.08.2018 – 67 S 73/18; LG Hamburg, Urteil vom 18.01.2018 – 304 O 69/17.

2. Rechtmäßigkeit – Art. 6 Absatz 1 DS-GVO

Mit einer Videokamera dürfen personenbezogene Daten nur verarbeitet werden, wenn eine gesetzliche Grundlage dies erlaubt. Die DS-GVO enthält für Videoüberwachungen durch Privatpersonen und Unternehmen keine spezielle Regelung. Rechtsgrundlage für solche Datenverarbeitungen ist daher regelmäßig **Art. 6 Absatz 1 Satz 1 Buchstabe f DS-GVO**. Grundsätzlich kann sich die Rechtmäßigkeit einer Videoüberwachung aber aus allen Rechtmäßigkeitstatbeständen des Art. 6 Absatz 1 Satz 1 DS-GVO ergeben.[7] [8]

2.1. Zweck

Bevor eine Videokamera aktiviert wird, ist für jede Verarbeitung eindeutig zu bestimmen und festzulegen, welcher Zweck mit der Videoüberwachung erreicht werden soll.[9] Eine Videoüberwachung kann beispielsweise eingesetzt werden, um vor Einbrüchen, Diebstählen, Vandalismus (Eigentumsschutz) oder Übergriffen (Personenschutz) zu schützen. Die jeweiligen Zwecke sind für jede einzelne Kamera schriftlich zu dokumentieren und ins Verzeichnis der Verarbeitungstätigkeiten aufzunehmen.[10] Der Zweck der Videobeobachtung oder -überwachung muss spätestens zum Zeitpunkt des Beginns der Verarbeitung der personenbezogenen Daten festgelegt sein. Personenbezogene Daten dürfen nicht „ins Blaue“ oder unter Berufung auf nicht näher genannte „Sicherheitsgründe“ verarbeitet werden. Bei derart unbestimmten Angaben werden die Daten der Betroffenen nicht nachvollziehbar und damit nicht datenschutzgerecht verarbeitet.

---

[7] Nur in Einzelfällen können Private eine Videoüberwachung auf die Buchstaben b bis e des Art. 6 Absatz 1 Satz 1 der DS-GVO stützen. Solche Fälle werden in dieser Orientierungshilfe nicht behandelt.

[8] Die Zulässigkeit von Videoüberwachungen privater Verantwortlicher richtet sich nicht nach § 4 BDSG (BVerwG, Urteil vom 27. März 2019 - 6C 2.18, Rn. 47). Beruht eine Datenverarbeitung auf Art. 6 Absatz 1 Satz 1 Buchstabe f DS-GVO, dürfen nationale Gesetzgeber hierzu keine ergänzenden Regelungen treffen. Gem. Art. 6 Absatz 2 und 3 DS-GVO dürfen nationale Regelungen nur bei solchen Datenverarbeitungen eingeführt werden, die auf der Grundlage des Art. 6 Absatz 1 Buchstaben c oder e der DS-GVO beruhen. In Deutschland sollte dies aber mit der Einführung des § 4 BDSG geschehen. Laut BT-Drucksache 18/11325 (S. 81) soll § 4 BDSG die Vorschrift des § 6b BDSG a.F. weitgehend ersetzen. Die Vorschrift des § 6b BDSG a.F. erfasste auch Videobeobachtungen durch Privatpersonen und Unternehmen. Unter Berücksichtigung des Anwendungsvorrangs der Datenschutz-Grundverordnung und um bei privaten Datenverarbeitungen eine europaweit einheitliche Anwendung der Datenschutz-Grundverordnung sicherzustellen, wenden die Aufsichtsbehörden § 4 BDSG nicht als Rechtsgrundlage für Videoüberwachungen durch Privatpersonen oder Unternehmen an.

[9] Vgl. Art. 5 Absatz 1 Buchstabe b DS-GVO.

[10] Vgl. Art. 5 Absatz 2 DS-GVO. Näheres zum Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DS-GVO unter Punkt 3.2. Auf die Ausnahmen nach Art. 30 Abs. 5 wird bereits hier hingewiesen.

2.2. Interessenabwägung – Buchstabe f

Eine Videoüberwachung ist rechtmäßig, wenn die Voraussetzungen des Art. 6 Absatz 1 Satz 1 Buchstabe f DS-GVO eingehalten werden.

Demnach ist eine Videoüberwachung zulässig, soweit die Verarbeitung zur *Wahrung der berechtigten Interessen (2.2.1)* des Verantwortlichen *erforderlich* ist *(2.2.2)*, sofern nicht die Interessen oder Grundreche und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, *überwiegen (2.2.3)*, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

2.2.1. Berechtigte Interessen

Die Videoüberwachung kann zur *Wahrung berechtigter Interessen* des Verantwortlichen oder eines Dritten erfolgen. Ein berechtigtes Interesse für den Betrieb einer Videoüberwachungsanlage kann ideeller, wirtschaftlicher oder rechtlicher Natur sein. Berechtigt ist ein Interesse, wenn es rechtmäßig, hinreichend klar formuliert und nicht rein spekulativ ist.[11]

Beispielsweise ist der Inhaber des Hausrechts grundsätzlich befugt, präventive und repressive Maßnahmen zu treffen, die zum Schutz des Objekts bzw. zur Abwehr unbefugten Betretens erforderlich sind. Das Hausrecht steht in unmittelbarer Verbindung zum überwachten Objekt und erfordert einen klar abgegrenzten Raum. Im öffentlichen Raum können Private kein Hausrecht ausüben. Soll daher die Videoüberwachung vor Einbrüchen,

Diebstählen oder Vandalismus schützen, ist darin grundsätzlich ein berechtigtes Interesse zu sehen. Gleiches gilt für Interessen wie Beweissicherung zur Durchsetzung von Rechtsansprüchen, Verhütung von Betrug, Leistungsmissbrauch oder Geldwäsche.[12]

(a) Konkreter Nachweis
Ein berechtigtes Interesse muss ein tatsächliches und gegenwärtig vorliegendes Interesse darstellen (d.h. nicht spekulativ sein).[13] Zu fordern sind *konkrete Tatsachen*, aus denen sich beispielsweise eine Gefahrenlage ergibt, die über das allgemeine Lebensrisiko hin-

---

[11] Vgl. Stellungnahme 06/2014 der Artikel-29-Datenschutzgruppe zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG (nachfolgend: *WP 217*), S. 32, S. 70. Abrufbar unter: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_de.pdf.
[12] Vgl. WP 217, S. 32.
[13] WP 217, S. 31ff.

ausgeht.[14] Eine Gefährdung kann sich nur aus tatsächlichen Erkenntnissen ergeben, subjektive Befürchtungen oder ein Gefühl der Unsicherheit reichen nicht aus. Daraus folgt, dass Beschädigungen, Vorfälle in der Vergangenheit oder andere Ereignisse, die eine Gefahrenlage objektiv begründen können, gegenüber der Aufsichtsbehörde nachgewiesen werden müssen.[15] Solche Vorfälle sollten daher entsprechend dokumentiert sein (Datum, Art und Ort des Vorfalls, Schadenshöhe, etc.) und etwaige Strafanzeigen aufbewahrt werden.[16] Konkrete Vorfälle müssen nicht in jedem Fall beim Überwachenden selbst stattgefunden haben.[17] In bestimmten Fällen kann sich eine Gefahrenlage auch daraus ergeben, dass - mit zeitlichem Zusammenhang - vergleichbare Vorfälle oder Übergriffe in der unmittelbaren Nachbarschaft stattgefunden haben. In diesen Fällen muss ein zeitlicher, sachlicher und örtlicher Bezug von Vorfällen nachweisbar vorliegen. Allgemeine Statistiken, z. B. zu Wohnungseinbrüchen im Bundesgebiet, reichen nicht als konkreter Nachweis aus, der eine Gefahrenlage begründen würde.

Nur im Ausnahmefall ist der Nachweis einer *abstrakten Gefahrenlage* ausreichend, beispielsweise, wenn eine Situation vorliegt, die nach allgemeiner Lebenserfahrung typischerweise gefährlich ist. Dies ist beispielsweise in Geschäften, die wertvolle Ware verkaufen (z.B. Juweliere) oder die im Hinblick auf Vermögens- und Eigentumsdelikte besonders gefährdet sind (z.B. Tankstellen) der Fall.

Eine vermeintlich abschreckende Wirkung von Videoüberwachung rechtfertigt *für sich genommen* keinen dauerhaften und anlasslosen Eingriff in das Grundrecht auf informationelle Selbstbestimmung. Anderenfalls könnte eine Überwachung uferlos zu Lasten von Betroffenen ausgedehnt werden.

(b) Drittinteresse
Eine Videoüberwachung kann auch zur Wahrung berechtigter Interessen eines *Dritten, in dessen Interesse die Daten verarbeitet oder an den die Daten übermittelt werden sollen,*

zulässig sein. „Dritter“ ist gem. Art. 4 Nr. 10 DS-GVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personen-

[14] Vgl. BVerwG, Urteil vom 27. März 2019 – 6C 2.18, Rn. 28.
[15] Der Verantwortliche ist für Einhaltung der Rechtmäßigkeitsvoraussetzungen seiner Datenverarbeitung verantwortlich. Nach Art. 5 Absatz 2 DS-GVO ist er damit auch zur „Rechenschaft“ verpflichtet, d.h. er muss die Einhaltung der Rechtmäßigkeitsvoraussetzungen nachweisen können.
[16] Zur Dokumentationspflicht siehe Punkt 3.1.1.
[17] EuGH, Urteil vom 11. Dezember 2019 – C-708/18 –, Rn. 44; Leitlinie Ziff. *3.1.1, Example.*

bezogenen Daten zu verarbeiten. „Dritter“ in diesem Sinn kann beispielsweise eine Versicherungsgesellschaft sein. Wenn ein Versicherer im Rahmen des Abschlusses eines Versicherungsvertrags eine Videoüberwachung fordert, kommt es auf ein „Drittinteresse“ jedoch in der Regel nicht an.[18] Ein Drittinteresse kann auch bei einer Videoüberwachung in einem Einkaufszentrum vorliegen, beispielsweise wenn der Vermieter der Ladenflächen eine Überwachung im Interesse und zum Eigentumsschutz seiner (Laden-) Mieter betreibt.

2.2.2. Erforderlichkeit

Auch für Videoüberwachungen gilt der Grundsatz der Datenminimierung nach Art. 5 Absatz 1 Buchstabe c DS-GVO. Vor dem Einsatz einer Videoüberwachung ist daher zu prüfen, ob die Maßnahme *geeignet* und *erforderlich* ist, um den festgelegten Zweck zu erreichen. Eine Videoüberwachung ist nur dann erforderlich, wenn der beabsichtigte Zweck nicht genauso gut mit einem anderen Mittel erreicht werden kann, das in die Rechte des Betroffenen weniger eingreift und dabei wirtschaftlich und organisatorisch zumutbar ist.

Nicht geeignet ist eine Videoüberwachung, wenn allein zum Zweck der Verhinderung von Unfällen oder Straftaten eine reine Aufzeichnung der Bilder stattfindet. Im Gegensatz zu einer Beobachtung in Echtzeit, besteht in diesem Fall für das Sicherheitspersonal keine Möglichkeit unmittelbar einzugreifen.

(a) Alternative Maßnahmen
Vor der Installation einer Videoüberwachungsanlage muss sich der Verantwortliche mit alternativen (Sicherheits-) Maßnahmen auseinandersetzen. Greifen diese weniger in die Rechte der betroffenen Personen ein und sind sie gleich geeignet, die Zwecke der Überwachung zu erreichen, müssen sie vorrangig gewählt werden. Eine Umzäunung, regelmäßige Kontrollgänge von Bewachungspersonal, Zugangs- und Zutrittssicherungen, Wertschließfächer, helle und durchgehende Beleuchtung, der Einbau von Sicherheitsschlössern oder einbruchsicheren Fenstern und Türen können einen wirksamen Schutz vor Einbruch, Diebstahl und unberechtigten Zugang bieten. Das Auftragen von spezieller Oberflächenbeschichtung oder Folien kann vor Beschädigungen durch Graffiti schützen. Die Ausschöpfung bzw. Prüfung alternativer Maßnahmen muss dokumentiert werden.

[18] Der Verantwortliche hat regelmäßig ein eigenes Interesse an dem Abschluss eines Versicherungsvertrags. Eine Risikobewertung durch den Versicherer kann sich z. B. auf die Prämienhöhe auswirken. Dieses Interesse ist hinsichtlich der *Erforderlichkeit der Maßnahme* kritisch zu prüfen, da für das Versicherungsverhältnis andere Sicherungsmaßnahmen als eine Videoüberwachung ausreichend sein können.

(b) Einschränkungen
Sind alternative Maßnahmen wirkungslos oder kommen sie nicht in Betracht, ist die Videoanlage weitestgehend am Zweck der Überwachung auszurichten. Bei jeder Kamera ist *einzeln* zu prüfen, auf welche *Betriebszeiten* und *Erfassungsbereiche* eine Überwachung eingeschränkt werden kann, ohne dass der Überwachungszweck gefährdet ist. Eine anlassbezogene Überwachung ist einer dauerhaften vorzuziehen. Zum Schutz vor Einbrüchen ist eine Überwachung in den Nachtstunden oder außerhalb von Öffnungs- oder Geschäftszeiten ausreichend. Sind bestimmte Bereiche oder Personen für den Zweck der Überwachung nicht von Interesse und kann die Kamera nicht anders ausgerichtet werden, sind diese Bereiche oder Personen irreversibel auszublenden, zu schwärzen oder zu verpixeln. Reicht eine Beobachtung in Echtzeit zur Erreichung des Zweckes aus, dürfen die Aufnahmen in aller Regel nicht zusätzlich gespeichert werden.

Werden Kameras zur Täteridentifikation und zur Beweissicherung bei Übergriffen eingesetzt, kann dieser Zweck damit erreicht werden, dass eine Überwachung mit einem Notfall- bzw. Alarmknopf verbunden wird. Im Ereignisfall aktiviert, kann dieser einen Alarm und gleichzeitig eine Videoaufzeichnung auslösen.

2.2.3. Interessenabwägung

Auch wenn eine Videoüberwachung zur Wahrung eines berechtigten Interesses des Verantwortlichen oder eines Dritten erforderlich ist, darf sie nur in Betrieb genommen werden, wenn schutzwürdige Interessen der Betroffenen nicht *überwiegen*. Maßstab der Abwägung sind die Grundrechte und Grundfreiheiten der betroffenen Personen auf der einen und das berechtigte Interesse des Verantwortlichen oder eines Dritten auf der anderen Seite.

An dieser Stelle sind die Interessen zwingend anhand des *konkreten Einzelfalles* abzuwägen. Es reicht nicht aus, auf eine abstrakte oder im Allgemeinen vergleichbare Interessenlage abzustellen. Dabei sind die Gesamtumstände jedes Einzelfalls maßgeblich. Anhand des konkreten Lebenssachverhalts ist zu beurteilen, wie bedeutend die Interessen des Verantwortlichen bzw. des Dritten sind, die mit der Videoüberwachung verfolgt werden und inwieweit die Videoüberwachung auch tatsächlich zur Wahrung dieser Interessen beiträgt. Auf der anderen Seite ist zu prüfen, inwiefern die Überwachung schutzwürdige Interessen, Grundrechte und Grundfreiheiten beeinträchtigt und welche Folgen dies für die Betroffenen haben kann.

Beobachtungen, die die Intimsphäre von Betroffenen betreffen, etwa die Überwachung von Toiletten, Saunas, Duschen und Umkleidekabinen oder -bereichen sind regelmäßig unverhältnismäßig und damit unzulässig.

(a) Interesse des Verantwortlichen oder eines Dritten
Festzustellen ist, welche Bedeutung der verfolgte Zweck des Verantwortlichen hat. Insbesondere bei Sicherheitsinteressen sind diese erheblich, wenn die Maßnahme höherrangige Rechtsgüter (Leben, Gesundheit oder Freiheit) schützen soll und der Verhinderung und Aufdeckung *strafrechtsrelevanter Vorfälle* dient. Dagegen überwiegt der Schutz vor Bagatelldelikten das Interesse der betroffenen Personen regelmäßig nicht. Die Bedeutung des Sicherheitsinteresses bemisst sich auch danach, ob und in welchem Umfang eine Gefahr vorliegt. Je abstrakter eine Gefahrenlage ist, desto weniger eingriffsintensiv darf eine Maßnahme sein. Auch der objektive Wert eines überwachten Objekts (bzw. ein potentieller Schaden) kann ein besonderes Sicherheitsinteresse begründen. Zu berücksichtigen ist auch, ob dem Verantwortlichen zumutbare Alternativen zur Verfügung stehen oder ob er zwingend auf die Videoüberwachung angewiesen ist.

Ob die Interessen der Betroffenen im Einzelfall schutzwürdiger sind, entscheidet die Intensität des Eingriffs. Diese bestimmt sich u.a. anhand des *betroffenen Personenkreises (b),* der *Art und des Umfangs der erfassten Informationen (c)* und der *Art und Weise der Datenverarbeitung (d)*.

(b) Betroffener Personenkreis
Je nach Einsatz der Kamera können unterschiedliche *Personenkreise* betroffen sein. Personenbezogene Daten von Kindern sind besonders schützenswert.[19] Von einer Überwachung sind solche Bereiche frei zu halten, in denen Menschen kommunizieren, essen und trinken, sich austauschen, erholen oder Sport treiben. Hier steht die Entfaltung der Persönlichkeit im Vordergrund. In Freizeiteinrichtungen und Gastronomieanlagen überwiegen die schutzwürdigen Interessen der Betroffenen regelmäßig die Interessen des Kamerabetreibers. Auf den Schutz der Betroffenen ist besonders zu achten, wenn Beschäftigte im Sinne der Definition des § 26 Absatz 8 BDSG von einer Überwachung (teil-) erfasst sind.[20]

Zu berücksichtigten sind auch die vernünftigen Erwartungen der betroffenen Personen.[21] Diese Erwartungen können sich aus *objektiven* Umständen ergeben, beispielsweise aus der jeweiligen Transparenz der Datenverarbeitung und der Sozialsphäre des überwachten

[19] Vgl. Erwägungsgrund 38 DS-GVO.
[20] Zur Bewertung der Interessen von betroffenen Beschäftigten, s.u. Punkt 5.1.5 und Punkt 5.1.6.
[21] Vgl. Erwägungsgrund 47 DS-GVO.

Bereichs, d.h. ob die Videoüberwachung in bestimmten Bereichen typischerweise gesellschaftlich akzeptiert oder abgelehnt wird. Der Hinweis auf eine Videoüberwachung allein hat keine Auswirkungen auf die vernünftigen Erwartungen der Betroffenen. Typischerweise akzeptiert ist beispielsweise eine Videoüberwachung in einer Bank oder an einem Bankautomat. Nicht erwartet wird eine Überwachung beispielsweise in Wäldern, in Sanitärbereichen, Sport-, Schwimm- oder Saunaeinrichtungen.

Abzuwägen sind auch die Folgen der Verarbeitung für die betroffene Person. Diese sind dem Nutzen gegenüber zu stellen, den der Verantwortliche von einer Datenverarbeitung erwartet.[22]

(c) Informationsgehalt
Je mehr persönliche Informationen mit einer Videoüberwachung erhoben werden, desto intensiver ist der Eingriff in die Rechte und schutzwürdigen Interessen der Betroffenen. Überwachungsmaßnahmen, denen ein Betroffener *nicht ausweichen* kann und die *dauerhaft* erfolgen, intensivieren einen Eingriff. Dies kann bei einer ständigen Überwachung von Zufahrten und Ein- und Ausgängen von Gebäuden der Fall sein, wenn Besucher und Beschäftigte gezwungen sind, diese zu nutzen.

(d) Art und Weise der Datenverarbeitung
Je nach Art und Weise einer Datenverarbeitung ist der Eingriff in die Rechte und schutzwürdigen Interessen der Betroffenen mehr oder weniger intensiv. Kriterien hierfür sind u.a., ob eine Videoaufnahme anlassbezogen oder anlasslos, zeitlich beschränkt oder dauerhaft erfolgt, ob ein reines Monitoring stattfindet oder die Bilder dauerhaft gespeichert werden. Auch technische Funktionen und Einstellungen von Kameras sind an dieser Stelle zu berücksichtigen, beispielsweise die optische Auflösung einer Kamera oder technische Funktionen wie Pre-Recording, Nachtsicht, Fernzugriff, Zoom- und Schwenkbarkeit und ob die Möglichkeit einer Verarbeitung biometrischer Daten besteht. Auch ob eine Datenverarbeitung mit Drittstaatbezug (Verarbeitung in einer „Cloud“) oder mit automatisierter Softwareunterstützung („Tracking“, „Profiling“, etc.) erfolgt, wird an dieser Stelle berücksichtigt.

Mit technischen Schutzmaßnahmen oder durch den Verzicht auf bestimmte technische Funktionalitäten kann der Eingriff abgemildert oder ausgeglichen werden. Beispielsweise mit einem strengen Zugriffs- und Löschkonzept, der Nutzung technischer Anonymisierungsverfahren (Schwärzen, Verpixeln, etc.) oder mit einem sogenannten Black-Box-

[22] Vgl. WP 217, S.71.

Verfahren, das u. a. strenge Zugriffsbeschränkungen mit einer automatisierten Datenlöschung nach kurzer Zeit verbindet.

2.3. Einwilligung – Buchstabe a

Die Rechtmäßigkeit einer Datenverarbeitung kann sich gem. Art. 6 Absatz 1 Satz 1 Buchstabe a DS-GVO aus einer Einwilligung der Betroffenen ergeben. Im Sinne der DS-GVO bezeichnet der Ausdruck „Einwilligung“ jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist, Art. 4 Nr. 11 DS-GVO.[23]

Bei einer Videoüberwachung kann der Verantwortliche diese gesetzlichen Anforderungen in der Regel nicht erfüllen. Grund dafür ist, dass Kameras regelmäßig öffentlich zugängliche Räume und damit eine unbestimmte Zahl von Personen überwachen. Entsprechend wird der Verantwortliche die Einwilligungen aller überwachten Personen nur schwer nachweisen können.[24] Zudem müsste sichergestellt sein, dass keine weitere Datenverarbeitung mehr erfolgt und personenbezogene Daten unverzüglich gelöscht werden, nachdem eine Person ihre Einwilligung widerrufen hat.[25]

Das bloße Betreten eines speziell gekennzeichneten Bereichs ist keine Einwilligung in eine Videoüberwachung.[26] Es handelt sich bei einem solchen Verhalten regelmäßig nicht um eine unmissverständlich abgegebene Willensbekundung oder um eine „eindeutig bestätigende Handlung“ i.S. des Art. 4 Nr. 11 DS-GVO.[27]

Weitere Informationen hierzu finden sich in den *Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679*[28] (WP 259 rev.01) der Artikel-29-Datenschutzgruppe, die vom Europäischen Datenschutzausschuss angenommen wurden, und im *Kurzpapier*

---

[23] Weitere Voraussetzungen sind in Art. 7 DS-GVO und den Erwägungsgründen 32, 33, 42 und 43 aufgeführt.
[24] Vgl. Art. 7 Absatz 1 DS-GVO, Erwägungsgrund 42 Satz 1.
[25] Vgl. Art. 7 Absatz 3 Satz 2 DS-GVO und Art. 17 Absatz 1 Buchstabe b DS-GVO.
[26] vgl. BVerfG, Kammerbeschluss vom 23.02.2007 – 1 BvR 2368/06; vgl. BVerwG, Urteil vom 27. März 2019 – 6C 2.18, Rn. 23.
[27] Vgl. Erwägungsgrund 32 Satz 1 DS-GVO.
[28] Abrufbar unter: https://www.datenschutzkonferenz-online.de/media/wp/20180410_wp259_rev01.pdf.

Nr. 20[29] der Datenschutzkonferenz. Bei der Einwilligung von Beschäftigten gelten besondere Wirksamkeitsvoraussetzungen (siehe Punkt 5.1.2.).

3. Maßnahmen vor der Durchführung

Die DS-GVO enthält eine Reihe von Pflichten, die an den Verantwortlichen[30] gerichtet sind und die bei Beginn der Datenverarbeitung erfüllt sein müssen. Art. 24 DS-GVO stellt diese im Überblick dar. Die Norm legt aber auch allgemeine Pflichten für den Verantwortlichen und den Auftragsverarbeiter fest. Beim Betrieb einer Videoüberwachungsanlage wird oft ein Unternehmen mit der Wartung dieser Anlage beauftragt. Dieses Unternehmen ist i. d. R. als Auftragsverarbeiter zu betrachten, soweit es personenbezogene Daten aus der Videoüberwachung verarbeitet, weshalb neben weiteren gesetzlichen Pflichten insbesondere ein Auftragsverarbeitungsvertrag abzuschließen ist (s. a. Punkt 3.1.1.).[31]

3.1. Dokumentation und Rechenschaftspflicht

Für Videoüberwachungen gelten umfassende Dokumentations- und Rechenschaftspflichten.

3.1.1. Dokumentationspflicht

Eine Dokumentation ist erforderlich, damit ein Verantwortlicher seine Nachweispflichten erfüllen kann. Eine der wichtigsten Dokumentationspflichten, die vor der Durchführung einer Videoüberwachungsmaßnahme zu erfüllen ist, ist die Erstellung eines *Verzeichnisses von Verarbeitungstätigkeiten* gem. Art. 30 DS-GVO.[32] Hierbei sind insbesondere die Zwecke der Videoüberwachung schriftlich oder in einem elektronischen Format festzuhalten. Eine weitere Dokumentationspflicht im Vorfeld einer Datenverarbeitung durch Videoüberwachung ist beispielweise die Pflicht des Verantwortlichen, mit dem Auftragsverarbeiter einen Vertrag zu schließen oder die Auftragsverarbeitung auf ein anderes Rechtsinstrument zu stützen, vgl. Art. 28 DS-GVO. Verstöße gegen diese Pflichten können mit Bußgeldern geahndet werden.[33]

---

[29] Abrufbar unter: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_20.pdf.
[30] *Verantwortlicher* ist, wer allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, vgl. Art. 4 Nr. 7 DS-GVO.
[31] Den Fall einer Auftragsverarbeitung regelt Art. 28 Absatz 1 DS-GVO.
[32] Vgl. Erwägungsgrund 82 DS-GVO.
[33] Vgl. Art. 83 Absatz 4 Buchstabe a DS-GVO.

3.1.2. Rechenschaftspflicht

Der Verantwortliche ist verpflichtet, die Einhaltung der Grundsätze des Art. 5 Absatz 1 DS-GVO nachweisen zu können („Rechenschaftspflicht“). Bezüglich der Datenverarbeitung muss er der Aufsichtsbehörde Folgendes nachweisen können: Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit. In welcher Form der Nachweis zu erfolgen hat, ist nicht geregelt. Welche Nachweismittel ausreichend sind, hängt vom jeweiligen Risikoniveau der Datenverarbeitung ab. Möglich ist der Nachweis beispielsweise durch:

- das Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DS-GVO
- die Umsetzung geeigneter technischer und organisatorischer Maßnahmen, insbesondere für den laufenden Betrieb nach Art. 32 DS-GVO
- die Datenschutz-Folgenabschätzung nach Art. 35 Absatz 7 DS-GVO
- die Einhaltung genehmigter Verhaltensregeln gem. Art. 40 DS-GVO
- die Einhaltung eines genehmigten Zertifizierungsverfahrens gem. Art. 42 DS-GVO
- Datenschutz durch Technikgestaltung oder durch datenschutzfreundliche Voreinstellungen nach Art. 25 DS-GVO
- Beruht eine Datenverarbeitung auf einer Einwilligung, normiert Art. 7 Absatz 1 DS-GVO eine spezielle Nachweispflicht in Bezug auf das Vorliegen der Einwilligung.

3.2. Verzeichnis von Verarbeitungstätigkeiten

In der Regel ist eine Datenverarbeitung mittels Videoüberwachung in das Verzeichnis der Verarbeitungstätigkeiten gem. Art. 30 DS-GVO aufzunehmen. Im Verzeichnis der Verarbeitungstätigkeiten muss der Verantwortliche dokumentieren, welche personenbezogenen Daten mit Hilfe welcher Verfahren auf welche Weise verarbeitet und welche Datenschutzmaßnahmen getroffen wurden. Es enthält insbesondere den Namen und die Kontaktdaten des Verantwortlichen, die Zwecke der Verarbeitung, eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten und die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen. Hierbei sollte jede Kamera (oder bei Vergleichbarkeit jede Kameragruppe) einzeln aufgenommen und dokumentiert werden. Das Verzeichnis ist der Aufsichtsbehörde auf Antrag zur Verfügung zu stellen.

Weitere Hinweise zum Verzeichnis der Verarbeitungstätigkeiten sind auf der Webseite der Datenschutzkonferenz veröffentlicht.[34] Muster-Verzeichnisse der Verarbeitungstätigkeiten für Verantwortliche[35] und Auftragsverarbeiter[36] sind dort ebenfalls abrufbar.

3.3. Hinweispflicht

Die Art. 12 ff. DS-GVO regeln die Anforderungen an eine transparente und umfassende Information der betroffenen Person. Diese Anforderungen sind auch bei Videoüberwachungen angemessen und adressatengerecht umzusetzen. Auf die Datenverarbeitung ist transparent und fair nach den Vorgaben der Art. 12 ff. DS-GVO hinzuweisen.

Der Umstand der Beobachtung und der Name und die Kontaktdaten des Verantwortlichen sind durch *geeignete Maßnahmen* zum *frühestmöglichen Zeitpunkt* erkennbar zu machen. Zum *frühestmöglichen Zeitpunkt* bedeutet, dass vor dem Betreten videoüberwachter Bereiche auf die Datenverarbeitung hingewiesen wird, damit betroffene Personen ihr Verhalten entsprechend ausrichten können.

Die Betroffenen können in zwei Schritten informiert werden. Zunächst mit einem *vorgelagerten Hinweisschild* (Anlage 1), das auf Augenhöhe angebracht sein sollte und den Betroffenen einen schnell wahrnehmbaren Überblick über die wichtigsten Informationen verschafft. In einem zweiten Schritt mit einem *vollständigen Informationsblatt* (Anlage 2). Die vollständigen Informationen können an geeigneter Stelle ausgelegt oder ausgehängt und zusätzlich auf einer Webseite vorgehalten werden. Die überwachten Bereiche und der jeweils Verantwortliche sollten für die Betroffenen erkennbar sein. Könnte eine Verarbeitung für die Betroffenen überraschend sein, beispielsweise weil deren personenbezogene Daten an Dritte übermittelt oder zu Marketingzwecken verarbeitet werden, muss darauf deutlich hingewiesen werden.

Auf der Grundlage des Art. 13 Absatz 1 und 2 DS-GVO muss bei einer Videoüberwachung auf dem vorgelagerten Hinweisschild auf Folgendes hingewiesen werden:

---

[34] Abrufbar unter: https://www.datenschutzkonferenz-online.de/media/ah/201802_ah_verzeichnis_verarbeitungstaetigkeiten.pdf.
[35] Abrufbar unter: https://www.datenschutzkonferenz-online.de/media/ah/201802_ah_muster_verantwortliche.pdf.
[36] Abrufbar unter: https://www.datenschutzkonferenz-online.de/media/ah/201802_ah_muster_auftragsverarbeiter.pdf.

- Umstand der Beobachtung - Piktogramm, Kamerasymbol
- Identität des Verantwortlichen sowie gegebenenfalls seines Vertreters (nach Art. 27 DS-GVO), Name einschl. Kontaktdaten
- Kontaktdaten des betrieblichen Datenschutzbeauftragten – soweit benannt, dann aber zwingend
- Verarbeitungszwecke und Rechtsgrundlage in Schlagworten
- Angabe des berechtigten Interesses (soweit die Verarbeitung auf Art. 6 Absatz 1 Satz 1 Buchstabe f DS-GVO beruht)
- ggf. Dauer der Speicherung
- Hinweis auf die weiteren Pflichtinformationen (insbes. Auskunftsrecht, Beschwerderecht, ggf. Empfänger der Daten) und den Zugang hierzu.

Diese Informationen können in Kombination mit standardisierten Bildsymbolen[37] bereitgestellt werden. Allein das Aufstellen einer geeigneten Beschilderung führt nicht zur Zulässigkeit einer ansonsten rechtswidrigen Videoüberwachung. Weitere Informationen hierzu finden Sie in den *Leitlinien für Transparenz* (WP 260 rev.01).[38]

3.4. Datenschutz-Folgenabschätzung

Der Verantwortliche einer Videoüberwachungsanlage hat vorab eine Datenschutz-Folgenabschätzung durchzuführen, wenn eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein *hohes Risiko für die Rechte und Freiheiten natürlicher Personen* zur Folge hat, vgl. Art. 35 Absatz 1 DS-GVO. Die Datenschutz-Folgenabschätzung befasst sich insbesondere mit Abhilfemaßnahmen, durch die der Schutz personenbezogener Daten sichergestellt und die Einhaltung der Verordnung nachgewiesen werden kann. Allgemeine Informationen zur Datenschutz-Folgenabschätzung finden Sie im Kurzpapier Nr. 5 der Datenschutzkonferenz.[39]

Bei einer Videoüberwachung muss insbesondere dann von einem *hohen Risiko* für die Rechte und Freiheiten natürlicher Personen ausgegangen werden, wenn eine *systematische und umfangreiche Überwachung öffentlich zugänglicher Bereiche* erfolgt oder *biometrische Verfahren* zur Datenverarbeitung eingesetzt werden. Die Überwachung einer großen, weiträumigen Fläche kann ein hohes Risiko für die Rechte der betroffenen Perso-

---

[37] Vgl. Art. 12 Absatz 7 Satz 1 DS-GVO; Erwägungsgrund 60 Satz 5 DS-GVO.
[38] WP 260 rev.01 abrufbar unter: https://www.datenschutzkonferenz-online.de/wp29-leitlinien.html.
[39] Abrufbar unter: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf.

nen darstellen und in der Folge eine Pflicht zur Erstellung einer Datenschutz-Folgenabschätzung auslösen.

3.4.1. Systematische und umfangreiche Überwachung

Bei der Beobachtung, Überwachung oder Kontrolle von Personen in *öffentlich zugänglichen Bereichen* (Einkaufszentrum, Straße oder Bahnhof) mittels Videoüberwachung kann es sich um eine *systematische* und *umfangreiche* Überwachung handeln.[40] Ob eine Verarbeitung *umfangreich* ist, hängt von der Zahl der Betroffenen, der Datenmenge, der Dauer und dem geografischen Ausmaß der Überwachung ab.[41] In der Regel erfolgt eine Videoüberwachung in öffentlich zugänglichen Bereichen dauerhaft, sie erfasst - abhängig vom Einzelfall - einen unbestimmten Personenkreis und eine große Datenmenge. Eine Datenschutz-Folgenabschätzung ist bei einer Videoüberwachung vor allem erforderlich, wenn *weiträumig* öffentlich zugängliche Bereiche von Kameras erfasst sind, d.h. die Überwachung ein bedeutendes geografisches Ausmaß erreicht.[42] Gleiches gilt für Überwachungen, die mit einer Vielzahl von Kameras durchgeführt werden. Eine weiträumige Erfassung liegt jedenfalls dann vor, wenn öffentlich zugängliche großflächige Anlagen überwacht werden. Dabei handelt es sich um bauliche Anlagen, die nach dem erkennbaren Willen des Betreibers von jedermann betreten oder genutzt werden können und von ihrer Größe her geeignet sind, eine größere Anzahl von Menschen aufzunehmen. Insbesondere kommen hierbei Sport-, Versammlungs- und Vergnügungsstätten, Einkaufszentren und Parkräume in Betracht, die einen entsprechenden Publikumsverkehr aufweisen. Hierzu gehören auch Flächen, die eine gleichzeitige Anwesenheit vieler Menschen bei Veranstaltungen ermöglichen, und ganz oder teilweise aus baulichen Anlagen bestehen und daher auch besonderen baurechtlichen Bestimmungen der Länder und der Baunutzungsverordnung unterliegen.

3.4.2. Verarbeitung besonderer Kategorien personenbezogener Daten

Eine Datenschutz-Folgenabschätzung ist erforderlich, wenn mittels Kameratechnik *besondere Kategorien von personenbezogenen Daten* gem. Art. 9 Absatz 1 DS-GVO *umfangreich* verarbeitet werden, vgl. Art. 35 Absatz 3 Buchstabe b DS-GVO. Nähere Informationen zu den besonderen Kategorien personenbezogener Daten enthalten das Kurzpapier

---

[40] Vgl. Leitlinien zur Datenschutz-Folgenabschätzung und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“ (nachfolgend: WP 248 Rev. 01), S. 10 ff. Abrufbar unter: https://www.datenschutzkonferenz-online.de/media/wp/20171004_wp248_rev01.pdf.

[41] Siehe dazu WP 248 Rev. 01, S. 11 ff.

[42] Vgl. Art. 35 Absatz 3 Buchstabe c DS-GVO i.V. mit Erwägungsgrund 91 Satz 3.

Nr. 17[43] der Datenschutzkonferenz und die Leitlinie 03/2019[44] des Europäischen Datenschutzausschusses zur Videoüberwachung.

Unter die Kategorie der besonderen personenbezogenen Daten kann beispielsweise die Verarbeitung *biometrischer Daten zur eindeutigen Identifizierung fallen*. Werden biometrische Daten mit einer Gesichtserkennungssoftware verarbeitet, beispielsweise um den Zutritt- oder Zugang zu einem Bereich zu kontrollieren, um Werbe- und Marketingmaßnahmen durchzuführen oder um Personen zu beobachten oder zu überwachen, ist im Vorfeld der Verarbeitung zwingend eine Datenschutz-Folgenabschätzung durchzuführen. Dabei ist die bloße Eignung von Videoaufnahmen für eine biometrische Analyse bei der Risikoabschätzung und der Auswahl der technischen und organisatorischen Maßnahmen zu berücksichtigen. Nähere Informationen hierzu finden Sie im Positionspapier zur biometrischen Analyse der Datenschutzkonferenz[45] und der Leitlinie 03/2019[46] des Europäischen Datenschutzausschusses zur Videoüberwachung.

3.4.3. Hohes Risiko

Die Aufzählung in Art. 35 Absatz 3 DS-GVO ist nicht abschließend. Unabhängig von der räumlichen Ausdehnung der Überwachung oder der Verarbeitung biometrischer Daten, kann sich ein *hohes Risiko* i.S. des Art. 35 Absatz 1 DS-GVO für die Rechte und Freiheiten natürlicher Personen aus den besonderen Umständen der Datenverarbeitung ergeben. Beispielsweise wenn ein besonders schützenswerter Personenkreis überwacht wird (Beschäftigte, Kinder, etc.), die Datenverarbeitung einen hohen Informationsgehalt besitzt (z.B. politische Veranstaltungen oder Werbe- und Marketingmaßnahmen mit Gesichtserkennungssoftware) oder eine bestimmte Art und Weise der Datenverarbeitung erfolgt (hohe Auflösung, Fernzugriff, Zoom- und Schwenkbarkeit, Webcam, etc.). Zur Frage, ob eine Verarbeitung im Sinne der DS-GVO wahrscheinlich ein *hohes Risiko* mit sich bringt, finden sich weitere Informationen in der *Leitlinie zur Datenschutz-Folgenabschätzung* (WP 248 Rev. 01).[47] Die Datenschutzaufsichtsbehörden haben ergänzend eine *Liste von Verarbeitungstätigkeiten* aufgestellt, bei der eine Datenschutz-Folgenabschätzung durchzuführen ist.[48] Dort sind auch Kriterien zur Bewertung von Verarbeitungsvorgängen festgelegt. Eine

---

[43] Abrufbar unter: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_17.pdf.
[44] Leitlinie Punkt 5, S.17 f.
[45] Abrufbar unter: https://www.datenschutzkonferenz-online.de/media/oh/20190405_positionspapier-biometrie.pdf.
[46] Leitlinie Punkt 5.1, S.18 f.
[47] Abrufbar unter: https://www.datenschutzkonferenz-online.de/media/wp/20171004_wp248_rev01.pdf.
[48] Abrufbar unter: https://www.datenschutzkonferenz-online.de/media/ah/20181017_ah_DSK_DSFA_Muss-Liste_Version_1.1_Deutsch.pdf.

Datenschutz-Folgenabschätzung ist demnach zwingend erforderlich, sobald zwei oder mehr der neun Kriterien bei einer Datenverarbeitung zutreffen.

3.5. Technisch-organisatorische Schutzmaßnahmen

Bei einer Videoüberwachung ist mit technisch-organisatorischen Maßnahmen gem. Art. 24, 25 und 32 der DS-GVO nachweisbar sicherzustellen, dass eine Verarbeitung nach den Vorgaben der DS-GVO erfolgt. Risiken für die Rechte und Freiheiten natürlicher Personen sind damit zu minimieren und es ist ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit einer Videoüberwachung oder -beobachtung verbunden sind, insbesondere durch – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von bzw. unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet werden, Art. 32 Absatz 2 Satz 2 DS-GVO. Auch sind technisch-organisatorische Maßnahmen umzusetzen, die Betroffenen die Wahrung ihrer Rechte nach den Art. 15 ff. DS-GVO ermöglichen. Insbesondere sollte geregelt sein, wie mit Auskunfts- und Löschersuchen von Betroffenen umgegangen wird. Die Einhaltung der technisch-organisatorischen Maßnahmen sollte von Verantwortlichen durch interne Rahmenbedingungen und Richtlinien unterstützt werden. Dies gilt bei der Planung, während der Durchführung der Videoüberwachung und ggf. bei einer regelmäßigen Überprüfung der getroffenen Maßnahmen.

Es gilt, dem Datenschutz durch Technikgestaltung (*data protection by design*) und durch datenschutzfreundliche Voreinstellungen (*data protection by default*) nachzukommen, wie sie im Art. 25 DS-GVO und im Erwägungsgrund 78 gefordert werden. Umsetzbar ist dies für den Verantwortlichen u.a. durch eine geeignete Wahl des videoüberwachten Bereichs. Dieser sollte möglichst nur den zur Zweckerfüllung erforderlichen Bereich umfassen. Sollte dies nicht möglich sein, kann durch *irreversible* Verpixelung und *irreversibles* Ausblenden von nicht relevanten Bereichen, durch die Wahl der Videoauflösung[49] und durch eine möglichst kurze Speicherdauer eine Datenminimierung erreicht werden. Technische Möglichkeiten wie Schwenken, Neigen oder Zoomen, biometrische Erkennung, Verhaltenserkennung und Audioaufnahmen sind in der Regel nicht zulässig. Bei netzwerkfähigen Videokameras ist regelmäßig die Sicherheit (Firmware-Aktualisierungen, Passwortschutz, Zugriffsrechte, Benutzerkonten, etc.) zu überprüfen, insbesondere, wenn das Gerät per

[49] DIN EN 62676-4, ehemals DIN EN 50132-7.

W-LAN angebunden/und oder mit dem Internet verbunden ist.[50] Sonstige nicht benötigte Funktionen sind zu deaktivieren.

4. Weitere Datenverarbeitungen

Nach Art. 32 der DS-GVO müssen alle Komponenten eines Videoüberwachungssystems und die erfassten Daten in allen Bereichen geschützt werden. Hierzu zählen die ruhenden Daten (gespeicherte Daten), die Datenübertragung (von der Kamera zum Videosystem, ggf. die Übermittlung zu einem Dienstleister) und die Verarbeitung der Videodaten. Hilfreich bei der Umsetzung sind gängige Normen und Richtlinien.[51] Die Richtlinien und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik sollten beachtet werden. [52]

4.1. Speicherdauer

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.[53] Sind die Videoaufnahmen für die Zwecke, für die sie erhoben wurden, nicht mehr notwendig, ist der Verantwortliche verpflichtet, die Videoaufnahmen *unverzüglich zu löschen*, vgl. Art. 17 Absatz 1 Buchstabe a DS-GVO.

Die Speicherdauer ist an den jeweiligen Zweck der Überwachung gebunden. Werden die Daten für die Verfolgung der ursprünglichen Zwecke nicht mehr benötigt, ist der Verantwortliche verpflichtet, die Videoaufzeichnungen unverzüglich zu löschen. Das kann beispielsweise der Fall sein, wenn eine Gefahr nicht weiter abgewendet werden muss oder eine Beweissicherung nicht mehr notwendig ist. Kommt es zu keinem Ereignis, wie beispielsweise einem Überfall oder Diebstahl, dann werden die Videoaufzeichnungen für Beweiszwecke nicht mehr benötigt und sind unverzüglich zu löschen. Ob eine Sicherung des Materials notwendig ist, kann in den meisten Fällen innerhalb von ein bis zwei Arbeitstagen geklärt werden. Das bedeutet, dass eine Speicherdauer von 72 Stunden in der Regel

---

[50] vgl. BSI IT-Grundschutz-Kompendium (2019) NET.2.1 WLAN-Betrieb und NET.2.2 WLAN-Nutzung.
[51] IEC TS 62045 - Multimedia-Sicherheit. Leitfaden für den Datenschutz bei genutzten oder ungenutzten Einrichtungen und Systemen. DIN EN ISO/IEC 27000 - Informationstechnik - Sicherheitsverfahren - Informationssicherheits-Managementsysteme.
[52] BSI IT-Grundschutz-Kompendium (2019).
[53] Die Löschpflicht folgt dem Grundsatz der Datenminimierung und der Speicherbegrenzung in Art. 5 Absatz 1 Buchstaben c und e DS-GVO und Erwägungsgrund 39 Satz 8 DS-GVO.

zulässig ist.[54] Innerhalb dieses Zeitraumes kann der Verantwortliche regelmäßig Schäden an überwachten Objekten, Einrichtungen oder Übergriffe auf Personen üblicherweise feststellen und eine Löschung der relevanten Sequenzen unterbinden.

Die Speicherung der Aufnahmen ist ein selbstständiger Verarbeitungsvorgang.[55] Je länger die Speicherdauer, desto höher ist der Begründungsaufwand hinsichtlich des Zwecks sowie der Notwendigkeit der Speicherung, insbesondere, wenn die Speicherdauer mehr als 72 Stunden beträgt. Eine verlängerte Speicherfrist ist beispielsweise an mehrtägigen Feiertagen und in Urlaubszeiten möglich, wenn kein Geschäftsbetrieb erfolgt und Schäden nicht unmittelbar bemerkt werden können. Ggf. kann ein besonderer Überwachungszweck eine längere Speicherung rechtfertigen. Beispielsweise wenn ein besonderer Sachverhalt nachvollzogen werden muss, der sich über einen längeren Zeitraum erstreckt. Mit internen Arbeitsabläufen können längere Speicherfristen in der Regel nicht begründet werden.

Eine verlängerte Speicherdauer gilt dabei *nur* für Kameras, die einen besonderen Überwachungszweck verfolgen oder für die eine besondere Begründung vorliegt. Als Standard-Speicherdauer darf sie nicht *auf alle Kameras übertragen* werden. Sie gilt - nach dem Grundsatz der Datenminimierung - außerdem *nur für die Zeiten*, zu denen ein besonderer Grund oder Zweck tatsächlich vorliegt. Die Speicherdauer darf beispielsweise nur an Wochenenden, in den Ferien oder in den Urlaubszeiten verlängert werden, wenn eine Kontrolle der überwachten Bereiche nicht möglich oder unzumutbar ist.

4.2. Tonaufzeichnung

Wird eine Videoüberwachungskamera mit Audiofunktion eingesetzt, kann dies unter den Straftatbestand des § 201 Absatz 1 und Absatz 2 Strafgesetzbuch fallen. Demnach ist das

---

[54] Auch bei der Speicherung von Aufnahmen müssen die unterschiedlichen Interessen in Einklang gebracht werden: Mit einer Speicherdauer von 72 Stunden kann der Überwachende regelmäßig seine Sicherheitsinteressen verfolgen, gleichzeitig bleiben die schutzwürdigen Interessen der Betroffenen gewahrt. Erfolgt eine Videoüberwachung in einem öffentlichen Raum zum Zweck des Eigentums- oder Personenschutzes, ist der Schadens- oder Ereignisfall die Ausnahme. Eine gängige Videoüberwachung speichert hier weit überwiegend Daten von Unbeteiligten. Diese Betroffenen haben weder Einfluss auf ihre Überwachung noch Anlass für eine Speicherung ihrer Daten gegeben. Je länger die Aufnahmen aufbewahrt werden, desto stärker ist der Eingriff in deren Rechte. Die Rechte *dieser* Betroffenen (und *nicht* die der Tatverdächtigen) werden durch die unverzügliche Löschung nach Zweckerreichung gewahrt. Innerhalb von 72 Stunden ist es dabei für den Überwachenden möglich und zumutbar, Eigentums- oder Personenschäden festzustellen. Dazu *muss* er innerhalb dieses Zeitraums prüfen, ob ein entsprechender Anlass oder ein Anhaltspunkt für einen solchen Schaden vorliegt (Fehlbestände, Schadensmeldungen, Übergriffe, Überfälle, Einbruchsspuren, Notruf-, Alarm- oder Kontrollmeldungen, etc.). Ist dies der Fall, können die relevanten Videosequenzen unmittelbar gesichert werden. Die Prüf- und Reaktionspflicht orientiert sich am jeweiligen Zweck der Überwachung. Teil der Prüfpflicht ist es nicht, die Videoaufnahmen innerhalb der Speicherzeiten anlasslos „ins Blaue“ hinein sichten zu müssen.

[55] Art. 4 Nr. 2 DS-GVO.

unbefugt heimliche Abhören oder Aufzeichnen des nichtöffentlich gesprochenen Wortes strafbar. Verfügt eine Videoüberwachungskamera über eine Audiofunktion, ist diese unumkehrbar zu deaktivieren.

4.3. Regelmäßige Prüfung

Der Betreiber einer Videoüberwachungsanlage sollte in regelmäßigen Abständen prüfen, ob die Datenverarbeitung die Rechtmäßigkeitsvoraussetzungen noch immer erfüllt. Insbesondere die Frage der Geeignetheit und Erforderlichkeit einer Maßnahme sollte periodisch beurteilt werden. Die Videoüberwachung darf nicht weiter betrieben werden, wenn die Rechtmäßigkeitsvoraussetzungen der Datenschutz-Grundverordnung nicht mehr erfüllt sind, beispielweise wenn nach einem gewissen Zeitablauf ersichtlich wird, dass keine Tatsachen für eine Gefährdung des Objekts mehr festgestellt werden oder weitere Sicherheitsmaßnahmen eine Videoüberwachung entbehrlich machen. Dies kann auch Teilbereiche einer Überwachung betreffen. Das Ergebnis der Prüfung ist schriftlich zu dokumentieren.

5. Besondere Fallkonstellationen

Ob ein Verantwortlicher personenbezogene Daten rechtmäßig verarbeitet, richtet sich u.a. nach dem jeweiligen Zweck der Überwachung, dem betroffenen Personenkreis und der Art und Weise der Datenverarbeitung. Bestimmte Konstellationen treten bei Videoüberwachungen regelmäßig auf und werden von den Aufsichtsbehörden i. d. R. wie folgt bewertet:

5.1. Überwachung von Beschäftigten

Eine dauerhafte Videoüberwachung im Arbeitsverhältnis greift erheblich in die Persönlichkeitsrechte von Beschäftigten ein und ist regelmäßig unzulässig. Müssen Beschäftigte während ihrer gesamten Arbeitszeit befürchten, dass ihr Verhalten aufgezeichnet, später rekonstruiert und kontrolliert wird, erzeugt dies einen ständigen Überwachungs- und Anpassungsdruck. Bei auffälligem oder abweichendem Verhalten setzen sie sich der Gefahr aus, später kritisiert, verspottet oder sanktioniert zu werden. Weigern sich Beschäftigte unter diesen Bedingungen zu arbeiten, verstoßen sie ggf. gegen arbeitsvertragliche Pflichten. Diese besondere Situation in einem Arbeitsverhältnis ist bei der Einrichtung einer Videoüberwachung zu berücksichtigen.

5.1.1. Allgemein

Eine Videoüberwachung von Beschäftigten kann von einer beiläufigen Aufnahme bis hin zur gezielten Kontrolle reichen. Kameras sind nicht erlaubt, wenn damit die Arbeitsleistung, Sorgfalt und Effizienz von Beschäftigten kontrolliert werden soll. Zum Zweck einer Verhaltens- oder Leistungskontrolle von Beschäftigten ist eine Videoüberwachung daher unzulässig. Wo eine persönliche Geschäftsführung und -kontrolle im Betrieb erforderlich ist, darf eine Kamera diese nicht ersetzen.

Die Intim- oder Persönlichkeitssphäre von Personen darf auch im Arbeitsverhältnis nicht verletzt werden. Ein Kameraeinsatz in sensiblen Bereichen wie Umkleidekabinen, Sanitär-, Pausen-, Sozial- und Aufenthaltsräumen ist daher unzulässig.

Dauerhafte Arbeitsplätze oder Bereiche, in denen sich Beschäftigte über längere Zeit aufhalten, dürfen grundsätzlich nicht gefilmt werden. Auch eine Videoüberwachung von Beschäftigten an ihren Arbeitsplätzen oder in Pausenräumen zur Vorbeugung von Diebstählen und anderen pflichtwidrigen Handlungen ist unzulässig.

In einer Interessenabwägung wird u.a. berücksichtigt, ob Betroffenen ein kontrollfreier und unbeobachteter Arbeitsbereich verbleibt. Je weniger Rückzugsraum zur Verfügung steht, desto eher überwiegen die schutzwürdigen Interessen der Beschäftigten.

5.1.2. Einwilligung

Eine wirksame Einwilligung von Beschäftigten in eine Videoüberwachung kann auch im Rahmen eines Arbeitsverhältnisses nur erteilt werden, wenn die gesetzlichen Voraussetzungen einer Einwilligung vorliegen.[56] Verfolgt eine solche Datenverarbeitung den Zweck, Beschäftigte zu *kontrollieren oder zu überwachen*, zum Beispiel um innerhalb der Belegschaft Straftaten zu verhindern, liegen die Voraussetzungen einer wirksamen Einwilligung regelmäßig nicht vor.

In die eigene Überwachung durch Videokameras willigen Beschäftigte regelmäßig *nicht freiwillig* ein.[57] Die im Beschäftigungsverhältnis bestehende *Abhängigkeit* der beschäftigten Personen sowie die Umstände, unter denen die Einwilligung erteilt worden ist, sind für die Beurteilung der Freiwilligkeit der Einwilligung besonders zu berücksichtigen, vgl. § 26

[56] S.o. Punkt 2.3. i.V. mit § 26 Absatz 2 BDSG.
[57] *Freiwilligkeit* kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen, vgl. § 26 Absatz 2 Satz 2 BDSG.

Absatz 2 Satz 1 BDSG. Zwischen Arbeitgebern und Beschäftigten herrscht regelmäßig ein klares Ungleichgewicht.[58] Es ist unwahrscheinlich, dass ein Beschäftigter frei auf ein Ersuchen seines Arbeitgebers um Einwilligung beispielsweise in die Aktivierung von Überwachungssystemen wie einer Kameraüberwachung des Arbeitsplatzes antworten kann, ohne sich gedrängt zu fühlen, eine Einwilligung zu erteilen.[59] In einer solchen Situation müssen Beschäftigte auch arbeitsrechtliche Konsequenzen fürchten, wenn sie - ggf. als einzige der Belegschaft - eine Überwachung ablehnen. Zudem besteht für die Beschäftigen die vertragliche Pflicht, sich an dem von ihrem Arbeitgeber bestimmten Ort aufzuhalten, um dort die geschuldete Arbeitsleistung zu erbringen. Sie haben gerade nicht die Möglichkeit, sich der Überwachung durch Verlassen der Räumlichkeiten zu entziehen, ohne ihre vertragliche Pflicht zu verletzen.

Die Erfüllung des Arbeitsvertrags darf nicht von der Einwilligung in eine Verarbeitung von personenbezogenen Daten abhängig sein, die für die Erfüllung des Vertrags nicht erforderlich ist.[60]

5.1.3. Gezielte Überwachung von Beschäftigten

Zur Aufdeckung von Straftaten dürfen personenbezogene Daten von Beschäftigten nur nach der Maßgabe des § 26 Absatz 1 Satz 2 BDSG verarbeitet werden. Eine Datenverarbeitung ist dann zulässig, wenn zu dokumentierende *tatsächliche Anhaltspunkte* den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind. Eine dauerhafte permanente Videoüberwachung kann jedoch nicht auf § 26 Absatz 1 Satz 2 BDSG gestützt werden. Es ist hier nur eine zeitweise Überwachung möglich.

Bezweckt eine Videoüberwachung beispielsweise Diebstähle durch Beschäftigte aufzudecken, müssen zunächst tatsächliche Anhaltspunkte den *konkreten Verdacht einer strafbaren Handlung* gegen eine beschäftigte Person oder einen eng eingrenzbaren Personenkreis begründen. Liegt ein solcher Verdacht nicht vor, d.h. will der Arbeitgeber mit einer Videoüberwachung nur *befürchteten* Verfehlungen von Beschäftigten begegnen, ist eine

---

[58] Es besteht eine Drucksituation, dem Willen des Arbeitgebers zu entsprechen; dies gilt insbesondere *vor* und *bei* Abschluss eines Arbeitsvertrages. Hat der Arbeitgeber bereits Geld in eine Überwachungsanlage investiert, kann ein Beschäftigter seine Zustimmung in die Überwachung kaum verweigern, ohne sich offen den Plänen und finanziellen Interessen seines Arbeitgebers entgegenzustellen.
[59] Vgl. WP 259 rev.01, S.7 f.
[60] vgl. Erwägungsgrund 43 Satz 2 DS-GVO.

Videoüberwachung unzulässig.[61] Ein konkreter Verdacht muss *im Vorfeld* einer solchen Überwachungsmaßnahme dokumentiert sein. Der Arbeitgeber darf also gerade nicht vorbeugend Daten von Beschäftigen sammeln, ohne einen bestimmten Anlass für eine Überwachungsmaßnahme zu haben. Dies gilt auch für den Fall, dass ein Zugriff auf die Aufnahmen unter der Bedingung erfolgt, dass sich ein bestimmter Tatverdacht erst *im Nachhinein* konkretisiert (Speicherung auf Vorrat).

Selbst wenn ein konkreter Verdacht einer strafbaren Handlung besteht, *muss* der Arbeitgeber vor einer Videoüberwachung alle anderen, gleich effektiven Maßnahmen erfolglos eingesetzt haben bzw. deren Verwendung geprüft und nachvollziehbar verworfen haben. Dies kann geschehen durch die Einsichtnahme in Personaleinsatzpläne, den Abgleich von Abwesenheits- und Anwesenheitslisten mit Warenverlusten, die Kontrolle von gebuchten Warenrücknahmen, die Kontrolle von Kassenjournalen (einschließlich detaillierter Auswertung der Umsätze), die Kontrolle von Warenflüssen (Belieferung und Abverkauf) und stichprobenartige Tor- oder Taschenkontrollen. Ein betriebliches Kontrollsystem sollte bei strafrechtlichen Auffälligkeiten Maßnahmen in Gang setzen, die im Hinblick auf ihre Eingriffstiefe gestaffelt aufeinander aufbauen und eine Dokumentation der einzelnen Maßnahmen vorsehen.[62] Nach einer Abwägungsentscheidung kann und darf am Ende eine zulässige Videoüberwachung gem. § 26 Absatz 1 Satz 2 BDSG stehen.

Eine *heimliche oder verdeckte Videoüberwachun*g zu den oben genannten Zwecken ist nur in absoluten Ausnahmefällen möglich, wenn Ausnahmen von der Informationspflicht gem. Art. 13 DS-GVO bestehen, beispielsweise nach § 32 Abs. 1 Nr. 4 BDSG. Alle möglichen Mittel zur Aufklärung des Verdachts, die weniger in Persönlichkeitsrechte einschneiden, *müssen* vorher ausgeschöpft sein. Eine heimliche Videoüberwachung sollte praktisch die einzig verbleibende Möglichkeit darstellen, eine Straftat aufzuklären oder zu verhindern.

5.1.4. Betriebsvereinbarung

Auch Betriebsvereinbarungen können eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten darstellen. Soweit eine Videoüberwachung im Arbeitsverhältnis den Vorgaben von Art. 88 DS-GVO i.V. mit § 26 Absatz 4 BDSG entspricht, kann sie durch eine datenschutzrechtskonforme Betriebsvereinbarung geregelt werden. Die Verfahren zur

[61] Die Beschäftigten müssen ihre Persönlichkeitsrechte nicht für einen Generalverdacht ihres Arbeitgebers aufgeben - VG Hannover, Beschluss v. 13.08.2019 – 10 B 1883/19 – nicht veröffentlicht.
[62] Ein solches Kontrollsystem ist im Übrigen auch geeignet, einen bislang *unbestimmten* Verdacht gegen Beschäftigte auf einen *bestimmten* Personenkreis einzugrenzen.

Verarbeitung personenbezogener Daten müssen dabei den Anforderungen des Art. 88 Absatz 2 DS-GVO entsprechen. Danach muss eine Betriebsvereinbarung angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Personen umfassen. Dies gilt insbesondere im Hinblick auf die Transparenz der Verarbeitung, die Übermittlung personenbezogener Daten innerhalb eines Unternehmensverbunds und die Überwachungssysteme am Arbeitsplatz. In einer Betriebsvereinbarung sollte deutlich werden, dass der Zweck einer Leistungskontrolle ausdrücklich ausgeschlossen ist. Es sollte darin insbesondere festgelegt werden:

- Gegenstand der Datenerhebung, -verarbeitung oder -nutzung
- Zweckbindung
- Datenvermeidung- und Datensparsamkeit
- Art und Umfang der erhobenen, verarbeiteten oder genutzten Daten
- Empfänger der Daten
- Rechte der Betroffenen
- Löschfristen
- Technische und organisatorische Maßnahmen wie beispielsweise das Berechtigungs- und Zugriffskonzept

Zulässige Verfahren zur Videoüberwachung ermöglichen in der Regel eine Bewertung der Persönlichkeit der Beschäftigten einschließlich ihrer Fähigkeiten, ihrer Leistungen und ihres Verhaltens. Sofern ein Betriebsrat existiert, ist dieser, gem. § 87 Absatz 1 Nr. 6 Betriebsverfassungsgesetz vor der Einführung und Anwendung der Einrichtungen zu beteiligen. Falls kein Betriebsrat existiert, sollte der Arbeitgeber die Einrichtung von Videoüberwachungsanlagen regeln, z. B. durch datenschutzkonforme Dienstanweisungen.

5.1.5. Miterfasste Beschäftigte

In *öffentlich zugänglichen Räumen* mit Publikums- und Kundenverkehr kann es vorkommen, dass Arbeitsbereiche von Beschäftigten gefilmt werden. Beschäftigte werden zwar nicht gezielt überwacht (s.o.), sie sind aber regelmäßig von einer Überwachung betroffen. Die Überwachung richtet sich dann nach Art. 6 Absatz 1 Satz 1 Buchstabe f DS-GVO. Beispiel hierfür sind Videoüberwachungen von Verkaufsflächen im Einzelhandel oder in Einkaufszentren, um die Ware während der Öffnungszeiten vor Kundendiebstahl zu schützen.

Eine Videoüberwachung in einem *öffentlich zugänglichen* Betriebs- oder Geschäftsbereich ist möglich, wenn sie zur Wahrung berechtigter Interessen des Arbeitgebers oder der Ar-

beitgeberin erforderlich ist und schutzwürdige Interessen der Beschäftigten nicht überwiegen. Die Interessen der Beschäftigten können bereits dadurch geschützt werden, dass sich die Überwachung auf das erforderliche Maß[63] beschränkt, beispielsweise auf Auslagen und Regale mit besonders hochpreisigen Waren. Außerdem können bestimmte Arbeits- und Kommunikationsbereiche von der Überwachung ausgenommen werden.

Im Rahmen der Abwägung[64] ist zu berücksichtigen, dass Warendiebstahl auf Verkaufsflächen im Einzelhandel oder in Einkaufszentren zum geschäftstypischen Risiko gehört und eine Überwachung den vernünftigen Erwartungen der betroffenen Personen regelmäßig entspricht. Dagegen sind Beschäftigte als bloße Nebenfolge einer Warenüberwachung miterfasst, werden aber nicht gezielt überwacht. Verbleibt den Beschäftigten eine Rückzugsmöglichkeit und ist die Überwachung auf gefährdete Bereiche beschränkt, überwiegt grundsätzlich das Interesse des Eigentümers am Schutz seiner Waren. Dies gilt nicht, wenn Beschäftigte im Fokus einer Videoüberwachung stehen oder dauerhaft erfasst sind. Es gelten dann die einschränkenden Vorschriften des Art. 88 DS-GVO i.V. mit § 26 BDSG.

5.1.6. Überwachung in nicht-öffentlichen Betriebsbereichen

Sofern die Überwachung von Beschäftigten nicht Zweck der Überwachung ist, kann eine Videoüberwachung gem. Art. 6 Absatz 1 Satz 1 Buchstabe f DS-GVO in *nicht-öffentlichen* Bereichen eines Betriebs eingesetzt werden, beispielsweise um Produktionsabläufe zu verfolgen oder den Zutritt unberechtigter Personen zu sensiblen Bereichen zu verhindern. Eine Überwachung allein zu dem Zweck, einen ordnungsgemäßen Arbeitsablauf zu gewährleisten, ist nicht gerechtfertigt.
Möglich sind Überwachungsmaßnahmen jedenfalls dann, wenn ein Arbeitgeber oder eine Arbeitgeberin in besonders gefahrträchtigen Arbeitsbereichen Schutzpflichten gegenüber seinen Beschäftigten erfüllen muss. Der Erfassungsbereich ist dabei auf den sicherheitsrelevanten Bereich zu beschränken. Arbeitsbereiche von Beschäftigten sind soweit wie möglich auszublenden. Zur Verhinderung und Aufklärung von Diebstählen können Lagerräume außerhalb der Betriebszeiten überwacht werden. Ist patrouillierendes Sicherheitspersonal miterfasst, sind technisch-organisatorische Maßnahmen zu treffen, die einen Eingriff in deren Rechte abmildern.

---

[63] S.o. Punkt 2.2.2.
[64] S.o. Punkt 2.2.3.

5.2. Überwachung in der Nachbarschaft

In Wohngebieten dürfen Privatpersonen den öffentlichen Raum nicht überwachen. Die Beobachtungsbefugnis endet an der eigenen Grundstücksgrenze. Geht eine Überwachung darüber hinaus, kann sich der Überwachende nicht auf sein Hausrecht berufen. Auch ein konkretes Überwachungsinteresse rechtfertigt regelmäßig keine Videoüberwachung öffentlich zugänglicher Räume, wie Straßen, Gehwege oder Parkplätze. Nachbarn, Passanten, Kinder, Lieferanten, Besucher und sonstige Verkehrsteilnehmer müssen eine dauerhafte und ggf. anlasslose Überwachung in Wohnbereichen nicht hinnehmen. In diesen Bereichen überwiegen grundsätzlich die schutzwürdigen Interessen der Betroffenen.

Sofern sich eine Videoüberwachung auf das Grundstück eines Nachbarn erstreckt, können unter Umständen auch zivilrechtliche Unterlassungs- und Abwehransprüche gegen den Verantwortlichen der Datenverarbeitung geltend gemacht werden. Diese Ansprüche können auf dem Zivilrechtsweg geltend gemacht werden, ggf. mit der Hilfe eines Rechtsanwalts. Eine Rundumüberwachung des sozialen Lebens kann auch anhand zivilrechtlicher Maßstäbe nicht mit dem Schutz vor Schmierereien, Verschmutzungen oder einmaligem Vandalismus gerechtfertigt werden. Regelmäßig überwiegen hier die schutzwürdigen Interessen der betroffenen Bewohner und deren Besucher.

Wird mit einer Videobeobachtung der höchst persönliche Lebensbereich einer Person verletzt, kann dies einen Straftatbestand erfüllen (vgl. § 201a des Strafgesetzbuchs).

5.3. Überwachung in der Gastronomie

Eine Videoüberwachung von *Ess- und Aufenthaltsbereichen* in einer Gaststätte ist im Regelfall datenschutzrechtlich unzulässig. Gleiches gilt für *Café-* und *Gastronomieflächen* in Bäckereien, Tankstellen, Hotels, etc. In Sitzbereichen, der Außengastronomie, an der Theke und an einer Bar halten sich Gäste typischerweise über längere Zeit auf, sie essen, trinken und unterhalten sich. Die Rechtsprechung ordnet dieses Verhalten dem Freizeitbereich der Gäste zu.[65] Persönlichkeitsrechte sind hier besonders zu schützen. Eine Videoüberwachung stört die unbeeinträchtigte Kommunikation und den unbeobachteten Aufenthalt der Gaststättenbesucher und greift intensiv in deren Rechte ein. In den Ess- und Aufenthaltsbereichen besteht während der Öffnungszeiten auch keine hohe Gefahr für das Eigentum des Gastronomen. Neben den Gästen befindet sich zu diesen Zeiten Personal

[65] Vgl. AG Hamburg, Urteil vom 22.04.2008 – 4 C 134/08.

in der Gaststätte, das bei entsprechenden Vorfällen unmittelbar die Polizei verständigen kann. Bereiche, die zum längeren Verweilen, Entspannen und Kommunizieren einladen, dürfen daher regelmäßig nicht mit Kameras überwacht werden.

Dient eine Überwachung in *Ein- und Ausgangsbereichen*, *Fluren* und *Treppenhäusern* dem Schutz vor Einbrüchen und ist eine Alarmanlage nicht geeignet wirksam davor zu schützen, dürfen Kameras an dieser Stelle außerhalb der Öffnungszeiten betrieben werden.

Lager und Tresorräume sind in einer Gaststätte für Gäste üblicherweise nicht frei zugänglich. Sie können überwacht werden, wenn in diesen Bereichen keine dauerhaften Arbeitsplätze eingerichtet sind und keine milderen Mittel zur Zweckerreichung zur Verfügung stehen, beispielsweise den Zutritt nur berechtigten Personen zu ermöglichen. Der Erfassungsbereich der Kamera ist auf das Notwendigste zu beschränken. In *Küchen* dürfen Kameras nicht eingesetzt werden.

Die *Kasse* selbst kann während der Öffnungszeiten videoüberwacht werden, wenn Überfälle oder Diebstähle von Dritten verübt wurden und diese ohne Videoüberwachung nicht aufgeklärt oder nachgewiesen werden können. Zudem darf es keine anderen, milderen Maßnahmen zur Sicherung der Kasse geben. Zu prüfen ist, ob die Kasse in einen geschützten Bereich innerhalb der Gaststätte verlegt oder das Kassensystem mit technischen Maßnahmen (Codekarte, Passwort, etc.) vor Zugriffen gesichert werden kann. Persönlichkeitsrechte von Beschäftigten sind auch in diesem Bereich zu achten, weshalb eine Kameraerfassung *auf das Kassenterminal zu begrenzen* ist.

Soll die Kasse, das Lager oder der Tresorraum zu dem Zweck überwacht werden, um *Diebstähle von Beschäftigten* aufzuklären oder nachzuweisen, müssen besondere gesetzliche Voraussetzungen eingehalten werden (Punkt 5.1.3.).

Liegt ein berechtigtes Interesse vor, ist eine Videoüberwachung von *Glücksspielautomaten* begrenzt möglich. Eine Überwachung ist dabei unmittelbar auf den Automaten zu beschränken. Der Innenraum der Gaststätte darf nicht erfasst sein.

5.4. Übersichtsaufnahmen und Webcams

Übersichtskameras verfolgen meist den Zweck, z. B. die aktuelle Wetter- oder Verkehrslage anzuzeigen oder den Fortschritt einer Baustelle zu dokumentieren. Eine Überwachung von Personen ist dabei regelmäßig nicht gewollt oder beabsichtigt. Allerdings besteht – je nach Kameraeinstellung und Art und Weise der Datenverarbeitung – bei Übersichtsauf-

nahmen ein besonderes Risiko für die Persönlichkeitsrechte der Betroffenen. Dies gilt vor allem dann, wenn Kamerabilder aus öffentlich zugänglichen Bereichen live und frei zugänglich im Internet per Webcam übertragen werden. Dritte können die digitalen Aufnahmen dann weltweit abrufen, kopieren und unbegrenzt speichern. Eine Verletzung von Persönlichkeitsrechten wiegt hier besonders schwer, da sich die Bilder sehr weit verbreiten, die Datenverarbeitung meist intransparent ist und ein Verstoß nicht rückgängig gemacht werden kann.

Der Einsatz einer Übersichtskamera und insbesondere einer Webcam ist daher nur zulässig, wenn die Aufnahmen keinen Bezug zu bestimmten Personen ermöglichen.[66] Erkennbar dürfen Einzelpersonen nicht abgebildet werden. Das bedeutet, dass Personen und Kraftfahrzeuge nur schemenhaft erkennbar und (Wohn-) Gebäude oder Geschäfte nicht erfasst sein dürfen. Dies kann mit einer entsprechenden Kamerapositionierung, fehlender Zoom-Möglichkeit und einer niedrigen Bildauflösung erreicht werden.
Die Bildübertragung muss außerdem so eingestellt sein, dass ein Bezug oder Rückschluss zum Verhalten einzelner Personen auch über einen längeren Beobachtungszeitraum nicht möglich ist.[67] Um einen Personenbezug auszuschließen, sollte daher auf eine dauerhafte Bildübertragung verzichtet und stattdessen Einzelbilder dargestellt werden. Der Betrachter sollte Bilder nicht selbst aktualisieren können. Der Zeitraum einer automatischen Bildaktualisierung sollte so gewählt sein, dass z. B. die Wetter- oder Verkehrslage abgebildet oder ein Baufortschritt dokumentiert wird, ohne dass dabei ein Rückschluss auf einzelne Personen möglich ist. Eine laufende Bildübertragung ist in der Regel nicht erforderlich und nur zulässig, wenn ein Personenbezug komplett ausgeschlossen werden kann.

Werden Übersichtskameras *auch* zu dem Zweck eingesetzt, um vor Einbrüchen, Diebstählen oder Vandalismus zu schützen und um einzelne Personen oder Tatverdächtige im Nachhinein zu identifizieren oder Beweisaufnahmen eines Tathergangs zu erstellen, handelt es sich um eine herkömmliche Videoüberwachung. In diesem Fall sind alle gesetzlichen Voraussetzungen (ab Punkt 2) einzuhalten. Von einer Bildübertragung in Echtzeit im Internet ist dann abzusehen.

5.5. Dashcams

Dashcams (oder Unfallkameras) sind kleine Videokameras, die an einem Kraftfahrzeug

---

[66] Eine Videobeobachtung liegt dann nicht vor – s.o. Punkt 1.1.
[67] Auch ohne personenscharfe Aufnahmen einer Kamera ist ein Rückschluss auf einzelne Personen möglich. Beispielsweise, indem wiederkehrenden Verhaltens- und Bewegungsmuster mit Informationen zum Aufnahmeort und zur Aufnahmezeit verbunden werden.

oder Fahrrad befestigt sind und aus der Perspektive des Fahrers das Verkehrsgeschehen filmen. Die Kameras werden zu dem Zweck eingesetzt, Unfälle oder andere Vorfälle im Straßenverkehr aufzuzeichnen, um einen Unfallhergang dokumentieren und ggf. ein Verschulden des Unfallgegners nachweisen zu können.

Unzulässig ist der Einsatz solcher Dashcams dann, wenn das Verkehrsgeschehen im öffentlichen Raum permanent und anlasslos aufgezeichnet wird. Das anlasslose Filmen anderer Verkehrsteilnehmer und Passanten ist nicht nur ein geringfügiger Eingriff in Persönlichkeitsrechte der betroffenen Verkehrsteilnehmer.[68] Die Voraussetzungen für eine Videoüberwachung sind in einem solchen Fall regelmäßig nicht erfüllt. Bei einer dauerhaften und anlasslosen Videoaufzeichnung fehlt es schon am konkreten Zweck der Videoaufnahmen.[69] Eine dauerhafte Videoaufzeichnung ist daher nicht erforderlich, um das Beweissicherungsinteresse des Verantwortlichen zu wahren. Außerdem überwiegen bei einem solchen Kameraeinsatz die schutzwürdigen Interessen der Verkehrsteilnehmer und Passanten, die sich in der Nähe einer Straße aufhalten. Sie werden in der Regel gefilmt, ohne dass ein besonderer Anlass vorliegt und ohne dass sie von einer Videoüberwachung Kenntnis nehmen können.

Ein datenschutzkonformer Einsatz von Dashcams kommt nur in Betracht, wenn technische Möglichkeiten zum Einsatz gebracht werden, die sicherstellen, dass eine Kamera lediglich kurzzeitig anlassbezogen aufzeichnet.[70]

Die schutzwürdigen Interessen der Betroffenen überwiegen immer dann, wenn im ruhenden Verkehr der öffentliche Raum aus einem Fahrzeug heraus überwacht wird.[71] Der Betrieb einer Dashcam ist daher ausschließlich im fließenden Verkehr möglich.

Weitere Informationen wurden im „Positionspapier zur Unzulässigkeit von Videoüberwachung aus Fahrzeugen (sog. Dashcams)“ [72] veröffentlicht.

Daneben ist der Betreiber einer Dashcam gemäß Art. 12 ff. DS-GVO verpflichtet, transparente Informationen über seine Datenverarbeitung zur Verfügung zu stellen.
Der Betreiber einer Dashcam entscheidet über die Zwecke und Mittel der Datenverarbeitung und ist daher gem. Art. 4 Absatz 1 Nr. 7 der DS-GVO für die Verarbeitung der perso-

---

[68] Vgl. VG Ansbach, Urteil vom 12.08.2014 – Az. 4 K 13.01634.
[69] Vgl. BGH, Urteil vom 15.05.2018 – VI ZR 233/17.
[70] Vgl. BGH, Urteil vom 15.05.2018, a.a.O.
[71] Ist ein Fahrzeug im öffentlichen Raum geparkt, darf dieser Raum aus dem Fahrzeug heraus nicht überwacht werden; vgl. AG München, Urteil vom 9.08.2017 – 1112 OWi 300 Js 121012/17.
[72] Abzurufen unter https://www.datenschutzkonferenz-online.de/orientierungshilfen.html

nenbezogenen Daten verantwortlich. Er hat alle Pflichten zu erfüllen, die sich aus der DS-GVO ergeben. Betroffene können gegenüber dem Verantwortlichen ihre Rechte vollumfänglich geltend machen, beispielsweise ihr Recht auf Auskunft nach Art. 15 DS-GVO.

5.6. Tür- und Klingelkameras

Erfassen digitale Tür- oder Klingelkameras den *öffentlichen Raum,* können sie nur mit bestimmten technischen Einstellungen eingesetzt werden. Unbedenklich ist ein System, das eine Bildübertragung erst nach Betätigung der Klingel ermöglicht, eine dauerhafte Speicherung der Bildaufnahmen ausschließt, räumlich nicht mehr abbildet, als ein Blick durch einen Türspion gewähren würde, und das die Übertragung nach einigen Sekunden automatisch unterbricht. Eine dauerhafte und anlasslose Bildübertragung öffentlicher Räume muss technisch ausgeschlossen sein.[73]

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, erfüllt die rechtlichen Anforderungen an eine Videoüberwachung öffentlicher Räume in der Regel nicht.

5.7. Drohnen[74]

Kameradrohnen ermöglichen Blicke in fremde Gärten, Sonnenterrassen, Freibäder oder öffentliche Straßen und Plätze. Das Risiko ist groß, dass eine Kameradrohne im öffentlichen Raum in Persönlichkeitsrechte Dritter eingreift. Grundsätzlich dürfen Drohnen mit Foto- oder Videoausstattung daher nur eingesetzt werden, wenn Persönlichkeitsrechte Dritter nicht verletzt werden. Erfasst eine Drohne mit einer Kamera personenbezogene Daten im öffentlichen Raum, handelt es sich in der Regel um eine Datenverarbeitung im Anwendungsbereich der DS-GVO. Die gesetzlichen Voraussetzungen, die für eine solche mobile Datenverarbeitung gelten, können beim Einsatz einer Drohne kaum eingehalten werden. Das betrifft insbesondere Hinweispflichten, die eine Verarbeitung personenbezogener Daten kenntlich machen sollen.

---

[73] Zur Videoü*berwachung* nicht-öffentlicher Räume in privaten Wohnbereichen siehe auch Punkt 5.2.

[74] Siehe auch das Positionspapier zur Nutzung von Kameradrohnen durch nicht-öffentliche Stellen, veröffentlicht auf der Homepage der Datenschutzkonferenz unter https://www.datenschutzkonferenz-online.de/orientierungshilfen.html

Im Rahmen der geltenden Gesetze ist der Betrieb von Drohnen mit Film- und Videotechnik vor allem in städtischen Gebieten in der Regel kaum möglich. Zu beachten sind außerdem diverse weitere Rechtsvorschriften, die die Nutzung von Drohnen reglementieren. Ein Beispiel hierfür ist die Luftverkehrs-Verordnung (LuftVO). Diese enthält ein Verbot zum Betrieb unbemannter Luftfahrtsysteme und Flugmodelle an bestimmten Orten. Nach § 21b Absatz 1 Ziff. 2 der LuftVO ist der Betrieb von Drohnen u. a. über und in einem seitlichen Abstand von 100 Metern von Menschenansammlungen, Unglücksorten, Katastrophengebieten und anderen Einsatzorten von Behörden und Organisationen mit Sicherheitsaufgaben verboten. Zudem ist nach Ziff. 7 der gleichen Vorschrift u.a. auch der Betrieb von Drohnen, die elektronische Bildaufnahmen anfertigen können, über Wohngrundstücken verboten, wenn der betroffene Eigentümer oder sonstige Nutzungsberechtigte nicht ausdrücklich zugestimmt hat. Dadurch wird der zulässige örtliche Einsatzbereich von Kameradrohnen durch nicht-öffentliche Stellen von vornherein eingeschränkt.

5.8. Wildkameras

Die Landeswaldgesetze gestatten es grundsätzlich jedem, den Wald zum Zweck der Erholung zu betreten. Wird eine Waldfläche mit einer (Wild-) Kamera überwacht und besteht für diesen Bereich kein erkennbares Betretungsverbot, handelt es sich regelmäßig um eine Videoüberwachung öffentlicher Räume.

Bei einer Überwachung mittels Wildkamera ist den Persönlichkeitsrechten der betroffenen Waldbesucher, Spaziergänger und Wanderer ein hoher Stellenwert einzuräumen. Sie nutzen den Wald in ihrer Freizeit und um sich zu erholen. Waldbesucher müssen nicht mit einer (ggf. heimlichen oder versteckten) Kameraüberwachung rechnen. Liegt ein berechtigtes Interesse des Überwachenden vor, kann eine Videoüberwachung mit einer Wildkamera zulässig sein, wenn die Aufnahme von Menschen äußerst unwahrscheinlich ist und mit allen verfügbaren Mitteln vom Betreiber ausgeschlossen wird. Beispielsweise indem eine Kirr- oder Futterstelle nur unmittelbar auf Kniehöhe aufgenommen wird, d.h. die Kamera auf ungefähr einem Meter Höhe angebracht und direkt auf den Waldboden oder eine Futterstelle ausgerichtet ist. Bereiche, die sich in unmittelbarer Nähe zu einem Waldweg, einer Grillstelle und insbesondere einem Spielplatz befinden, dürfen nicht überwacht werden. Der überwachte Bereich sollte für Waldbesucher erkennbar mit einem Betretungsverbot ausgeschildert sein. Hinweise auf eine Kameraüberwachung mit der Angabe des Verantwortlichen (Anlage 1) sind in jedem Fall erforderlich.[75] Die Kamera ist technisch so einzustellen, dass keine Videosequenzen, sondern Einzelbilder mit einigen Sekunden Ab-

[75] S.o. Punkt 3.3.

stand aufgenommen werden. Die Auflösung der Kamera sollte gering gewählt sein. Ist eine Überwachung von Tieren in der Nacht geplant, ist die Kamera tagsüber auszuschalten. Vor dem Einsatz einer Wildkamera müssen zudem immer mildere Mittel geprüft werden, beispielsweise der Einsatz von Wilduhren.

6. Checkliste für den Betreiber

Planen Sie die Installation von Videokameras oder betreiben Sie bereits eine Videoüberwachungsanlage? Folgende Fragen sollten Sie für die Überwachungsmaßnahme beantworten können:

1. Welche Bereiche sollen überwacht werden?
   Z.B.:
   - öffentlicher Raum (z.B. Kundenbereiche);
   - Mitarbeiterräume;
   - öffentliche Flächen (z.B. Gehwege)

2. Welcher Zweck wird mit der (jeweiligen Videokamera verfolgt?

   Dient die Überwachung einem berechtigten Interesse?

   Besteht eine Gefährdungslage und auf welche Tatsachen, z.B. Vorkommnisse in der Vergangenheit, gründet sich diese?

3. Wurde der Zweck der Videoüberwachung dokumentiert?

4. Warum ist die Videoüberwachung geeignet, den festgelegten Zweck zu erreichen?

5. Warum ist die Videoüberwachung *erforderlich* und warum gibt es keine milderen Mittel, die für das Persönlichkeitsrecht der Betroffenen weniger einschneidend sind?

6. Welche schutzwürdigen Interessen der Betroffenen haben Sie mit welchem Ergebnis in die Interessenabwägung einbezogen?

7. Ist eine Beobachtung der Bilder auf einem Monitor ohne Speicherung der Bilddaten ausreichend? Wenn nein, warum nicht?

8. Sofern die Bilder gespeichert werden, wann werden die Aufnahmen gelöscht? Werden die Aufnahmen länger als 72 Stunden gespeichert? Wie begründen Sie die spätere Löschung?

9. Zu welchen Zeiten erfolgt die Videoüberwachung und wer hält sich üblicherweise zu dieser Zeit im überwachten Bereich auf?

10. Wenn eine Videoüberwachung rund um die Uhr erfolgt, warum ist dies erforderlich bzw. warum kann sie nicht zeitlich eingeschränkt werden, z.B. auf außerhalb der Geschäftszeiten oder die Nachtstunden?

11. Werden bestimmte Bereiche der Überwachung ausgeblendet oder verpixelt? Wenn nein, warum nicht?

12. Über welche technischen Möglichkeiten verfügt die Videokamera und welche hiervon sind für die Überwachung nicht erforderlich und ggfs. zu deaktivieren?

    - hinsichtlich der Ausrichtung, z.B. schwenkbar oder variabel, Dome-Kamera
    - bezüglich der Funktionalität, z.B. Zoomobjektive, Funkkameras, Audiofunktion, Fernzugriff

13. Wurde eine Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO durchgeführt? Wenn nein, warum ist eine Datenschutz-Folgenabschätzung nicht erforderlich?

14. Wird auf die Videoüberwachung so hingewiesen, dass betroffene Personen vor Betreten des überwachten Bereichs den Umstand der Beobachtung erkennen können? Beinhaltet der Hinweis alle wesentlichen Informationen?

15. Wurde daneben ein umfassender Hinweis erstellt und wo können Betroffene diesen erhalten?

16. Unter welchen Voraussetzungen wird Einsicht in die Aufnahmen genommen? und durch wen?

    Ist die Protokollierung aller Zugriffe sichergestellt?

    Wurden die zugriffsberechtigten Personen auf das Datengeheimnis verpflichtet?

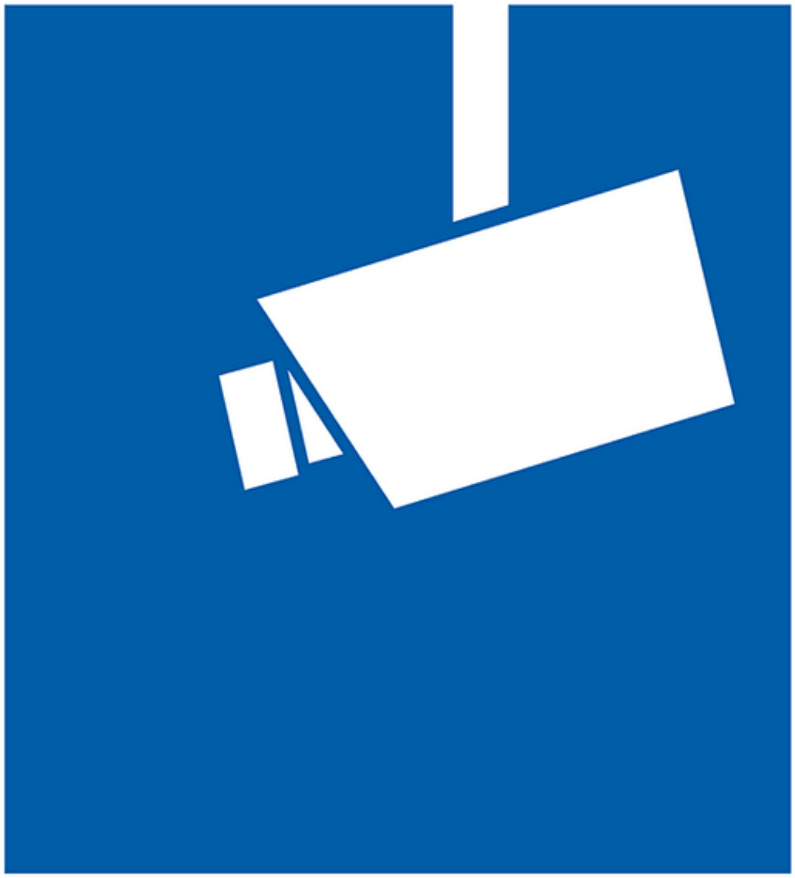
17. Wurden die technisch-organisatorischen Maßnahmen zum Schutz der Daten nach Art. 25 und Art. 32 DS-GVO getroffen und dokumentiert?

18. Sofern hier relevant: Gibt es im Unternehmen einen Betriebsrat und wurde mit diesem eine Betriebsvereinbarung zur Videoüberwachung abgeschlossen?

Rein vorsorglich weisen wir darauf hin, dass die aufgelisteten Fragen nicht abschließend sind und dass eine Befassung mit diesen Fragen nicht automatisch zur Zulässigkeit der Videoüberwachung führt.

Haben Sie zu dem Betrieb der Videoüberwachungsanlage konkrete Fragen, können Sie sich gerne an die für Sie zuständige Datenschutzaufsichtsbehörde wenden. Maßgeblich ist gem. § 40 Abs. 2 BDSG die (Haupt-)Niederlassung des Verantwortlichen. Eine Übersicht über die Kontaktdaten erhalten Sie unter https://www.datenschutzkonferenz-online.de/datenschutzaufsichtsbehoerden.html.

Anlage 1 – Vorgelagertes Hinweisschild



Achtung

Videoüberwachung!

Name und Kontaktdaten des Verantwortlichen und ggf. seines Vertreters:

Kontaktdaten des Datenschutzbeauftragten (sofern vorhanden):

Zwecke und Rechtsgrundlage der Datenverarbeitung:

Berechtigte Interessen:

Weitere Informationen erhalten Sie:

- per Aushang (wo genau?)
- an unserer Kundeninformation / Rezeption/Kasse im Erdgeschoss

***Speicherdauer oder Kriterien für die* Festlegung der Dauer:**

Hinweis: Die Informationen sind unentgeltlich in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache bereitzustellen. Sie können in Kombination mit standardisierten Bildsymbolen bereitgestellt werden (vgl. Art. 12 DSGVO). Um Lesbarkeit zu erreichen, sollte der Ausdruck mindestens in DIN A4 erfolgen.

Anlage 2 – Vollständiges Informationsblatt

Sie finden diese Informationen zusätzlich im Internet unter…

Name und Kontaktdaten des Verantwortlichen und ggf. seines Vertreters:

Kontaktdaten des Datenschutzbeauftragten (sofern vorhanden):

Zwecke und Rechtsgrundlage der Datenverarbeitung:

Berechtigte Interessen, die verfolgt werden:

Speicherdauer oder Kriterien für die Festlegung der Dauer:

Empfänger oder Kategorien von Empfänger der Daten (sofern Datenübermittlung stattfindet):

bei Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln: Informationen über Angemessenheitsbeschluss der Kommission bzw. geeignete oder angemessene Garantien:

Hinweise auf die Rechte der Betroffenen

Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein **Recht auf Auskunft** über diese personenbezogenen Daten und auf die in Art. 15 DSGVO im einzelnen aufgeführten Informationen.

Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die **Berichtigung** sie betreffender unrichtiger personenbezogener Daten und ggf. die **Vervollständigung** unvollständiger personenbezogener Daten zu verlangen (Art. 16 DSGVO).

Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, sofern einer der in Art. 17 DSGVO im einzelnen aufgeführten Gründe zutrifft, z. B. wenn die Daten für die verfolgten Zwecke nicht mehr benötigt werden (**Recht auf Löschung**).

Die betroffene Person hat das Recht, von dem Verantwortlichen die **Einschränkung der Verarbeitung** zu verlangen, wenn eine der in Art. 18 DSGVO aufgeführten Voraussetzungen gegeben ist, z. B. wenn die betroffene Person Widerspruch gegen die Verarbeitung eingelegt hat, für die Dauer der Prüfung durch den Verantwortlichen.

Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten **Widerspruch** einzulegen. Der Verantwortliche verarbeitet die personenbezogenen Daten dann nicht mehr, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (Art. 21 DSGVO).

Jede betroffene Person hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs das **Recht auf Beschwerde bei einer Aufsichtsbehörde**, wenn die betroffene Person der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen die DSGVO verstößt (Art. 77 DSGVO). Die betroffene Person kann dieses Recht bei einer Aufsichtsbehörde in dem Mitgliedstaat ihres Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes geltend machen. In (Bundesland) ist die zuständige Aufsichtsbehörde: ***(…)***

Hinweis: Die Informationen sind unentgeltlich in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache bereitzustellen. Sie können in Kombination mit standardisierten Bildsymbolen bereitgestellt werden (vgl. Art. 12 DSGVO). Um Lesbarkeit zu erreichen, sollte der Ausdruck mindestens in DIN A3 erfolgen.