



**Mittelstand 4.0**  
Kompetenzzentrum  
Chemnitz

**Betrieb 4.0**  
machen!



**Recht  
behalten!**



**Nachgelesen**

# **(Video-) Kameraeinsatz im Unternehmen**

**Prof. Dr. Gesmann-Nuissl & Stefanie Meyer**

Mittelstand-  
Digital 

Gefördert durch:



Bundesministerium  
für Wirtschaft  
und Energie

aufgrund eines Beschlusses  
des Deutschen Bundestages

Mehr denn je werden heute Kamerasysteme, insbesondere aber Videoüberwachungssysteme in den Unternehmen offen oder verdeckt verbaut. Einfach bedienbare Kameratechniken, vergleichsweise günstige und leicht beziehbare Hard- und Software, große Speicherkapazitäten verbunden mit der Möglichkeit, die Aufzeichnungen anschließend sichtbar zu machen und auszuwerten, befördern diesen Trend. Dabei sind die von den Unternehmern angedachten Einsatzgebiete durchaus verschieden – nicht immer steht dabei die viel diskutierte Mitarbeiterüberwachung als Leistungs- und Aktivitätskontrolle im Vordergrund. Vielmehr sollen Geschäftsräume überwacht werden, um die Aufklärung von Straftatbeständen wie Diebstahl, Unterschlagung und Betrug zu erleichtern oder um an besonders sicherheitssensiblen Arbeitsplätzen (bspw. Bankfilialen) Unternehmensgegenstände, Mitarbeiter und Kunden zu schützen.

Außerdem kann in der Arbeitswelt 4.0 eine kamerabasierte Begleitung von Arbeits- und Maschinenabläufen die Mitarbeiter bei der Erbringung ihrer Arbeitsleistung visuell unterstützen und dabei obendrein Sach- und/oder Personenschäden vorbeugen. Unabhängig von der zugrundeliegenden Motivation und unabhängig davon, ob die Systeme verdeckt oder offen eingerichtet werden, sind Kamerasysteme gerade weil sie auch Menschen im Arbeitsumfeld aufzeichnen immer wieder Gegenstand auch juristischer Diskussionen, die sich mit dem Inkrafttreten der DSGVO und dem damit verbundenen gesteigerten Schutz der Privatsphäre noch weiter intensiviert haben. Bei Unternehmen führt dies mitunter zu Verunsicherung, weshalb nachfolgend ein kurzer Überblick zum rechtmäßigen Einsatz von Videoüberwachungssystemen in Unternehmen gewährt werden soll.

## **Videoüberwachungssysteme im Unternehmen**

Videoüberwachung ist begrifflich zunächst einmal die Beobachtung mittels optisch-elektronischer Einrichtungen<sup>1</sup>. Sofern das Videoüberwachungssystem in erster Linie dazu bestimmt ist, Arbeitnehmerverhalten und -leistung am Arbeitsplatz zu erfassen, wird nach der Definition des BAG<sup>2</sup> von Arbeitnehmer- bzw.

Mitarbeiterüberwachungssystemen gesprochen.

Es gibt verschiedene Formen von Videoüberwachungssystemen, wobei festzuhalten ist, dass mit der Zunahme von Funktionalitäten auch deren Eingriffsintensität in die Persönlichkeitsrechte der Betroffenen

(Arbeitnehmer, Dritte) steigt:

- Systeme mit einer reinen Monitoring-Funktion (Fernbeobachtung) arbeiten wie ein „verlängertes Auge“. Das erfasste Bild wird an einen Dritten (z. B. einen Wachmann) in Echtzeit übertragen und eine weitere Verarbeitung, wie etwa das Abspeichern der Bildsequenzen findet i. d. R. nicht immer statt. Die Interessen der Mitarbeiter oder Kunden sind insofern betroffen, als diese beobachtet werden, was gegebenenfalls mit Zoomfunktion oder auch heimlich geschehen kann.
- Analoge oder digitale Videotechniken ohne vorgenannte Einschränkung zielen dagegen geradezu auf das Verarbeiten der Bilddaten ab und eröffnen neben dem Abspeichern zumeist zahlreiche weitere Bearbeitungsoptionen, die bei der digitalen Videotechnik auch das Versenden des Materials an Dritte einschließen können. Während also eine Fernbeobachtung automatisch endet,

wenn der Betroffene den von der Kamera erfassten Bereich verlässt oder der Beobachtende das Kamerasystem ausschaltet, soll das Aufnahmematerial bei diesen Systemen ausdrücklich konserviert, jederzeit erneut wiedergegeben und das Ergebnis ggf. auch an Dritte weitergegeben werden.

- Moderne Thinking Cameras besitzen noch weitergehende Funktionen; sie agieren bereits teilautonom. Neben der Zoom- oder Zeitlupenfunktion können sie schwenken und den zu beobachtenden Objekten nachfolgen und damit eine lückenlose Überwachung im Raum gewährleisten. Ferner sind sie in der Lage, fortlaufend Bild- und Datenabgleiche zu Referenzdaten vorzunehmen und vorprogrammierte Maßnahmen einzuleiten (z. B. Zugangssperren zu aktivieren). Insofern ist die Eingriffsintensität hier am stärksten, weil sich Mitarbeiter und Dritte den Systemen nicht entziehen können.



## Einschlägige Rechtsvorschriften zur Reglementierung der Videoüberwachung

Ein Gesetz, das die Videoüberwachung im Unternehmen regelt, gibt es nicht. Allerdings bestehen diverse Rechtsvorschriften, die beim Einsatz von Videoüberwachungssystemen

im unternehmerischen Alltag zu berücksichtigen sind. Neben Bestimmungen, die das Recht am eigenen Bild (§§ 22ff. KunstUrhG) oder die Vertraulichkeit des höchstpersönli-

chen Lebensbereichs schützen (§§ 200, 201 a StGB) werden im unternehmerischen Umfeld insbesondere die Regelungen des Datenschutz-

rechts (DSGVO, BDSG), des kollektiven Arbeitsrechts (§ 87 Abs. 1 Nr. 6 BetrVG) und ggf. des Telekommunikationsrechts (§ 98 TKG) relevant.

## Datenschutzgrundverordnung (DSGVO) und Bundesdatenschutzgesetz (BDSG)

Unabhängig von der Ausgestaltung einer Videoüberwachung bedeutet sie immer einen besonders intensiven Eingriff in das Persönlichkeitsrecht des Betroffenen, da nicht nur einzelne Aspekte seines Verhaltens, sondern sein Gesamtverhalten wie Gestik und Mimik, bewusste oder unbewusste Gebärden, der Gesichtsausdruck bei der Arbeit oder bei der Kommunikation mit Vorgesetzten und Kollegen beobachtet und zum Teil reproduzierbar und analysierbar gemacht wird.<sup>3</sup> Insofern muss sich deren Zulässigkeit auch am allgemeinen Persönlichkeitsrecht des Arbeitnehmers messen lassen, welches verfassungsrechtlich in Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG garantiert ist. Obschon der Grundrechtsschutz in erster Linie als Abwehrrecht des Bürgers gegen den Staat gilt, sind die Grundrechte mittelbar auch im Arbeitsverhältnis zu beachten und gewähren auch dort jedermann das Recht, selbst darüber zu entscheiden, welche Informationen von ihm erhoben, verarbeitet und gespeichert werden.

In diesem Zusammenhang spielen die im Jahr 2018 in Kraft getretenen Datenschutz-Grundverordnung (DSGVO), die innerhalb Europas unmittelbar und zwingend anzuwenden ist, sowie das Bundesdatenschutzgesetz (BDSG) mit seinen Regelungen zum Beschäftigtendatenschutz eine erhebliche Rolle. Ihnen liegt das datenschutzrechtliche Grundprinzip zugrunde, dass die Erhebung personenbezogener Daten verboten ist, sofern nicht ein Erlaubnistatbestand den schwerwiegenden Eingriff in die Persönlichkeitsrechte des Arbeitnehmers rechtfertigt.

Personenbezogene Daten sind dabei alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art. 4 Nr. 1 DSGVO). Das von einer Kamera aufgezeichnete Bild einer Person, des Körpers oder eines charakteristischen Körperteils, wie etwa das Gesicht, fällt jedenfalls unter den Begriff „personenbezogene Daten“, weil es die Identifikation der betroffenen Person ermöglicht. Insofern

werden mittels Videoüberwachungssystemen – gleich ob dies das primäre Ziel des Kameraeinsatzes ist oder nur bei Gelegenheit geschieht – personenbezogene Daten der Arbeitnehmer erhoben und zugleich verarbeitet i. S. des Art. 4 Nr. 2 DSGVO. Das ist zunächst einmal verboten.

Die Verarbeitung personenbezogener Daten kann allerdings nach der DSGVO gerechtfertigt sein, wenn der Eingriff in das Persönlichkeitsrecht erlaubt ist, weil

- ein Gesetz oder eine andere Rechtsvorschrift dies ausdrücklich anordnet (im Unternehmensalltag nicht von Relevanz),
- der Betroffene in den Eingriff ausdrücklich und informiert eingewilligt (Art. 6 Abs. 1 lit. a), 7 DSGVO),
- die Verarbeitung in Erfüllung einer rechtlichen Verpflichtung erfolgt (Art. 6 Abs. 1 lit. c) DSGVO, Art. 88 Abs. 1 DSGVO),
- deren Verarbeitung zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist und das Persönlichkeitsinteresse des Betroffenen überwiegen (Art. 6 Abs. 1 lit. f) DSGVO).

Sofern besondere Kategorien von Daten erhoben werden (z. B. biometrische Daten) ist ferner Art. 9 Abs. 1 DSGVO zu berücksichtigen, der den rechtfertigenden Rückgriff auf Art. 6

Abs. 1 lit. f) DSGVO („berechtigte Interessen“) ausschließt.

Neben der DSGVO hält auch das BDSG rechtfertigende Regelungen in Bezug auf die Videoüberwachung bereit, namentlich § 4 BDSG und § 26 BDSG. Solche die DSGVO ergänzenden Regelungen sind auf nationaler Ebene möglich, sofern die DSGVO den Mitgliedstaaten die Regelungskompetenz einräumt, wie etwa in Art. 88 DSGVO für den Beschäftigtenkontext.

§ 4 BDSG regelt die Videoüberwachung in öffentlich zugänglichen Räumen.<sup>4</sup> Öffentlich zugänglich sind dabei diejenigen Räume, die dazu bestimmt sind, dass sich Menschen darin aufhalten können, weil die Bereiche entweder dem öffentlichen Verkehr gewidmet sind oder nach dem erkennbaren Willen des Berechtigten von jedermann genutzt oder betreten werden können. Hierzu zählen etwa Bahnsteige, Parkplätze, Ausstellungsräume, aber auch Fabrikgelände ohne Zugangskontrollen, Verkaufsräume, Eingangsbereiche von Bürogebäuden und Schalterhallen.

Die Beobachtung des öffentlich zugänglichen Raums ist eigentlich staatlichen Stellen im Rahmen ihrer Aufgabenerfüllung vorbehalten (§ 4 Abs. 1 Nr. 1 BDSG). In Ausnahmefällen kann die Videoüberwachung eines öffentlichen Raums auch von privater Seite erfolgen, insbesondere zur Wahrnehmung des Hausrechts

(Nr. 2) oder anderer berechtigter Interessen für konkret festgelegte Zwecke (Nr. 3). Die private Beobachtung öffentlicher Räume muss dabei erforderlich und verhältnismäßig sein, d. h. sie muss den beabsichtigten Zweck – z. B. Sicherung von Gesundheit und Leben der Mitarbeiter und Kunden in Kassenbereichen – erreichen oder zumindest fördern können und es dürfen keine milderen Mittel zur Erfüllung dieses Zwecks zur Verfügung stehen. Ferner muss eine ausführliche Interessenabwägung zwischen dem Eingriff in das Persönlichkeitsrecht der Betroffenen einerseits und dem berechtigten Interesse des Verantwortlichen an einer Überwachung andererseits stattfinden. Nur wenn die berechtigten Interessen des Verantwortlichen die Nachteile, die mit der Videoüberwachung verbunden sind, überwiegen, ist der Eingriff in das Persönlichkeitsrecht der Betroffenen gerechtfertigt. Abzuwägen ist das berechnete Interesse des Betreibers an der Verwirklichung des von ihm festgelegten Zwecks der Videoüberwachung mit möglichen gegenläufigen Interessen der betroffenen Personen. Dabei darf eine Überwachung bereits dann nicht mehr erfolgen, wenn Anhaltspunkte für ein Überwiegen der privaten Interessen nicht sicher ausgeräumt werden können.<sup>5</sup> Von der Rechtsprechung zum Schutz vor Straftaten ggü. Mitarbeitern und Kunden für zulässig erachtet wurde z. B. die Überwachung von Schalter- und Kassenbereichen, Eingangsbereichen, Treppenhäusern oder Tiefgaragen.

Neben dem § 4 BDSG ist außerdem der § 26 BDSG, Art. 88 Abs. 1 DSGVO zu beachten, der die Datenverarbeitung zum Zwecke des Beschäftigungsverhältnisses und damit zumeist in nicht öffentlich zugänglichen Räumen bzw. betriebsöffentlichen Bereichen regelt und weiter ausgestaltet. Dabei knüpft der § 26 BDSG die Zulässigkeit der Videoüberwachung an die aus der DSGVO bekannten Erlaubnistatbestände: die Einwilligung (Abs. 2), die Kollektivvereinbarung (Abs. 1) sowie anderweitige gesetzliche Regelungen (Abs. 3). Außerdem muss auch im Rahmen des § 26 BDSG die Videoüberwachung zur Erreichung des angestrebten Zwecks erforderlich sein und eine gründliche Abwägung der schützenswerten Interessen der Arbeitnehmer (Persönlichkeitsrecht) mit denen des Arbeitgebers (Recht am eingerichteten und ausgeübten Gewerbebetrieb Art. 14 GG) stattgefunden haben (Abs. 4), die zudem von speziellen arbeitsrechtlichen Vorschriften (z. B. dem Vorliegen von Betriebsvereinbarungen) und Gerichtsurteilen beeinflusst werden.

Ist eine Datenverarbeitung nach der DSGVO und/oder dem BDSG erlaubt, sind obendrein vom Verantwortlichen bzw. dem Arbeitgeber die allgemeinen Grundsätze zur Datenverarbeitung zu beachten, die weitere unternehmerische Pflichten begründen, wie insbesondere

- die Transparenzpflicht gemäß Art. 5 Abs. 1 lit. a) DSGVO, § 4 Abs. 2 BDSG, die besagt, dass die betrof-

fene Person die Datenverarbeitung nachvollziehen können muss.

- die Informations- und Mitteilungspflichten nach Art. 13 und 14 DSGVO, §§ 4 Abs. 4, 32 BDSG, welche erfordern, dass der Betroffene über den Einsatz der Systeme verständlich und umfassend zu informieren ist.
- die Löschungspflicht nach Art. 17 DSGVO, § 4 Abs. 5 BDSG, die bedeutet, dass der Verantwortliche nach Erreichung des Zwecks die Daten zu löschen hat.

- die organisationsrechtliche Verpflichtung zur vorherigen Datenschutzfolgeabschätzung nach Art. 35 DSGVO sowie dem Führen von Verarbeitungsverzeichnissen nach Art. 30 DSGVO.

Zusammenfassend folgt aus den Grundsätzen, dass die Überwachung kenntlich zu machen ist, die erhobenen Daten nur zu dem Zweck, zu dem sie erhoben wurden genutzt werden dürfen und danach in jedem Fall zu löschen sind.

## Betriebsverfassungsgesetz (BetrVG)

Im kollektiven Arbeitsrecht befindet sich die Norm des § 87 Abs. 1 Nr. 6 BetrVG, welcher dem Betriebsrat bei „*Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen*“ ein Mitbestimmungsrecht einräumt. Da Videoüberwachungssysteme am Arbeitsplatz regelmäßig eine solche verhaltens- und leistungsüberwachende Funktion erfüllen können, ist die Beteiligung des Betriebsrates bei deren Implementierung Wirksamkeitsvoraussetzung.<sup>6</sup>

Führt der Arbeitgeber ohne die Beteiligung des Betriebsrats eine Videoüberwachung am Arbeitsplatz ein, handelt es sich um eine rechtswidrige, da mitbestimmungswidrige

Maßnahme. Der Betriebsrat kann mit einem Unterlassungs- und Beseitigungsanspruch dagegen vorgehen, d. h. er kann die De-Installation verlangen.

Sind bereits arbeitnehmerbezogene Daten erhoben und verarbeitet worden (z. B. Videos wurden betrachtet, Bilddaten abgespeichert) steht auch den betroffenen Arbeitnehmern ein Beseitigungs- und Unterlassungsanspruch, ggf. sogar Schmerzensgeld wegen Verletzung der arbeitsvertraglichen Treue- und Rücksichtnahmepflicht aufgrund des Eingriffs in das Persönlichkeitsrecht zu.

Ob die zu Unrecht gewonnenen Informationen gegen den Arbeitnehmer verwertbar sind, wird dagegen

unterschiedlich beurteilt. Jedenfalls unterliegen mitbestimmungswidrig erlangte Informationen, die zudem in das Persönlichkeitsrecht des Arbeitnehmers eingreifen (was zumeist der Fall sein wird) einem Beweisverwer-

tungsverbot, d. h. selbst wenn ein deliktisches Verhalten eines Arbeitnehmers aufgezeichnet würde, wäre das Bildmaterial in einem Prozess nicht verwertbar.<sup>7</sup>

## Telekommunikationsgesetz (TKG)

Das Telekommunikationsgesetz ist zu beachten, wenn z. B. mit dem Kamerasystem auch Standortdaten erhoben werden und die Daten in Nutzer öffentlichen Telekommunikationsnetzen oder öffentlich zugänglichen Telekommunikationsdienst verwendet werden (§ 98 TKG). Zwar betrifft das Telekommunikationsrecht in erster Linie das Verhältnis zwischen dem Arbeitgeber und dem Telekommunikationsdiensteanbieter und nicht das Verhältnis zwischen Arbeitgeber und Arbeitnehmer, aber es bestehen Informationspflichten, deren Nicht-einhalten auch die Zulässigkeit des Überwachungssystems insgesamt berührt.

Nach § 98 Abs. 1 S. 1 TKG dürfen Standortdaten in dem zur Bereitstellung von Diensten mit Zusatznutzen erforderlichen Umfang und innerhalb des dafür erforderlichen Zeitraums verarbeitet werden, wenn sie anonymisiert wurden oder wenn der Teilnehmer dem Anbieter des Dienstes seine Einwilligung erteilt hat. Teilnehmer im Sinne des TKG ist der Arbeitgeber, da dieser in der Vertragsbeziehung zum Telekommunikationsdiensteanbieter steht. Es kommt somit ggf. auf

dessen Einwilligung an. Einer Einwilligung der jeweiligen Beschäftigten als Betroffene bedarf es nach dem TKG nicht.

Allerdings ist der Arbeitgeber gemäß § 98 Abs. 1 S. 4 TKG verpflichtet, jeden Mitbenutzer, also ggf. auch den Beschäftigten, dessen Standort erhoben wird, über seine gegenüber dem Telekommunikationsdiensteanbieter erklärte Einwilligung zu unterrichten. Die Verletzung dieser Verpflichtung stellt einen arbeitsrechtlichen Pflichtverstoß dar, der Unterlassungs- und Schadensersatzansprüche des Arbeitnehmers begründen kann.





## Was ist nun bei einem beabsichtigten Einsatz von Videokameras konkret zu beachten?

Nachfolgend soll dargestellt werden, worauf Sie als Unternehmer beim Einsatz von Videokameras in Ihrem Unternehmen achten müssen, wobei grundsätzlich zwischen einer „offenen“ und „verdeckten“ Videoüberwachung zu differenzieren ist.

Eine Videoüberwachung ist „offen“, wenn die Kamera gut sichtbar angebracht ist und auf deren Einsatz ausdrücklich hingewiesen wurde. Sie ist „verdeckt“, wenn dies gerade nicht geschieht.

### Offene Videoüberwachung

Sofern Sie eine offene (sichtbare) Videoüberwachung anstreben, kann diese über § 26 Abs. 1 BDSG, ggf. i. V. m. § 4 BDSG, legitimiert werden. Dies gilt allerdings nicht für sog. „Intimzonen“ (z. B. Toiletten oder Umkleide-räume), da in diesen Bereichen eine Videoüberwachung (selbst das Aufhängen von Kamera-Attrappen) in jedem Fall unzulässig ist.

Eine offene Videoüberwachung in nichtöffentlichen Bereichen, zu denen also nur die Mitarbeiter Zugang haben (z. B. Produktionsbereich, Labore), könnte durch eine Einwilligung der Betroffenen gerechtfertigt werden.<sup>8</sup> Die Einwilligung muss förmlich, d. h. schriftlich oder elektro-

nisch erfolgen, autonom und freiwillig abgegeben sein und sich auf einen bestimmten dem Betroffenen transparenten Vorgang beziehen („Videoaufnahmen für bzw. zu welchem Zweck ...“). Ferner müssen Aufklärungen z. B. über die Widerrufsmöglichkeit vorausgehen. Nur dann liegt eine sog. „informierte Einwilligung“ des Arbeitnehmers vor, auf deren Grundlage die Verarbeitung seiner Daten gemäß Art. 6 Abs. 1 S. 1 lit. a) DSGVO, § 26 Abs. 2 BDSG erfolgen kann.

## PRAXISTIPP

Achten Sie daher darauf, dass Sie den Arbeitnehmer vor der Erklärung umfassend über Zweck und Umfang der Anwendung informieren, sich die Einwilligung schriftlich einholen<sup>[9]</sup> und Sie den Arbeitnehmer über seine bestehende Widerrufsmöglichkeiten aufklären.

Beachten Sie ferner, dass das Vorliegen einzelner Arbeitnehmer-Einwilligungen bei offenen Überwachungsmaßnahmen mitunter nicht ausreichend ist. Es besteht nämlich die Gefahr, dass ein Mitarbeiter in den überwachten Bereich eintritt, von dem Sie gerade keine Einwilligung erhalten haben. Diesem gegenüber würden Sie dann – sofern sie dem Mitarbeiter gegenüber kein Zutrittsverbot ausgesprochen hatten<sup>10</sup> – einen ggf. bußgeldbewährten DSGVO-Verstoß begehen.

Aufgrund dieser Problematik empfiehlt es sich, auch den Rechtfertigungsgrund des Art. 6 Abs. 1 S. 1 lit. f) DSGVO mit im Blick zu haben, der die Verarbeitung der Daten zur Wahrung berechtigter Interessen (auch ohne Einwilligung) ermöglicht. Sofern sich die Verarbeitung der Daten (z. B. Speicherung der relevanten Sequenzen) im Verhältnis zu den Arbeitnehmern nach § 26 I 1 BDSG, Art. 6 Abs. 1 S. 1 lit. f) DSGVO als gerechtfertigt darstellt, müssen grundsätzlich auch die mitunter miterfassten Dritten (z. B. Kunden) die weitere Verarbeitung und mögliche Nutzung dieses Videomaterials dulden.<sup>11</sup> Welche Interessen die Persönlichkeitsinteressen der Arbeitnehmer (und die der Dritten) überwiegen kann, muss aber gut überlegt sein. Ferner steht dieser Rechtfertigungsgrund gerade nicht mehr zur Verfügung, wenn sensible Daten (genetische oder biometrische Daten) erfasst werden (Art. 9 DSGVO).

Neben der Einwilligung des Betroffenen kommen zur Rechtfertigung auch Betriebs- oder Dienstvereinbarungen in Betracht, die sich allerdings in dem vorgegebenen Rahmen der DSGVO zu bewegen haben, d. h. die Überwachung muss auch weiter berechtigten, schutzwürdigen Interessen dienen, erforderlich sein und verhältnismäßig. Für über die

DSGVO/BDSG hinausgehende Befugnisse des Arbeitgebers besteht im Rahmen der kollektiven Regelungen kein Spielraum. Die Zuständigkeit der Betriebsparteien ergibt sich aus § 87 Abs. 1 Nr. 6 BetrVG.

Die offene Videoüberwachung ist jedenfalls – und zwar unabhängig von ihrer Rechtfertigung (Einwilligung

oder Betriebsvereinbarung) – hinreichend kenntlich zu machen. In welcher Weise dies geschehen muss, ist gesetzlich nicht festgeschrieben. Die Mindestanforderungen an den Inhalt des Hinweises ergeben sich jedoch indirekt aus den Informationspflichten nach Art. 13 Abs. 1 u. 2 bzw. Art. 14 DSGVO. Daran angelehnt ist zuvörderst darauf hinzuweisen, dass eine Videoüberwachung stattfindet (etwa durch ein Kamerasymbol) und welcher Rechtfertigungsgrund die Überwachung stützt (Betriebs-

vereinbarung, berechtigtes Interesse). Ferner ist die Identität des für die Videoüberwachung Verantwortlichen bekannt zu geben, ebenso Kontaktinformationen zum Datenschutzbeauftragten bzw. ein Hinweis darauf, wo man weitergehende Informationen zur Videoüberwachung erhalten kann. Schließlich sind auch die Verarbeitungszwecke bekannt zu geben, die Dauer der Speicherung sowie die Rechtsgrundlagen für die Verarbeitung.

### PRAXISTIPP

Sie sollten darauf achten, dass der Hinweis mit vorgenannten Informationen gut sichtbar und bei Betreten des Raumes erkennbar ist. Um der Pflicht zur Kenntlichmachung rechtssicher nachzukommen, bietet sich ein ausdrücklicher Hinweis auf die Überwachung im Unternehmen (z. B. durch Anbringen eines Hinweisschildes) an, der wie nachfolgend ausgestaltet sein könnte (die offenen Stellen ausgefüllt wären dabei auszufüllen):<sup>12</sup>

Beispiel für ein vorgelagertes Hinweisschild nach Art. 13 der Datenschutz-Grundverordnung bei Videoüberwachung<sup>1</sup>



 <p><b>Achtung</b> <b>Videoüberwachung!</b></p> <p>Weitere Informationen finden Sie:</p> <ul style="list-style-type: none"> <li>• per Aushang (wenn möglich)</li> <li>• bei unserer Kundeninformation /</li> <li>Rezeption / Kasse im Erdgeschoss</li> <li>• ggf. / zusätzlich im Internet unter</li> </ul> 	Name und Kontaktdaten des Verantwortlichen und ggf. seines Vertreters:
	Kontaktdaten des Datenschutzbeauftragten (sofern vorhanden):
	Zwecke und Rechtsgrundlage der Datenverarbeitung: berechtigter Interessen, die verfolgt werden:
	Speicherdauer oder Kriterien für die Festlegung der Dauer:
	<small><sup>1</sup> Hinweis: Die Informationen sind unverzüglich in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache bereitzustellen. Sie können in Kombination mit standardisierter Bildschirmanzeige (z.B. Art. 13 DSGVO), im Zusammenhang zu erreichen, welche der Ausdrücke mindestens in 100% zu erfüllen.</small>

Abbildung 1: Beispiel für ein vorgelagertes Hinweisschild nach Art 13 der DSGVO bei Videoüberwachung

Im Allgemeinen ist eine offene Videoüberwachung natürlich weniger eingriffsintensiv als eine verdeckte, da der Arbeitnehmer sein Verhalten auf die für ihn sichtbare Situation einstellen und dem überwachten Bereich ausweichen kann. Auf dieses Ausweichenkönnen sollte aber schon bei der Installation einer Überwachungsanlage Wert gelegt werden, da das BAG

in einem zuletzt ergangenen Urteil<sup>13</sup> den durch eine fortdauernde Aufnahme entstehenden Leistungs- und Überwachungsdruck aufseiten des Arbeitnehmers, der ihn obendrein in seinem selbstbestimmten Handeln hemmt, im Rahmen der Abwägungsentscheidung zu Lasten des Arbeitgebers wertete.

#### PRAXISTIPP

Es ist daher zu empfehlen, dass bei einer offenen Videoüberwachung dem Arbeitnehmer auch die Möglichkeit eröffnet wird, sich aus der Überwachung zurückzuziehen und zumindest einen Teil der Arbeitszeit unbeobachtet bleiben zu können („überwachungsfreie Zonen“).

## Verdeckte Videoüberwachung

Die verdeckte oder heimliche Videoüberwachung von Beschäftigten wurde bereits vor Inkrafttreten der DSGVO kritisch beurteilt, da aufgrund des heimlichen Agierens die Eingriffsintensität in das Allgemeine Persönlichkeitsrecht der Mitarbeiter besonders hoch ist. Insofern wird eine solche Überwachung überhaupt nur in sehr eng begrenzten Ausnahmefällen für zulässig erachtet (§ 26 Abs. 1 S. 2 BDSG).

Ein solcher Ausnahmefall liegt vor, wenn der konkrete Anfangsverdacht einer schweren arbeitsvertraglichen Pflichtverletzung besteht. Der Verdacht muss sich auf eine konkrete strafbare Handlung oder eine andere

schwere Verfehlung knapp unterhalb der Straftaten-Schwelle erstrecken sowie auf einen zumindest räumlich und funktional abgrenzbaren Kreis von Arbeitnehmern begrenzt sein.<sup>14</sup> Allgemeine Mutmaßungen oder ein Verdacht „ins Blaue hinein“ reichen zur Rechtfertigung der verdeckten Videoüberwachung nicht aus.<sup>15</sup> Die heimliche Überwachung muss für den Arbeitgeber obendrein das noch einzig verbleibende Mittel sein, um den Sachverhalt aufzuklären zu können. Stehen mildere oder alternative Mittel zur Verfügung (z. B. Befragung von Kollegen; Beobachtung durch Aufsichtspersonal oder Detektive; eine offene Videoüberwachung zur Abschreckung), kann selbst die avi-

sierte Vermeidung von Straftaten die heimliche Videoüberwachung nicht mehr rechtfertigen.

Problematisch sind bei einer berechtigten verdeckten Videoüberwachung die Regelungen der DSGVO, namentlich die dort normierten umfassenden Transparenz- und Informationspflichten (Art. 5 Abs. 1 lit a) und Art. 13 DSGVO). Sie stehen einer heimlichen Überwachung eigentlich entgegen. Nach dem Wortlaut des Art. 13

DSGVO müssen – wie zuvor beschrieben – die betroffenen Mitarbeiter vor der Durchführung der Videoüberwachung über die Umstände der Kontrollen aufgeklärt werden. Realistisch betrachtet würde dann aber der Zweck der (berechtigten) Überwachung leerlaufen. Deshalb ist in diesen Fallgestaltungen die Videoüberwachung von Arbeitnehmern auch ohne vorherige Information zulässig.<sup>16</sup>

#### PRAXISTIPP

Beachten Sie, dass die verdeckte Videoüberwachung nur in ganz engen Grenzen gestattet ist und obendrein nur „ultima ratio“ in Betracht kommt. Sie wird daher in den allermeisten Sachverhaltskonstellationen nicht möglich sein.

## Sonderfall: Videosysteme zur Unterstützung von Arbeitsabläufen

Auch wenn Videosysteme zur Unterstützung von Arbeitsabläufen eingesetzt werden sollen, gelten grundsätzlich die zuvor beschriebenen datenschutzrechtlichen Anforderungen, sofern Mitarbeiter erkennbar bzw. identifizierbar werden. Auf die Zielrichtung des Kameraeinsatzes kommt es hier gerade nicht an, sondern alleine auf das Faktum des Erkennens einer Person und dem Verarbeiten personenbezogener Daten.

Da es aber dem Unternehmer mitunter gar nicht auf die Personen ankommt, sondern eben auf die Visualisierung technischer Abläufe und Begebenheiten, sollte beim beabsichtigten Einsatz solcher Systeme darauf geachtet werden, dass sie von Anfang an technische Möglichkeiten vorhalten, um agierenden Personen aus dem Bild zu nehmen oder unkenntlich zu machen.

<p><b>Offene Videoüberwachung in öffentlich zugänglichen Räumen</b></p> <ul style="list-style-type: none"><li>• Zulässig zur Wahrnehmung des Hausrechts und zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke.</li><li>• Offenes und sichtbares Anbringen der Kamera.</li><li>• Hinweis auf die Videoüberwachung erforderlich.</li><li>• Unverzügliche Löschung der Bildsequenzen, wenn der Verarbeitungszweck erreicht ist.</li></ul>	<p><b>Offene Videoüberwachung in nicht öffentlich zugänglichen Räumen</b></p> <ul style="list-style-type: none"><li>• Gerechtfertigt durch freiwillige und informierte Einwilligung seitens der Mitarbeiter → umfassende Aufklärung über Umfang und Zweck erforderlich sowie über die Möglichkeit des Widerrufs.</li><li>• Gerechtfertigt bei überwiegendem Interesse des Arbeitgebers (Ausnahme: sensible Daten) → Interessenabwägung erforderlich.</li><li>• Hinweis auf die Videoüberwachung erforderlich.</li><li>• Unverzügliche Löschung der Bildsequenzen, wenn der Verarbeitungszweck erreicht ist.</li></ul>
<p><b>Verdeckte Videoüberwachung in öffentlich zugänglichen Räumen</b></p> <ul style="list-style-type: none"><li>• Nur in eng begrenzten Ausnahmefällen zum Schutz des Unternehmenseigentums zulässig, ansonsten unzulässig.</li><li>• Unverzügliche Löschung der Bildsequenzen, wenn der Verarbeitungszweck erreicht ist.</li></ul>	<p><b>Verdeckte Videoüberwachung in nicht öffentlich zugänglichen Räumen</b></p> <ul style="list-style-type: none"><li>• Nur in eng begrenzten Ausnahmefällen zur Aufdeckung einer Straftat, der ein konkreter Verdacht zugrunde liegt, oder zur Aufdeckung einer schweren Verfehlung zulässig, ansonsten unzulässig.</li><li>• Unverzügliche Löschung der Bildsequenzen, wenn der Verarbeitungszweck erreicht ist.</li></ul>

Abbildung 2: Übersicht Videoüberwachungsarten

## Weiterer Umgang mit den Daten - Löschungsverpflichtung

Personenbezogene Daten, die mit einer Videoüberwachungsanlage gespeichert werden, sind nach den allgemeinen Grundsätzen (Art. 17 DSGVO) wieder zu löschen. Eine Löschungsverpflichtung besteht insbesondere dann, wenn die Voraussetzungen, die eine Speicherung ursprünglich gerechtfertigt haben, entfallen sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.

Von datenschutzrechtlichen Aufsichtsbehörden wird die Auffassung vertreten, dass Videoaufzeichnungen grundsätzlich nur 48 Stunden oder jedenfalls nur wenige Tage aufbewahrt werden dürften.<sup>17</sup> Dies korrespondiert auch mit Urteilen des BAG<sup>18</sup> welches einen 72-Stunden-Zeitraum präferierte, da – so das BAG – der Unternehmer oftmals das Bildmaterial nicht sofort auswerten kann. Im Einzelfall und unter Berücksichtigung

der datenschutzrechtlichen Grundsätze „Datenminimierung“ und „Speicherbegrenzung“ kann bei einer offenen Überwachung auch eine längere Aufbewahrungs- und Auswertzeit in Betracht kommen, z. B. wenn ein wie-

derkehrender Verstoß gegen strafrechtliche Bestimmungen nachgewiesen werden soll. Die Grenze bildet jedenfalls ein missbräuchliches in die Länge ziehen der Materialsichtung.

#### PRAXISTIPP

Videoaufnahmen sollten – wenn möglich – binnen 72 Stunden gelöscht werden.



## Verwertbarkeit der Videoaufzeichnungen

Mit der Arbeitnehmerüberwachung verfolgt der Arbeitgeber in der Regel keinen rein informatorischen Zweck, sondern er will präventiv Straftaten vermeiden oder sie zumindest aufdecken. Letzteres führt häufig zur Abmahnung und im Wiederholungsfall zur verhaltensbedingten Kündigung, wobei die Erkenntnisse aus den Videoaufzeichnungen den Kündigungsgrund belegen sollen. Wurden die Überwachungsmaterialien rechtswidrig erlangt, weil z. B. gegen datenschutzrechtliche Bestimmung verstoßen wurde, unterliegen sie einem Beweisverwertungsverbot und eine darauf beruhende Kündigung wird

für unwirksam erklärt. Zwar gilt der sog. Grundsatz der freien Beweiswürdigung, der erst einmal besagt, dass nicht jede rechtswidrig erlangte Erkenntnis zwangsläufig in ihrer Verwertung verboten ist. Allerdings ist mit einer rechtswidrigen Videoüberwachung zumeist auch ein intensiver Eingriff in das Allgemeine Persönlichkeitsrecht verbunden, woraus dann regelmäßig das Beweisverwertungsverbot abgeleitet wird. Deswegen sollten bereits bei der Installation der Überwachungssysteme die gesetzlichen Vorgaben berücksichtigt werden.



## Rechtsfolgen

Sofern mithilfe der Videoüberwachung das Fehlverhalten eines Arbeitnehmers ermittelt wurde, können die für die Überwachung aufgewendeten Kosten vom Arbeitnehmer zu ersetzen sein. Anspruchsgrundlage ist § 280 Abs. 1 S. 1 BGB bzw. § 823 BGB. Dieser Anspruch besteht allerdings nur, sofern die Videoüberwachung rechtmäßig erfolgte.

Erfolgte sie unrechtmäßig, kann der Arbeitnehmer zum einen seine Leistungsverpflichtung verweigern und zudem Ansprüche auf Unterlassen und Beseitigung der Überwachung geltend machen, welche sich arbeitsvertraglich aus §§ 611, 241 Abs. 2 BGB und generell aus §§ 1004, 823 BGB analog ergeben. Daneben kann er das Löschen unzulässiger Aufnahmen verlangen. Obendrein bestehen ggf. Schadensersatz- oder Schmerzensgeldansprüche (§§ 823, 254 Abs. 2 BGB). In einem Sachverhalt, der vor dem hessischen LAG beurteilt wurde, überwachte ein Arbeitgeber das Verhalten seiner Arbeitnehmerin über mehrere Monate hinweg mit einer an der Bürotür montierten Kamera, ohne ihre Zustimmung dafür erhalten zu haben. Das Gericht sah es als erwiesen an, dass in das Allgemeine

Persönlichkeitsrecht und das Recht auf informationelle Selbstbestimmung in rechtswidriger Weise eingegriffen wurde und sprach der Mitarbeiterin eine Entschädigung in Höhe von 7.000 Euro zu.<sup>19</sup>

Werden vertrauliche Gespräche mit aufgezeichnet, die Intimsphäre der Mitarbeiter tangiert oder gelangen personenbezogene Daten an unberechtigte Dritte, drohen auch strafrechtliche Konsequenzen. Solche strafrechtlichen Verstöße werden durchweg mit Freiheitsstrafe von bis zu 3 Jahren oder Geldstrafe geahndet (§§ 200, 201, 201 a, 240 StGB).

Schließlich sind alle Verstöße gegen die DSGVO und das BDSG bußgeldbewehrt. Wird z. B. gegen die Transparenz- und Informationspflichten aus Art. 13 und 14 DSGVO verstoßen, können drakonische Bußgelder nach Art. 83 Abs. 5 DSGVO verhängt werden. Dasselbe gilt, wenn materielle Pflichten verletzt werden, wie etwa, wenn ein überwachungsfrei zu bleibender Ort per Kamera kontrolliert wird (§ 43 BDSG); hier drohen Bußgelder bis zu 50.000 EUR.





## Exkurs: Drohneneinsatz

Die Videoüberwachung kann nicht nur durch ein fest installiertes Gerät erfolgen, sondern auch mithilfe einer Drohne. Eine Drohne ist ein unbemanntes Fluggerät, was gem. § 1 Abs. 2 S. 3 LuftVG als Luftfahrzeug gilt. Das Gesetz unterscheidet zwischen unbemannten Luftfahrtsystemen, d. h. Drohnen die gewerblich betrieben werden, und Flugmodellen, welche privat, d. h. zu Sport- oder Freizeit Zwecken genutzt werden.

Beim Einsatz von solchen Geräten, die bei weitläufigen Betriebsgeländern oder Baustellen eine große Hilfe

darstellen können, sind zum einen die vorgenannten datenschutzrechtlichen Aspekte zu berücksichtigen. Werden personenbezogene Daten verarbeitet, muss eine Rechtfertigung nach Art. 6 Abs. 1 S. 1 lit a), f) DSGVO, §§ 4, 26 BDSG möglich sein und ein entsprechender Hinweis auf deren Einsatz gewährt werden.

Daneben sind auch luftrechtliche Vorgaben zu beachten, die in aller Kürze dargestellt werden sollen.

## Pflichten im Vorfeld der Inbetriebnahme

§ 19 Abs. 3 LuftVZO verlangt, dass ein unbemanntes Luftfahrtsystem, welches eine Startmasse von mehr als 0,25 kg aufweist, gekennzeichnet sein muss. Die Kennzeichnung mit Name und kompletter Adresse des Halters muss als feuerfeste und dauerhafte Beschriftung (in der Regel durch eine Plakette) an dem Fluggerät deutlich sichtbar angebracht sein. Dies dient dem Zweck, den Halter oder Betreiber im Schadensfall für die zivilrechtliche oder strafrechtliche Inanspruchnahme schneller identifizieren zu können<sup>20</sup>.

Betreiber unbemannter Luftfahrtsysteme mit einem Gewicht ab 2 kg benötigen einen Nachweis über hinreichende Kenntnisse bzgl. der Anwendung und Navigation solcher Fluggeräte, der einschlägigen luftrechtlichen Grundlagen und der örtlichen Raumzuordnung, vgl. § 21a Abs. 4 S. 1 Nrn. 1-3 LuftVO. Ein solcher Nachweis („Führerschein“) kann nach erfolgreicher Prüfung vom Luftfahrt-Bundesamt ausgestellt werden.

Während lange Zeit eine gewichts-unabhängige Aufstiegserlaubnis für

Drohnen erforderlich war<sup>21</sup>, ist dieses Erfordernis bei unbemannten Luftfahrzeugen mit einem Gewicht von unter 5 kg nunmehr entfallen<sup>22</sup>. Bei Drohnen mit einer Gesamtmasse von über 5 kg ist die Aufstiegserlaub-

nis weiterhin erforderlich, welche die Landesluftfahrtbehörden erteilen. Einer gesonderten Erlaubnis bedarf auch, wer Drohnen in der Nacht benutzen will.

## Regelungen der LuftVG, LuftVZO, LuftVO beim Betrieb der Drohne

Der Betrieb der Drohne außerhalb des Sichtfeldes des Betreibers ist verboten, § 21 b Abs. 1 S. 1 Nr. 1 LuftVO. Laut der Definition des Gesetzes befindet sich die Drohne außerhalb der Sichtweite, wenn das unbemannte Fluggerät ohne besondere optische Hilfsmittel nicht mehr gesehen werden kann oder seine Fluglage nicht mehr eindeutig zu erkennen ist.

Besonderheiten ergeben sich bei Verwendung eines audiovisuellen Ausgabegerätes. Wird die Drohne mittels einer Videobrille betrieben, sind Flüge erlaubt, sofern sie bis zu einer Höhe von 30 Metern stattfinden und das Gerät nicht schwerer als 0,25 kg ist oder eine andere Person es ständig in Sichtweite beobachtet und in der Lage ist, den Steuerer auf Gefahren aufmerksam zu machen. Letzteres gilt als Betrieb innerhalb der Sichtweite des Steuerers.

Eine Drohne ist jedenfalls außerhalb der Sichtweite, wenn beim Umfliegen von großen Gebäuden, Krans etc. kein Sichtkontakt mehr zum Flugsys-

tem besteht<sup>23</sup>.

Für die Verwendung von Drohnen im Umfeld von Baustellen ist zudem darauf hinzuweisen, dass sie einen seitlichen Abstand von 100 m zu sensiblen Bereichen einhalten müssen. Darunter fallen: Einsatzorte von Polizei bzw. sonstigen Rettungskräften, Krankenhäuser, Menschenansammlungen, JVA, Industrieanlagen, oberste Bundes- oder Landesbehörden, Naturschutzgebiete, bestimmte Verkehrswege, Kontrollzonen von Flugplätzen (§ 21 b Abs. 1 S. 1 Nrn. 2-6 LuftVO). Ebenso ist der Flug über Wohnungsgrundstücke verboten, die ggf. an die Baufläche angrenzen, sofern die Drohne über 0,25 kg wiegt bzw. das Gerät in der Lage ist, optische oder akustische Aufzeichnungen zu machen, und der Eigentümer des Grundstückes keine Einwilligung erteilt hat, § 21 b Abs. 1 S. 1 Nr. 7 LuftVO. Bezogen auf die Einhaltung des Sicherheitsabstandes kann eine Ausnahmegenehmigung beantragt werden, sofern keine Gefahr für die Sicherheit des Luftverkehrs und der

öffentlichen Sicherheit oder Ordnung besteht<sup>24</sup>.

In dem Bereich von über 100 Metern über dem Boden ist der Betrieb von unbemannten Flugfahrtsystemen generell verboten, ebenso wie die Verwendung einer Drohne mit einem Gewicht von über 25 kg.

Im Übrigen ist darauf zu achten, dass gem. § 21 f LuftVO eine Ausweichpflicht angeordnet ist. Bemannten Luftfahrzeugen und unbemannten Freiballons ist stets auszuweichen.

## Haftung

Der Halter des Luftfahrzeuges haftet für Personen- und Sachschäden, die durch einen Unfall beim Betrieb des Luftfahrzeugs verursacht werden. Diese Gefährdungshaftung gilt auch dann, wenn der Halter selbst nicht am

Unfall schuld ist. Um die Schadensregulierung zu gewährleisten, schreibt § 43 Abs. 2 LuftVG vor, dass der Halter zur Deckung seiner Haftung, wie auch beim Kfz, eine Haftpflichtversicherung besitzen muss.



## Fazit

Es empfiehlt sich, mit der Installation von Videoanlagen im Unternehmen grundsätzlich offen umzugehen. Informieren Sie Ihre Mitarbeiter über den beabsichtigten Zweck, klären Sie so weit als möglich auf und holen Sie Einwilligungen ein oder setzen eine Betriebsvereinbarung in Kraft. Achten Sie darauf, dass Sie auf die Videoüberwachung hinweisen, sodass jeder (auch jeder Außenstehende) selbstständig entscheiden kann, ob er sich in den überwachten Bereich begeben will. Die heimliche Überwachung ist nur in Ausnahmefällen bei

begründetem Verdacht erlaubt!

Im Interesse Ihrer Mitarbeiter müssen die Aufnahmen binnen 72 Stunden spätestens gelöscht werden, sofern Sie die Aufzeichnungen nicht zu Beweis Zwecken benötigen.

## Anmerkungen

1. vgl. § 4 BDSG.
2. BAG NZA 2004, 1278, 1279; BAG NZA 2008, 1187, 1189.
3. Riesenhuber BeckOK DatenschutzR, 32. Ed. 2020, BDSG, § 26 Rn. 144.
4. Dabei ist streitig, ob die DSGVO dem nationalen Gesetzgeber die Befugnis zur spezifischeren Regelung eingeräumt hat – die Legitimation soll sich aus Art. 6 Abs. 1 S. 1 lit. c und e DSGVO ergeben, wonach eine nationale Regelung möglich sein soll, wenn sie für die Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe erforderlich ist, Gola DSGVO, 2. Aufl. 2018, DSGVO Art. 6 Rn. 157; Wilhelm BeckOK DatenschutzR, 32. Ed. 2020, BDSG, § 4 Rn. 18.
5. Wilhelm BeckOK BDSG, 32. Ed. 2020, § 4 Rn. 34.
6. Weth/Herberger/Wächter/Sorge/Byers Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, 2. Aufl. 2019, DSGVO Teil B. VIII. Rn. 44.
7. Kania Erfurter Kommentar zum Arbeitsrecht, 20. Aufl. 2020, § 87 Rn. 137; Bacher BeckOK ZPO, 37. Ed. 2020, § 284 Rn. 19 ff.
8. Art. 6 Abs. 1 lit. a), 7 DSGVO; § 26 Absatz 2 BDSG.
9. § 26 Abs. 2 BDSG.
10. BAG Urt. v. 20.10.2016 – 2 AZR 395/15, NZA 2017, S. 443 ff.
11. Schaub/Linck Arbeitsrechts-Handbuch, 18. Aufl. 2019, § 153 Beschäftigtendatenschutz Rn. 11.
12. [https://www.lida.bayern.de/media/muster/video\\_hinweis.pdf](https://www.lida.bayern.de/media/muster/video_hinweis.pdf) (aufger. 24.06.2020).
13. BAG Urt. v. 28.03.2019, Az.: 8 AZR 421/17, besprochen in der Wissensbox.
14. BAG Urt. v. 20.10.2016 – 2 AZR 395/15, NJW 2017, 1193 Rn. 22; BAG Urt. v. 27. 3. 2003 - 2 AZR 51/02, NJW 2003, 3436.
15. Schaub/Linck Arbeitsrechts-Handbuch, 18. Aufl. 2019, § 153 Beschäftig-

tendatenschutz Rn. 9.

16. Weth/Herberger/Wächter/Sorge/Byers Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, 2. Aufl. 2019, DSGVO Teil B. VIII. Rn. 26g; EGMR Urte. v. 17.10.2019 – 1874/13 u. 8567/13, NZA 2019, 1697 – López Ribalda ua/Spanien.

17. Vgl. Kurzpapier Nr. 15 der Datenschutzkonferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, S. 3.

18. BAG Urte. v. 28.03.2018, Az.: 2 AZR 133/18, besprochen in der Wissensbox.

19. Hessisches LAG, Urte. v. 25.10.2010, Az. 7 Sa 1586/09.

20. BR-Drs. 39/17, 16.

21. Brahms/Maslaton Die gewerbliche Nutzung von Drohnen im Lichte der geplanten Novelle der LuftVO, NVwZ 2016, 1125, 1126.

22. Stellpflug/Hilbert Novellierter Rechtsrahmen für den Betrieb unbemannter Fluggeräte, NVwZ 2017, 1490, 1491.

23. Uschkereit/Zdanowiecki Rechtsrahmen für den Betrieb ziviler Drohnen, NJW 2016, 444, 446.m.w.N.

24. Uschkereit/Zdanowiecki Rechtsrahmen für den Betrieb ziviler Drohnen, NJW 2016, 444, 446.

## Autoren

Prof. Dr. Dagmar Gesmann-Nuissl ist die Leiterin der Professur für Privatrecht und Recht des geistigen Eigentums der Technischen Universität Chemnitz mit einem Forschungsschwerpunkt im Innovations- und Technikrecht. Als Konsortialpartnerin des Mittelstand 4.0-Kompetenzzentrums Chemnitz leitet sie außerdem die „Arbeitsgemeinschaft Recht 4.0“ aller Mittelstand 4.0-Kompetenzzentren in Deutschland.

[dagmar.gesmann-nuissl@betrieb-machen.de](mailto:dagmar.gesmann-nuissl@betrieb-machen.de)

Stefanie Meyer ist wissenschaftliche Mitarbeiterin an der Professur für Privatrecht und Recht des geistigen Eigentums von Prof. Dr. Dagmar Gesmann-Nuissl an der Technischen Universität Chemnitz.

## Weitere Informationen

Das Mittelstand 4.0-Kompetenzzentrum Chemnitz gehört zu Mittelstand-Digital. Mit Mittelstand-Digital unterstützt das Bundesministerium für Wirtschaft und Energie die Digitalisierung in kleinen und mittleren Unternehmen und dem Handwerk.

### Was ist Mittelstand-Digital?

Mittelstand-Digital informiert kleine und mittlere Unternehmen über die Chancen und Herausforderungen der Digitalisierung. Die geförderten Kompetenzzentren helfen mit Expertenwissen, Demonstrationszentren, Best-Practice-Beispielen sowie Netzwerken, die dem Erfahrungsaustausch dienen. Das Bundesministerium für Wirtschaft und Energie (BMWi) ermöglicht die kostenfreie Nutzung aller Angebote von Mittelstand-Digital.

Der DLR Projektträger begleitet im Auftrag des BMWi die Kompetenzzentren fachlich und sorgt für eine bedarfs- und mittelstandsgerechte Umsetzung der Angebote. Das Wissenschaftliche Institut für Infrastruktur und Kommunikationsdienste (WIK) unterstützt mit wissenschaftlicher Begleitung, Vernetzung und Öffentlichkeitsarbeit.

Weitere Informationen finden Sie unter [www.mittelstand-digital.de](http://www.mittelstand-digital.de)

## **IMPRESSUM:**

### **Herausgeber:**

Mittelstand 4.0-Kompetenzzentrum Chemnitz  
Geschäftsstelle  
c/o Technische Universität Chemnitz  
Prof. Dr.-Ing. habil. Ralph Riedel  
DE – 09107 Chemnitz  
Tel: 0371 531 19935  
Fax: 0371 531 819935  
E-Mail: [info@betrieb-machen.de](mailto:info@betrieb-machen.de)  
Web: [www.betrieb-machen.de](http://www.betrieb-machen.de)  
[www.kompetenzzentrum-chemnitz.digital](http://www.kompetenzzentrum-chemnitz.digital)

### **Redaktion & Gestaltung**

Prof. Dr. Dagmar Gesmann-Nuissl, Stefanie Meyer &  
Anikó Lessi

### **Bildnachweis Titel:**

© Rishabh Varshney auf Unsplash