Achtung Kamera!

Hinweise zur Videoüberwachung
für Bürgerinnen und Bürger, Wirtschaft und Behörden

Meine Daten.
Meine Freiheit.

SÄCHSISCHE
DATENSCHUTZ- UND
TRANSPARENZBEAUFTRAGTE

Freistaat
SACHSEN

Achtung Kamera!

Hinweise zur Videoüberwachung
für Bürgerinnen und Bürger,
Wirtschaft und Behörden

Stand: 9. November 2023

Liebe Leserinnen und Leser,

wohl bei kaum einem anderen Thema ist die Relevanz von Datenschutz so nachvollziehbar wie bei der Videoüberwachung. Wer kennt es nicht, das Gefühl, wenn man von einer fremden Kamera beobachtet wird? Viele Menschen empfinden dabei einen unangenehmen Überwachungsdruck, gepaart mit den Botschaften: „Hier ist es gefährlich" oder „Ich traue dir nicht, du könntest auch eine Straftat begehen, weshalb ich dich lieber mal im Auge behalte."

Wissenschaftlich ist es erwiesen: Wenn wir uns beobachtet fühlen, verstellen wir uns. Dieses Phänomen heißt in der Fachsprache „Chilling-Effekt". Indem wir unter Beobachtung unser Verhalten ändern, verlieren wir zugleich die Freiheit, wir selbst zu sein – ein immenser Eingriff in die Privatsphäre. Und genau deshalb ist Videoüberwachung nicht permanent und flächendeckend, sondern nur unter bestimmten Voraussetzungen oder auch gar nicht zulässig. Das gilt sowohl für öffentliche Stellen, wie Kommunen oder die Polizei, als auch für nichtöffentliche Stellen, zum Beispiel Privatpersonen, Unternehmen und Vereine.

Trotz hoher rechtlicher Auflagen begegnen uns heutzutage allerorten und nahezu täglich Videokameras: an Haustüren und Wohngebäuden, bei Tankstellen, in Geschäften und auf Baustellen, in Autos (Dashcams), auf Demonstrationen, im öffentlichen Personennahverkehr, im Wald (Wildkameras) und an vielen anderen Orten. Gefühlt nimmt die Videoüberwachung im Alltag zu, was sicherlich auch am technischen Fortschritt sowie an der Verfügbarkeit und dem Preisverfall der Kameratechnik liegt. Nicht zu vergessen ist auch, dass Videokameras nicht nur in der politischen Diskussion oftmals als Allheilmittel gelten. Was liegt da näher, als sich selbst auch eine Videokamera anzuschaffen, wo doch bereits in der Nachbarschaft mehrere angebracht sind?

Dabei werden selbst von einfachen Videoüberwachungsanlagen große Mengen an personenbezogenen Daten verarbeitet: Wer ist wann wie lange an welchem Ort? Was macht

diese Person dort? Wie verhält sie sich? Von wem wird sie begleitet oder wen trifft sie da? In welchem Zustand befindet sich die Person und wie ist ihr Erscheinungsbild?

Auf diese und viele weitere Informationen haben Kamerabetreibende – im Fachjargon der „Verantwortliche" – Zugriff. In den allermeisten Fällen sind diese Daten für den Überwachungszweck jedoch völlig irrelevant. Nicht selten – vor allem bei nichtöffentlichen Stellen – ist diese Datenverarbeitung sogar rechtswidrig und damit ein Fall für die zuständige Datenschutzaufsichtsbehörde.

Seit Jahren verzeichnet meine Dienststelle ein hohes Geschäftsaufkommen in diesem Tätigkeitsbereich. Meist reicht eine von der Überwachung betroffene Person eine Beschwerde ein, der ich als Sächsische Datenschutz- und Transparenzbeauftragte nachgehe – ein durchaus aufwendiges Verfahren für alle Beteiligten: für den Verantwortlichen, die betroffene Person, meine Mitarbeiterinnen und Mitarbeiter und manchmal auch für Strafverfolgungsbehörden und Gerichte. Nicht selten resultiert aus einem Verfahren ein Bußgeld. Auch Schadensersatzklagen der betroffenen Personen sind möglich.

Das alles können sich Verantwortliche ersparen, indem sie sich vor dem Kauf einer Überwachungskamera mit den datenschutzrechtlichen Anforderungen befassen. Dabei soll die vorliegende Broschüre unterstützen. Sie richtet sich aber nicht nur an (potenzielle) Kamerabetreibende, sondern ebenso an die überwachten Personen.

Diese Broschüre soll auch einen Beitrag dazu leisten, manche Missverständnisse und sich hartnäckig haltende Vorstellungen richtigzustellen, mit denen sich nicht wenige Verantwortliche auf der rechtlich sicheren Seite wähnen. So herrscht noch immer der Eindruck vor, dass erst bei der Anfertigung von Videoaufzeichnungen personenbezogene Daten verarbeitet werden. Oder Verantwortliche argumentieren, dass sie doch keine öffentlichen Verkehrsbereiche überwachen würden und im Übrigen in der Überwachung ihres eigenen Grundstücks frei seien. Nicht zuletzt erlebe ich immer wieder, dass Verantwortliche davon ausgehen, allein das Anbringen

eines Hinweisaufklebers – oftmals nur in Form eines Kamerapiktogramms – würde ausreichen, um eine Videoüberwachung zu legalisieren.

Auf der anderen Seite machen die sich an mich wendenden betroffenen Personen häufig geltend, dass sie vor der Installation einer Videokamera nicht informiert und ihre Einwilligung nicht eingeholt worden sei, wodurch die Videoüberwachung mangels ausdrücklichen Einverständnisses rechtswidrig wäre.

Anhand verschiedener Verarbeitungssituationen werden in dieser Broschüre insbesondere die Grenzen der Videoüberwachung durch nichtöffentliche Stellen sowie durch Kommunen und die Polizei aufgezeigt. Außerdem erfahren Sie, welche Pflichten Kamerabetreibende zu erfüllen haben. Diese Broschüre enthält zudem zahlreiche Verweise auf weiterführende Informationen und Vorlagen. So hat bereits die unabhängige Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) in den zurückliegenden Jahren eine Reihe an Orientierungshilfen und Dokumenten zur Videoüberwachung herausgegeben. Diese bilden auch die Grundlage für diese Broschüre.

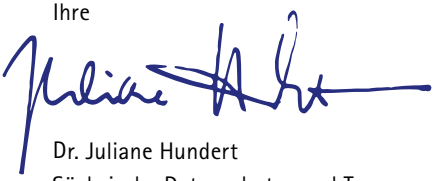
Wenn Sie sich das erste Mal mit den datenschutzrechtlichen Regelungen zur Videoüberwachung beschäftigten, werden Sie feststellen, dass diese durchaus komplex sind. Daher möchte ich Ihnen, insbesondere, wenn Sie als Privatperson, Unternehmen oder Verein selbst eine Videoüberwachung einsetzen (möchten), noch folgende Hinweise und Denkanstöße mitgeben:

1. Beschäftigen Sie sich zunächst mit den Inhalten dieser Broschüre, insbesondere mit Kapitel 1 „Videoüberwachung durch nichtöffentliche Stellen".
2. Binden Sie bei Ihrem Vorhaben eine/n Datenschutzbeauftragte/n oder einen externen Sachverständigen (z. B. einen Fachanwalt/eine Fachanwältin für Datenschutzfragen) ein.
3. Haben Sie Zweifel, ob Ihre Videoüberwachung zulässig ist, verzichten Sie lieber auf den Kameraeinsatz.

Denn: Kameras sind kein Allheilmittel, verhindern keine Straftaten und sorgen nur gefühlt für mehr Sicherheit. Andernfalls gäbe es in videoüberwachten Städten wie London kaum noch Überfälle, Einbrüche oder Vandalismus. Ebenso bleiben Tankstellen, Banken und Juweliergeschäfte nicht davon verschont – trotz umfangreicher Aufzeichnung. Auch löst eine Videokamera keine Konflikte mit den Nachbarn, sondern trägt eher zur Eskalation bei.

Meiner Erfahrung nach haben selbst sehr hochwertige Kameras im gewerblichen Bereich nur in Ausnahmefällen dazu geführt, dass der oder die Täter/innen ermittelt werden konnten. Um sich zu schützen, gibt es in den allermeisten Fällen bessere Möglichkeiten als eine Videoüberwachung. Einige Anregungen finden Sie an passender Stelle auf den folgenden Seiten. Schauen Sie gern auch auf meiner Website vorbei. Ich freue mich, wenn Ihnen das Informationsangebot weiterhilft: www.datenschutz.sachsen.de

Ihre



Dr. Juliane Hundert
Sächsische Datenschutz- und Transparenzbeauftragte

Inhaltsverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

Nachstehend werden Abkürzungen nach der alphabetischen Reihenfolge aufgeführt.

Vorschriften

a. F.	alte Fassung
Abs.	Absatz
Art.	Artikel
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
Buchst.	Buchstabe
DGUV	Deutsche Gesetzliche Unfallversicherung
DSGVO	Datenschutz-Grundverordnung
EuGH	Europäischer Gerichtshof
GG	Grundgesetz
Nr.	Nummer
SächsDSDG	Sächsisches Datenschutzdurchführungsgesetz
SächsPBG	Sächsisches Polizeibehördengesetz
SächsPVDG	Sächsisches Polizeivollzugsdienstgesetz
SächsVersG	Sächsisches Versammlungsgesetz
StGB	Strafgesetzbuch

1 Videoüberwachung durch nichtöffentliche Stellen

1.1 Grundsätzliches

1.1.1 Was versteht man unter Videoüberwachung?

Eine **Videoüberwachung** liegt dann vor, wenn mithilfe optisch-elektronischer Einrichtungen personenbezogene Daten (Bild- und/oder Audiodaten) verarbeitet werden. Entscheidend für die datenschutzrechtliche Einordnung ist es, dass personenbezogene Daten automatisiert verarbeitet werden (siehe Art. 2 Abs. 1 DSGVO).

Neben handelsüblichen Überwachungskameras zählen alle Geräte, die zur längerfristigen Beobachtung und somit für einen Überwachungszweck eingesetzt werden (können), zu den **optisch-elektronischen Einrichtungen**. Eine Videoüberwachung kann daher auch vorliegen, wenn zum Beispiel mit Webcams, Smartphones, Dashcams, Drohnen, Wildkameras sowie Tür- und Klingelkameras gefilmt wird. Entscheidend ist allein der Überwachungszweck. Unerheblich ist, ob eine Kamera fest montiert, veränderbar (Schwenk-, Neig-, Zoomfunktion) oder frei beweglich bzw. mobil einsetzbar ist.

Um **personenbezogene Daten** (Art. 4 Nr. 1 DSGVO) handelt es sich dann, wenn einzelne Personen auf den Bildern eindeutig zu erkennen sind oder Videoaufnahmen Rückschlüsse auf die Identität der bzw. des Gefilmten ermöglichen. Personen können regelmäßig identifiziert werden, wenn Gesichtszüge erkennbar abgebildet sind. Auch aus den Begleitumständen kann sich ein Bezug zu einer bestimmten Person ergeben, beispielsweise durch die Kleidung, ein bestimmtes

Körperbild, mitgeführte Gegenstände, besondere oder einzigartige Verhaltensweisen, zusätzliche Audioaufnahmen oder durch eine Kombination entsprechender Informationen (Ort, Datum, Zeit, Verhalten etc.).

Eine Verarbeitung im Sinne des Datenschutzrechts (Art. 4 Nr. 2 DSGVO) liegt bereits dann vor, wenn (nur) **Livebilder** (Monitoring bzw. Echtzeitüberwachung; siehe auch 2.6.1, Seite 54) betrachtet werden (Erfassung). Erst recht gilt dies für die Erstellung von **Videoaufzeichnungen** (Speicherung) und deren anschließende Verwendung (Sichtung, Weitergabe an Dritte, Ausdruck etc.). Eine personenbezogene Aufnahme liegt auch dann vor, wenn 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/die Kamerabetreiber/in die Videoaufzeichnungen später ungesehen löscht (Speicherung auf Vorrat) oder wenn Videokameras nur im Bedarfs- oder Alarmfall aufzeichnen.

Eine Verarbeitung personenbezogener Daten in Form der Videoüberwachung natürlicher Personen greift unmittelbar in das vom Bundesverfassungsgericht anerkannte **Grundrecht auf informationelle Selbstbestimmung** ein (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz). Dieses Grundrecht als besondere Ausprägung des allgemeinen Persönlichkeitsrechts verbürgt das Recht jedes Einzelnen, selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu entscheiden. Im Gegensatz zu einer Livebeobachtung kommt bei der Speicherung eingriffsverschärfend hinzu, dass betroffene Personen nicht mehr kontrollieren können, was im weiteren Verlauf mit ihren personenbezogenen Daten geschieht.

1.1.2 Zählt Livebeobachtung (Monitoring) ohne Aufzeichnung auch zur Videoüberwachung?

Ja. Der Begriff der Videoüberwachung umfasst sowohl die Videobeobachtung als Erfassungsvorgang (siehe Art. 4 Nr. 2 DSGVO), bei der eine Liveübertragung der Bilder auf einen

Monitor oder auch ein Smartphone erfolgt, als auch die Videoaufzeichnung, bei der Aufnahmen gespeichert und später ausgelesen werden können. Dem liegt der weite Verarbeitungsbegriff der DSGVO zugrunde, der den gesamten Werdegang der Daten abbildet und ausgehend von der Erhebung über die Speicherung und Weiterleitung bis zu deren Löschung reicht. Dementsprechend werden nicht nur bei der Speicherung und weiteren Verwendung, sondern bereits bei der Sichtung von Livebildern personenbezogene Daten verarbeitet.

1.1.3 Gelten die Datenschutzvorschriften auch bei Kameraattrappen?

Kameraattrappen enthalten keine technischen Komponenten, mit denen personenbezogene Daten erfasst und gespeichert werden können. Daher sind bei diesen die Vorschriften der DSGVO und des BDSG nicht anwendbar. Sie erwecken lediglich den Eindruck, dass Bild- und Videodaten von Personen verarbeitet werden und eine Überwachung stattfindet. Der einzige Zweck einer Kameraattrappe liegt somit darin, das Verhalten von Menschen in eine gewünschte Richtung zu lenken.

Ist eine tatsächlich funktionstüchtige Videokamera nicht in Betrieb, will also der/die Betreiber/in damit lediglich einen Kamerabetrieb vortäuschen, ist die rechtliche Wertung gleich der einer Kameraattrappe. Entscheidend für die Frage der Anwendbarkeit der Datenschutzvorschriften und damit auch für die Kontrollzuständigkeit der Sächsischen Datenschutz- und Transparenzbeauftragten sind nicht die technischen Möglichkeiten, sondern nur, ob eine Videokamera tatsächlich in Betrieb ist oder nicht.

Die Hinweispflichten und andere datenschutzrechtliche Vorgaben gelten infolgedessen für Kameraattrappen nicht. Obwohl tatsächlich niemand gefilmt wird, erzeugen täuschend echte Kameragehäuse dennoch einen erheblichen Überwachungsdruck. Müssen Dritte eine Überwachung aufgrund der tatsächlichen objektiven Gegebenheiten befürchten, kann der erzeugte Verhaltensdruck für eine Verletzung der Persönlichkeitsrechte ausreichen. Wer eine Attrappe zur Verhaltens-

steuerung Dritter einsetzt, muss also damit rechnen, dass zivilrechtliche Abwehransprüche (beispielsweise auf Unterlassung, Beseitigung oder Schadensersatz) gegen ihn oder sie geltend gemacht werden. In der Zivilrechtsprechung werden Kameraattrappen kaum anders bewertet werden als dem Datenschutzrecht unterfallende funktionstüchtige, tatsächlich aufzeichnende Kameras. Den Betroffenen sind insoweit nach den §§ 823, 1004 BGB je nach konkreter Sachlage Entschädigungs-, Beseitigungs- oder Unterlassungsansprüche zuerkannt worden, allerdings müssen diese dafür selbst tätig werden.

1.1.4 Wann ist Videoüberwachung erlaubt?

Mit einer optisch-elektronischen Einrichtung dürfen personenbezogene Daten nur verarbeitet werden, wenn eine gesetzliche Grundlage dies erlaubt. Die DSGVO enthält für Videoüberwachungen durch Privatpersonen, Unternehmen, Vereine und andere nichtöffentliche Stellen keine spezielle Regelung. In diesem Fall gelten die allgemeinen datenschutzrechtlichen Vorgaben an eine Verarbeitung personenbezogener Daten.

Demzufolge ist als Rechtsgrundlage für solche Datenverarbeitungen regelmäßig die Vorschrift des Art. 6 Abs. 1 Buchst. f DSGVO heranzuziehen. Danach ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Zunächst muss also ein berechtigtes Interesse des Verantwortlichen vorliegen. Jedoch reicht dieses allein für eine zulässige Videoüberwachung nicht aus. Die Videoüberwachung muss darüber hinaus auch erforderlich sein, um damit den Überwachungszweck zu erreichen. Schließlich dürfen die Belange der betroffenen Personen in der Abwägung mit dem Betreiberinteresse nicht überwiegen.

1. Das **berechtigte Interesse** bezieht sich auf das konkrete Ziel, das mit der Videoüberwachung verfolgt wird. Bei einer Videoüberwachung besteht dieses beispielsweise in der Abschreckung potenzieller Straftäter/innen (präventiv) oder der Aufklärung von Straftaten (repressiv/Beweissicherung). Den diesen Interessen übergeordneten Zweck bildet zumeist der Eigentums- oder Personenschutz oder die Ausübung des Hausrechts.
   Das geltend gemachte Interesse darf nicht spekulativ sein; es muss auf Tatsachen, beispielsweise einer konkreten Gefährdungslage, die das allgemeine Lebensrisiko übersteigt, beruhen. Dies ist dann gegeben, wenn tatsächliche und nachweisbare Ereignisse für eine konkrete Gefährdung vorliegen. Im Gegensatz dazu reichen rein subjektive Befürchtungen oder Unsicherheitsgefühle zur Begründung einer konkreten Gefährdungslage nicht aus. Nur ausnahmsweise ist der Nachweis einer abstrakten Gefahrenlage anzuerkennen. Dies betrifft wegen der Art ihrer Geschäftstätigkeit typischerweise besonders gefährdete Unternehmen wie beispielsweise Juweliere oder Tankstellen.
2. Das Tatbestandsmerkmal der **Erforderlichkeit** ist auf der Grundlage des Verhältnismäßigkeitsprinzips zu bestimmen. Erforderlich bzw. verhältnismäßig im Sinne einer Beschränkung des allgemeinen Persönlichkeitsrechts kann eine Videoüberwachung nur sein, wenn sie geeignet, erforderlich und angemessen ist.
   Zunächst einmal muss die Videoüberwachung den erstrebten Zweck also überhaupt verwirklichen können, das heißt zur Zweckerreichung geeignet sein. Die Videoüberwachung muss zumindest einen Beitrag zu dem angestrebten Zweck leisten können.
   Die Erforderlichkeit im engeren Sinn ist dann nicht gegeben, wenn sich der beabsichtigte Zweck auch mit einem anderen – milderen – Mittel erreicht lässt, das weniger in die Rechte der betroffenen Personen eingreift und dabei wirtschaftlich und organisatorisch

auch zumutbar ist. Wirksame Alternativen zur Videoüberwachung können beispielsweise sein:

- eine Umzäunung des Grundstücks
- eine herkömmliche Alarmanlage (Einbruchmeldeanlage) mit Tür- und Fenstersensoren, Bewegungs- oder Glasbruchmelder, Lichtschranken sowie einer akustischen oder optischen Sirene
- regelmäßige Kontrollgänge von Bewachungspersonal (bei Gewerbeobjekten)
- Zugangs- und Zutrittssicherungen
- Wertschließfächer (in Arztpraxen, Fitnessstudios, o. Ä.)
- helle und durchgehende Beleuchtung
- der Einbau von Sicherheitsschlössern
- einbruchsichere Fenster und Türen
- spezielle Oberflächenbeschichtungen oder Folien (Graffiti)

Die Prüfung der Angemessenheit betrifft die Verhältnismäßigkeit im engeren Sinn. Es ist eine Interessenabwägung auf der Grundlage der betroffenen Grundrechtspositionen vorzunehmen; der beabsichtigte Zweck darf nicht außer Verhältnis zu der Schwere des Eingriffs stehen. Dazu gehört beispielsweise auch, den räumlichen und zeitlichen Umfang einer Videoüberwachung auf das unbedingt notwendige Maß zu beschränken. So ereignen sich Einbrüche oftmals in den Abend- oder Nachtstunden, folglich ginge eine permanente Videoüberwachung zu weit. Oder Beschädigungen finden aufgrund von Erfahrungen aus der Vergangenheit nur an einzelnen Stellen eines Grundstücks statt, was gegen eine weiträumige Videoüberwachung spricht.

3. Auch wenn eine Videoüberwachung zur Wahrung eines berechtigten Interesses des Verantwortlichen oder eines Dritten erforderlich ist, ist sie nur dann zulässig, wenn bei der **Interessenabwägung** die schutzwürdigen 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.
Je nach Art und Weise einer Datenverarbeitung ist der **Eingriff** in die Rechte und schutzwürdigen Belange der Betroffenen mehr oder weniger intensiv. Kriterien hierfür sind unter anderem,

- ob eine Videoaufnahme anlassbezogen oder anlasslos erfolgt,
- ob es eine zeitliche Beschränkung gibt oder die Videoüberwachung ununterbrochen, also dauerhaft, erfolgt,
- welche räumlichen Bereiche überwacht werden (z. B. Gemeinschaftsbereiche eines Mietshauses oder private Parkflächen auf dem eigenen Grundstück),
- ob ein reines Monitoring stattfindet oder die Bilder dauerhaft gespeichert werden,
- welche technischen Funktionen (z. B. Pre-Recording, Nachtsicht, Fernzugriff, Zoom- und Schwenkbarkeit) und Kameraeinstellungen (z. B. optische Auflösung einer Kamera) bestehen,
- welche Personenkreise betroffen sind, wobei dem Schutz von Kindern ein besonders hoher Stellenwert zukommt und bei einer (Teil-)Erfassung von Beschäftigten im Sinne der Definition des § 26 Abs. 8 BDSG spezielle Voraussetzungen gelten,
- welche Folgen die Überwachung für die betroffene Person hat, also ob sie Überwachungsmaßnahmen ausweichen kann und ob diese dauerhaft erfolgen (z. B. bei einer ständigen Überwachung von Zufahrten und Ein- und Ausgängen von Gebäuden, wenn Besucher und Beschäftigte gezwungen sind, diese zu nutzen),
- welche vernünftigen Erwartungen die betroffenen Personen haben – diese können sich aus objektiven Umständen ergeben (z. B. aus der jeweiligen Transparenz der Datenverarbeitung und der Sozialsphäre des

überwachten Bereichs), das heißt, ob die Videoüberwachung in bestimmten Bereichen typischerweise gesellschaftlich akzeptiert oder abgelehnt wird.

Generell gilt Folgendes:

- Der Hinweis auf eine Videoüberwachung allein hat keine Auswirkungen auf die vernünftigen Erwartungen der betroffenen Personen und damit die Rechtmäßigkeit der Videoüberwachung.
- Typischerweise akzeptiert ist beispielsweise die Videoüberwachung an einer **Tankstelle**, in einem **Juweliergeschäft**, in einer **Bank** oder an einem **Bankautomaten**. Nicht erwartet wird eine Überwachung beispielsweise in **Wäldern**, in **Sanitärbereichen**, **Sport-**, **Schwimm- oder Sauna-Einrichtungen**.
- 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 freie Entfaltung der Persönlichkeit im Vordergrund. Daher überwiegen in **Freizeiteinrichtungen und Gastronomiebetrieben** regelmäßig die schutzwürdigen Interessen der betroffenen Personen die Interessen des Kamerabetreibers bzw. der Kamerabetreiberin.
- Beobachtungen, die die **Intimsphäre** von Betroffenen berühren, etwa die Überwachung von Toiletten, Saunen, Duschen und Umkleidekabinen oder -bereichen oder deren Vorräumen, sind regelmäßig unverhältnismäßig und damit unzulässig.
- Insbesondere in **Sicherheitsfragen** sind die Interessen des Verantwortlichen erheblich, wenn die Maßnahme höherrangige Rechtsgüter (Leben, Gesundheit oder Freiheit) schützen soll und der Verhinderung und Aufdeckung strafrechtsrelevanter Vorfälle dient. Dagegen überwiegt das Interesse am Schutz vor **Bagatelldelikten** das Interesse der betroffenen Personen regelmäßig nicht.

1.1.5 Wie lange dürfen die Daten gespeichert werden?

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 Abs. 1 Buchst. a DSGVO). Das kann beispielsweise der Fall sein, wenn eine Gefahr nicht weiter abgewendet werden muss oder eine Beweissicherung nicht mehr notwendig ist. Ist es zu keinem Ereignis, beispielsweise einem Überfall oder Diebstahl, gekommen, dann werden die Videoaufzeichnungen auch für Beweiszwecke nicht mehr benötigt.

Die **Speicherdauer** wird begrenzt durch den Grundsatz der Datenminimierung (Art. 5 Abs. 1 Buchst. c DSGVO). Im Einzelfall wird ein Zeitraum von maximal 72 Stunden als zulässige Höchstspeicherdauer erachtet. In dieser Zeit kann der Verantwortliche regelmäßig feststellen, ob es Schäden an überwachten Objekten, Einrichtungen oder Übergriffe auf Personen gegeben hat. Ist dies der Fall, lässt sich eine Sicherung des relevanten Videomaterials vornehmen und so eine (automatische) Löschung der wesentlichen Sequenzen unterbinden.

Entscheidend ist der Einzelfall. Von den vorab dargestellten Vorgaben kann es Ausnahmen geben: Unter Umständen kann ein besonderer Überwachungszweck eine **längere Speicherung** rechtfertigen, wenn beispielsweise ein spezieller Sachverhalt nachvollzogen werden muss, der sich über einen längeren Zeitraum erstreckt. Eine verlängerte Speicherdauer gilt dabei nur für diejenigen Kameras, die einen besonderen Überwachungszweck verfolgen oder für die eine besondere Begründung vorliegt. Außerdem kommt sie nur für die Zeiten infrage, in denen dieser besondere Grund oder Zweck tatsächlich vorliegt. Keinesfalls darf sie etwa als Standard-Speicherdauer auf alle Kameras übertragen werden. Je länger jedoch die Speicherdauer gewählt wird, desto höher ist der Begründungsaufwand aufseiten des Verantwortlichen. Die Speicherdauer darf beispielsweise an Wochenenden, in den Ferien oder in den Urlaubszeiten verlängert werden, wenn eine Kontrolle

der überwachten Bereiche innerhalb der zulässigen Höchstspeicherdauer von 72 Stunden aus nachvollziehbaren und dokumentierten Gründen nicht möglich oder unzumutbar ist. Allein mit internen Arbeitsabläufen können längere Speicherfristen in der Regel aber nicht begründet werden.

1.1.6 Was muss der Verantwortliche bei einer Videoüberwachung dokumentieren und nachweisen können?

a) Rechenschaftspflicht

Der Verantwortliche muss in der Lage sein, die Einhaltung der Grundsätze des Art. 5 Abs. 1 DSGVO gegenüber der zuständigen Datenschutzaufsichtsbehörde nachzuweisen („Rechenschaftspflicht"). Hierzu gehören 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 DSGVO
- die Umsetzung geeigneter technischer und organisatorischer Maßnahmen in einem IT-Sicherheitskonzept nach Art. 32 DSGVO
- die Datenschutz-Folgenabschätzung nach Art. 35 Abs. 7 DSGVO
- genehmigte Verhaltensregeln gemäß Art. 40 DSGVO
- die Dokumentation eines erfolgreich durchlaufenen Zertifizierungsverfahrens gemäß Art. 42 DSGVO
- den Datenschutz mittels Technikgestaltung oder mittels datenschutzfreundlicher Voreinstellungen nach Art. 25 DSGVO

Videoüberwachung auf Einwilligungsbasis ist in der Praxis bei einer Vielzahl Betroffener oder bei einer nicht eingrenzbaren

Menge potenziell betroffener Personen kaum umsetzbar, siehe auch 1.1.7, Seite 31. Beruht eine Datenverarbeitung in anders gelagerten Fällen ausnahmsweise auf einer Einwilligung, normiert Art. 7 Abs. 1 DSGVO eine spezielle Nachweispflicht in Bezug auf das Vorliegen der erfolgten Einwilligung. Dokumentiert werden muss ebenfalls:

- die Ausschöpfung bzw. Prüfung alternativer Maßnahmen zur Videoüberwachung (vgl. Erforderlichkeit, siehe 1.1.7, Seite 31)
- die Prüfung der Rechtmäßigkeitsvoraussetzungen:
  Der/Die Betreiber/in 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 nicht mehr erfüllt sind, beispielweise wenn nach einem gewissen Zeitablauf ersichtlich wird, dass keine Tatsachen für eine Gefährdung des überwachten Objekts mehr festgestellt werden oder weitere Sicherheitsmaßnahmen eine Videoüberwachung entbehrlich machen. Dies kann auch Teilbereiche einer Überwachung betreffen. Angemessene Löschfristen sind gegebenenfalls zu beachten (vgl. 1.1.5, Seite 27)
  Das Ergebnis der Prüfung ist schriftlich zu dokumentieren.

b) Dokumentationspflicht

Hinweise und Muster zur Erstellung eines Verzeichnisses von Verarbeitungstätigkeiten:
↗ sdb.de/vue01

Eine der wichtigsten Dokumentationspflichten, die vor Aktivierung einer Videokamera zu erfüllen ist, ist die Erstellung eines Verzeichnisses von Verarbeitungstätigkeiten (Art. 30 DSGVO). Hierbei sind insbesondere die Zwecke der Videoüberwachung schriftlich oder in einem elektronischen Format festzuhalten. Ebenso sollte jede Kamera (oder bei Vergleichbarkeit jede Kameragruppe) einzeln in das Verzeichnis aufgenommen und dort dokumentiert werden. Das Verzeich-

nis ist der Datenschutzaufsichtsbehörde auf Antrag zur Verfügung zu stellen (Art. 30 Abs. 4 DSGVO).
Beauftragt ein Verantwortlicher eine andere Person oder Stelle mit der Verarbeitung personenbezogener Daten, ist der Verantwortliche verpflichtet, dies mit einem Vertrag mit dem **Auftragsverarbeiter** zu dokumentieren (vgl. Art. 28 DSGVO). Verstöße gegen diese Dokumentationspflichten können mit empfindlichen Bußgeldern bis zu 10 Millionen Euro geahndet werden (Art. 83 Abs. 4 Buchst. a DSGVO).

c) 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 Abs. 1 DSGVO).
Die Datenschutz-Folgenabschätzung befasst sich insbesondere mit Abhilfemaßnahmen, durch die der Schutz personenbezogener Daten sichergestellt und die Einhaltung der Datenschutz-Grundverordnung nachgewiesen werden kann.

Informationen zur Datenschutz-Folgenabschätzung:
↗ sdb.de/vue02

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 – auf physiologische Charakteristika bzw. Verhaltensmerkmale zum Zweck der Identifikation einer Person referenzierende Informationen – zur Datenverarbeitung eingesetzt werden.
Von einem öffentlich zugänglichen Bereich ist dann auszugehen, wenn dieser nach seinem Zweck von jedermann – das heißt, von einem unbestimmten oder nur anhand allgemeiner Merkmale eingrenzbaren Personenkreis – betreten oder genutzt werden kann. Auf die Eigentumsverhältnisse kommt es dabei nicht an. Beispiele hierfür sind Verkaufsräume, Restaurants, Supermärkte, Einkaufspassagen, Freizeiteinrichtungen etc.

Weitere Anhaltspunkte, wann eine Videoüberwachung ein hohes Risiko für die Rechte der betroffenen Person darstellt und demzufolge eine Pflicht zur Erstellung einer Datenschutz-Folgenabschätzung besteht, finden Sie auf Seite 18ff. in der „Orientierungshilfe Videoüberwachung durch nichtöffentliche Stellen" der Datenschutzkonferenz.

Orientierungshilfe der Datenschutzkonferenz zur Videoüberwachung durch nichtöffentliche Stellen:
↗ sdb.de/tb2107

1.1.7 Ist Videoüberwachung erlaubt, wenn der Verantwortliche zuvor eine Einwilligung einholt?

Eine Videoüberwachung lässt sich regelmäßig nicht auf den Erlaubnistatbestand der Einwilligung stützen (Art. 6 Abs. 1 Buchst. a DSGVO), da der Verantwortliche die gesetzlichen Anforderungen an eine Einwilligung praktisch nicht erfüllen kann. Insbesondere und vor allem gilt dies für öffentlich zugängliche Bereiche, das heißt für Bereiche sowohl innerhalb als auch außerhalb von Gebäuden, die erkennbar von jedermann genutzt oder betreten werden können (z. B. Restaurants oder Freizeiteinrichtungen). Überwachen Videokameras solche öffentlich zugänglichen Bereiche, wird damit eine unbestimmte bzw. nicht näher bestimmbare Anzahl von Personen erfasst. Bereits dieser unbestimmte Personenkreis schließt eine Einwilligungslösung praktisch aus.

Dazu ist zunächst klarzustellen, dass allein das bloße Betreten eines speziell gekennzeichneten videoüberwachten Bereichs keine datenschutzrechtliche Einwilligung in eine Videoüberwachung darstellt. Denn bei einem solchen Verhalten handelt es sich regelmäßig nicht um eine unmissverständlich abgegebene Willensbekundung und eine „eindeutig bestätigende Handlung" im Sinne des Art. 4 Nr. 11 DSGVO.

Der Verantwortliche wird zudem das Vorliegen von Einwilligungen aller überwachten Personen aus rein praktischen Erwägungen nur schwer nachweisen können, denn dazu müssten diese entsprechend dokumentiert werden.

Eine Einwilligung (Art. 7 DSGVO) muss schließlich freiwillig erteilt werden, also auf der freien Entscheidung der überwachten Person beruhen. Hierüber muss die betroffene Person

ausreichend und verständlich informiert werden, ebenso wie darüber, welche Daten aufgrund der Einwilligung für welchen Zweck verarbeitet werden sollen, wie lange die Speicherdauer ist und was die Einwilligung rechtlich für die betroffene Person bedeutet. Es muss auch ein Hinweis auf die jederzeitige Widerrufsmöglichkeit ergehen. Dies bedeutet im Ergebnis, dass das Betreten des überwachten Bereichs nicht von der Erteilung der Einwilligung abhängig gemacht werden kann, denn bereits eine einzelne nicht erteilte Einwilligung bzw. ein einziger Widerruf würde damit zur Unzulässigkeit der Videoüberwachung führen. Eine Einwilligungslösung ist damit bei einer Videoüberwachung weder praktisch umsetzbar noch rechtssicher gestaltbar.
Für die Einwilligung von Beschäftigten gelten besondere Wirksamkeitsvoraussetzungen (siehe 1.4.2, Seite 46).

„Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679" des Europäischen Datenschutzausschusses:
↗ sdb.de/vue03

„Kurzpapier Nr. 20 Einwilligung nach der DSGVO" der Datenschutzkonferenz:
↗ sdb.de/vue04

1.1.8 Wann unterliegen Videoaufnahmen nicht dem Datenschutzrecht und der Datenschutzaufsicht („Haushaltsausnahme")?

Das Datenschutzrecht gilt nicht für Videoaufnahmen, die von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten erstellt werden (Art. 2 Abs. 2 Buchst. c DSGVO). Diese sogenannte „Haushaltsausnahme" ist rein tätigkeitsbezogen; Eigentumsverhältnissen kommt dabei keine rechtliche Relevanz zu.
Eine Videoüberwachung fällt dann unter die „Haushaltsausnahme", wenn sie auf die private Sphäre begrenzt ist. Im Fall einer Grundstücksüberwachung bedeutet dies, sie muss in jedem Fall an der Grenze des ausschließlich selbstgenutzten Grundstücks bzw. der selbstbewohnten Miet- oder Eigentumswohnung enden. Gegen ein Kamerasystem an einem Einfamilienhaus zum Zweck des Schutzes des Eigentums, der Gesundheit und des Lebens der Bewohner spricht damit nichts, solange der Überwachungsbereich die Grundstücksgrenze nicht überschreitet. Denn reicht die Überwachung auch auf den öffentlichen Verkehrsraum oder private Grundstücke der Nachbarn, wird dadurch die persönliche und fa-

miliäre Sphäre und somit der Anwendungsbereich der „Haushaltsausnahme" verlassen.
Die Überwachung des privaten selbstgenutzten Grundstücks des Kamerabetreibers bzw. der Kamerabetreiberin oder von Bereichen innerhalb eines Gebäudes ist allerdings dann eingeschränkt, wenn es dort einen Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit gibt. Für alle Bereiche, die nicht ausschließlich dem/der Kamerabetreiber/in zur Verfügung stehen, scheidet ein Rückgriff auf die „Haushaltsausnahme" aus. Dies betrifft bei (teil-)vermieteten Grundstücken die Gemeinschaftsflächen, insbesondere die von den Mieterinnen und Mietern zu nutzenden Hauseingänge und Flure. Bei einem gewerblichen Betrieb, zum Beispiel einem Nagelstudio oder Steuerbüro, sind davon alle Kundenbereiche betroffen.
Auch in den Zeiten, in denen sich zum Beispiel ein Pflegedienst um eine pflegebedürftige Person in der eigenen Wohnung kümmert oder etwa Handwerker auf dem eigenen Grundstück oder innerhalb überwachter Gebäude tätig sind, hat eine ansonsten unter die „Haushaltsausnahme" fallende Videoüberwachung der betroffenen Bereiche zu unterbleiben.
Im Übrigen sind von der „Haushaltsausnahme" insbesondere Urlaubs- oder Freizeitaufnahmen zum Zweck der privaten Erinnerung umfasst. Jedoch gilt dies nicht mehr, wenn Videoaufnahmen im Internet veröffentlicht und diese damit einer unbegrenzten Anzahl von Personen zugänglich gemacht werden.

1.1.9 Ist unrechtmäßige Videoüberwachung strafbar?

Nach den Datenschutzvorschriften ist eine Videoüberwachung nur dann strafrechtlich relevant, wenn jemand **gewerbsmäßig** Video- oder Bildaufzeichnungen an einen Dritten **übermittelt** oder auf andere Art und Weise **zugänglich macht** (§ 42 Abs. 1 BDSG). Dies wird jedoch nur auf Antrag verfolgt (§ 42 Abs. 3 BDSG).
Verletzt ein/e Kamerabetreiber/in den **höchstpersönlichen Lebensbereich** einer Person, in dem er/sie in einer Wohnung

oder einem gegen Einblick besonders geschützten Raum unbefugt Bildaufnahmen herstellt, kann dies den Straftatbestand des § 201a Strafgesetzbuch (StGB) erfüllen. Der „gegen Einblick besonders geschützte Raum" betrifft dabei die Intimsphäre. Beispiele hierfür sind die Überwachung von Toiletten, Umkleidekabinen, Saunen und auch (ärztlichen) Behandlungszimmern.

Wird eine Videoüberwachungskamera mit **Audiofunktion** eingesetzt, kommt eine Strafbarkeit nach § 201 Abs. 1 und Abs. 2 StGB infrage. Demnach ist das unbefugte heimliche Abhören oder Aufzeichnen des nichtöffentlich gesprochenen Wortes strafbar. Verfügt eine Videoüberwachungskamera über eine Audiofunktion, sollte diese deaktiviert werden.

Bei dem dargestellten strafbaren Verhalten handelt es sich jeweils um sogenannte **Antragsdelikte**. Damit die Strafverfolgungsbehörden in diesen Fällen tätig werden, muss die geschädigte Person einen Strafantrag stellen. Bei den Straftatbeständen nach dem BDSG sind darüber hinaus auch der Verantwortliche und die Aufsichtsbehörde antragsberechtigt.

1.1.10 Muss ein Verantwortlicher seine Videoüberwachung von der zuständigen Datenschutzaufsichtsbehörde genehmigen lassen?

Für den Betrieb einer Videokamera bestehen weder eine Genehmigungs- noch eine Anzeige- oder Meldepflicht. Dies bedeutet gleichwohl nicht, dass für eine Videoüberwachung keine rechtlichen Anforderungen gelten.

Wie bei jeder Verarbeitung personenbezogener Daten sind auch bei einer Videoüberwachung die allgemeinen datenschutzrechtlichen Anforderungen zu beachten. Jede/r Kamerabetreiber/in ist also gehalten, von sich aus die geltenden Datenschutzvorschriften zu prüfen, um einen zulässigen Kamerabetrieb sowie die Einhaltung der weiteren, sich an Verantwortliche richtenden datenschutzrechtlichen Pflichten sicherzustellen, falls notwendig unter Inanspruchnahme externer Hilfe, zum Beispiel einer/eines Sachverständigen

in Datenschutzfragen oder einer Rechtsanwältin bzw. eines Rechtsanwalts.

1.1.11 Was kann man unternehmen, wenn man von einer vermutlich unrechtmäßigen Videoüberwachung betroffen ist?

Stellt eine betroffene Person eine Videokamera fest, mit der womöglich Bereiche außerhalb des eigenen selbstbewohnten Grundstücks überwacht werden oder die außen an einer Miet- oder Eigentumswohnung angebracht ist, kann sie sich zunächst an den/die Kamerabetreiber/in wenden. Hierzu steht ihr das Auskunftsrecht in Art. 15 DSGVO zu. Damit lässt sich überprüfen, ob die Kamera in Betrieb ist und die betroffene Person damit überwacht wird.

Sollte dieser Weg nicht weiterführen, hat jede betroffene Person die Möglichkeit, ihre Rechte entweder zivilrechtlich durchzusetzen (vgl. dazu 1.1.12, Seite 35) oder aber sich mit einer datenschutzrechtlichen Beschwerde an die zuständige Aufsichtsbehörde zu wenden.

Die Bestimmung der zuständigen Aufsichtsbehörde orientiert sich am (Wohn-)Sitz oder der (Haupt-)Niederlassung des/der verantwortlichen Betreibers/Betreiberin. Wenn es der betroffenen Person nicht möglich ist, Angaben zum/zur Kamerabetreiber/in zu machen, kann sie sich an die für den Wohnsitz oder die Arbeitsstätte zuständige Aufsichtsbehörde wenden. Diese nimmt dann eigene Ermittlungen auf und leitet die eingegangene Beschwerde im Bedarfsfall an die zuständige Aufsichtsbehörde weiter.

Übersicht aller Datenschutzaufsichtsbehörden:
↗ sdb.de/vue05

1.1.12 Wie geht die Sächsische Datenschutz- und Transparenzbeauftragte gegen unrechtmäßige Videoüberwachung vor?

Im **Aufsichtsverfahren** liegt der Schwerpunkt darauf, die Zulässigkeit einer Videoüberwachung zu prüfen und im Fall von festgestellten Verstößen datenschutzkonforme Zustände herzustellen. Im Fall einer unrechtmäßigen Videoüberwachung

wirkt die Aufsichtsbehörde mit dem ihr zur Verfügung stehenden rechtlichen Instrumentarium darauf hin, dass der/die Kamerabetreiber/in eine unzulässige Videoüberwachung einstellt oder rechtswidrig überwachte Bereiche ausblendet. Die Demontage einer Videokamera lässt sich mit den Mitteln des Datenschutzrechts nicht durchsetzen, sondern einzig auf dem Zivilrechtsweg erreichen. Auch einem sich aus der bloßen Existenz einer rechtmäßig betriebenen Videokamera möglicherweise ergebenden Überwachungs- oder Anpassungsdruck kann nur durch Beschreiten des Zivilrechtswegs wirksam begegnet werden.

Im **Ordnungswidrigkeitsverfahren** geht es darum, bei schwerwiegenden Verstößen gegen den/die verantwortliche/n Kamerabetreiber/in ein Bußgeld zu verhängen. Die Datenschutzvorschriften ermöglichen bei einem rechtswidrigen Betrieb die Verhängung einer Geldbuße von bis zu 20 Millionen Euro (Art. 83 Abs. 5 Buchst. a DSGVO). Auch ein Verstoß gegen die weiteren den Verantwortlichen auferlegten Pflichten kann ein Bußgeld zur Folge haben (siehe 1.1.6, Seite 28).

Sowohl im Aufsichts- als auch im Ordnungswidrigkeitsverfahren richtet sich die **Zulässigkeitsprüfung** der Videoüberwachung nach Art. 6 Abs. 1 DSGVO. Bei der Videoüberwachung von Beschäftigten kommt noch die Vorschrift des § 26 Bundesdatenschutzgesetz (BDSG) hinzu. Zwar enthält die Vorschrift des § 4 Abs. 1 BDSG (noch) eine ausdrückliche Regelung zur Videoüberwachung nichtöffentlicher Stellen, jedoch hat das Bundesverwaltungsgericht (Urteil vom 27. März 2019, Az. 6 C 2/18) diese für europarechtswidrig erklärt. Damit findet § 4 Abs. 1 BDSG bei der Zulässigkeitsbeurteilung keine Anwendung.

1.1.13 Wie muss ein Verantwortlicher auf die Videoüberwachung hinweisen?

Auch bei einer Videoüberwachung muss der Verantwortliche seinen gesetzlichen Informationspflichten nachkommen. Nach den Vorgaben des Art. 13 DSGVO ist auf die Videoüberwachung transparent und fair und damit adressatengerecht

hinzuweisen. Diese Hinweise haben regelmäßig so frühzeitig zu erfolgen, also vor dem Betreten des videoüberwachten Bereichs, dass betroffenen Personen noch die Möglichkeit bleibt, der Videoüberwachung auszuweichen bzw. ihr Verhalten darauf entsprechend auszurichten.

Praktische Umsetzung:

Um dem Umfang der nach Art. 13 DSGVO bereitzustellenden Informationen praxisgerecht entsprechen zu können, haben sich die deutschen Datenschutzaufsichtsbehörden auf die Empfehlung verständigt, dass betroffene Personen in zwei Schritten informiert werden können.
Ein optisch präsentes, das heißt auf Augenhöhe angebrachtes und optisch schnell erfassbares Hinweisschild (**vorgelagertes Hinweisschild**) soll zunächst sicherstellen, dass die betroffenen Personen über den Umstand der Videoüberwachung informiert werden. Es soll einen schnellen Überblick über die wichtigsten Informationen ermöglichen. Auf dem Hinweisschild muss auf Folgendes hingewiesen werden:

- Umstand der Beobachtung – Piktogramm, Kamerasymbol
- Identität des Verantwortlichen sowie gegebenenfalls seines Vertreters (nach Art. 27 DSGVO), Name einschließlich Kontaktdaten (inklusive Telefonnummer oder E-Mail-Adresse)
- Kontaktdaten des betrieblichen Datenschutzbeauftragten – soweit benannt, dann aber zwingend (inkl. Telefonnummer oder E-Mail-Adresse)
- Verarbeitungszwecke und Rechtsgrundlage in Schlagworten
- Angabe des berechtigten Interesses (soweit die Verarbeitung auf Art. 6 Abs. 1 Buchst. f DSGVO beruht) Speicherdauer oder Kriterien für die Speicherdauer (nur im Fall der Speicherung)

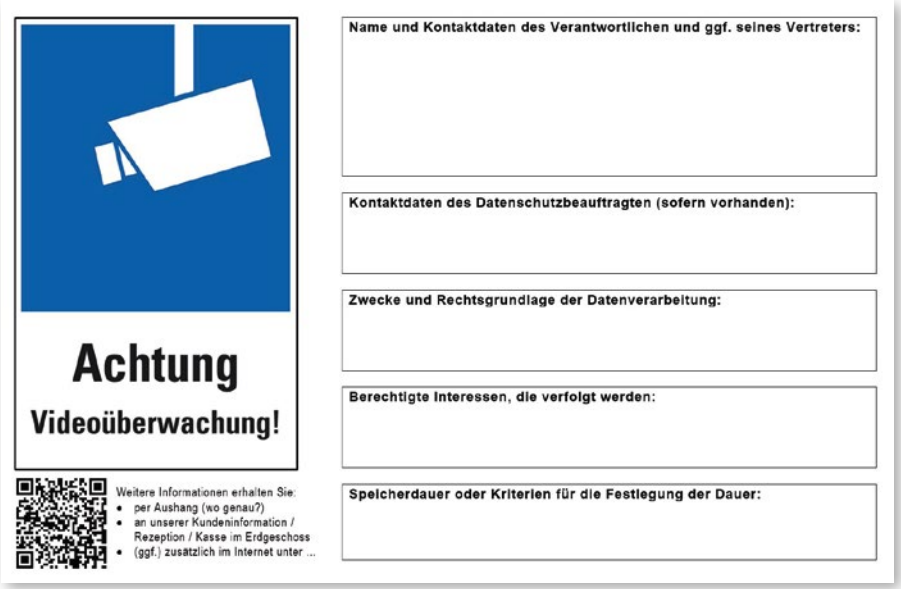


Abbildung 1 (oben):
Beispiel für ein vorgelagertes Hinweisschild nach Art. 13 DSGVO bei Videoüberwachung, Download unter: ↗ sdb.de/vue06

Die vollständigen Informationen nach Art. 13 DSGVO kann der/die Kamerabetreiber/in dann innerhalb des überwachten Bereichs – an geeigneter, gut zugänglicher Stelle – auslegen oder aushängen oder auch im Internet zum Abruf vorhalten. Auf dem vollständigen Informationsblatt ist noch Folgendes zu vermerken:

- Empfänger oder Empfängerkategorien (nur bei Datenübermittlung)
- weitere Pflichtinformationen (insbesondere Hinweise zum Auskunftsrecht und Beschwerderecht)

Abbildung 2 (rechts):
Beispiel eines vollständigen Informationsblatts nach Art. 13 DSGVO bei Videoüberwachung, Download unter: ↗ sdb.de/vue07

Wesentlich ist dabei, dass das vorgelagerte Hinweisschild einen klaren Verweis darauf enthalten muss, wo die vollständigen Informationen eingesehen werden können.
Es gibt spezifische Anwendungsbereiche, in denen das vorgelagerte Hinweisschild wenig praktikabel ist, weil eine Wahrnehmung der darin enthaltenen Informationen durch die betroffenen Personen praktisch nicht möglich ist, etwa weil sie das Hinweisschild zu schnell passieren oder im Verkehrsbereich

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

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. Zuständige Aufsichtsbehörde in Sachsen: Sächsische Datenschutz- und Transparenzbeauftragte

unter Umständen der Verkehrsfluss beeinträchtigt werden kann. Beispiele hierfür sind Tankstellen, an deren Einfahrt bereits Hinweisschilder angebracht werden müssten, oder öffentliche Verkehrsmittel, bei denen diese Schilder außen am Verkehrsmittel anzubringen wären. In solchen Fällen wird als Erstinformation ein Hinweisschild mit dem bloßen Piktogramm Videoüberwachung (standardisiertes Bildsymbol nach DIN 33450) zu akzeptieren sein. Jedoch muss das vorgelagerte Hinweisschild dann an der Tanksäule bzw. im Fahrgastraum angebracht sein. Die vollständigen Informationen könnten im/am Tankstellenshop bzw. auf der Website der Verkehrsbetriebe bereitgestellt werden. Es bleibt den Verantwortlichen selbstredend unbenommen, die umfassende Information auch bereits an den Tanksäulen bzw. im Verkehrsmittel selbst anzubringen.

Inhalt der vollständigen Informationen:

Bei der Angabe des Zweckes sollten Verantwortliche eine eher allgemein gehaltene, schlagwortartige Angabe (übergeordnetes Ziel) wählen. Denkbar als Zweckangabe wären daher beispielsweise Angaben wie

- Eigentumsschutz (Einbruch, Diebstahl, Vandalismus)
- Personenschutz (Schutz der körperlichen Unversehrtheit)
- Wahrnehmung der Aufsichtspflicht
- Wahrnehmung des Hausrechts
- Gebührenabrechnung (z. B. bei der Nutzung von Parkflächen)

Im Gegensatz dazu sollte die Darstellung bei den berechtigten Interessen konkreter und detaillierter erfolgen, um den betroffenen Personen das Nachvollziehen der nach Art. 6 Abs. 1 Buchst. f DSGVO vorgenommenen Interessenabwägung zu ermöglichen. Als berechtigte Interessen wären dann Angaben vorstellbar wie

- Abschreckung potenzieller Straftäter
- Aufklärung von Straftaten/Beweissicherung
- Durchsetzung zivilrechtlicher Ansprüche/Beweissicherung

- Sicherung/Überwachung von Gefahrenbereichen
- Verhinderung und Verfolgung von Diebstahl, Vandalismus und Einbruch
- Ermittlung der Standzeiten (z. B. auf Parkflächen)
- Ein- und Ausfahrtskontrolle
- Prüfung der Durchfahrtsberechtigung

In der Gesamtschau kommt es darauf an, dass den Adressaten mit beiden Angaben klar wird, aus welchem – berechtigten – Grund die Videoüberwachungsanlage betrieben wird. Soweit Verantwortliche schon unter dem Zweck ausreichend detaillierte Angaben machen, sollte es dessen ungeachtet auch legitim sein, bei den berechtigten Interessen lediglich auf den Zweck zu verweisen.

Achtung:

Allein das Anbringen eines Hinweisschildes führt nicht zur Zulässigkeit einer ansonsten rechtswidrigen Videoüberwachung. Insbesondere lässt sich daraus nicht ableiten, dass die betroffenen Personen allein durch das Passieren eines Hinweisschildes in die Videoüberwachung einwilligen, wenn sie davon überhaupt Kenntnis nehmen (können), siehe hierzu 1.1.7, Seite 31.

Muster für ein vorgelagertes Hinweisschild (docx-Datei):
↗ sdb.de/vue06

Muster für ein vollständiges Informationsblatt (docx-Datei):
↗ sdb.de/vue07

1.2 Videoüberwachung im Nachbarschaftskontext

Eine Videoüberwachung hat grundsätzlich an der **Grenze der eigenen Wohnung** (Eigentums/Mietwohnung) bzw. **des eigenen Grundstücks** zu enden. Nur auf dem eigenen Grundstück kann sich der/die Kamerabetreiber/in auf sein **Hausrecht** berufen.

Öffentliche Verkehrsbereiche sowie **nachbarliche Grundstücke** dürfen von Privaten im Regelfall nicht überwacht werden, denn dort überwiegen grundsätzlich die schutzwürdigen Interessen der betroffenen Personen (siehe Art. 6 Abs. 1 Buchst. f DSGVO). Nachbarn, Passanten, Kinder, Lieferanten, Besucher

und sonstige Verkehrsteilnehmer müssen eine dauerhafte und gegebenenfalls anlasslose Überwachung nicht hinnehmen. Auch ein konkretes Überwachungsinteresse (z. B. Eigentumsschutz) rechtfertigt regelmäßig keine Videoüberwachung öffentlicher Verkehrsräume, wie Straßen, Gehwege oder Parkplätze, und nachbarlicher Privatgrundstücke.

Aber selbst auf dem eigenen Grundstück ist die Überwachung nicht in jedem Fall zulässig, denn sie bezieht sich nur auf ausschließlich selbstgenutzte Bereiche. Nur insoweit trifft die sogenannte **„Haushaltsausnahme"** (Art. 2 Abs. 2 Buchst. c DSGVO) zu (siehe 1.1.8, Seite 32). Werden das Grundstück oder Teile davon wirtschaftlich oder gewerblich genutzt, darf der/die Kamerabetreiber/in diese Flächen nicht überwachen.

So ist bei einem **Mietshaus** die Überwachung von Gemeinschaftsflächen, Zugangsbereichen, Gartenflächen und Außenanlagen nicht von der „Haushaltsausnahme" gedeckt. 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. Gleiches gilt bei einem **Wegerecht** auf dem eigenen Grundstück. Damit wird im Regelfall einem Nachbarn bzw. einer Nachbarin der Zugang zu seinem/ihrem Hinterliegergrundstück ermöglicht. Die betreffenden im Grundbuch eingetragenen Flächen (Zugangsbereiche) oder auf andere Weise gewährte Wegerechte für Dritte sind im Ergebnis von einer Überwachung frei zu halten.

Erstreckt sich eine Videoüberwachung (auch) auf demnach davon auszunehmende Bereiche des eigenen Grundstücks, das Grundstück eines Nachbarn oder dinglich gesicherte Flächen, kann dies **zivilrechtliche Ansprüche** nach sich ziehen, die von Unterlassungs- und Beseitigungs- bis hin zu Schadensersatzansprüchen reichen können. Wird mit einer Videobeobachtung der höchst **persönliche Lebensbereich** einer Person verletzt, kommt sogar der Verdacht auf das Vorliegen eines Straftatbestands in Betracht (vgl. § 201a StGB).

Hinweisblatt zur Videoüberwachung auf Privatgrundstücken und in der Nachbarschaft:
↗ sdb.de/vue08

Gleiches gilt dann, wenn Gespräche von Nachbarn oder anderen Personen außerhalb des eigenen selbstgenutzten Grundstücks aufgezeichnet werden (vgl. § 201 StGB), siehe hierzu 1.1.9, Seite 33.

1.3 Videoüberwachung im gewerblichen Bereich

Werden gewerbliche Bereiche, zum Beispiel das Betriebsgrundstück, überwacht und findet eine Videoüberwachung nur außerhalb der Betriebszeiten statt, bestehen hiergegen keine datenschutzrechtlichen Einwände. Insoweit kann sich der Verantwortliche auf die Wahrung berechtigter Interessen berufen (Art. 6 Abs. 1 Buchst. f DSGVO). Die zeitliche Begrenzung lässt sich softwareseitig durch entsprechende Einstellungen oder auf andere geeignete Weise sicherstellen.

Erstrecken sich die Überwachungszeiten auch auf die Öffnungszeiten bzw. die Anwesenheit von Kundinnen und Kunden, gilt es verschiedene Gewerbebetriebe zu unterscheiden. Zur Überwachung Beschäftigter siehe 1.4, Seite 43.
Datenschutzrechtlich unproblematisch ist beispielsweise die Videoüberwachung an Tankstellen (siehe 1.12, Seite 64), in Juweliergeschäften (siehe 1.8, Seite 57) sowie in Banken (siehe 1.6, Seite 55). Nicht zulässig ist die Überwachung von Ess- und Aufenthaltsbereichen. Gleiches gilt für Bereiche, in denen Personen der Ausübung einer Freizeitbeschäftigung nachgehen. Dazu zählen zum Beispiel Tanzflächen und Kegelbahnen. Im Einzelhandel dürfen Flure und die Warenauslage überwacht werden.
In jedem Fall sind bei einer datenschutzkonformen Videoüberwachung die Informationspflichten in Art. 13 DSGVO zu erfüllen. Dies gilt auch, wenn die Videoüberwachung nur außerhalb der Öffnungszeiten eines Gewerbebetriebs stattfindet, da auch in diesen Fällen mit Betroffenenanträgen nach Art. 15ff. DSGVO zu rechnen ist. Geeignete Vorlagen hierzu finden sich unter 1.1.13, Seite 36.

1.4 Überwachung von Beschäftigten

1.4.1 Ist die Videoüberwachung von Beschäftigten erlaubt?

Im Beschäftigungsverhältnis unterliegt die Videoüberwachung und die damit verbundene Datenverarbeitung aufgrund des bestehenden Abhängigkeits- sowie des Über/Unterordnungsverhältnisses zwischen Arbeitgeber/in und Beschäftigten sehr hohen Anforderungen.

Dies ergibt sich unter anderem aus dem qualitativen Unterschied der Überwachung mittels Videokameras im Gegensatz zu einer Kontrolle durch eine Aufsichtsperson. Beschäftigte, die permanent mit einer Videoüberwachung durch den/die Arbeitgeber/in rechnen müssen, sind einem ständigen Überwachungsdruck ausgesetzt, dem sie sich während ihrer Arbeitszeit nicht entziehen können. Eine allgemeine Videoüberwachung, die losgelöst von konkreten Anlässen stattfindet, ist daher unzulässig. Dies gilt sowohl für eine offene als auch für die heimliche (verdeckte) Videoüberwachung.

Für Verarbeitungen von Beschäftigtendaten in Form der Videoüberwachung gelten daher besondere Regelungen. Sowohl der Bundesgesetzgeber als auch der Landesgesetzgeber haben von ihrer Befugnis nach Art. 88 Abs. 1 DSGVO (sogenannte Öffnungsklausel) Gebrauch gemacht, spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigtenkontext vorzusehen.

Für die Beschäftigten öffentlicher Stellen des Freistaates Sachsen gemäß § 2 SächsDSDG regelt § 11 SächsDSDG die Verarbeitung von Beschäftigtendaten (siehe 2.7, Seite 95). Für die Beschäftigten der nichtöffentlichen Stellen ist die Verarbeitung von Beschäftigtendaten dagegen nach gegenwärtigem Rechtsstand in § 26 BDSG normiert, vgl. zur weitergehenden Frage der Anwendbarkeit nationaler Vorschriften die Entscheidung des EuGH mit Urteil vom 30. März 2023 – C-34/21.

Für die Beschäftigtendatenverarbeitung nichtöffentlicher Stellen ist ein Rückgriff auf die weiteren Öffnungsklauseln des Art. 6 Abs. 3 in Verbindung mit Art. 6 Abs. 1 Satz 1 Buchst. e oder c DSGVO nicht möglich. Die Datenverarbeitung müsste dann – soweit § 26 Abs. 1 Satz 1 BDSG nicht mehr angewandt werden kann – unter Rückgriff auf die allgemeinen Rechtsgrundlagen des Art. 6 Abs. 1 DSGVO erfolgen. Dazu zählt im Bereich der Videoüberwachung unter anderem Art. 6 Abs. 1 Buchst. f DSGVO („berechtigtes Interesse").

Für die Beurteilung der Frage, ob die Videoüberwachung von Beschäftigten nichtöffentlicher Stellen zulässig ist, ist zunächst der Zweck der Videoüberwachung festzustellen. Abhängig von diesem Zweck sind unterschiedliche Rechtsgrundlagen für die Prüfung der Zulässigkeit der Videoüberwachung heranzuziehen.

Ist der Zweck der Videoüberwachung die Beschäftigtenüberwachung selbst, ist § 26 BDSG als Rechtsgrundlage anwendbar. Sollen mit der Videoüberwachung nicht (gezielt) Beschäftigte überwacht werden, sondern werden diese bei der Überwachung von Räumlichkeiten wie zum Beispiel Verkaufsflächen im Einzelhandel oder Lagerräumen die Arbeitsbereiche der Beschäftigten lediglich miterfasst, ist Art. 6 Abs. 1 Buchst. f DSGVO einschlägige Rechtsgrundlage.

Der Begriff des **Beschäftigten** ist dabei weit gefasst und reicht von Arbeitnehmern, Beamten, Richtern und Soldaten bis hin zu Leiharbeitern oder Auszubildenden und auch Heimarbeiterinnen/Heimarbeitern (§ 26 Abs. 8 BDSG). In der Vorschrift des § 26 BDSG hat der Bundesgesetzgeber von einer Öffnungsklausel (Art. 88 Abs. 1 DSGVO) Gebrauch gemacht und die europäischen Regelungen durch nationale Vorschriften ergänzt und konkretisiert.

In Bereichen, in denen sich Beschäftigte nur vorübergehend und gelegentlich aufhalten, stehen einer Videoüberwachung im Regelfall keine überwiegenden schutzwürdigen Interessen entgegen. Anders verhält es sich bei **dauerhaften Arbeitsplätzen** oder Bereichen, in denen sich Beschäftigte über längere Zeit aufhalten. Dort dürfen sie grundsätzlich nicht gefilmt werden. Dabei wird unter anderem berücksich-

tigt, ob den Beschäftigten ein kontrollfreier und unbeobachteter Arbeitsbereich verbleibt. Je weniger Rückzugsraum zur Verfügung steht, desto eher überwiegen die schutzwürdigen Interessen der Beschäftigten.

Eine Videoüberwachung liegt nicht erst bei einer länger andauernden gezielten Kontrolle vor, sondern schon bei einer **beiläufigen Aufnahme**.

Möchte der/die Arbeitgeber/in die Arbeitsleistung, Sorgfalt und Effizienz von Beschäftigten per Videoüberwachung kontrollieren, ist dies nicht erlaubt. Denn zum Zweck einer **Verhaltens- oder Leistungskontrolle** von Beschäftigten ist eine Videoüberwachung aufgrund der Eingriffsintensität, insbesondere des damit verbundenen persönlichkeitsrechtsverletzenden Überwachungsdrucks und der dadurch erzeugten umfassenden Bewegungs- und Leistungsprofile, grundsätzlich unzulässig. Wo eine persönliche Geschäftsführung und -kontrolle im Betrieb erforderlich ist, darf eine Kamera diese nicht ersetzen. Auch die Videoüberwachung von Beschäftigten zur **Vorbeugung von Diebstählen und anderen pflichtwidrigen Handlungen** ist unzulässig.

Die **Intim- oder Persönlichkeitssphäre** von Personen darf auch im Arbeitsverhältnis nicht verletzt werden und stellt einen Straftatbestand dar (vgl. § 201a StGB). Ein Kameraeinsatz in sensiblen Bereichen wie Umkleidekabinen, Sanitär-, Pausen-, Sozial- und Aufenthaltsräumen ist daher unzulässig. Werden Gespräche aufgezeichnet, kann dies auch strafrechtlich relevant sein (vgl. § 201 StGB). Die genannten Straftaten sind indes Antragsdelikte. Die Strafverfolgungsbehörden werden im Regelfall also erst auf Antrag der geschädigten Person tätig (siehe hierzu auch 1.1.9, Seite 33).

1.4.2 Ist die Videoüberwachung von Beschäftigten zulässig, wenn der/die Arbeitgeber/in eine Einwilligung einholt?

Zwar sieht der Bundesgesetzgeber in der Vorschrift des § 26 Abs. 2 BDSG ausdrücklich eine Einwilligung als Rechtsgrundlage vor. Jedoch müssen bei einer Einwilligung in eine Video-

überwachung im Rahmen eines Arbeitsverhältnisses die hierfür geltenden **gesetzlichen Voraussetzungen** vorliegen. Maßgebliches Kriterium ist, ob die Einwilligung freiwillig erteilt wurde. Dabei sind die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Personen sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen.
Es ist davon auszugehen, dass Beschäftigte regelmäßig **nicht freiwillig** in die eigene Überwachung durch Videokameras einwilligen, da zwischen Arbeitgeberinnen/Arbeitgebern und Beschäftigten regelmäßig ein klares Ungleichgewicht herrscht. Aus diesem Grund ist es unwahrscheinlich, dass Beschäftigte frei, also ohne Nachteile befürchten zu müssen, auf ein Ersuchen ihrer Arbeitgeberin/ihres Arbeitgebers um Einwilligung – beispielsweise in die Aktivierung von Überwachungssystemen wie einer Kameraüberwachung des Arbeitsplatzes – antworten können.
Gegen eine Freiwilligkeit sprechen folgende Punkte:

- Beschäftigte können sich von dem/der Arbeitgeber/in gedrängt fühlen.
- Beschäftigte müssen auch arbeitsrechtliche Konsequenzen fürchten, wenn sie – gegebenenfalls als Einzige der Belegschaft – eine Überwachung ablehnen.
- Beschäftigte haben die vertragliche Pflicht, sich an dem von dem/der Arbeitgeber/in bestimmten Ort aufzuhalten, um dort die geschuldete Arbeitsleistung zu erbringen.
- Beschäftigte haben nicht die Möglichkeit, sich der Überwachung durch Verlassen der Räumlichkeiten zu entziehen, ohne gegebenenfalls arbeitsvertragliche Pflichten zu verletzen.
- Auch das Ansehen innerhalb der Belegschaft kann leiden, insbesondere, wenn nur ein oder einige wenige Beschäftigte die Überwachungsmaßnahme durch Nichterteilung der Einwilligung blockieren.

Letztlich darf die Erfüllung des Arbeitsvertrags nicht von der Einwilligung in die Videoüberwachung und damit in eine Verarbeitung von personenbezogenen Daten abhängig sein, wenn diese hierzu nicht erforderlich ist.

Verfolgt eine Videoüberwachung 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.
Unter Missachtung der vorliegenden Anforderungen eingeholte Einwilligungen sind unwirksam und stellen damit keine Rechtsgrundlage dar, auf die sich die Videoüberwachung von Beschäftigten stützen lässt.

1.4.3 Dürfen Beschäftigte per Video überwacht werden, um Straftaten aufzudecken?

Zur Aufdeckung von Straftaten dürfen personenbezogene Daten von Beschäftigten nur nach der Maßgabe des § 26 Abs. 1 Satz 2 BDSG verarbeitet werden. Eine Datenverarbeitung ist dann zulässig, wenn

(1) zu dokumentierende **tatsächliche Anhaltspunkte** den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat,
(2) die Verarbeitung zur Aufdeckung **erforderlich** ist und
(3) das **schutzwürdige Interesse** der/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 nicht auf § 26 Abs. 1 Satz 2 BDSG gestützt werden. Auf dieser Grundlage ist allenfalls eine zeitweilige, das heißt vorübergehende und zeitlich begrenzte 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. Will der/die Arbeitgeber/in mit einer Videoüberwachung nur **befürchteten** Verfehlungen von Beschäftigten begegnen, liegt

ein solcher Verdacht nicht vor, und die Videoüberwachung wäre unzulässig. Ein konkreter Verdacht muss im Vorfeld einer solchen Überwachungsmaßnahme dokumentiert sein. Allgemeine Vermutungen reichen nicht aus. Der/Die Arbeitgeber/in darf also gerade nicht vorbeugend Video-/Bilddaten von Beschäftigen sammeln, ohne einen bestimmten Anlass für eine Überwachungsmaßnahme zu haben. Dies gilt auch für den Fall, dass der Zugriff auf die Aufnahmen unter der Bedingung erfolgt, dass sich ein bestimmter Tatverdacht erst **im Nachhinein** konkretisiert (Speicherung auf Vorrat).
Selbst wenn der konkrete Verdacht einer strafbaren Handlung besteht, muss der/die Arbeitgeber/in vor einer Videoüberwachung alle anderen, gleich effektiven Maßnahmen erfolglos eingesetzt haben bzw. deren Verwendung geprüft und nachvollziehbar verworfen haben (**Erforderlichkeitsgebot**). Alternative Maßnahmen in diesem Sinne sind:

- die Einsichtnahme in Personaleinsatzpläne,
- der 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.

Der/Die Arbeitgeber/in hat eine Verhältnismäßigkeitsprüfung unter Berücksichtigung der Umstände des Einzelfalles vorzunehmen. Neben der hohen Eingriffsintensität der zumeist heimlichen Videoüberwachung, hat der/die Arbeitgeber/in zum Beispiel zu berücksichtigen, dass durch die Maßnahme gegebenenfalls unbeteiligte Dritte betroffen sind. Im Rahmen dieser Prüfung hat der/die Arbeitgeber/in, insbesondere bei einer avisierten heimlichen Videoüberwachung, zu beachten, dass für jede Datenverarbeitung Informationspflichten nach Art. 13 und 14 DSGVO des Verantwortlichen bestehen und diese nur dann nicht bestehen, wenn die Information die Verwirklichung der mit der Überwachung verfolg-

ten Ziele unmöglich machen oder ernsthaft beeinträchtigen würde (vgl. Art. 14 Abs. 5 Buchst. b DSGVO).
Nach einer **Abwägungsentscheidung** kann und darf am Ende eine zulässige Videoüberwachung gemäß § 26 Abs. 1 Satz 2 BDSG stehen. Diese kann auch zu einer **heimlichen oder verdeckten Videoüberwachung** führen, wenn es kein milderes Mittel zur Aufklärung eines gegen Beschäftigte bestehenden Verdachts einer Straftat gibt. Jedoch ist diese nur in absoluten Ausnahmefällen möglich. In jedem Fall sollten Maßnahmen aufgrund eines betrieblichen Kontrollsystems im Hinblick auf ihre Eingriffstiefe aufeinander aufbauen und eine Dokumentation der einzelnen Maßnahmen vorsehen (siehe 1.1.6, Seite 18).

1.4.4 Kann die Videoüberwachung von Beschäftigten in einer Betriebsvereinbarung geregelt werden?

Auch Betriebsvereinbarungen können eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten darstellen. Allerdings darf auch diese die Datenschutzanforderungen der DSGVO bzw. BDSG nicht unterschreiten. Soweit eine Videoüberwachung im Arbeitsverhältnis den Vorgaben von Art. 88 DSGVO in Verbindung mit § 26 Abs. 4 BDSG entspricht, kann sie durch eine datenschutzrechtskonforme Betriebsvereinbarung geregelt werden.
Die Verfahren zur Verarbeitung personenbezogener Daten müssen dabei den Anforderungen des Art. 88 Abs. 2 DSGVO genügen. 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.

Bei Betriebsvereinbarungen ist aufgrund der bestehenden Rechtslage nachhaltig anzuraten, den Zweck einer Leistungskontrolle auszuschließen.

- 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
  Hinweis: Transparente Zugriffsberechtigungskonzepte sind wegen der Einsichtnahme in die Bilddaten der Videoüberwachung für die betroffenen Beschäftigten von erheblicher praktischer Bedeutung.

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 gemäß § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz vor der Einführung und Anwendung der Einrichtungen zu beteiligen. Falls kein Betriebsrat existiert, sollte der/die Arbeitgeber/in die Einrichtung von Videoüberwachungsanlagen regeln (z. B. durch datenschutzkonforme Dienstanweisungen).

1.4.5 Müssen Beschäftigte dulden, wenn sie bei der Videoüberwachung von Verkaufsflächen miterfasst werden?

Werden öffentlich zugängliche Räume mit Publikums- und Kundenverkehr überwacht (z. B. Verkaufsflächen im Einzelhandel oder in Einkaufszentren), kann es vorkommen, dass Arbeitsbereiche von Beschäftigten gefilmt werden. Beschäftigte werden damit zwar nicht gezielt überwacht (siehe

oben), sind aber regelmäßig (auch) von einer Überwachung betroffen.

Die Zulässigkeit der Überwachung öffentlich zugänglicher Räume (Betriebs- oder Geschäftsbereiche) richtet sich nach Art. 6 Abs. 1 Buchst. f DSGVO. Sie ist dann rechtlich möglich, wenn sie zur Wahrung berechtigter Interessen des Arbeitgebers/der Arbeitgeberin erforderlich ist und schutzwürdige Interessen der Beschäftigten nicht überwiegen.

Die berechtigten Interessen der Geschäftsinhaber/innen liegen darin, ihre Ware während der Öffnungszeiten vor Kundendiebstahl zu schützen sowie Straftäter/innen zu überführen. Die Überwachung muss sich aber auf das erforderliche Maß beschränken, beispielsweise auf Auslagen und Regale mit besonders hochpreisigen Waren. Nicht betroffene Arbeits- und Kommunikationsbereiche sind von der Überwachung auszunehmen. Im Rahmen der Abwägung ist zu berücksichtigen, dass Warendiebstahl auf Verkaufsflächen im Einzelhandel oder in Einkaufszentren zum geschäftstypischen Risiko gehört. Außerdem entspricht eine dortige Überwachung regelmäßig den vernünftigen Erwartungen der betroffenen Personen. 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 (Warenauslagen und Regale), beschränkt, überwiegt grundsätzlich das Interesse der Geschäftsinhaberin bzw. des Geschäftsinhabers am Schutz der Waren.

Stehen jedoch Beschäftigte im Fokus einer Videoüberwachung oder werden Dauerarbeitsplätze erfasst, gelten in diesen Bereichen die einschränkenden Vorschriften des Art. 88 DSGVO in Verbindung mit § 26 BDSG.

1.4.6 Wann ist die Überwachung von Beschäftigten in nichtöffentlichen Betriebsbereichen zulässig?

Sofern die Überwachung von Beschäftigten nicht Zweck der Überwachung ist (siehe 1.4.1, Seite 44), kann eine Video-

überwachung gemäß Art. 6 Abs. 1 Buchst. f DSGVO in nichtöffentlichen Bereichen eines Betriebs eingesetzt werden, beispielsweise, um **Produktionsabläufe** zu verfolgen oder den **Zutritt unberechtigter Personen** zu sensiblen Bereichen zu erfassen. Eine Überwachung allein zu dem Zweck, einen ordnungsgemäßen **Arbeitsablauf** zu gewährleisten, ist im Regelfall nicht gerechtfertigt.

Möglich sind Überwachungsmaßnahmen jedenfalls dann, wenn ein/e Arbeitgeber/in in besonders gefahrträchtigen Arbeitsbereichen **Schutzpflichten** gegenüber seinen/ihren Beschäftigten erfüllen muss. Der Erfassungsbereich ist dabei auf die sicherheitsrelevanten Bereiche bzw. solche mit besonderer Verletzungsgefahr für Beschäftigte oder einer potenziellen Allgemeingefährdung zu beschränken. Im Übrigen sind Arbeitsbereiche von Beschäftigten so weit 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.

1.5 Gastronomie

In einer gastronomischen Einrichtung bemisst sich die Zulässigkeit einer Videoüberwachung an der Vorschrift des Art. 6 Abs. 1 Buchst. f DSGVO. Sie ist nur dann rechtmäßig, wenn sie zur Wahrung berechtigter Interessen des Gastronomen bzw. der Gastronomin erforderlich ist und schutzwürdige Interessen der betroffenen Personen nicht überwiegen. Neben Gaststätten zählen auch Café- und Gastronomieflächen (auch Stehtische) an einem Imbiss sowie in Bäckereien, Metzgereien, Tankstellen, Hotels etc. zu den gastronomischen Einrichtungen in diesem Sinne. Nicht nur Gäste sind von einer dortigen Videoüberwachung betroffen, sondern auch Beschäftigte.

Ess- und Aufenthaltsbereiche dürfen während der Öffnungszeiten regelmäßig nicht mit Kameras überwacht werden. Sie

laden zum längeren Verweilen, Entspannen und Kommunizieren ein, außerdem besteht dort keine hohe Gefahr für das Eigentum des Gastronomen bzw. der Gastronomin, da das neben den Gästen anwesende Personal bei entsprechenden Vorfällen unmittelbar eingreifen und gegebenenfalls die Polizei verständigen kann. Der dortige Aufenthalt ist dem Freizeitbereich zuzurechnen, und die Persönlichkeitsrechte sind deshalb auch besonders schützenswert.

Einer Videoüberwachung der Betriebsräume außerhalb der Öffnungszeiten stehen keine datenschutzrechtlichen Gründe entgegen.

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

Lager und Tresorräume sind für Gäste üblicherweise nicht frei zugänglich und dürfen nur dann überwacht werden, wenn in diesen Bereichen keine dauerhaften Arbeitsplätze eingerichtet sind. Es darf auch keine milderen Mittel zur Zweckerreichung geben, beispielsweise eine Zutrittsbeschränkung nur für berechtigte Personen (Schloss, Zahlencode, Chipkarte etc.). In dem Fall ist der Erfassungsbereich der Kamera auf das Notwendigste zu beschränken. In **Küchen** dürfen Kameras wegen der dort vorhandenen Dauerarbeitsplätze nicht eingesetzt werden.

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 (siehe 1.4.3, Seite 46). Die Videoüberwachung von gegebenenfalls vorhandenen

Glücksspielautomaten ist grundsätzlich möglich. Die Überwachung ist dabei unmittelbar auf den Automaten zu beschränken. Der sonstige Innenraum der gastronomischen Einrichtung darf nicht erfasst sein.

1.6 Banken

Unfallversicherungsträger schreiben in der Vorschrift 25 der Deutschen Gesetzlichen Unfallversicherung (DGUV) den Kreditinstituten zur „Überfallprävention" vor, optische Raumüberwachungsanlagen in öffentlich-zugänglichen Bankbereichen anzubringen. Allerdings beschränkt sich die rechtliche Vorgabe auf jene Bereiche, in denen Banknoten ausgegeben oder angenommen werden (§ 7 DGUV Vorschrift 25). Damit besteht seitens der Kreditinstitute eine rechtliche Verpflichtung zur Videoüberwachung (siehe Art. 6 Abs. 1 Buchst. c und Abs. 2 DSGVO).

Daneben können sich Kreditinstitute auch auf die Wahrung berechtigter Interessen berufen (siehe Art. 6 Abs. 1 Buchst. f DSGVO). Diese bestehen nicht nur im Hinblick auf den Umgang mit dort verwahrten Banknoten, sondern auch im Schutz der Einrichtung innerhalb der Bankfilialen sowie der Gebäude und Räumlichkeiten. In diesem Zusammenhang sei auf die Sprengung von Geldautomaten hingewiesen, die oftmals im Vergleich zum finanziellen Verlust durch entwendete Geldscheine größere Schäden am Gebäude sowie in den Bankräumen verursacht, wenn es die Täter/innen überhaupt schaffen, an die in den Automaten befindlichen Geldscheine zu gelangen.

Statistisch kommt es im Durchschnitt zu zehn Geldautomatensprengungen pro Woche. Für das Jahr 2022 geht man von rund 500 versuchten oder vollendeten Geldautomatensprengungen aus. Dazu kommt die erhöhte Gefahr von Raubüberfällen, auch wenn sich deren Anzahl in den vergangenen Jahren kontinuierlich verringert und sich im unteren zweistelligen Bereich eingependelt hat. Letztlich korrespondiert die Videoüberwachung in den Bankräumlichkeiten auch mit der Erwartungshaltung der Kundinnen und Kunden, für die die Videoüberwachung im Umfeld der Bankautomaten und

im Schalterbereich mittlerweile normal ist und als typischerweise akzeptiert gilt.

1.7 Baustellenüberwachung

Der Begriff Baustellenüberwachung umfasst sowohl die Dokumentation des Baufortschritts als auch den Schutz von Baumaschinen oder Werkzeugen sowie auf dem Baustellengelände gelagerten Materialien (berechtigte Interessen, siehe Art. 6 Abs. 1 Buchst. f DSGVO).

Eigentumsschutz:

Ein Bauzaun allein reicht in der heutigen Zeit nicht (mehr) aus, um ungebetene Besucher/innen vom Betreten der Baustelle abzuhalten. Deshalb findet man auf Baustellen oftmals Überwachungstürme, die von darauf spezialisierten Unternehmen aufgestellt und betrieben werden, und an denen eine oder mehrere Dome-Kameras angebracht sind. Auch wenn die Videokameras oftmals den Eindruck erwecken, sich auch auf Bereiche jenseits der Baugrenze zu richten, zeigen die Erfahrungen, dass die beauftragten Unternehmen die datenschutzrechtlichen Vorgaben zumeist einhalten. Letztlich haben die Überwachungsfirmen auch kein Interesse daran, die Nachbarschaft zu beobachten oder den öffentlichen Verkehrsraum zu überwachen.

Die technischen Möglichkeiten beim Einsatz von Überwachungstürmen erlauben die Einstellung genau festgelegter Überwachungsbereiche (sogenannter Presets). Zumeist sind die Kameras auch mit Lautsprecher ausgestattet und erlauben so eine direkte Gefährderansprache. Schlägt bei einer unbefugten Person auf der Baustelle ein Bewegungssensor an, wird die Leitstelle informiert. Zusätzlich kann eingestellt werden, dass dort oder auch in den Videokameras vor Ort eine Videoaufzeichnung startet.

Aus Datenschutzsicht spricht nichts gegen die Videoüberwachung einer Baustelle, wenn sich die Überwachungsbereiche auf das Baustellengelände beschränken und die Betriebszeiten der Videokameras außerhalb der Zeiten des Baustellenbe-

triebs liegen. Nicht zulässig ist es hingegen, während des Baustellenbetriebs die dort tätigen Bauarbeiter zu überwachen. Die Gefahr von Diebstählen durch Dritte besteht ohnehin nur nach dem arbeitstäglichen Ende der Bautätigkeit sowie bei ruhendem Baustellenbetrieb (an Wochenenden und Feiertagen). Außerhalb des Bauzauns bzw. der Grenze des zu schützenden Grundstücks dürfen keine öffentlichen Verkehrsbereiche oder nachbarlichen Grundstücke überwacht werden.

Dokumentation des Baufortschritts:

Für eine Dokumentation des Baufortschritts ist es nicht erforderlich, den Baustellenbetrieb permanent zu überwachen. Vielmehr reicht es hierzu aus, wenn arbeitstäglich einzelne Bilder erstellt werden. Diese können im Regelfall außerhalb der Zeiten des Baustellenbetriebs aufgenommen werden. Auch hierbei gilt, dass Bereiche jenseits der Grenze der Baustelle von der Erfassung auszunehmen sind.
In jedem Fall sind bei einer Baustellenüberwachung am Bauzaun oder an anderer geeigneter Stelle außerhalb der Baustelle Hinweisschilder anzubringen, die auf die Videoüberwachung verweisen (Informationspflichten, siehe Art. 13 DSGO). Dort reicht das „vorgelagerte Hinweisschild". Die vollständigen Informationen in Art. 13 DSGVO können dann im Internet oder auf der Baustelle selbst angebracht werden („vollständiges Informationsblatt"). Geeignete Vorlagen und weitere Informationen finden Sie unter 1.1.13, Seite 36.

1.8 Einzelhandel

In Geschäften des Einzelhandels ist eine Videoüberwachung inzwischen weit verbreitet, nicht ausschließlich in Supermärkten oder Discountern, sondern zunehmend auch in kleineren Geschäften.
Unter datenschutzrechtlichen Gesichtspunkten ist nichts dagegen einzuwenden, wenn Verkaufsflächen und Kassen per Videokamera überwacht werden, sei es in Form der Livebeobachtung oder mittels Videoaufzeichnungen. Letztere dürfen allerdings nur maximal für 72 Stunden gespeichert

werden und sind, soweit keine relevanten Ereignisse gefilmt wurden, dann zu löschen.

Die Geschäftsinhaber/innen wollen mit dem Einsatz von Videokameras potenzielle Straftäter/innen abschrecken. Kommt es trotzdem zu einer Straftat, können Videoaufnahmen zur Aufklärung und Rekonstruktion von Diebstählen, Sachbeschädigungen durch Vandalismus, Körperverletzungsdelikten gegenüber Beschäftigten oder auch bei Raubüberfällen herangezogen werden. Ein berechtigtes Überwachungsinteresse liegt allein darin begründet, dass es deutschlandweit pro Jahr zu einer hohen sechsstelligen Zahl an Fällen von Ladendiebstahl (2022: 344.669, 2021: 256.694) kommt, mit einer Aufklärungsquote von zuletzt mehr als 90 Prozent (Quelle: Polizeiliche Kriminalstatistik 2022).

Eine Videoüberwachung ermöglicht außerdem die Ausübung des Hausrechts, indem Hausverbote ausgesprochen und überwacht werden. Auch dabei handelt es sich um berechtigte Interessen (siehe Art. 6 Abs. 1 Buchst. f DSGVO). Der Überwachungsbereich hat sich jedoch auf die Verkaufsflächen (Warenauslage und Flure/Gänge) zu beschränken. In Anbetracht der kurzen Verweildauer sowie des geringen Informationsgehalts der erhobenen Bild- und Videodaten überwiegen die Betroffeneninteressen in diesem Fall auch nicht die berechtigten Betreiberinteressen (Eigentumsschutz, Schutz der körperlichen Unversehrtheit, Ausübung des Hausrechts). Intimbereiche wie Umkleiden oder Toiletten dürfen nicht überwacht werden.

Seit dem 1. Januar 2022 gibt es für die Videoüberwachung im Kassenbereich sowie auch des Verkaufsraums auch in Sachsen zusätzlich entsprechende Vorgaben des Unfallversicherungsträgers (DGUV Vorschrift 25 „Überfallprävention"/ Unfallkasse Sachsen), die die Betreiber/innen zur Videoüberwachung von Bereichen verpflichten, in denen Banknoten ausgegeben und entgegengenommen werden. Damit können sich Einzelhandelsunternehmen jetzt insoweit auch auf Art. 6 Abs. 1 Buchst. c und Abs. 2 DSGVO stützen.

Zu beachten ist jedoch, dass eine gezielte Überwachung von Beschäftigten sowie von Dauerarbeitsplätzen nur unter

besonderen Voraussetzungen zulässig ist. Sozialräume und Intimbereiche (Umkleiden, Duschen, Toiletten) dürfen in keinem Fall überwacht werden.
Weitere Informationen zur Videoüberwachung von Beschäftigten finden Sie unter 1.4, Seite 44.
Um der gesetzlichen Informationspflicht (siehe Art. 13 DSGVO) nachzukommen, muss sich vor oder beim Betreten des Ladengeschäfts ein entsprechender Hinweis auf die Videoüberwachung finden. Nur dann können betroffene Personen ihr Verhalten danach ausrichten und sich über die wesentlichen Umstände der Videoüberwachung informieren. Geeignete Vorlagen und weitere Informationen finden Sie unter 1.1.13, Seite 36.

1.9 Videoüberwachung in medizinischen Einrichtungen

Bei Videoüberwachungen in privaten medizinischen Einrichtungen – hierzu zählen nicht nur Krankenhäuser und Arztpraxen, sondern auch ambulante Einrichtungen (unter anderem Physio-/Psychotherapie, Logopädie) – gelten die allgemeinen rechtlichen Vorgaben an eine Videoüberwachungsanlage. Allerdings kann die Eingriffstiefe schon ungleich größer sein, denn bereits die Tatsache, dass eine Person eine Arztpraxis aufsucht, kann im Einzelfall schon als Gesundheitsdatum zu qualifizieren sein, vgl. Art. 4 Nr. 15 DSGVO. Dies hat zur Folge, dass bei derart sensiblen Informationen die rechtlichen Anforderungen nochmals höher sind.
Das Bundesverwaltungsgericht hatte sich im Jahr 2019 mit einer Videoüberwachung in einer Zahnarztpraxis auseinandergesetzt (Urteil vom 27. März 2019, Az. 6 C 2.18) und in seiner Entscheidung klargestellt, dass sich die rechtliche Zulässigkeit (einzig) an der Vorschrift des Art. 6 Abs. 1 Buchst. f DSGVO zu messen hat. Danach muss die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich sein. Außerdem dürfen die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, nicht schwe-

rer wiegen. Es hat also eine zweistufige Prüfung stattzufinden, bei der auf der ersten Stufe zu prüfen ist, ob der Verantwortliche überhaupt schützenswerte Interessen verfolgt und die Videoüberwachung zu deren Wahrnehmung geeignet und erforderlich ist. Auf der zweiten Stufe folgt dann eine Abwägung der wechselseitigen Interessen.

In dem zu entscheidenden Fall hatte die Zahnärztin in den Praxisräumen ein Kamera-Monitor-System angebracht, mit dem sie den Bereich hinter dem Empfangstresen sowie diejenigen Bereiche überwachen konnte, in denen sich die Praxisbesucher – nach dem ungehinderten Betreten der Praxis – aufhalten (Bereich vor dem Empfangstresen, Flur zwischen Eingangstür und Tresen und ein Teil des vom Flur abgehenden Wartebereichs). Hierzu hatte sie oberhalb des Tresens eine Digitalkamera installiert. An der Eingangstür außen sowie am Tresen war jeweils ein Schild mit der Aufschrift „Videogesichert" angebracht. Die Zahnärztin gab vor, durch den ungehinderten Praxiszugang könnten dort unerkannt Straftaten begangen werden. Außerdem müsse sie im Wartebereich sitzenden Patienten rasch zu Hilfe kommen können. Schließlich sei die Zahnärztin auf die Videoüberwachung angewiesen, um ihre Praxisbetriebskosten zu senken.

Das Bundesverwaltungsgericht kam bereits auf der ersten Prüfstufe zu dem Ergebnis, dass keine das allgemeine Lebensrisiko übersteigende Gefahr der Verwirklichung von Straftatbeständen bestand, es also nicht notwendig sei, zur Interessenwahrung die öffentlich zugänglichen Praxisbereiche während der Öffnungszeiten zu überwachen.

Ausschlaggebend hierfür war, dass die Zahnärztin keine einzige Straftat in ihrer eigenen Praxis oder in anderen im selben Gebäude untergebrachten Arztpraxen anführen konnte. Allein das Vorhandensein von Betäubungsmitteln und Wertgegenständen begründe für sich gesehen keine besondere Gefährdung, zumal die Zahnärztin Diebstähle dadurch verhindern konnte, dass sie für eine sichere Aufbewahrung ihrer eigenen werthaltigen Gegenstände sorge. Patienten könne geraten werden, ihre Wertsachen immer bei sich zu haben. Alternativ ließen sich abschließbare Behälter

für Wertgegenstände zur Verfügung stellen. Patienten im Wartebereich könnte ein Notfallknopf in die Hand gegeben werden, um notfalls Hilfe herbeizurufen. Bei der Einsparung von Personalkosten fehlte es an nachprüfbaren Angaben; die Argumentation beschränkte sich auf eine pauschale Behauptung vielfach höherer Kosten.

Weiter stellte das Bundesverwaltungsgericht heraus, dass eine nicht erforderliche Videoüberwachung immer unzulässig ist, sodass sich eine Interessenabwägung erübrigt, wenn keine Gründe aufseiten des Verantwortlichen bestehen, die zu einer Einschränkung des Rechts auf informationelle Selbstbestimmung der betroffenen Personen berechtigen.

Das Anbringen von Hinweisschildern allein führt nicht dazu, dass eine rechtlich unzulässige Videoüberwachung legal wird. Auch deutlich sichtbare Hinweisschilder lassen nicht den Schluss zu, die Praxisbesucher willigten in die Videoüberwachung ein. Mit der bloßen Kenntnisnahme, dem Passieren eines Hinweisschilds oder dem Betreten der überwachten Räume bringen die überwachten Personen nicht ihr Einverständnis mit der Videoüberwachung zum Ausdruck. Es liegt also keine rechtlich wirksame Einwilligung in die Verarbeitung vor (Art. 6 Abs. 1 Buchst. a DSGVO). Vielmehr stehen die Informationspflichten des Art. 13 DSGVO (siehe 1.1.13, Seite 36) in einer Reihe mit den Verantwortlichen treffenden Pflichten nach der DSGVO und knüpfen somit daran an, dass die Videoüberwachung nach der Vorschrift des Art. 6 Abs. 1 DSGVO überhaupt zulässig ist (siehe 1.1.4, Seite 22).

Zusammenfassend lässt sich feststellen, dass eine Videoüberwachung in medizinischen Einrichtungen jedenfalls während der gewöhnlichen Praxisöffnungszeiten dann nicht zulässig ist, wenn Bereiche überwacht werden, die der Allgemeinheit frei zugänglich sind. Hierzu zählen der Eingangs- sowie der Wartebereich ebenso wie die Flure. Während der Praxiszeiten kommt eine Videoüberwachung überhaupt nur im besonderen Ausnahmefall infrage, wenn beispielsweise eine besonders hohe, über dem allgemeinen Lebensrisiko liegende Gefahr für die Begehung von Straftaten besteht. Jedoch gilt auch hier,

dass zuvor alle milderen Mittel geprüft und ausgeschöpft sein müssen. Diese könnten darin bestehen,

- den Empfangstresen permanent mit Personal zu besetzen,
- Schließfächer für Wertsachen bereitzustellen,
- Patienten anzuhalten, ihre Wertsachen mit in das Behandlungszimmer zu nehmen,
- teure medizinische Instrumente, Wertsachen (z. B. Zahngold), Geräte und Medikamente (z. B. Betäubungsmittel) in verschließbaren Schänken oder Behältern aufzubewahren und
- den Patienten die Eingangstür zur Praxis nur mittels eines manuell zu betätigenden oder eines automatischen Türöffners zu öffnen.

Kosteneinsparungen durch einen nicht permanent besetzten Empfangstresen (Personalkosten) kommen nur dann zum Tragen, wenn sich diese Kosten insbesondere durch organisatorische Veränderungen nicht vermeiden oder in einer hinnehmbaren Größenordnung halten lassen. Um die Erforderlichkeit der Videoüberwachung zu begründen, müssen die ohne eine Videoüberwachung entstehenden Kosten im Verhältnis zum Umfang der geschäftlichen Tätigkeit ins Gewicht fallen oder gar deren Wirtschaftlichkeit infrage stellen.
Sollten auch Mitarbeiterbereiche überwacht werden, gelten dort separate Vorschriften (siehe 1.4, Seite 44).

1.10 Freizeiteinrichtungen

Es gibt heute eine Vielzahl an Freizeitangeboten, die von Kinos, Bowlingcentern, Kletterhallen, Escape-Rooms und Spielhallen bis zu Schwimm- oder Erlebnisbädern, Fitnessstudios und Ähnlichem reichen. Aus der Art der Einrichtung sowie der individuellen Gefährdungslage ergeben sich unterschiedliche Anforderungen an eine Videoüberwachung. Zum Teil gibt es auch spezialgesetzliche Vorschriften, die eine Videoüberwachung regeln, wie zum Beispiel die Unfallverhütungsvorschriften in Spielhallen (DGUV Vorschrift 25 „Überfallprävention").

Generell lässt sich feststellen, das **Sitz- und Aufenthaltsebenso wie Wartebereiche** von einer Videoüberwachung auszunehmen sind (siehe 1.5, Seite 53).

Auch in Bereichen mit Dauerarbeitsplätzen ist eine Videoüberwachung im Regelfall unzulässig, zumal bei der **Überwachung von Beschäftigten** strengere rechtliche Vorschriften gelten (siehe 1.4, Seite 44).

Verwaltungsgericht Ansbach, Urteil vom 23. Februar 2022, Az. AN 14 K 20.00083:
↗ sdb.de/vue09

Für **Fitnessstudios** haben die Verwaltungsgerichte entschieden, dass Trainingsflächen nicht überwacht werden dürfen.

Da **Spielhallen** potenziell überfallgefährdet sind, müssen die Betreiber/innen aufgrund der Vorgaben der Unfallversicherungsträger zur Unfallverhütung bestimmte Bereiche (z. B. Zugänge, Kassenbereiche) per Videokamera überwachen, um den Tathergang eines Überfalls zu dokumentieren.

Umkleideräume dürfen grundsätzlich nicht überwacht werden. Eine Ausnahme kann dann gelten, wenn es sowohl überwachte als auch nicht überwachte Umkleidebereiche und Spinde gibt, sodass der Kunde bzw. die Kundin eine echte und freie Wahlmöglichkeit hat, diese wahrzunehmen und zu verstehen in der Lage ist und die persönlichkeitsrechtlichen Interessen Minderjähriger angemessen berücksichtigt werden. Das heißt, Toiletten, Sanitärräume, Saunen und Ähnliches dürfen unter keinen Umständen überwacht werden (siehe 1.1.9, Seite 33).

In jedem Fall muss der/die Betreiber/in die gesetzliche Informationspflicht (siehe Art. 13 DSGVO) einhalten und mit entsprechenden Hinweisen auf die Videoüberwachung aufmerksam machen. Geeignete Vorlagen und weitere Informationen finden Sie unter 1.1.13, Seite 36.

1.11 Öffentlicher Personennahverkehr

Während die Videoüberwachung im Fernverkehr im Regelfall unzulässig ist, dürfen im Nahverkehr Videokameras eingesetzt werden, insbesondere, um Gewalt gegen Fahrgäste zu verhindern oder zu verfolgen, aber auch zum Schutz der Beförderungseinrichtungen (berechtigte Interessen, siehe Art. 6 Abs. 1 Buchst. f DSGVO).

Denkbar ist ein reines Monitoring, wenn interventionsbereites Personal bereitsteht, das bei beobachteten Rechtsverstößen unmittelbar eingreifen kann. Als reine Aufzeichnungslösung kann Videoüberwachung zur Beweissicherung eingesetzt werden, um bei der Aufklärung von Straftaten oder der Durchsetzung von Schadensersatzansprüchen zu helfen.
In jedem Fall haben sich an den Türen von Bussen und Bahnen entsprechende Hinweisschilder zu befinden, mit denen der Verkehrsbetrieb den Kunden/Kundinnen die Pflichtinformationen nach Art. 13 DSGVO zur Verfügung zu stellen hat. Geeignete Vorlagen und weitere Informationen finden Sie unter 1.1.13, Seite 36.

1.12 Tankstellen

Es gibt heutzutage nahezu keine Tankstelle mehr, in der man nicht sowohl rund um die Zapfsäulen als auch innerhalb des Verkaufsraums eine Videoüberwachung vorfindet. Bei der Videoüberwachung dieser Bereiche kann sich der/die Betreiber/in oder Pächter/in auf die Wahrung berechtigter Interessen beziehen (Art. 6 Abs. 1 Buchst. f DSGVO).
Für die Videoüberwachung innerhalb des Kassen- bzw. Verkaufsraums gibt es zusätzlich entsprechende Vorgaben der Unfallversicherungsträger (DGUV Vorschrift 25 „Überfallprävention"), die die Betreiber/innen zur Videoüberwachung von Bereichen verpflichten, in denen Banknoten ausgegeben und entgegengenommen werden (siehe Art. 6 Abs. 1 Buchst. c und Abs. 2 DSGVO).
Tankstellen sind potenziell gefährdete Bereiche, da es dort laut polizeilicher Kriminalitätsstatistik jährlich zu einer fünfstelligen Anzahl an Fällen von Tankbetrug kommt (2022: 85.260, 2021: 58.108). Außerdem bewegt sich die Anzahl polizeilich erfasster Raubüberfälle (Raub und räuberische Erpressung) auf Tankstellen in Deutschland in den letzten zehn Jahren zwischen 500 und 700 Fällen pro Jahr (Quelle: Statista). Demgemäß sind Tankstellen gerade im Hinblick auf Vermögens- und Eigentumsdelikte besonders gefährdet.

Für die datenschutzrechtliche Zulässigkeit reicht diese abstrakte Gefahrenlage aus, von der man dann spricht, wenn eine Situation nach allgemeiner Lebenserfahrung typischerweise gefährlich ist. Die Anzahl der dort begangenen Straftaten sowie die sich daraus ergebenden objektiven Umstände haben auch Einfluss auf die vernünftigen Erwartungen der Tankstellenkundschaft (betroffene Personen). Diese sind darauf eingestellt, dass sich in den besonders gefahrträchtigen Bereichen Videokameras befinden. Diese gelten inzwischen als gesellschaftlich akzeptiert.
Der oder die Tankstellenpächter/in bzw. Inhaber/in hat in jedem Fall mit entsprechenden Hinweisschildern auf die Videoüberwachung aufmerksam zu machen (Informationspflichten, siehe Art. 13 DSGVO). Geeignete Vorlagen und weitere Informationen finden Sie unter 1.1.13, Seite 36.

1.13 Kleingärten

In Kleingärten sind Videokameras zwischenzeitlich sehr verbreitet, wenn man jedenfalls die Anzahl der Datenschutzbeschwerden zugrunde legt. Oftmals bringen Parzelleninhaber/innen Videokameras an. Aber auch Kleingartenvereine versuchen damit, die Kleingartenanlage – gerade außerhalb der Öffnungszeiten – zu schützen.

Kleingartenpächter/in als Betreiber/in:

Betreibt ein/eine Parzelleninhaber/in eine Videokamera, so ist diese genauso zu bewerten wie bei einem privaten selbstbewohnten Grundstück. Der/Die Betreiber/in darf also nur Bereiche bis zur Grenze der eigenen Parzelle überwachen. (Zu berücksichtigen ist bei der Angemessenheit allerdings die Begehbarkeit der einzelnen Parzellen durch weitere Pächter.) Nur dann kann die sogenannte „Haushaltsausnahme" (Art. 2 Abs. 2 Buchst. c DSGVO, siehe 1.1.8, Seite 32) greifen. Überwacht der/die Parzelleninhaber/in jedoch auch Gemeinschaftswege innerhalb einer Kleingartensparte oder andere Bereiche (z. B. öffentliche Verkehrswege oder Parzellen anderer Kleingärtner/innen) ist dies im Regelfall nicht zulässig.

Zwar ließe sich dagegen auch mit den Mitteln des Datenschutzrechts vorgehen, weil es dem/der Kamerabetreiber/in regelmäßig an einem Rechtsgrund aus der Auflistung in Art. 6 Abs. 1 DSGVO fehlen dürfte. Zielführender und erfolgversprechender ist jedoch das privatrechtliche Vorgehen des Kleingartenvereins gegen den/die Parzelleninhaber/in. Denn aktiv betriebene Videokameras stellen eine Leistungsstörung sowie eine Beeinträchtigung des Persönlichkeitsrechts der Mitpächter/innen dar und bedeuten damit letztlich eine Störung des nachbarlichen Verhältnisses innerhalb der Kleingartenanlage.

Der Kleingartenverein als Treuhänder bzw. der Regional-/Kreis-/Stadtverband als Hauptpächter sind deshalb gehalten, gegen den mutmaßlich rechtswidrigen Betrieb der Videoüberwachungsanlage unter Ausschöpfung der zur Verfügung stehenden rechtlichen Möglichkeiten vorzugehen. Diese finden sich in der sowohl für einen Regional-/Kreis-/Stadtverband als auch für jeden Kleingartenverein geltenden Rahmenkleingartenordnung des Landesverbandes Sachsen der Kleingärtner e. V. Die Rahmenkleingartenordnung enthält separate Bestimmungen zu elektronischen Überwachungseinrichtungen und wird automatisch Bestandteil des mit den einzelnen Pächtern bzw. Pächterinnen geschlossenen (Unter-)Pachtvertrags.

Die Rahmenkleingartenordnung verbietet den Einsatz eines automatischen Bildaufzeichnungsgerätes (also einer Videokamera) zur Überwachung außerhalb der Parzellengrenze liegender Flächen (Nummer 7.4). Wird dieses Verbot missachtet, reichen die Maßnahmen des Vereins oder Dachverbandes bei vertragswidrigem Verhalten des Pächters bzw. der Pächterin von der Abmahnung bis zur Kündigung des Pachtvertrags (Nummer 7.6).

Kleingartenverein als Betreiber:

Will ein Kleingartenverein das Vereinsgelände überwachen (Gemeinschaftswege und/oder Parkplätze auf dem Vereinsgelände), um festzustellen, ob sich Unbefugte in der Anlage aufhalten, oder etwa, um eine Beschädigung an geparkten

Fahrzeugen auf dem Mitgliederparkplatz festzustellen, ist dies nach den datenschutzrechtlichen Vorschriften nur in den Zeiten zulässig, in denen sich regulär keine Pächter/innen in der Anlage aufhalten (siehe Art. 6 Abs. 1 Buchst. f DSGVO).
Gibt es hingegen keine zeitlichen Einschränkungen, kann also der bzw. die einzelne Parzelleninhaber/in jederzeit die Kleingartensparte betreten und verlassen, wäre eine Videoüberwachung ein unzulässiger Eingriff in das Grundrecht auf informationelle Selbstbestimmung. Ein/Eine Parzelleninhaber/in sowie seine/ihre Familienangehörigen und Besucher/innen müssen es nicht hinnehmen, dass sie beim Aufsuchen und Verlassen der Kleingartenanlage und insbesondere beim Besuch der eigenen Parzelle überwacht werden.
Gerade bei abgelegenen Kleingartensparten kommt es vor, dass dort neben dem Zaun, der die Anlage umgibt, wild Müll abgelagert wird oder sich Hinterlassenschaften von Hunden finden. Zwar ist hier dem Verein kein berechtigtes Interesse abzusprechen. Jedoch gilt auch hier, dass er nicht das Recht hat, öffentliche Verkehrsflächen oder private Grundstücke anderer, die an die Kleingartensparte angrenzen, zu überwachen. Dort überwiegen die Interessen der betroffenen Personen bei der nach Art. 6 Abs. 1 Buchst. f DSGVO vorzunehmenden Interessenabwägung.
Selbstverständlich dürfen aus den gleichen Gründen von Vereinsseite auch nicht einzelne Parzellen überwacht werden.

1.14 Videoüberwachung zur Dokumentation von Ordnungswidrigkeiten

Die Verarbeitung personenbezogener Daten zum Zweck einer Anzeige und des Nachweises einer wahrgenommenen Ordnungswidrigkeit – unter anderem durch Beweisfotos oder Videoaufnahmen – gegenüber der jeweils zuständigen Behörde stellt regelmäßig keine ausschließlich persönliche oder familiäre Tätigkeit im Sinne von Art. 2 Abs. 2 Buchst. c DSGVO (siehe auch 1.1.8, Seite 32) dar und bedarf daher einer

Rechtsgrundlage gemäß Art. 6 Abs. 1 DSGVO. Der/Die Anzeigeerstatter/in ist insoweit, zum Beispiel bei der Erstellung einer Abbildung mit Personen oder personenbeziehbaren Informationen zum Beweis einer Verfehlung, Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO.

Die einschlägige Rechtsprechung differenzierte in dieser Frage bislang im Wesentlichen nach dem Interesse, das die anzeigende Privatperson verfolgt. In der Regel wurden Anzeigen von Gesetzesverstößen (inklusive Beweisfotos) dann als gerechtfertigt angesehen, wenn der/die Anzeigeerstatter/in von dem Gesetzesverstoß in seinen eigenen Rechten beeinträchtigt war, auch wenn durch sie zugleich in subjektive Rechte der/des Angezeigten eingegriffen bzw. deren/dessen persönliche Belange beeinträchtigt werden. In diesen Fällen wird die in der Anzeigeerstattung liegende Verarbeitung der Daten des Dritten als zur Wahrung der berechtigten Interessen des Verantwortlichen (Anzeigeerstatter/in) erforderlich angesehen, weil dieser mit der Anzeige das legitime Ziel verfolgt, die Beeinträchtigung seiner Rechte zu beenden und den/die Verursacher/in von künftigen Rechtsbeeinträchtigungen abzuhalten. Der/Die Anzeigeerstatter/in kann sich dabei auf den Erlaubnistatbestand in Art. 6 Abs. 1 Buchst. f DSGVO beziehen.

Nicht ausreichend als Rechtfertigung ist beispielsweise das Fertigen von Fotografien oder Videoaufnahmen einer mutmaßlichen Ordnungswidrigkeit und deren Übersendung an die Verfolgungsbehörde zum Zweck des beabsichtigten Schutzes der öffentlichen Ordnung, ohne dass eigene Interessen des Aufnehmenden tangiert bzw. beeinträchtigt sind. Zu betonen ist, dass der/die Einzelne eben nicht Sachwalter/in öffentlicher Interessen ist.

Vereinzelt wird hingegen seitens öffentlicher Stellen, zum Teil ohne Differenzierung, immer noch davon ausgegangen, dass jedermann gegenüber Polizeibehörden bzw. dem Ordnungsamt Rechtsverstöße melden und dabei auch Fotografien oder Videoclips von Handlungen, etwa von unzulässig abgestellten Kraftfahrzeugen, anfertigen und dorthin übermitteln könne. Entscheidend ist nach Einschätzung der

Sächsischen Datenschutz- und Transparenzbeauftragten aber, ob Anzeige und „Beweisfotos" des/der privaten Anzeigeerstatters/Anzeigeerstatterin zur Wahrung dessen/deren eigener berechtigten Interessen oder derjenigen eines Dritten erforderlich sind und die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, nicht überwiegen, vgl. den Wortlaut des Art. 6 Abs. 1 Buchst. f DSGVO. Das Verwaltungsgericht Ansbach hat in der Rechtssache AN 14 K 22.00468 und AN 14 K 21.01431 vom 2.11.2022 eine andere Auffassung vertreten. Eine höchstrichterliche Rechtsprechung in dieser Frage steht bislang noch aus.

1.15 Besondere Verarbeitungssituationen

1.15.1 Bodycams

Nicht nur die Polizei (siehe 3.1.2, Seite 101), sondern auch private Sicherheitsunternehmen statten ihre Beschäftigten mit an der Kleidung befestigten Kameras aus, den sogenannten Bodycams. Damit möchten die Firmen ihre Beschäftigten vor Übergriffen schützen, Beweismittel für zivilrechtliche Ansprüche beschaffen oder eine abschreckende bzw. deeskalierende Wirkung erzielen.

Die Nutzung von Bodycams ist jedoch oft mit Eingriffen in die Datenschutzrechte einer unkontrollierbaren Anzahl von Personen verbunden. Deshalb können Bodycams nur unter bestimmten Voraussetzungen rechtmäßig eingesetzt werden. Insbesondere ist zwischen dem Interesse der Betreibenden und den Rechten der Gefilmten gemäß Art. 6 Abs. 1 Buchst. f DSGVO abzuwägen. Des Weiteren lassen sich die Transparenzvorgaben gemäß Art. 12ff. DSGVO nur schwer umsetzen, was auf die sich ständig ändernden Aufnahmebereiche zurückzuführen ist. Der Einsatz von Bodycams muss daher stets anlassbezogen sowie zweckgebunden sein. Außerdem wird ein Einsatzkonzept benötigt, das vor Inbetriebnahme erstellt werden muss. Die Beschäftigten sind zumindest mittelbar vom Einsatz

der Bodycams betroffen, insbesondere erlauben diese Rückschlüsse auf das Verhalten und die Leistung von Beschäftigten. Die Verarbeitung personenbezogener Beschäftigtendaten ist daher in einer Betriebsvereinbarung zu regeln.

Orientierungshilfe der Datenschutzkonferenz zum Einsatz von Bodycams durch private Sicherheitsunternehmen:
↗ sdb.de/vue10

Ausführlichere datenschutzrechtliche Informationen zu Bodycams für private Sicherheitsunternehmen hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) zusammengestellt.

1.15.2 Dashcams und Fahrzeugüberwachung

Dashcams (oder Unfallkameras) sind kleine Videokameras, die an einem Kraftfahrzeug oder einem Zweirad, gegebenenfalls auch am Helm des Fahrers, 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 gegebenenfalls ein Verschulden des Unfallgegners nachweisen zu können.

Die für den Betrieb einer Dashcam einzig infrage kommende **Zulässigkeitsvorschrift** ist Art. 6 Abs. 1 Buchst. f DSGVO. Danach ist die Verarbeitung, mithin der Betrieb einer Dashcam einschließlich der Speicherung von Videoaufnahmen, nur dann zulässig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Diese Voraussetzungen sind grundsätzlich nur bei anlassbedingten Aufzeichnungen, das heißt bei besonderen Verkehrssituationen (z. B. Unfällen) erfüllt. Um den Ablauf des betreffenden Geschehens auch in seiner Entstehung nachvollziehen zu können, ist ein gewisser – zunächst einmal anlassfreier – Vorlauf der Videoaufzeichnungen notwendig. Dafür sind aber regelmäßig **ein bis drei Minuten** vollkommen ausreichend. Ohne besondere Vorkommnisse dürfen also in

aller Regel nicht mehr als maximal drei Minuten Videoaufzeichnungen auf der Speicherkarte einer Dashcam enthalten sein. Eine durch besondere Verkehrsereignisse gerechtfertigte längerfristige Speicherung (Überschreibschutz) kann durch manuelle Bedienhandlungen an der Dashcam selbst (Speichertaste), außergewöhnliche Fahrzeugbewegungen (G-Sensoren) oder für Gefahrensituationen typische Bedienhandlungen am Fahrzeug (Vollbremsung) ausgelöst werden.
Der **Bundesgerichtshof** hat diesbezüglich festgestellt (Urteil vom 15. Mai 2018, VI ZR 233/17), dass eine permanente anlasslose Aufzeichnung des gesamten Geschehens auf und entlang der Fahrstrecke zur Wahrnehmung von Beweissicherungsinteressen nicht erforderlich und damit nach den geltenden datenschutzrechtlichen Bestimmungen **unzulässig** ist. Weder könne sie auf eine Einwilligung noch auf eine entsprechende Interessenabwägung gestützt werden. Es sei technisch möglich, eine kurze, anlassbezogene Aufzeichnung des unmittelbaren Unfallgeschehens zu gestalten, beispielsweise durch ein dauerndes Überschreiben der Aufzeichnungen in kurzen Abständen und Auslösen der dauerhaften Speicherung erst bei Kollision oder starker Verzögerung des Fahrzeuges.

1.15.2.1 Sind Innenkameras zulässig?

Ohne datenschutzrechtliche Relevanz sind Innenaufnahmen nur, soweit eventuelle Mitfahrer/innen zum familiären Umfeld der Fahrerin/des Fahrers gehören. In diesem Fall greift die sogenannte „Haushaltsausnahme" (siehe 1.1.8, Seite 32). Nicht zum Familienkreis zählende Mitfahrer/innen müssten ausdrücklich vorab in die Videoaufzeichnung einwilligen (siehe hierzu auch 1.1.7, Seite 31). Diesbezüglich ist der/die Fahrer/in in der Nachweispflicht (siehe 1.1.6, Seite 28).
Angesichts der damit verbundenen praktischen Schwierigkeiten sollten gegebenenfalls vorhandene Innenkameras in jedem Fall deaktiviert werden, zumal nicht ersichtlich ist, inwieweit derartige Aufnahmen zum Erreichen des verfolgten Zweckes – Beweissicherung bei Verkehrsvorkommnissen – geeignet und erforderlich sein sollen.

1.15.2.2 Darf ich das Mikrofon einer Dashcam aktivieren?

Die in Dashcams standardmäßig integrierten Mikrofone ermöglichen Aufnahmen der im oder aus dem Fahrzeug geführten Gespräche, insbesondere auch der über Freisprechanlage geführten Telefonate. Auch hier ist nicht ersichtlich, inwieweit derartige Aufnahmen zum Erreichen des verfolgten Zweckes – Beweissicherung bei Verkehrsvorkommnissen – beitragen und dementsprechend erforderlich sein sollen. Audioaufnahmen verstoßen damit regelmäßig gegen Datenschutzvorschriften und sind daher rechtswidrig.
Werden die Gesprächsteilnehmer nicht darauf hingewiesen, steht darüber hinaus der Straftatbestand des § 201 Abs. 1 Nr. 1 StGB im Raum (siehe hierzu auch 1.1.9, Seite 33).

1.15.2.3 Darf ich zusätzlich eine Heckkamera einsetzen?

Für eine gegebenenfalls eingesetzte Heckkamera gelten grundsätzlich die gleichen Voraussetzungen wie für eine Frontkamera.

1.15.2.4 Wie ist die Rechtslage bei fest eingebauten Kameras?

Fest in das Fahrzeug integrierte Kameras unterstützen spezielle Fahrzeugfunktionen bzw. ermöglichen diese überhaupt erst (z. B. Verkehrszeichenerkennung, Rückfahrkamera, Spurhalteassistent). Dies erfolgt regelmäßig ohne Aufzeichnung; die damit gegebenenfalls verbundene Verarbeitung personenbezogener Daten ist daher über die Interessenabwägung des Art. 6 Abs. 1 Buchst. f DSGVO zu rechtfertigen.
Soweit entsprechende Kameras (wie beispielsweise beim Tesla) auch im Sinne einer Dashcam betrieben werden, gelten die oben beschriebenen Anforderungen.

1.15.2.5 Darf ich eine Dashcam im geparkten Fahrzeug betreiben?

Wird eine Dashcam im Parkmodus betrieben, sind an sie die gleichen rechtlichen Anforderungen wie bei einer stationären Kamera zu stellen.

Unkritisch ist demnach der Kamerabetrieb, wenn das Fahrzeug auf nichtöffentlichem, ausschließlich selbstgenutztem Gelände abgestellt wird, zum Beispiel in einer Garage oder einem Carport. Anders verhält es sich beim Einsatz auf öffentlichen Parkflächen, am Straßenrand oder auch in sonstigen durch Dritte nutzbaren Bereichen (z. B. Tiefgaragen in Mietobjekten). Dort ist der Betrieb der Dashcam unzulässig, da regelmäßig das Interesse der sich im Umfeld des Fahrzeugs bewegenden Personen (z. B. Passanten oder Mitmieter/innen), nicht von Privatpersonen grundlos videografiert zu werden, überwiegt.
In Analogie zum fahrenden Fahrzeug als Ausnahme vorstellbar wäre eine anlassgesteuerte Videoaufzeichnung über einen kurzen Zeitraum, wobei aber entsprechend hohe Anforderungen an den auslösenden Anlass zu stellen wären (z. B. unbefugt versuchte Fahrzeugöffnung). Solcherart (rechtskonforme) Umsetzungen des Parkmodus sind aber bislang nicht bekannt.

1.15.2.6 Darf ich eine Panoramafahrt aufzeichnen?

Gegen persönlich bzw. familiär motivierte Dashcam-Aufnahmen im Urlaub (z. B. bei landschaftlich reizvoller Streckenführung) oder bei Freizeitaktivitäten (z. B. Motorradausfahrten, Fahrradtouren) bestehen keine Einwände. Hier ist die Berufung auf die sogenannte „Haushaltsausnahme", das heißt die Ausnahmeregelung des Art. 2 Abs. 2 Buchst. c DSGVO, möglich.

1.15.2.7 Was gilt für Fahrrad- und Motorradfahrer?

Die an Dashcams in Autos gestellten Anforderungen gelten grundsätzlich auch für durch Fahrrad- oder Motorradfahrer genutzte Helmkameras bzw. für an Fahrrädern oder Motorrädern anderweitig befestigte Kameras.

1.15.2.8 Muss ich an meinem Fahrzeug Hinweise zum Einsatz einer Dashcam anbringen?

Es liegt auf der Hand, dass die Umsetzung der in Art. 12ff. DSGVO geregelten Informationspflichten jedenfalls bei fahrenden Fahrzeugen erhebliche Schwierigkeiten bereitet.

Unabhängig von der Frage der Zulässigkeit des Dashcam-Betriebs wird diesbezüglich wohl regelmäßig formal von einem Datenschutzverstoß auszugehen sein. Bei parkenden Fahrzeugen hingegen dürften einer gesetzeskonformen Kennzeichnung, mithin also einer vollständigen Information nach Art. 13 DSGVO, sicherlich keine maßgeblichen Einwände entgegengestellt werden können; gleichwohl stellt sich hier wie dargestellt zunächst die Frage der Zulässigkeit des Kamerabetriebs überhaupt und damit der praktischen Relevanz.

1.15.2.9 Weshalb werden Dashcams verkauft, obwohl sie sich überwiegend gar nicht rechtskonform einsetzen lassen?

Auch wenn der Einsatz von Dashcams vorrangig auf die Beweissicherung im Straßenverkehr zielt, ist ihr Anwendungsbereich nicht darauf beschränkt. Das heißt, es gibt darüber hinaus auch andere Anwendungsgebiete, in denen die Datenschutzvorschriften entweder nicht greifen oder einem Einsatz nicht entgegenstehen. So kann eine Dashcam auch außerhalb des öffentlichen Verkehrsraumes oder für ausschließlich persönliche Zwecke eingesetzt werden. Mithin ist der Einsatz einer Dashcam nicht per se unzulässig, das heißt, ein generelles Einsatzverbot existiert nicht.
Inzwischen sind auch erste Typen am Markt, die den eingangs dargestellten Anforderungen an einen zulässigen Dashcam-Betrieb zur Beweissicherung im Straßenverkehr entsprechen und insoweit datenschutzkonform eingesetzt werden können.

1.15.2.10 Warum soll ich eine Dashcam nicht betreiben dürfen, obwohl die Gerichte damit erstellte Aufzeichnungen doch als Beweismittel anerkennen?

Die Frage der zivil- bzw. strafrechtlichen Beweisverwertung ist strikt von der datenschutzrechtlichen Zulässigkeit zu trennen. Wenn **Zivil- und Strafgerichte** im Einzelfall mit Dashcams erstellte Videoaufzeichnungen als Beweismittel anerkennen, lassen sie regelmäßig die datenschutzrechtliche Zulässigkeit des Einsatzes der Dashcams offen und setzen sich allein mit der Frage auseinander, ob aus einer datenschutzrechtlichen

Unzulässigkeit des Betriebs einer Dashcam ein sogenanntes Beweisverwertungsverbot im konkreten Zivil- oder Strafverfahren folgt. Die stattdessen mit der Frage der datenschutzrechtlichen Zulässigkeit befassten **Verwaltungsgerichte** haben hingegen klargestellt, dass der Einsatz von Dashcams durch Private im öffentlichen Straßenverkehr datenschutzrechtswidrig ist.

In diesem Sinne ist auch das Urteil des Bundesgerichtshofs (BGH, Urteil vom 15. Mai 2018, VI ZR 233/17) zu verstehen. Einerseits hat der BGH entschieden, dass Dashcam-Aufnahmen unter gewissen Voraussetzungen als Beweismittel bei Unfall-Prozessen verwertbar sind. Andererseits hat der BGH aber klar festgestellt, dass eine permanente anlasslose Aufzeichnung des gesamten Geschehens auf und entlang der Fahrstrecke zur Wahrnehmung von Beweissicherungsinteressen nicht erforderlich und damit nach den geltenden datenschutzrechtlichen Bestimmungen unzulässig ist. Denn es sei technisch möglich, eine kurze, anlassbezogene Aufzeichnung des unmittelbaren Unfallgeschehens zu gestalten, beispielsweise durch ein dauerndes Überschreiben der Aufzeichnungen in kurzen Abständen und Auslösen der dauerhaften Speicherung erst bei Kollision oder starker Verzögerung des Fahrzeuges.

Wird also eine Dashcam eingesetzt, die diesen Anforderungen genügt, stehen ihrem Einsatz im Ergebnis auch keine datenschutzrechtlichen Bedenken entgegen.

1.15.2.11 Welche Bußgelder drohen bei unrechtmäßigem Dashcam-Einsatz?

Gegen Privatpersonen wurden in Sachsen bisher Bußgelder bis zu 1.000 Euro festgesetzt; bei gewerblicher Nutzung können diese auch deutlich höher ausfallen.

1.15.2.12 Gegen wen richten sich diesbezügliche Ordnungswidrigkeitsverfahren?

Diesbezügliche Ordnungswidrigkeitsverfahren richten sich regelmäßig gegen den/die Fahrer/in des betreffenden Fahrzeugs, nicht hingegen gegen den/die Fahrzeughalter/in, auch wenn diese/r die Dashcam installiert hat.

1.15.2.13 Wann tritt bei festgestellten Dashcam-Verstößen Verjährung ein?

Bei Verstößen gegen die Datenschutz-Grundverordnung beträgt die Verjährung drei Jahre. Danach kann die Tat nicht mehr als Ordnungswidrigkeit verfolgt werden.

1.15.2.14 Weitere Informationen zu Dashcams

- Positionspapier der Datenschutzkonferenz zur Videoüberwachung aus Fahrzeugen mit sogenannten Dashcams: ↗ sdb.de/vue11
- Dashcams und Helmkameras
  in: Tätigkeitsbericht 2020, 2.2.30, Seite 86ff., abrufbar unter: ↗ sdb.de/tb2020

1.15.3 Drohnen

Kameradrohnen sind – ebenso wie herkömmliche Videokameras – in den letzten Jahren stets preiswerter geworden und lassen sich jetzt zu erschwinglichen Preisen erwerben. Deshalb werden sie auch häufig privat in der Freizeit oder für gewerbliche Zwecke eingesetzt. Natürliche Barrieren, wie Mauern, Zäune oder Sichtschutze, die vor neugierigen Blicken schützen, stellen keine Hindernisse mehr dar und lassen sich ohne Probleme überwinden. Einzig die technischen Spezifikationen der eingesetzten Kamera setzen dem überwachten Bereich und der Qualität der Bildaufnahmen Grenzen. Sie ermöglichen damit den Blick in fremde Gärten, Sonnenterrassen, Freibäder oder öffentliche Straßen und Plätze und geben so immer wieder Anlass für Streitigkeiten und Beschwerden. Denn ob eine Drohne mit einer Kamera ausgestattet ist und welche Bereiche mit dieser erfasst werden, lässt sich für betroffene Personen kaum feststellen.
Grundsätzlich dürfen Drohnen mit Foto- oder Videoausstattung nur eingesetzt werden, wenn Persönlichkeitsrechte Dritter nicht verletzt werden. Erfasst eine mit einer Kamera versehene Drohne nur den eigenen Garten oder andere Bereiche des ausschließlich selbstbewohnten Grundstücks, kann sich

der/die Drohnenpilot/in auf die sogenannte „Haushaltsausnahme" (Art. 2 Abs. 2 Buchst. c DSGVO) berufen (siehe hierzu auch 1.1.8, Seite 19). Werden hingegen Aufnahmen im öffentlichen Raum oder auf Grundstücken in der Nachbarschaft getätigt, ist das Risiko groß, dass dort in Persönlichkeitsrechte Dritter – das heißt das Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG) – eingegriffen wird, da dann der Anwendungsbereich der Datenschutz-Grundverordnung eröffnet ist. Für einen legalen Betrieb gilt auch hier, dass der Verantwortliche eine Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO benötigt.
Den für eine mobile Datenverarbeitung zusätzlich geltenden gesetzlichen Anforderungen, insbesondere der damit verbundenen Informationspflicht (Art. 13 DSGVO), kann beim Einsatz einer Kameradrohne jedoch kaum entsprochen werden (siehe hierzu 1.15.2.8, Seite 73). Erschwerend kommt hinzu, dass eine betroffene Person nicht ohne Weiteres erkennen kann, wer der/die Drohnenpilot/in und damit der/die im Datenschutzsinne Verantwortliche ist.

Positionspapier der Datenschutzkonferenz zur Nutzung von Kameradrohnen durch nichtöffentliche Stellen:
↗ sdb.de/vue12

1.15.4 Klingelkameras und Türspione

Gegen den Einsatz von digitalen Türspionen sowie Klingelkameras gibt es dann keine Einwände, wenn folgende Voraussetzungen erfüllt sind:

- Die Kamera darf nur anlassbezogen durch das Klingeln an der Tür aktiviert werden können.
- Die Kamera darf nur den unmittelbaren Eingangsbereich (Nahbereich) vor der Tür erfassen.
- Die Kamera muss nach kurzer Zeit automatisch wieder deaktiviert werden.
- Es darf keine Übertragung des Livebildes über das Internet erfolgen.
- Es darf keine Aufzeichnung der Bilder erfolgen.

Die dauerhafte und anlasslose Bildübertragung öffentlicher Räume muss also technisch ausgeschlossen sein. Ein System, das in Wohnbereichen sowohl als Überwachungs- wie auch

als Tür- und Klingelkamera eingesetzt, also durch Bewegung, manuell oder per Smartphone aktiviert werden kann (gegebenenfalls ein Pre-Recording einsetzt) und dabei den öffentlichen Raum oder nichtöffentliche Gemeinschaftsflächen erfasst, erfüllt die rechtlichen Anforderungen an eine Videoüberwachung in der Regel nicht.

1.15.5 Webcams

Übersichtskameras verfolgen meist den Zweck, die aktuelle Wetter- oder Verkehrslage anzuzeigen oder den Baufortschritt zu dokumentieren (siehe hierzu auch 1.7, Seite 56). Die Überwachung von Personen ist dabei regelmäßig nicht gewollt oder beabsichtigt.

Allerdings besteht – je nach Kameraeinstellung und Art und Weise der Datenverarbeitung – auch bei Übersichtsaufnahmen ein besonderes Risiko für die Persönlichkeitsrechte der Betroffenen. Dies gilt vor allem dann, wenn Kamerabilder des öffentlichen Verkehrsraums oder von 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 Datenschutzverstoß 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, es sich also nicht um personenbezogene Daten handelt (siehe Art. 4 Nr. 1 DSGVO). Dies ist dann der Fall, wenn Einzelpersonen, Kraftfahrzeuge und (Wohn-)Gebäude oder Geschäfte nur schemenhaft abgebildet werden und sich damit keine Zuordnung zu einer bestimmten natürlichen Person vornehmen lässt.

Erreichen lässt sich dies mit der entsprechenden Kamerapositionierung, fehlender Zoom-Möglichkeit und einer niedrigen Bildauflösung. Eine laufende Bildübertragung ist in der Regel nicht erforderlich und daher nur zulässig, wenn ein Personen-

bezug ausgeschlossen werden kann. Die Bildübertragung muss so eingestellt sein, dass ein Bezug oder Rückschluss auf einzelne Personen auch über einen längeren Beobachtungszeitraum nicht möglich ist. Statt der dauerhaften Bildübertragung sollten deshalb nur Einzelbilder dargestellt werden. Die dargestellten Bilder sollten automatisch aktualisiert werden und nicht vom Betrachter selbst. Dabei sollte der Aktualisierungszyklus möglichst groß gewählt werden.
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 einzuhalten (siehe hierzu insbesondere 1.1.4, Seite 22). Von der Bildübertragung in Echtzeit ins Internet ist dann dringend abzusehen.

1.15.6 Wildkameras

Waldbesucher, Spaziergänger und Wanderer nutzen den Wald in ihrer Freizeit und um sich zu erholen. Besteht kein erkennbares Betretungsverbot, ist es den Waldbesuchern nach den Landeswaldgesetzen gestattet, den Wald zum Zweck der Erholung zu betreten (§ 11 Abs. 1 Satz 1 Sächsisches Waldgesetz). Damit handelt es sich um öffentlich zugängliche Bereiche. Dementsprechend kommt bei der Überwachung mittels Wildkamera den Persönlichkeitsrechten der betroffenen Personen hier ein hoher Stellenwert zu.
So dürfen Bereiche, die sich in **unmittelbarer Nähe zu einem Waldweg, einer Grillstelle und insbesondere zu einem Spielplatz** befinden, nicht überwacht werden. Dort überwiegen die schützenswerten Interessen der Waldbesucher. Sie müssen in diesen Bereichen nicht mit einer (gegebenenfalls heimlichen oder versteckten) Kameraüberwachung rechnen.
Die Videoüberwachung mit Wildkameras lässt sich bei Vorliegen der rechtlichen Voraussetzungen nur auf die Wahrung berechtigter Interessen stützen (Art. 6 Abs. 1 Buchst. f DSGVO).

Liegt ein berechtigtes Interesse des Überwachenden vor (z. B. bei einer Kirr- oder Futterstelle), ist vor dem Einsatz einer Wildkamera immer zu prüfen, ob es mildere Mittel gibt, also beispielsweise ob der Einsatz von Wilduhren infrage kommt. Die Videoüberwachung mit einer Wildkamera kann nur dann zulässig sein, wenn die Aufnahme von Menschen äußerst unwahrscheinlich ist und mit allen verfügbaren Mitteln von dem/der Betreiber/in ausgeschlossen wird.

Erreichen lässt sich dies wie folgt:

- Die Kamera wird auf ungefähr einem Meter Höhe angebracht und ist direkt auf den Waldboden oder eine Futterstelle ausgerichtet.
- Es wird nur unmittelbar auf Kniehöhe aufgenommen.
- Die Kamera ist technisch so eingestellt, dass ausschließlich Einzelbilder (keine Videos) mit einigen Sekunden Abstand aufgenommen werden.
- Die Auflösung der Kamera sollte gering gewählt sein, da eine personenscharfe Darstellung zur Wildtierbeobachtung nicht erforderlich ist.
- Ist die Überwachung von Tieren in der Nacht geplant, ist die Kamera zudem tagsüber auszuschalten.

Der überwachte Bereich sollte für Waldbesucher erkennbar mit einem **Betretungsverbot** ausgeschildert sein. In jedem Fall sind auch hier die datenschutzrechtlichen Informationspflichten zu beachten (Art. 13 DSGVO). **Hinweise** auf eine Kameraüberwachung mit der Angabe des Verantwortlichen sind in jedem Fall erforderlich (siehe 1.1.13, Seite 36).

1.15.7 Parkraumüberwachung

Es gibt zwischenzeitlich zahlreiche Unternehmen, die die digitale Parkraumüberwachung unter Einsatz von Videotechnik anbieten. Immer häufiger sind diese deshalb auf Parkplätzen anzutreffen, beispielsweise von Supermärkten und Discountern, aber auch in Parkhäusern und Tiefgaragen. Auf dem Markt existieren unterschiedliche Kennzeichener-

fassungssysteme, je nach Hersteller sowie beabsichtigtem Einsatzgebiet.

Bei gebührenpflichtigen Parkflächen (Parkhäuser, Tiefgaragen) soll mittels Videokameras überwacht werden, dass jedes ausfahrende Fahrzeug die fällige Parkgebühr beglichen hat. Supermärkte, Discounter und anderen Geschäfte des Einzelhandels hingegen stellen ihren Kundinnen und Kunden kostenfreie Parkplätze zur Verfügung. Sie haben allerdings ein großes Interesse daran, dort Dauer- und Fremdparker/innen zu vermeiden und diese von den Kundenparkplätzen fernzuhalten. Deshalb geben sie eine Höchstparkdauer für die Dauer des Einkaufs vor, bei deren Überschreitung eine Vertragsstrafe verhängt wird.

Die technische Umsetzung stellt sich so dar: Bei der Einfahrt wird das Kfz-Kennzeichen gescannt. Zum Einsatz kommen dabei spezielle Kameras, die nur das Kfz-Kennzeichen fotografieren, mittels Texterkennung aus der Bilddatei dann das jeweilige Kfz-Kennzeichen ermitteln und in einer Datenbank speichern, zusammen mit Datum und Uhrzeit. Beim Verlassen des Parkplatzes wird das Kfz-Kennzeichen nochmals erfasst und mit den zum Zeitpunkt der Einfahrt gespeicherten Daten verglichen. Bei kostenpflichtigen Parkplätzen wird auf diese Art ermittelt, ob die Parkgebühr bezahlt wurde. In diesem Fall gibt der Kunde/die Kundin zuvor beim Bezahlvorgang sein Kfz-Kennzeichen am Parkautomaten ein. Bei für einen bestimmten Zeitraum kostenfreien Parkplätzen wird geprüft, inwieweit der Benutzer die Höchstparkdauer überschritten hat. Wird bei diesem Abgleich festgestellt, dass die Zeitgrenze nicht eingehalten wurde oder bei kostenpflichtigem Parkraum die fällige Gebühr nicht entrichtet wurde, wird dies entsprechend dokumentiert und längerfristig gespeichert, um auf dieser Grundlage entsprechende finanzielle Ansprüche geltend zu machen.

Wird die Höchstparkdauer nicht beachtet, verhängt der Parkraumbewirtschafter gegenüber dem/der Kfz-Halter/in eine Vertragsstrafe. Rechtlich gesehen schließt der/die Benutzer/in mit dem Abstellen seines/ihres Fahrzeugs auf dem Privatparkplatz einen privatrechtlichen Vertrag ab, dessen

Bestandteil auch allgemeine Geschäftsbedingungen sind, in denen diese Vertragsstrafe geregelt ist. Um an die Halterdaten zu gelangen, wird das gespeicherte Kfz-Kennzeichen für eine sogenannte einfache Halterabfrage (§ 39 Abs. 1 Straßenverkehrsgesetz) verwendet. Stellt sich bei kostenpflichtigen Parkplätzen (Parkhaus, Tiefgarage) bei Ausfahrt an der Schranke heraus, dass das fällige Parkentgelt nicht beglichen wurde, bleibt die Schranke bis zur Entrichtung der Parkgebühr geschlossen.

Bei der automatisierten Kennzeichenerfassung werden personenbezogene Daten der Fahrzeughalter/innen verarbeitet. Für die Erfassung (Scanvorgang), die Speicherung sowie die weitere Datenverarbeitung benötigt der/die Betreiber/in eine Rechtsgrundlage aus dem Katalog des Art. 6 Abs. 1 DSGVO. Hierfür kommen zunächst vertragliche Regelungen (Art. 6 Abs. 1 Buchst. b DSGVO) in Betracht, insbesondere bei Dauerparkern. Ansonsten richtet sich die Bewertung der Zulässigkeit der Kennzeichenverarbeitung nach der Vorschrift des Art. 6 Abs. 1 Buchst. f DSGVO. Hierbei wird das berechtigte Interesse des Parkraumbewirtschafters an einer ordnungsgemäßen Nutzung des Parkplatzes höher bewertet als die Rechte und Freiheiten der Parkplatznutzer/innen.

Problematisch könnte sein, zu welchem Zeitpunkt der Kunde/die Kundin über den Kennzeichenscan informiert wird, da auch in diesem Fall die Informationspflichten des Art. 13 DSGVO zu beachten sind. Insbesondere gilt es dabei zu berücksichtigen, ob die Kundschaft bei Kenntnis der Kennzeichenerfassung noch die Möglichkeit zum Umkehren hat. Ist ein Hinweisschild erst unmittelbar bei der Einfahrtschranke angebracht, könnte ein Umdrehen mit dem Fahrzeug kaum noch möglich sein. Inhaltlich muss sich den Hinweisen außerdem entnehmen lassen, dass (nur) eine Kennzeichenerfassung stattfindet und gerade keine Übersichtsaufnahmen oder Ähnliches erstellt werden – die Bezeichnung „Videoüberwachung" sollte daher auf dem Hinweisschild möglichst durch die Bezeichnung „Kfz-Kennzeichenerfassung" ersetzt werden.

1.16 Weitere Informationen zur Videoüberwachung durch nichtöffentliche Stellen

- Kurzpapier der Datenschutzkonferenz zur Videoüberwachung: ↗ sdb.de/vue13
- Orientierungshilfe der Datenschutzkonferenz zur Videoüberwachung durch nichtöffentliche Stellen: ↗ sdb.de/tb2107
- Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte: ↗ sdb.de/vue14
- Checkliste der Berliner Beauftragten für Datenschutz und Informationsfreiheit zur Prüfung der Zulässigkeit einer Videoüberwachung: ↗ sdb.de/vue15

2 Videoüberwachung im öffentlichen Bereich, insbesondere durch Kommunen

2.1 Rechtsgrundlagen der kommunalen Videoüberwachung

Die nachfolgenden Informationen basieren auf der „Orientierungshilfe zur Videoüberwachung durch Kommunen":
↗ sdb.de/vue16

Jegliche Überwachungsmaßnahmen stellen zunächst einen Eingriff in das verfassungsmäßig garantierte Persönlichkeitsrecht der betroffenen Person/en dar. Alle Menschen haben das Recht zur freien Bewegung in der Öffentlichkeit, und zwar, ohne dass dies von staatlichen oder öffentlichen Stellen kontrolliert oder erfasst wird. Videoüberwachung ist deshalb nur dann zulässig, wenn es dafür eine gesetzliche Grundlage gibt und die darin vorgesehenen Voraussetzungen allesamt erfüllt sind.

Weder in der Sächsischen Gemeindeordnung noch in der Sächsischen Landkreisordnung findet sich eine ausdrückliche Regelung zur Videoüberwachung. Die gesetzlichen Grundlagen finden sich vielmehr in zwei anderen Gesetzen.

Wird die Gemeinde als allgemeine oder besondere Polizeibehörde tätig, findet sich eine Regelung zur Videoüberwachung in § 30 Abs. 1 Sächsisches Polizeibehördengesetz (SächsPBG). Wird die Gemeinde nicht als Polizeibehörde tätig, kann bei Vorliegen der strengen Voraussetzungen auf die gesetzliche Grundlage des § 13 Sächsisches Datenschutzdurchführungsgesetz (SächsDSDG) zurückgegriffen werden.

2.1.1 Gesetzliche Grundlage des § 30 Abs. 1 SächsPBG

Mit der Novellierung des Polizeirechtes im Freistaat Sachsen mit Wirkung zum 1. Januar 2020 erfolgte eine grundlegende

Neustrukturierung der Polizei. Damit einher ging der Wechsel vom Einheitssystem zum Trennungssystem. Dadurch erfolgte die gesetzliche Trennung in Polizeivollzugsdienst (klassische Polizei in Uniform) und Polizeibehörden. Die Aufgabe der (nicht-straftatenbezogenen) Gefahrenabwehr obliegt dabei beiden öffentlichen Stellen. Ortspolizeibehörde ist die Gemeinde (§ 1 Abs. 1 Nr. 4 SächsPBG).

Anders als früher (vgl. § 1 Abs. 1 SächsPolG a. F.) liegt die Aufgabe der Verhinderung/Verhütung von Straftaten und deren vorbeugende Bekämpfung nunmehr allein beim Polizeivollzugsdienst (§ 2 Abs. 1 Satz 3 SächsPVDG); den Gemeinden als Polizeibehörden obliegt ausschließlich die Gefahrenabwehr (§ 2 Abs. 1 SächsPBG).

Im Übrigen wird § 30 Abs. 1 und 2 SächsPBG derzeit in einem Normenkontrollverfahren vor dem Sächsischen Verfassungsgerichtshof überprüft. Bis zu einer Entscheidung des SächsVerfGH bleibt die Norm in Kraft.

Der Erfüllung der Aufgaben der Gefahrenabwehr dient auch die Regelung des § 30 SächsPBG. Nach § 30 Abs. 1 SächsPBG können Gemeinden **als Polizeibehörden** *personenbezogene Daten in öffentlich zugänglichen Räumen durch den offenen Einsatz technischer Mittel zur Bildaufnahme und -aufzeichnung erheben,*

(1) soweit Tatsachen die Annahme rechtfertigen, dass dort künftig erhebliche Gefahren für die öffentliche Sicherheit entstehen,

(2) oder dies insbesondere zum Schutz gefährdeter öffentlicher Anlagen oder Einrichtungen erforderlich ist.

Zur Abgrenzung der Anwendungsbereiche von DSGVO und Richtlinie (EU) 2016/680: Tätigkeitsbericht 2019, 2.1.1, Seite 24:
↗ sdb.de/tb2103

2.1.2 Gesetzliche Grundlage des § 13 Abs. 1 SächsDSDG

Nach der Norm des § 13 Abs. 1 SächsDSDG – Videoüberwachung öffentlich zugänglicher Räume – ist eine Erhebung personenbezogener Daten mithilfe von optisch-elektronischen Einrichtungen (Videoüberwachung), deren Speicherung und sonstige Verarbeitung zulässig, soweit dies jeweils

1. Alternative: zur Wahrnehmung einer im **öffentlichen Interesse liegenden Aufgabe** oder
2. Alternative: in Ausübung des **Hausrechts** erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen betroffener Personen überwiegen.

2.2 Voraussetzungen der Videoüberwachung gemäß § 30 SächsPBG

Nach § 30 Abs. 1 SächsPBG können Gemeinden in ihrer Funktion als Polizeibehörden personenbezogene Daten in öffentlich zugänglichen Räumen durch den offenen Einsatz technischer Mittel zur Bildaufnahme und -aufzeichnung erheben, soweit Tatsachen die Annahme rechtfertigen, dass dort künftig erhebliche Gefahren für die öffentliche Sicherheit entstehen, oder dies insbesondere zum Schutz gefährdeter öffentlicher Anlagen oder Einrichtungen erforderlich ist (siehe 2.1.1, Seite 84).

Als datenschutzrechtlich vertretbare Gründe wurden anerkannt: Vandalismus oder Graffiti-Malereien in erheblichem Umfang, Brandstiftung und sonstige Sachbeschädigungen, Einbruch bzw. Diebstahl. Es muss zudem eine künftige erhebliche Gefahr vorliegen. Als Zweck der Überwachung wird eine Abschreckungs- und Vermeidungswirkung, aber auch Beweissicherung angeführt.

Knackpunkt der rechtlichen Prüfung für die Gemeinde ist an dieser Stelle, die richtige Norm zu wählen und ihren Anwendungsbereich zu bestimmen. Diese Abgrenzung tritt aus den erlassenen Gesetzesnormen selbst so nicht ganz eindeutig hervor und muss durch juristische Auslegung ermittelt werden. Für interessierte Bürger/innen und/oder Kommunen wird zu der Abgrenzung auf die bereits erwähnte „Orientierungshilfe zur Videoüberwachung durch Kommunen" (abrufbar unter: ↗ sdb.de/vue16) verwiesen. In dieser wird die Abgrenzung ausführlich beleuchtet.

Grob zusammenfassend lässt sich aber sagen, dass die Abgrenzung nach dem Zweck der Maßnahme erfolgt: Liegt der Zweck der Videoüberwachung hauptsächlich in der Beobachtung eines bestimmten Bereichs öffentlicher Straßen, Plätze oder Grünanlagen, weil es dort wiederholt zu Verhaltensweisen von Personen gekommen ist, die in wiederholten, erheblichen Rechtsgutverletzungen münden, und soll die Videoüberwachung der Abwehr dieser Gefahr dienen, ist die Maßnahme zulässig, wenn die Voraussetzungen von § 30 SächsPBG vorliegen. Wenn diese Voraussetzungen nicht gegeben sind, kann die Gemeinde auch nicht auf § 13 SächsDSDG zurückgreifen (Sperrwirkung).

> Beispiel: Auf einem städtischen Platz sammeln sich ständig Personengruppen zum gemeinsamen Drogen-/Alkoholkonsum. Es entstehen hieraus Pöbeleien, Belästigungen, Lärm, Müll; Passanten fühlen sich in der Gegenwart dieser Gruppe unsicher. Allein dieser Sachverhalt kann die Videoüberwachung des Platzes nicht rechtfertigen, da hier zwar durchaus eine unangenehme Situation, aber noch lange keine „erhebliche Gefahr", wie vom Gesetz gefordert, vorliegt. Die Annahme im Sinne von § 30 Abs. 1 Nr. 1 SächsPBG, § 4 Nr. 3 Buchst. c SächsPVDG würde dies nicht rechtfertigen. Die Voraussetzungen von § 30 Abs. 1 SächsPBG lägen nicht vor, eine Videoüberwachung wäre unzulässig. Ein Rückgriff auf § 13 SächsDSDG ist nicht möglich.

Nach der hier vertretenen Lesart der Vorschrift kann die Norm nur dann greifen, wenn der Aufgabenbereich des Ordnungsamtes („Polizeibehörde" im landläufigen Sinn) betroffen ist. Es spricht viel dafür, dass der Gesetzgeber nicht die Gemeinde als „Bündelungsbehörde" mit all ihren Aufgaben und verschiedenen besonderen Gefahrenabwehrzuständigkeiten in verschiedenen Ämtern im Blick hatte. Die besonderen gemeindlichen Polizeibehörden wie Umweltamt, Bauamt etc. sind in ihrer besonderen Aufgabe bei der Gefahrenabwehr nicht Normadressaten des § 30 Abs. 1 SächsPBG, sie können

bei Vorliegen der Voraussetzungen auch auf die Möglichkeit der speziellen, funktions- oder verfahrensbezogenen Videoüberwachung öffentlich zugänglichen Raums nach § 13 Abs. 1 SächsDSDG zurückgreifen.

2.3 Voraussetzungen der Videoüberwachung gemäß § 13 SächsDSDG

Handelt die Gemeinde somit nicht als Polizeibehörde, sondern im übrigen Aufgabenbereich, zur sogenannten Wahrung der **gemeindlich-funktionalen Aufgabenerfüllung**, richtet sich die Überwachung öffentlich zugänglicher Räume nach § 13 Abs. 1 SächsDSDG. Demnach ist Videoüberwachung nur zulässig, soweit dies zur Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe oder in Ausübung des Hausrechts erforderlich ist und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen betroffener Personen überwiegen.
Hier geht es um die Wahrung der Funktionalität der Behörde, um die Wahrnehmung besonderer Verwaltungsaufgaben zumeist in einem räumlich eng begrenzten Bereich (Bauamt, Umweltamt, Abfallamt usw.), nicht dagegen um die Gewährleistung der öffentlichen Sicherheit und Ordnung auf einem nicht kommunalaufgabenspezifisch ausgerichteten öffentlich zugänglichen Platz.

> Beispiel: Die Videoüberwachung im gemeindlichen Frei- oder Schwimmbad oder die Überwachung von Denkmälern zum Kulturgutschutz, die von Beschädigung/Graffiti betroffen ist. Auch kann beispielsweise die Überwachung von Abfallbeseitigungsanlagen inklusive des Umfeldes aufgrund illegaler Müllablagerungen darunter subsumiert werden.

Im Unterschied zu der oben erwähnten Überwachung nach § 30 Abs. 1 SächsPBG kann hier nur das Objekt selbst (Denkmal, Schwimmbecken oder Rutsche), nicht aber ganze Bereiche erfasst werden.

Zur Sicherung des Hausrechts können Gemeinden in den eigenen Räumen und den eigenen umfriedeten Bereichen videoüberwachen, soweit dies erforderlich ist und schutzwürdige Interessen nicht überwiegen. Auch hier kann nur das Gebäude (inklusive eines höchstens einen Meter breiten Streifens), nicht dagegen die Umgebung, überwacht werden. Zur Definition der weiteren Voraussetzungen wird auf die „Orientierungshilfe zur Videoüberwachung durch Kommunen" verwiesen, abrufbar unter: ↗ sdb.de/vue16.

2.4 Voraussetzungen der Videoüberwachung durch sonstige nichtkommunale öffentliche Stellen

Wollen sonstige öffentlichen Stellen, die weder kommunal oder polizeilich Aufgaben erfüllen – so beispielsweise Landesbehörden, Hochschuleinrichtungen, aber auch staatliche oder kommunale Kliniken, die eigenen Gebäude oder umfriedete Flächen videoüberwachen – so richtet sich dies ausschließlich nach § 13 Abs. 1 SächsDSDG. Die Norm des § 30 Abs. 1 SächsPBG spielt für diese Stellen keine Rolle. Hier wird der Schwerpunkt auf der Durchsetzung des Hausrechtes liegen. Dieser Punkt entspricht in etwa dem „berechtigten Interesse" für nichtöffentliche Einrichtungen (siehe dazu ausführlich 1.1.4, Seite 22).

Als Faustregel gilt: die Videoüberwachung zum Schutz des Hausrechtes ist dann zulässig, wenn diese erforderlich und verhältnismäßig ist. Es dürfen zudem die entgegenstehenden Interessen nicht überwiegen. Daraus folgt, dass allenfalls das Objekt (bzw. der umfriedete Bereich) samt eines höchstens einen Meter breiten Streifens überwacht werden kann (siehe 2.3, Seite 88). Der Verantwortliche muss geltend machen, dass es zu Vorfällen (Straftaten/erheblichen Störungen) gekommen ist, diese künftig auch befürchtet werden (ausführlicher zur Verhältnismäßigkeit siehe 2.5, Seite 90).

Eine Besonderheit ergibt sich für die Überwachung von öffentlichen Kliniken. Hierzu wird auf die obigen eingehenden Ausführungen zu den privaten medizinischen Einrichtungen – und insbesondere den dort aufgezeigten strengen Wertungen des Bundesverwaltungsgerichtes – verwiesen (siehe 1.9, Seite 59), da die Wertungen dem Grunde nach dieselben sind. Ob das Klinikum von privater oder öffentlicher Hand betrieben wird, kann schließlich dem Grunde nach nicht ausschlaggebend sein. Nur wenn das Klinikum sich auf Vorfälle in der Vergangenheit beruft und hinreichende Anhaltspunkte auf künftige Vorfälle hindeuten, kann die Überwachung des Eingangsbereiches bzw. des Vorplatzes oder der Zufahrt zulässig sein. Keinesfalls dürfen Behandlungsräume bzw. Stationen überwacht werden.

Für den Maßregelvollzug (freiheitsentziehende Unterbringung von psychisch kranken oder suchtkranken Straftätern) in psychiatrischen Krankenhäusern gilt zudem die Sonderregel des § 39b Sächsisches Psychisch-Kranken-Gesetz (SächsPsychKG).

2.5 Verhältnismäßigkeit, insbesondere Erforderlichkeit einer Videoüberwachung

Auf welcher Rechtsgrundlage eine Videoüberwachung auch beruht, sie muss in jedem Fall auch verhältnismäßig sein.

Für kommunale Überwachung nach § 30 SächsPBG ergibt sich das bereits unmittelbar aus § 13 SächsPBG, der explizit für jegliche polizeiliche Maßnahmen nach diesem Gesetz Verhältnismäßigkeit anordnet.

Verhältnismäßig ist eine Videoüberwachung nur dann, wenn diese für die Erreichung eines bestimmten legitimen Zweckes geeignet, erforderlich und angemessen ist.

Die Prüfung der Verhältnismäßigkeit muss nicht nur anfänglich, sondern bei jedem Verarbeitungsschritt (Bildaufnahme, Speicherung, Weitergabe, Zweckänderung etc.) separat erfolgen. Insbesondere bei der Prüfung der Erforderlichkeit des

§ 13 Abs. 1 SächsDSDG ist auf die Ultima Ratio zu achten. Erst nachdem andere, mildere Maßnahmen ausgeschlossen wurden oder gescheitert sind, kann diese Norm zur Anwendung kommen. Für § 30 Abs. 1 SächsPBG ist eine derartige Regelung nicht explizit formuliert. Jedoch muss es sich auch hier um das mildeste Mittel handeln, da sonst eine Verhältnismäßigkeit nicht bejaht werden kann.

Eine Videoüberwachung muss im Einzelfall insbesondere immer erforderlich, das heißt grundsätzlich anlassabhängig und angemessen sein. Die Erforderlichkeit ist in diesem Zusammenhang zu bejahen, wenn der Zweck bzw. das festgelegte Ziel mit der Videoüberwachung erreicht werden kann – Stichwort „geeignet" – und es dafür kein anderes, gleich wirksames, aber weniger eingriffsintensives – milderes – Mittel gibt.

Zu weiteren Einzelheiten und auch konkreten Beispielen für mildere Mittel, auf die die öffentlichen Stellen statt einer Videoüberwachung nach Möglichkeit und Verfügbarkeit zurückgreifen könnten, wird ebenfalls auf die „Orientierungshilfe zur Videoüberwachung durch Kommunen" (abrufbar unter: sdb.de/vue16) verwiesen.

Im Übrigen wurde hierzu auch bereits unter 1.1.4 (2.) auf Seite 22 zur Erforderlichkeit der Videoüberwachung durch nichtöffentliche Stellen ausführlich berichtet. Die Vorgaben sind weitestgehend für öffentliche Stellen, so auch für Kommunen, die gleichen, sodass durchaus hierauf verwiesen werden kann.

2.6 Häufige Fragen

2.6.1 Welche Arten der Videoüberwachung gibt es?

Von einer Videobeobachtung in Echtzeit (Monitoring) spricht man, wenn die aufgenommenen Bilder nur auf einen Monitor übertragen werden. Bei dieser Fallkonstellation stellt der Monitor sozusagen das „verlängerte Auge" des Betrachters dar. Dies ist nur dann rechtlich zulässig, wenn gewährleistet ist, dass eine lückenlose Beobachtung der Livebilder erfolgt. Nur in diesem Fall können Sicherheitsmaßnahmen rechtzeitig

ergriffen werden. Andernfalls ist die Videobeobachtung nicht geeignet und damit nicht zulässig.
Daneben gibt es die Videoaufzeichnung, bei der die Bilddaten nicht nur aufgenommen, sondern auch gespeichert werden. Diese Form der Videoüberwachung greift deswegen stärker in die Rechte der Betroffenen ein.
Noch eingriffsintensiver ist die zusätzliche Speicherung und Übermittlung von sogenannten Audiodaten, also von Tonaufnahmen. Sie ist deshalb grundsätzlich überhaupt nicht erlaubt.
Weitere Informationen dazu und was genau unter Videoüberwachung zu verstehen ist, finden Sie unter 1.1.1 und 1.1.2.

2.6.2 Was sind öffentlich zugängliche Räume?

Unter öffentlich zugänglichen Räumen sind Bereiche zu verstehen, die von einem unbestimmten oder nur nach allgemeinen Merkmalen bestimmten Personenkreis betreten und genutzt werden können und ihrem Zweck nach auch dazu bestimmt sind. Die Zweckbestimmung kann sich aus einer Widmung, z. B. für den öffentlichen Verkehr, oder aus dem erkennbaren Willen der Berechtigten ergeben. Ein solcher Raum kann innerhalb und außerhalb von Gebäuden liegen.
Öffentliche Räume sind z. B. Eingangsbereiche und für den Publikumsverkehr zugängliche Bereiche von Verwaltungsgebäuden, Schwimmbäder, Außenanlagen, öffentliche Plätze. Unter keinen Umständen (also auch bei noch so hoher Gefährdung) dürfen dagegen Bereiche überwacht werden, die der absoluten Privat- bzw. Intimsphäre zuzurechnen sind. Das ist immer dort der Fall, wo die Überwachung mit einem Eingriff in die Intimsphäre der Betroffenen verbunden wäre, was regelmäßig bei der Videoüberwachung vor oder in Umkleideräumen oder Toiletten einschließlich deren Vorräumen zuträfe. Auch an Orten wie Kantinen und „Raucherecken", die unter anderem auch zur Kommunikation mit anderen Personen besucht werden, ist von einer Videoüberwachung abzusehen.

2.6.3 Darf eine öffentliche Stelle öffentliche Bereiche mit verdeckten Kameras überwachen oder biometrische Verfahren einsetzen?

Eine Überwachung muss stets offen sein, und es muss vor der Überwachung mit Hinweisschildern hierauf aufmerksam gemacht werden (sogenanntes vorgelagertes Hinweisschild, vgl. auch 1.1.13, Seite 36). Der/Die Bürger/in muss selbst entscheiden können, ob er/sie den überwachten Bereich betreten möchte.
Der Einsatz biometrischer Verfahren ist für die Überwachung durch die Gemeinden nicht erlaubt.

2.6.4 Zu welchen Zwecken dürfen die gewonnenen Aufnahmen weiterverarbeitet werden?

Die Verarbeitung von personenbezogenen Daten, die im Rahmen einer Videoüberwachung rechtmäßig erhoben und gespeichert wurden, dürfen nicht beliebig, sondern ausschließlich zu gesetzlich festgelegten Zwecken weiterverarbeitet werden.
Die aufgrund von § 13 Abs. 1 SächsDSDG gespeicherten Aufnahmen dürfen nur dann weiterverwendet werden, wenn dies zur Abwehr von Gefahren für die öffentliche Sicherheit sowie zur Verfolgung von Straftaten, zur Geltendmachung von Rechtsansprüchen oder zur Wahrung schutzwürdiger Interessen betroffener Personen, insbesondere zur Behebung einer bestehenden Beweisnot, erforderlich ist, siehe § 13 Abs. 2 SächsDSDG.
Wurden die rechtmäßigen Aufnahmen in der polizeilichen Funktion der Gemeinde als Polizeibehörde gespeichert, ist die Weiterverarbeitung zulässig zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Gefahrenabwehr, insbesondere zur vorbeugenden Bekämpfung von Straftaten (nach Weitergabe an die Landespolizei), zur Geltendmachung von öffentlich-rechtlichen Ansprüchen und ebenfalls zum Schutz

privater Rechte, insbesondere zur Behebung einer bestehenden Beweisnot, § 30 Abs.2 SächsPBG.

2.6.5 Wann müssen die Aufnahmen wieder gelöscht werden?

Nach Art.17 Abs. 1 Buchst. a DSGVO gilt, dass personenbezogene Daten unverzüglich zu löschen sind, wenn sie für die Zwecke, für die sie verarbeitet wurden, nicht mehr notwendig sind. Aufnahmen, die für weitere Zwecke der Gemeinde bzw. öffentlichen Stelle nicht relevant sind, sind daher – je nach Auswertungskapazität – innerhalb von zwei bis drei Arbeitstagen zu löschen. Dies folgt aus dem Grundsatz der Datenminimierung nach Art. 5 Abs. 1 Buchst. c DSGVO.
Ungeachtet der Rechtsgrundlage der Videoüberwachung gilt zudem der Grundsatz, dass die Aufnahmen nach einer Höchstspeicherfrist von einem Monat zu löschen sind, § 13 Abs. 4 SächsDSDG und § 30 Abs. 2 SächsPBG.
Ausnahmsweise kann für rechtlich festgeschriebene Zwecke eine längere Speicherdauer zulässig sein. Dies kann nur auf entsprechender Rechtsgrundlage und im konkreten Einzelfall entschieden werden.

2.6.6 Welche Rechte habe ich, wenn von mir Bild- und/oder Tonaufnahmen gemacht wurden?

Die Rechte der von Videoüberwachung betroffenen Personen ergeben sich aus dem 3. Kapitel der DSGVO.
Den betroffenen Personen steht insbesondere das Recht auf Information über die Videoüberwachung zu, Art. 14 DSGVO, auch als Konsequenz der in § 13 Abs. 3 SächsDSDG (und § 30 Abs. 3 SächsPBG) verankerten Hinweispflicht. Dies bedeutet, dass jede betroffene Person von der verantwortlichen Gemeinde verlangen kann, auf die Videografie rechtzeitig und vollständig hingewiesen zu werden.

Zudem können betroffene Personen Auskunft über die von ihnen erhobenen Daten verlangen, Art. 15 DSGVO. Die Gemeinde ist allerdings nicht verpflichtet, personenbezogene Daten zu erheben, um einen Auskunftsanspruch erfüllen zu können. Das heißt, dass eine Auskunft grundsätzlich nur dann erfolgt, wenn die Person, die Auskunft verlangt, aufgrund bereits vorhandener Informationen eindeutig einer Bild- und/oder Tonaufnahme zugeordnet werden kann.
Es kann zudem verlangt werden, dass Videodaten, die nicht oder nicht mehr zulässigerweise verarbeitet werden, unverzüglich gelöscht werden, Art. 17 DSGVO.

2.7 Videoüberwachung von Beschäftigten

Für Datenverarbeitungen, die Beschäftigte betreffen, wie es bei der Videoüberwachung der Fall ist, gelten besondere Regelungen, da der Landesgesetzgeber von seiner Befugnis nach Art. 88 Abs. 1 DSGVO (sogenannte Öffnungsklausel) Gebrauch gemacht hat, spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigtenkontext zu erlassen.
Für die Beschäftigten öffentlicher Stellen des Freistaates Sachsen gemäß § 2 SächsDSDG findet sich eine entsprechende Regelung in § 11 SächsDSDG.
Diese Norm ist bis auf Weiteres auch nach der Entscheidung des EuGH mit Urteil vom 30. März 2023 – C-34/21 anwendbar. Zukünftig könnte eine weitere Anwendbarkeit des § 11 Abs. 1 Satz 1 SächsDSDG für Beschäftigte öffentlicher Stellen des Freistaates Sachsen auch auf die Öffnungsklausel des Art. 6 Abs. 3 in Verbindung mit Art. 6 Abs. 1 Satz 1 Buchst. c („zur Erfüllung einer rechtlichen Verpflichtung") oder Buchst. e („Datenverarbeitung liegt im öffentlichen Interesse oder erfolgt in Ausübung hoheitlicher Gewalt") DSGVO gestützt werden.

2.7.1 Wann ist die Überwachung von Beschäftigten erlaubt?

Erfolgt die Videoüberwachung zum Zwecke der Überwachung des Beschäftigten selbst, ist die Zulässigkeit der Videoüberwachung anhand der Voraussetzungen des § 11 Abs. 1 Satz 1 SächsDSDG zu beurteilen.

Da die Regelung des § 11 Abs. 1 Satz 1 SächsDSDG vergleichbar mit § 26 Abs. 1 Satz 1 BDSG (nichtöffentlicher Bereich) ist, gelten die unter 1.4.1 dargestellten Anforderungen an die Zulässigkeit einer Überwachung auch für Beschäftigte im öffentlichen Bereich.

Erfolgt die Videoüberwachung nicht zum Zweck der Beschäftigtenüberwachung bzw. hat diese nicht zum Ziel, sondern sind die Beschäftigten von einer Videoüberwachung lediglich mitbetroffen, da zum Beispiel Räumlichkeiten mit Publikums- und Kundenverkehr videoüberwacht werden, richtet sich die Zulässigkeit der Maßnahme (und damit auch die anzuwendende Rechtsgrundlage) danach, ob ein öffentlich zugänglicher Raum oder ein nicht öffentlich zugänglicher Raum überwacht wird.

Für **öffentlich zugängliche Räume** (zur Definition siehe Seite 92) sind die Voraussetzungen einer zulässigen Videoüberwachung in § 30 SächsPBG Abs. 1 bzw. in § 13 SächsDSDG geregelt (siehe dazu 2.3 bis 2.7). Soweit Beschäftigte mitbetroffen sind, müssen daneben die beschäftigtendatenschutzrechtlichen Anforderungen im Sinne der „schutzwürdigen Interessen betroffener Personen" – § 13 Abs. 1 SächsDSDG – erfüllt sein.

Für **nicht öffentlich zugängliche Räume** richtet sich die Zulässigkeit der Videoüberwachung, von der auch Beschäftigte mitbetroffen sind, nach der Generalklausel des § 3 SächsDSDG und § 11 Abs. 1 Satz 1 SächsDSDG. § 13 SächsDSDG findet keine Anwendung, da sich dieser ausdrücklich nur auf öffentlich zugängliche Räume bezieht.

Nicht öffentlich zugängliche Räume sind Räume, die nur durch Berechtigte betreten werden sollen. Dazu zählen zum

Beispiel Dienstzimmer, IT-Technikzimmer oder Produktions- oder Lagerräume.
Gemäß § 3 SächsDSDG muss die Verarbeitung personenbezogener Daten durch die öffentliche Stelle zur Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgabe oder in Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde, zur Aufrechterhaltung der Betriebsfähigkeit erforderlich sein. Soweit Maßnahmen zur Betriebsfähigkeit, die die Überwachung von Beschäftigten bedingen, korrespondiert § 3 insoweit mit den Voraussetzungen des § 11 Abs. 1 Satz 1 SächsDSDG.
Zu beachten ist dabei, dass eine Überwachung allein zu dem Zweck, einen ordnungsgemäßen Arbeitsablauf zu gewährleisten, im Regelfall nicht gerechtfertigt ist. Möglich sind Überwachungsmaßnahmen jedenfalls dann, wenn ein/e Arbeitgeber/in in besonders gefahrträchtigen Arbeitsbereichen Schutzpflichten gegenüber seinen/ihren Beschäftigten erfüllen muss. Der Erfassungsbereich ist dabei auf das sicherheitsrelevante Areal zu beschränken. Arbeitsbereiche von Beschäftigten sind so weit wie möglich auszublenden.
Weiterhin ist zu berücksichtigen, ob die Videoüberwachung außerhalb von Betriebs- bzw. Geschäfts- oder Öffnungszeiten ein weniger eingriffsintensives Mittel darstellt.

2.7.2 Ist die Videoüberwachung von Beschäftigten zulässig, wenn der Dienstherr eine Einwilligung einholt?

Es gelten die Ausführungen unter 1.4.2 (Seite 46) entsprechend.

2.7.3 Kann die Videoüberwachung von Beschäftigten in einer Dienst- oder Betriebsvereinbarung geregelt werden?

Auch Dienst- und Betriebsvereinbarungen können eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten darstellen. Allerdings darf auch diese die Datenschutz-

anforderungen der DSGVO bzw. BDSG nicht unterschreiten. Soweit die Videoüberwachung im Arbeitsverhältnis den Vorgaben von Art. 88 DSGVO in Verbindung mit § 11 Abs. 1 Satz 1 SächsDSDG entspricht, kann sie durch eine datenschutzrechtskonforme Dienst- und Betriebsvereinbarung geregelt werden.

Es gelten die unter 1.4.4 (Seite 50) dargestellten Voraussetzungen entsprechend.

3 Videoüberwachung durch die Polizei in Sachsen

3.1 Rechtsgrundlagen

Zur Abwehr von Gefahren sieht das Polizeirecht eine Reihe von Befugnissen vor, welche den Einsatz von Videotechnik im öffentlichen Raum zulassen.

Die Vorschriften sind technikoffen formuliert („technische Mittel"), das Gesetz bestimmt also nicht, welche Art von Technik für Bild- und/oder Tonaufnahmen eingesetzt werden darf. Damit werden, abgesehen von den gesetzlich normierten Voraussetzungen und Rahmenbedingungen für Bildaufnahmen, auch keine Vorgaben zur Art des Einsatzes der technischen Mittel gemacht. In Betracht kommt in der Praxis der Einsatz von fest installierten Kameras, von Hand- oder Mastkameras, aber auch von Kameras, die aus Hubschraubern oder an Drohnen befestigt Bilder aufnehmen.

Bildaufnahmen des öffentlich zugänglichen Raums im Bereich der Gefahrenabwehr (siehe 3.1.1bis 3.1.4) dürfen nur „offen" gefertigt werden, das heißt, es muss für Personen, die den Aufnahmebereich der Kameras betreten oder sich dort aufhalten, möglich sein zu erkennen, dass die Polizei Videoüberwachung betreibt. Hierfür hat die Polizei die notwendigen Vorkehrungen zu treffen. Je weiter die Aufnahmetechnik von den betroffenen Personen entfernt ist und je schwieriger es dadurch möglich wird, die Kamera und ihre polizeiliche Nutzung direkt zu erkennen, desto größer wird der Aufwand, den die Polizei betreiben muss, um die betroffenen Personen auf die Überwachung hinzuweisen und damit die Fertigung von Bildaufnahmen gesetzeskonform „offen" zu gestalten.

3.1.1 Bild- und Tonaufzeichnungen an gefährdeten Objekten und an Kriminalitätsschwerpunkten

Die Videoüberwachung in öffentlichen Bereichen kann zum einen auf Grundlage des § 57 Abs. 3 Sächsisches Polizeivollzugsdienstgesetz (SächsPVDG) geschehen.

Die Polizei ist gemäß § 57 Abs. 3 Nr. 1 SächsPVDG befugt, Bild- und Tonaufzeichnungen in oder an gefährdeten Objekten im Sinne des § 15 Abs. 1 Nr. 3 SächsPVDG anzufertigen, darunter fallen zum Beispiel öffentliche Verkehrsmittel, Amtsgebäude oder Versorgungsanlagen.

Auf Grundlage von § 57 Abs. 3 Nr. 2 SächsPVDG dürfen zudem Aufnahmen von öffentlichen Straßen, Wegen oder Plätzen gemacht werden, wenn es sich dabei um einen Kriminalitätsschwerpunkt handelt, das heißt, wenn die Kriminalitätsbelastung dort nach polizeilich dokumentierten Tatsachen gegenüber der des übrigen Gemeindegebietes deutlich erhöht ist. Beispielfälle sind Plätze, auf denen es gehäuft zu Eigentumsdelikten und Tätlichkeiten kommt oder die einen Schwerpunkt des Handels mit Betäubungsmitteln bilden.

In beiden oben genannten Fallkonstellationen ist Voraussetzung, dass Anhaltspunkte dafür bestehen, dass an den betroffenen Stellen auch künftig Straftaten begangen werden, durch die Personen oder Sach- oder Vermögenswerte gefährdet werden.

Der Umstand der Videoüberwachung wird in Fällen des § 57 Abs. 3 SächsPVDG in aller Regel durch gut erkennbare Hinweisschilder offenbart. Diese sollten bereits an den Grenzen des Aufnahmebereichs der Kameras angebracht sein und Passanten Kenntnis von der Überwachung geben, bevor sie von den Kameras erfasst werden.

Findet an einem Ort, der als Kriminalitätsschwerpunkt überwacht wird, eine vom Grundrecht der Versammlungsfreiheit geschützte Demonstration statt, ist die Überwachung für diesen Zeitraum zu unterbrechen. Bild- und Tonaufnahmen darf die Polizei dann nur unter den Voraussetzungen von § 20 Abs. 1 SächsVersG fertigen.

Die im Rahmen der Bild- und Tonaufzeichnungen erhobenen Daten dürfen ausschließlich zu bestimmten Zwecken, wie zur Verfolgung von Straftaten und Ordnungswidrigkeiten sowie zum Schutz privater Rechte, weiterverwendet werden. Sie sind gemäß § 57 Abs. 10 SächsPVDG spätestens nach einem Monat wieder zu löschen, soweit sie nicht zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Geltendmachung von öffentlich-rechtlichen Ansprüchen oder zum Schutz privater Rechte erforderlich sind.
Entfallen die tatsächlichen Voraussetzungen für eine Videoüberwachung, zum Beispiel, weil im überwachten Bereich keine Straftaten mehr begangen werden oder zu erwarten sind, ist die Überwachung zu beenden.

3.1.2 Aufnahmen zum Schutz vor einer Gefahr für Leib und Leben (Bodycams)

Rechtsgrundlage für den sehr begrenzten Einsatz von Videotechnik in öffentlich zugänglichen Bereichen kann zudem § 57 Abs. 4 SächsPVDG sein, wonach die Polizei Bild- und Tonaufnahmen anfertigen kann, wenn dies mit hinreichender Wahrscheinlichkeit zum Schutz vor einer Gefahr für Leib und Leben erforderlich ist. Die Vorschrift erfasst den Betrieb von sogenannten Bodycams, kleinen Kameras also, die von den Beamtinnen und Beamten am Körper getragen werden und den konkreten Polizeieinsatz dokumentieren. Solche Kameras erfassen naturgemäß einen viel kleineren Bereich als zum Beispiel erhöht installierte Kameras zur Überwachung von Kriminalitätsschwerpunkten (s. o.).
Die Daten dürfen nur offen erhoben werden, und der Einsatz technischer Mittel ist in besonderer Weise nach außen hin kenntlich zu machen.
Die Aufzeichnungen werden gemäß § 57 Abs. 7 Satz 3 SächsPVDG nach Ablauf von 30 Tagen automatisch gelöscht, wenn sie nicht zur Verfolgung von Straftaten oder zur Überprüfung der Rechtmäßigkeit der Maßnahme oder der Aufnahme selbst benötigt werden.

Siehe auch „Einsatz von Bodycams bei der sächsischen Polizei", in: Tätigkeitsbericht 2020, 8.2, Seite 166f.:
↗ sdb.de.de/tb2020

Personen, welche von einer Aufzeichnung betroffen sind, können gemäß § 57 Abs. 7 Satz 4 SächsPVDG auf Antrag Einsicht in die Aufzeichnung nehmen. Die Einsichtnahme ist beschränkt auf Aufzeichnungen, die den Antragsteller betreffen.

3.1.3 Videoüberwachung bei öffentlichen Veranstaltungen oder Ansammlungen

Öffentliche Veranstaltungen und Ansammlungen im Freien, die keine Versammlungen im Sinne des Sächsischen Versammlungsgesetzes sind, darf die Polizei unter bestimmten Voraussetzungen mittels Videotechnik beobachten. Hierunter zählen etwa Festivals, Stadtfeste, Sportereignisse (insbesondere Fußballspiele).

Bei einer abstrakten Gefahrenlage ist die Polizei nach § 57 Abs. 1 Satz 1 SächsPVDG befugt, Übersichtsbilder zu fertigen und zu übertragen, wenn und soweit dies wegen der Größe der Veranstaltung oder Ansammlung oder der Unübersichtlichkeit der Lage zur Lenkung und Leitung eines Polizeieinsatzes im Einzelfall erforderlich ist. Wegen dieser engen Zweckbestimmung verbietet das Gesetz allerdings die Aufzeichnung der Bilder; ebenso wenig dürfen aus diesen Bildern Personen identifiziert werden.

In der Regel werden Übersichtsbilder von erhöhten Kamerastandorten aus übertragen, um einen Überblick über das Geschehen zu ermöglichen. Zum Einsatz können auch Kameras an Hubschraubern oder Drohnen kommen.

Begründen Tatsachen die Annahme, dass bei solchen öffentlichen Veranstaltungen oder Ansammlungen Personen innerhalb absehbarer Zeit eine gegen Personen, Sach- oder Vermögenswerte gerichtete Straftat begehen werden oder dass von ihnen sonstige erhebliche Gefahren für die öffentliche Sicherheit ausgehen, darf die Polizei nach § 57 Abs. 2 SächsPVDG Bild- und Tonaufnahmen oder -aufzeichnungen dieser Personen fertigen. Solche Aufzeichnungen sind grundsätzlich auf die Personen zu beschränken, die durch ihr Verhalten Anlass für die Maßnahme geben; da es in Ansammlungen aber praktisch ausgeschlossen ist, dass Bildaufzeichnungen tatsächlich

ausschließlich die „Störer" erfassen, ist die Maßnahme auch zulässig, wenn Dritte unvermeidbar betroffen werden, etwa, weil sie sich im unmittelbaren räumlichen Umfeld der Störer bewegen.
Aufzeichnungen, die nach § 57 Abs. 2 SächsPVDG gefertigt wurden, sind gemäß § 57 Abs. 10 SächsPVDG spätestens nach einem Monat wieder zu löschen, soweit sie nicht zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Geltendmachung von öffentlich-rechtlichen Ansprüchen oder zum Schutz privater Rechte erforderlich sind.

3.1.4 Videoüberwachung zur Aufklärung von Straftaten

Der Einsatz stationärer Videokameras in öffentlichen Bereichen, insbesondere im Grenzbereich, wird im Einzelfall auch auf die Vorschrift des § 163f Strafprozessordnung (StPO) gestützt. Nach dieser Rechtsgrundlage darf die Polizei in Fällen von Straftaten erheblicher Bedeutung Beschuldigte planmäßig beobachten, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Täters auf andere Weise erheblich weniger Erfolg versprechend oder wesentlich erschwert wäre. Die sächsische Polizei nutzt hierfür auch Videoüberwachungstechnik an öffentlichen Straßen.
Diese Form der Videoüberwachung darf allerdings nur im konkreten Einzelfall und nur auf Anordnung eines Richters bzw. einer Richterin zur Anwendung kommen. Eine solche Anordnung ist gemäß § 163f Abs. 3 Satz 3 in Verbindung mit § 100e Abs. 1 Satz 4 StPO auf höchstens drei Monate befristet (nur in Ausnahmefällen ist eine Verlängerung um bis zu weiteren drei Monaten zulässig).
Eine solche Überwachung auf strafprozessualer Grundlage aus Anlass eines konkreten Ermittlungsverfahrens ist datenschutzrechtlich problematisch, weil ganz überwiegend – tatsächlich nahezu ausschließlich – Bilder von völlig unbeteiligten Personen gefertigt werden, die keinerlei Anlass für ein polizeiliches Tätigwerden gegeben haben und für das Ermittlungsverfahren ohne Bedeutung sind.

3.2 Häufige Fragen zur Videoüberwachung durch die Polizei im öffentlichen Bereich

3.2.1 Wann darf die Polizei im öffentlichen Raum Videoüberwachung einsetzen?

Unter bestimmten Voraussetzungen darf die Polizei im Rahmen der Gefahrenabwehr mithilfe von Videotechnik öffentliche Bereiche überwachen. Eine Videoüberwachung kann dabei auf unterschiedliche Rechtsgrundlagen gestützt sein:

- in oder an sogenannten gefährdeten Objekten (z. B. gefährdete Amtsgebäude oder öffentliche Verkehrsmittel) zur Abwehr von Straftaten gemäß § 57 Abs. 3 Nr. 1 SächsPVDG;
- an Kriminalitätsschwerpunkten zur Abwehr von Straftaten gemäß § 57 Abs. 3 Nr. 2 SächsPVDG;
- in öffentlich zugänglichen Bereichen zum Schutz von Leib und Leben gemäß § 57 Abs. 4 SächsPVDG (Bodycams);
- im Zusammenhang mit öffentlichen Veranstaltungen oder Ansammlungen zur Einsatzlenkung und zur Verhütung von Straftaten gemäß § 57 Abs. 1, 2 SächsPVDG
- zur Ermittlung im Strafverfahren bei Straftaten von erheblicher Bedeutung gemäß § 163f. Abs. 1 StPO auf Anordnung einer Richterin oder eines Richters.

3.2.2 Darf die Polizei öffentliche Bereiche mit verdeckten Kameras überwachen?

Der gefahrenabwehrrechtliche Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufnahmen erfolgt grundsätzlich offen. Der verdeckte Einsatz von Kameras oder Mikrofonen ist in den oben genannten Fällen gesetzlich nicht vorgesehen. Betroffenen Personen muss es möglich sein zu erkennen, dass die Polizei Videoüberwachung betreibt. Das kann z. B. durch feste Hinweisschilder bei stationärer Über-

wachung erreicht werden. Bei ortsveränderlicher Überwachung beispielsweise von Ansammlungen können die betroffenen Personen z. B. mittels Lautsprecherdurchsagen und transportabler optischer Hinweise informiert werden.

3.2.3 Dürfen biometrische Verfahren bei der Überwachung öffentlicher Bereiche zum Einsatz kommen?

Siehe auch „Einsatz eines Programms mit Gesichtserkennung für die Strafverfolgung durch die Polizeidirektion Dresden", in: Tätigkeitsbericht 2021, 8.2, Seite 199ff.:
↗ sdb.de/tb2021

Der Einsatz biometrischer Verfahren zu gefahrenabwehrrechtlichen Zwecken ist nicht erlaubt; das SächsPVDG bietet keine gesetzliche Grundlage.
Im Rahmen der Strafverfolgung kann im Einzelfall ein auf biometrische Verfahren gestützter Abgleich von erhobenem Bildmaterial mit bereits vorhandenen Lichtbildern zulässig sein.

3.2.4 Zu welchen Zwecken dürfen die Aufnahmen weiterverarbeitet werden?

Die Verarbeitung von personenbezogenen Daten, die im Rahmen einer polizeilichen Videoüberwachung gewonnen wurden, dürfen ausschließlich zu gesetzlich festgelegten Zwecken weiterverarbeitet werden.
Wurden personenbezogene Daten im Rahmen einer Videoüberwachung nach einer der Grundlagen des § 57 SächsPVDG erhoben (§ 57 Abs. 2: bei öffentlichen Veranstaltungen oder Ansammlungen, § 57 Abs. 3 Nr. 1: in oder an gefährdeten Objekten, § 57 Abs. 3 Nr. 2: an Kriminalitätsschwerpunkten, § 57 Abs. 4: in öffentlich zugänglichen Bereichen zum Schutz von Leib und Leben), dürfen diese Daten gemäß § 57 Abs. 7, 10 SächsPVDG ausschließlich zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Überprüfung der Rechtmäßigkeit der Maßnahme, zur Geltendmachung von öffentlich-rechtlichen Ansprüchen oder zum Schutz privater Rechte – insbesondere beim Mangel von Beweisen – weiterverarbeitet werden.
In Fällen einer Videoüberwachung öffentlicher Bereiche aufgrund schwerer Straftaten gemäß § 163f StPO dürfen die

erhobenen personenbezogenen Daten nur zu bestimmten Zwecken, darunter zur Gefahrenabwehr, zur Aufklärung von Straftaten sowie zu Beweiszwecken im Strafverfahren weiterverwendet werden.

3.2.5 Wann müssen die Aufnahmen wieder gelöscht werden?

Wann Daten, die während einer Videoüberwachung von öffentlichen Bereichen gewonnen wurden, wieder zu löschen sind, ist abhängig von der jeweiligen gesetzlichen Grundlage, auf die die Videoüberwachung gestützt ist. Die im Rahmen der Videoüberwachung von öffentlichen Veranstaltungen oder Ansammlungen und gefährdeten Objekten und Kriminalitätsschwerpunkten (Videoüberwachung nach § 57 Abs. 2, Abs. 3 Nr. 1 und Nr. 2 SächsPVDG) erhobenen Daten sind gemäß § 57 Abs. 10 SächsPVDG spätestens nach einem Monat wieder zu löschen, soweit sie nicht zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Geltendmachung von öffentlich-rechtlichen Ansprüchen oder zum Schutz privater Rechte erforderlich sind.

Videoaufzeichnungen von Bodycams sind gemäß § 57 Abs. 7 Satz 3 SächsPVDG nach Ablauf von 30 Tagen automatisch zu löschen, soweit sie nicht zur Verfolgung von Straftaten oder zur Überprüfung der Rechtmäßigkeit der Maßnahme oder der Aufnahme selbst benötigt werden.

In Fällen einer Videoüberwachung öffentlicher Bereiche aufgrund schwerer Straftaten gemäß § 163f. StPO sind die erhobenen personenbezogenen Daten zu löschen, soweit sie nicht mehr für die vorgeschriebenen Zwecke im Strafverfahren erforderlich sind. Weil in erster Linie Daten unbeteiligter Personen erfasst werden, trifft die Polizei bzw. die Staatsanwaltschaft eine besondere Pflicht zur Prüfung der Erforderlichkeit der Daten für die weitere Aufgabenerfüllung. Nicht verfahrensrelevante Daten sind umgehend zu löschen, auch wenn das Verfahren noch nicht abgeschlossen ist (§ 75 Abs. 2 BDSG, § 14 Abs. 2 SächsDSUG).

3.2.6 Welche Rechte habe ich, wenn von mir Bild- und/oder Tonaufnahmen gemacht wurden?

Betroffene Personen können grundsätzlich gemäß § 92 Abs. 2 SächsPVDG in Verbindung mit § 13 Sächsisches Datenschutz-Umsetzungsgesetz (SächsDSUG) einen Antrag auf Auskunft über die sie betreffende Verarbeitung personenbezogener Daten an die Polizei richten.
Die Polizei ist allerdings nicht verpflichtet, personenbezogene Daten zu erheben, um einen Auskunftsanspruch erfüllen zu können. Das heißt, dass eine Auskunft grundsätzlich nur dann erfolgt, wenn die Person, die Auskunft verlangt, aufgrund bereits vorhandener Informationen eindeutig einer Bild- und/oder Tonaufnahme zugeordnet werden kann.
Ferner besteht für den Fall, dass Polizeibeamte Bild- oder Tonaufzeichnungen mit einer sogenannten Bodycam anfertigen, eine Mitteilungspflicht der Polizei gegenüber der von der Aufzeichnung betroffenen Person. Personen, welche von einer Aufzeichnung betroffen sind, können gemäß § 57 Abs. 7 Satz 4 SächsPVDG auf Antrag Einsicht in die Aufzeichnung nehmen.

3.3 Polizeiliche Videoüberwachung von Versammlungen

Im Rahmen der Gefahrenabwehr ist die sächsische Polizei befugt, öffentliche Versammlungen und Aufzüge mit Videotechnik zu überwachen. Rechtsgrundlage sind § 12 Sächsisches Versammlungsgesetz (SächsVersG) (für Versammlungen in geschlossenen Räumen) und § 20 Sächsisches Versammlungsgesetz (für Versammlungen unter freiem Himmel und Aufzüge). Nach diesen Rechtsvorschriften darf die Polizei Bild- und Tonaufnahmen von Teilnehmenden bei öffentlichen Versammlungen und Aufzügen anfertigen, wenn im Einzelfall eine erhebliche Gefahr für die öffentliche Sicherheit und Ordnung zu befürchten ist, das heißt, wenn Anhaltspunkte vorliegen, dass von den betreffenden Teilnehmerinnen und Teilnehmern eine Gefahr für Leib, Leben oder bedeutende Sach- oder Vermö-

genswerte ausgeht. Aufnahmen dürfen auch gemacht werden, wenn Dritte dabei unvermeidbar mit betroffen sind. Der Polizeivollzugsdienst ist jedoch dazu angehalten, die Aufzeichnung unbeteiligter Dritter auf ein unumgängliches Mindestmaß zu beschränken.

Die Bildaufnahmen dürfen nicht verdeckt gefertigt werden – zulässig ist nur der offene Einsatz von technischen Mitteln zur Bild- und Tonaufnahme. Die Teilnehmer müssen erkennen können, ob Bildaufnahmen gefertigt werden oder nicht. Kameras im unmittelbaren räumlichen Zusammenhang mit der Versammlung, z. B. Handkameras von die Versammlung begleitenden Polizeibeamten oder Kameras auf Polizeifahrzeugen, müssen abgedeckt oder gut erkennbar vom Versammlungsgeschehen weggeschwenkt werden, wenn sie nicht in Betrieb sind. Beim Einsatz von Kameras in Hubschraubern oder an Drohnen muss die Polizei auf anderem Weg gewährleisten, dass die Versammlungsteilnehmer erkennen können, ob gerade eine Videoüberwachung stattfindet, etwa durch Lautsprecherdurchsagen oder optische Hinweise am Boden. Die erhobenen Daten dürfen ausschließlich zu Zwecken der Strafverfolgung weiterverarbeitet werden. Alle Aufnahmen, die nicht für diesen Zweck erforderlich sind, müssen gemäß § 12 Abs. 2 bzw. § 20 Abs. 3 SächsVersG nach Ende der Versammlung unverzüglich gelöscht werden.

Bei Versammlungen unter freiem Himmel und Aufzügen ist die Polizei zudem befugt, sogenannte Übersichtsbild-Übertragungen durchzuführen (z. B. aus dem Polizeihubschrauber oder von an Drohnen befestigten Kameras). Dabei handelt es sich um Livebild-Übertragungen, welche ausschließlich für die Lenkung und Leitung von Polizeieinsätzen verwendet werden dürfen. Übersichtsbildübertragungen sind nur zulässig, wenn sie angesichts der Größe der Versammlung oder aufgrund einer unübersichtlichen Lage für die Polizei erforderlich sind. Eine Identifizierung von einzelnen Personen durch Übersichtsbild-Übertragungen ist gesetzlich verboten. Die Übersichtsbilder dürfen nicht aufgezeichnet werden und auch in keiner anderen Art und Weise als der oben genannten weiterverwendet werden.

Siehe auch „Abschalten der Videoüberwachung der Chemnitzer Innenstadt bei Versammlungen", in: Tätigkeitsbericht 2019, 8.6, Seite 154ff.:
↗ sdb.de/tb2103

Auch Übersichtsbilder dürfen nur offen gefertigt werden. Auch in diesen Fällen muss die Polizei auf geeignete Weise den Teilnehmern ermöglichen, ohne Weiteres erkennen zu können, dass die Polizei Bilder der Versammlung fertigt bzw. überträgt (eine Aufzeichnung ist, wie erwähnt, gesetzlich ausgeschlossen).

3.3.1 Häufige Fragen

3.3.1.1 Wann darf die Polizei Versammlungen mit Videotechnik überwachen?

Die Polizei darf auf öffentlichen Versammlungen in geschlossenen Räumen oder unter freiem Himmel Bild-, Video- und Tonaufnahmen von Teilnehmern machen, wenn im Einzelfall eine erhebliche Gefahr für die öffentliche Sicherheit und Ordnung zu befürchten ist, das heißt, wenn Anhaltspunkte vorliegen, dass von diesen Teilnehmenden eine Gefahr für Leib, Leben oder bedeutende Sach- oder Vermögenswerte ausgeht.
Zudem darf die Polizei von öffentlichen Versammlungen unter freiem Himmel und Aufzügen sowie ihrem Umfeld sogenannte Übersichtsbild-Übertragungen machen. Dabei handelt es sich um Livebild-Übertragungen, welche ausschließlich für die Lenkung und Leitung von Polizeieinsätzen verwendet werden dürfen und keine Identifizierung von Einzelpersonen zulassen.

3.3.1.2 Darf die Polizei Versammlungen verdeckt überwachen?

Bild- und Tonaufnahmen sind gemäß § 12 SächsVersG (bei Versammlungen in geschlossenen Räumen) und § 20 SächsVersG (bei Versammlungen unter freiem Himmel und Aufzügen) offen zu erheben. Der Einsatz von verdeckten Kameras oder Mikrofonen durch die Polizei ist gesetzlich nicht zulässig. Den Teilnehmerinnen und Teilnehmern muss ermöglicht werden, den Umstand der Videoüberwachung ohne Weiteres erkennen zu können. Schwierigkeiten ergeben sich in diesem Zusammenhang, wenn die Versammlung aus räumlicher Dis-

tanz beobachtet wird (aus Hubschrauber oder von Drohnen aus). Es obliegt der Polizei, die Teilnehmenden in geeigneter Weise auf die Überwachung hinzuweisen, um die gesetzliche Vorgabe einer „offenen" Maßnahme zu erfüllen.

3.3.1.3 Dürfen biometrische Verfahren bei der Überwachung von Versammlungen zum Einsatz kommen?

Der Einsatz von sogenannten biometrischen Verfahren – darunter fällt beispielsweise die automatische Gesichtserkennung – ist bei der präventiven, polizeirechtlichen Überwachung von Versammlungen gesetzlich nicht erlaubt.

3.3.1.4 Zu welchen Zwecken dürfen die Aufnahmen weiterverarbeitet werden?

Gemäß § 12 Abs. 2 SächsVersG (bei Versammlungen in geschlossenen Räumen) bzw. § 20 Abs. 3 SächsVersG (bei Versammlungen unter freiem Himmel und Aufzügen) dürfen die erhobenen Daten nach Ende der Versammlung ausschließlich zur Verfolgung von Straftaten durch Teilnehmer weiterverarbeitet werden.

3.3.1.5 Wann müssen die Aufnahmen wieder gelöscht werden?

Die im Rahmen der Videoüberwachung der Versammlung erhobenen Daten müssen gemäß § 12 Abs. 2 bzw. § 20 Abs. 3 SächsVersG nach Ende der Versammlung unverzüglich gelöscht werden, sofern sie nicht für Zwecke der Strafverfolgung benötigt werden.

3.4 Einsatz von Bodycams bei der sächsischen Polizei

Im Herbst 2019 wurde dem Sächsischen Datenschutzbeauftragten das Konzept zur landesweiten Einführung von körpernah getragenen Aufnahmegeräten („Bodycams") in der sächsischen Polizei vorgestellt. Bereits zuvor wurde der Sächsische Datenschutzbeauftragte sowohl im Gesetzgebungsverfahren als auch bei der Erarbeitung der Errichtungsanordnung durch

das Sächsische Staatsministerium des Innern eng eingebunden. Nach einer vorangegangenen Erprobungsphase in ausgewählten Polizeidirektionen und Schaffung einer speziellen Ermächtigungsgrundlage im neuen Polizeivollzugsdienstgesetz war geplant – beginnend mit dem Jahr 2020 –, über einen Zeitraum von zwei Jahren die Organisationseinheiten (hierbei unter anderem die Einrichtungen für die Aus- und Fortbildung sowie den Streifendienst) mit insgesamt circa 1.500 Kameras, mit denen Bild- und Tonaufzeichnungen gefertigt werden können, auszustatten. Vorrangiges Ziel der Anwendung soll die Eigensicherung der Polizeibeamten sein. Die Bodycams sollen dazu beitragen, konfliktbehaftete Situationen zu deeskalieren und damit auch gewalttätige Übergriffe auf Dritte zu verhindern. Ferner soll das Verfahren die Beweisführung im Rahmen der Strafverfolgung unterstützen. Der präventive Einsatz von Bodycams zur Eigensicherung oder zum Schutz Dritter ist in allen öffentlich zugänglichen Bereichen möglich und richtet sich nach § 57 Abs. 4 bis 9 Sächsisches Polizeivollzugsdienstgesetz (SächsPVDG). Rechtsgrundlage für den Einsatz zur Strafverfolgung sind § 100h Abs. 1 Nr. 1 StPO, § 100f Abs. 1 Strafprozessordnung (StPO).

Gemäß § 57 Abs. 6 SächsPVDG ist der Einsatz der Bodycams in geeigneter Weise besonders erkennbar zu machen. Daher werden die Bodycams nur offen und in Verbindung mit dem entsprechenden neongelben Hinweisschild „Video Audio" getragen. Der Beginn der Aufzeichnung wird der betroffenen Person grundsätzlich mitgeteilt. Die Bodycams sind so konfiguriert, dass Aufzeichnungen äußerlich erkennbar sind. Die Polizeivollzugsbediensteten sind angehalten, die Aufzeichnung unbeteiligter Dritter auf ein unumgängliches Mindestmaß zu beschränken. Nach der gesetzlichen Regelung (in § 57 Abs. 4 SächsPVDG) ist das sogenannte Pre-Recording zulässig. Dabei werden die Aufzeichnungen kurzzeitig in einem Zwischenspeicher bis zu 60 Sekunden abgelegt, danach aber permanent überschrieben. Erst beim Starten der eigentlichen Aufnahme (unter den Voraussetzungen des § 57 Abs. 5 SächsPVDG – Vorliegen einer konkreten Gefahr für Leib oder Leben) werden die Bildaufnahmen dieser „Anbahnungsphase"

länger gespeichert und stehen zur Weiterverarbeitung zur Verfügung.

Die Aufzeichnungen werden gemäß § 57 Abs. 7 Satz 3 SächsPVDG nach Ablauf von 30 Tagen automatisch gelöscht, wenn sie nicht zur Verfolgung von Straftaten oder zur Überprüfung der Rechtmäßigkeit der Maßnahme oder der Aufnahme selbst benötigt werden.

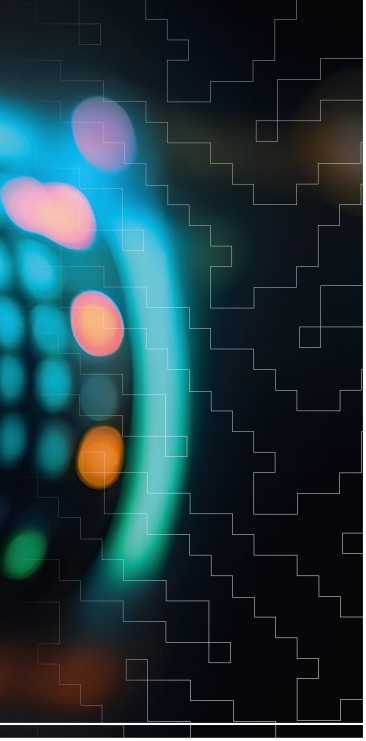
Entsprechend der gesetzlichen Anordnung in § 57 Abs. 7 Satz 4 und 5 SächsPVDG ist das Verfahren der Einsichtnahme in Aufzeichnungen von Bodycams in einer Verwaltungsvorschrift geregelt (VwV Einsicht Bodycam).

Hiernach erhalten betroffene Personen – dies sind alle Personen, von denen im Rahmen eines Bodycam-Einsatzes Bild- oder Tonaufzeichnungen gefertigt wurden, auch Polizeibedienstete und unbeteiligte Dritte – Einsicht in die Aufzeichnungen. Die Einsichtnahme ist beschränkt auf Aufzeichnungen, die den Antragsteller betreffen. Ausnahmsweise kann die Einsichtnahme auch in Aufzeichnungen gewährt werden, die Bild- und Tonsequenzen zu anderen Personen enthalten, soweit dies aus Gründen des Sachzusammenhangs zwingend erforderlich ist. Hierbei sollen die anderen Personen nach Möglichkeit anonymisiert werden.

Das Recht auf Einsichtnahme in Aufzeichnungen, die zu den anderen in § 57 Abs. 7 Satz 3 SächsPVDG genannten Zwecken, zum Beispiel in einem Strafverfahren, benötigt werden oder bereits zu diesem Zweck aufgenommen wurden, richtet sich nach den jeweiligen Regelungen der Akteneinsicht (beispielsweise § 147 StPO). Neben dem Recht auf Einsichtnahme haben die betroffenen Personen gegenüber der Polizei einen Auskunftsanspruch über die sie betreffende Verarbeitung personenbezogener Daten gemäß § 92 Abs. 2 SächsPVDG in Verbindung mit § 13 Sächsisches Datenschutz-Umsetzungsgesetz.

Der Einsatz von Bodycams wird nach der Anordnung in § 57 Abs. 9 SächsPVDG spätestens Ende 2024 durch die Staatsregierung evaluiert.

Aus datenschutzrechtlicher Sicht wird durch die gesetzliche Regelung und die untergesetzlichen Vorschriften ein erfreulich hohes Maß an Transparenz bei der Verarbeitung personenbezogener Daten mittels Bodycams erreicht. Es ist davon auszugehen, dass die gesetzlichen Anwendungsvoraussetzungen und Schutzvorkehrungen unangemessene Eingriffe in Rechte Betroffener auch in der praktischen Anwendung verhindern.



Herausgeberin
Sächsische Datenschutz- und Transparenzbeauftragte
Dr. Juliane Hundert
Devrientstraße 5, 01067 Dresden

Kontakt
Postanschrift: Postfach 11 01 32, 01330 Dresden
Telefon 0351 85471-101
Telefax 0351 85471-109
post@sdtb.sachsen.de
www.datenschutz.sachsen.de

Folgen Sie der SDTB auch auf Mastodon: social.sachsen.de/@sdtb

Fotos
Titel: © Denniro – stock.adobe.com
Weitere Fotos: ronaldbonss.com (Seite 5)

Druck
siblog – Gesellschaft für Dialogmarketing, Fulfillment & Lettershop mbH

Auflage
1.000 Exemplare

Bezug
kostenlos
Zentraler Broschürenversand der Sächsischen Staatsregierung
Hammerweg 30, 01127 Dresden
Telefon: 0351 210-3671 / -3672
publikationen@sachsen.de
www.publikationen.sachsen.de

Verteilerhinweis
Diese Broschüre wird von der Sächsischen Datenschutz- und Transparenzbeauftragten im Rahmen ihrer Aufgaben nach Artikel 57 Datenschutz-Grundverordnung herausgegeben. Die Informationsschrift darf weder von politischen Parteien noch von deren Kandidaten oder Helfern zum Zwecke der Wahlwerbung verwendet werden. Dies gilt für alle Wahlen. Missbräuchlich ist insbesondere die Verteilung auf Wahlveranstaltungen, an Informationsständen der Parteien sowie das Einlegen, Aufdrucken oder Aufkleben parteipolitischer Informationen oder Werbemittel. Untersagt ist auch die Weitergabe an Dritte zur Verwendung bei der Wahlwerbung.