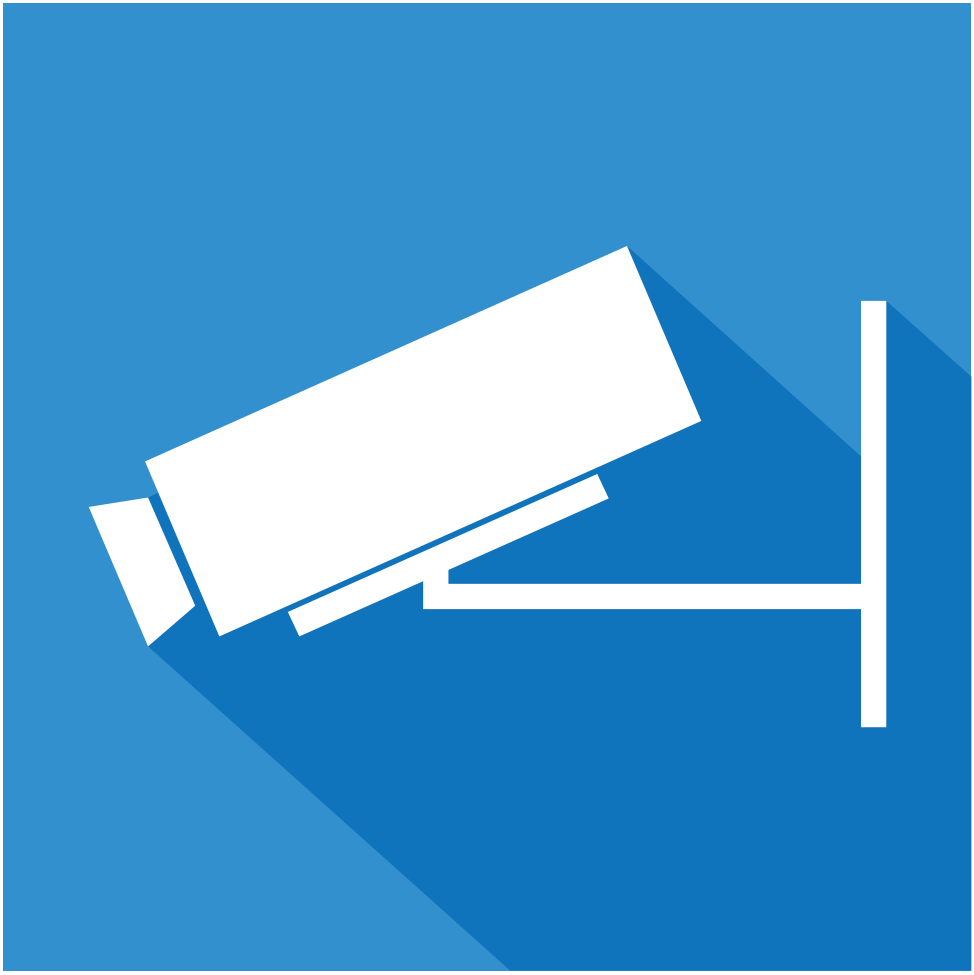

Videoüberwachung

PRIVACYXPERTS

Inhaltsverzeichnis

Fragen zur Videoüberwachung? So können Sie antworten 1

Videoüberwachung nach BDSG? So prüfen Sie richtig 5

Videoüberwachung per Betriebsvereinbarung regeln? So geht es richtig 8

Kein Hexenwerk: So gelingt der Hinweis auf Videoüberwachung 13

Fehler bei der Videoüberwachung: Vermeiden Sie die Top Ten der Stolperfallen 18

Fragen zur Videoüberwachung? So können Sie antworten

In vielen Unternehmen kommt sie zum Einsatz – die Videoüberwachung. Die Interessen und Gründe für einen Einsatz sind verschieden. Häufig will man das Eigentum schützen oder das Hausrecht absichern. Auch wenn die Technik immer einfacher wird, bleiben die datenschutzrechtlichen Rahmenbedingungen komplex. Zwangsläufig kommen viele Fragen auf. So können Sie darauf antworten:

Wo ist die Videoüberwachung geregelt?

Wenn Sie in die Datenschutz-Grundverordnung (DSGVO) schauen, stellen Sie schnell fest, dass Sie dort keine Regelung zum Thema Videoüberwachung finden. Dass dazu nichts ausdrücklich geregelt ist, heißt jedoch nicht, dass die Regelungen der DSGVO nicht gelten. Bei der Videoüberwachung handelt es sich um eine Verarbeitung wie jede andere, für die etwa

- eine Rechtsgrundlage nötig ist (Art. 6 DSGVO),
- die Grundprinzipien der Verarbeitung personenbezogener Daten eingehalten werden müssen (Art. 5 DSGVO),
- risikoangemessene Schutzmaßnahmen zu ergreifen sind (Art. 32 DSGVO),
- Betroffenenrechte umgesetzt werden müssen (Art. 12 ff. DSGVO).

Allerdings finden Sie in Deutschland im Bundesdatenschutzgesetz (BDSG) eine spezifische Regelung zur Videoüberwachung, und zwar in § 4 BDSG. Ob eine solche Regelung außerhalb der DSGVO überhaupt zulässig ist, ist umstritten. Bei der DSGVO handelt es sich um eine europäische Verordnung. Spezifische Datenschutzregelungen sind eigentlich nur dann zulässig, wenn die DSGVO dies erlaubt. Und genau hierüber streiten die Geister. Der deutsche Gesetzgeber sah eine solche Erlaubnis und schuf eine spezifische Regelung zur Videoüberwachung in § 4 BDSG. Juristen und Aufsichtsbehörden sehen jedoch keine Erlaubnis in der DSGVO und halten die deutschen Regeln zur Videoüberwachung für unzulässig. Sie raten zur Orientierung an der DSGVO.

§ Bundesgericht orientiert sich an der DSGVO

Dass es keine Erlaubnis für eine deutsche Videoüberwachungs-Regelung gibt, vertrat beispielsweise auch das Bundesverwaltungsgericht (Urteil vom 27.3.2019, Az. 6 C 2.18). Hier erwähnte das Gericht eher nebenbei, dass die Öffnungsklauseln des Art. 6 Abs. 2 und 3 DSGVO die Videoüberwachung durch nicht öffentliche Stellen (z. B. Unternehmen) nicht erfassen. Insofern sieht das Gericht keine Möglichkeit, § 4 Abs. 1 BDSG anzuwenden, der die Zwecke einer zulässigen Videoüberwachung regelt. Allerdings müssen Sie ebenso in diesem Fall wissen: Auch das Gericht vertritt hier nur eine Rechtsauffassung. Für die Interpretation der Regelungen der DSGVO und damit auch der Frage, ob Videoüberwachung im nationalen Gesetz geregelt werden kann, ist nur der Europäische Gerichtshof (EuGH) zuständig. Ggf. wäre die deutsche Regelung zulässig. Außerdem: Solange es sich um ein geltendes deutsches Gesetz handelt, darf Ihr Unternehmen sich auf dessen Rechtskonformität verlassen und berufen. Ihr Unternehmen ist kein Ersatz-EuGH.

Welche Rechtsgrundlage in der DSGVO ist die richtige bei Videoüberwachung?

Orientieren Sie sich an der Auffassung, dass lediglich die Regelungen der DSGVO gelten, kann das BDSG dennoch eine Rolle spielen. Das ist der Fall, wenn im Zusammenhang mit der Videoüberwachung Beschäftigtendaten verarbeitet werden. Dann müssen Sie $ 26 BDSG berücksichtigen.

Rechtsgrundlagen: Typische Szenarien für eine Videoüberwachung

- **Videoüberwachung im öffentlich zugänglichen Raum:** Ihr Unternehmen will den Besucherparkplatz oder einen Kassenautomaten überwachen, weil es zu Diebstählen kam.→ Rechtsgrundlage ist Art. 6 Abs. 1 Buchst. f DSGVO.
- **Videoüberwachung im nicht öffentlich zugänglichen Raum:** Soll beispielsweise das Betriebsgelände oder der Mitarbeiterparkplatz überwacht werden und sind Beschäftigte die Betroffenen, orientiert sich die rechtliche Zulässigkeit in erster Linie an § 26 Abs. 1 Satz 1 BDSG. Auch Betriebsvereinbarungen können Rechtsgrundlagen sein, wenn sie den Anforderungen aus Art. 88 Abs. 2 DSGVO entsprechen. Alternativ kann auch Art. 6 Abs. 1 Buchst. f DSGVO herangezogen werden, wenn die Videoüberwachung nicht für Zwecke des Beschäftigungsverhältnisses durchgeführt wird.

- **Videoüberwachung zur Aufdeckung von Straftaten durch Mitarbeiter:** Es kommt zu Diebstählen im Lager. Als letzte verbliebene Möglichkeit soll (heimliche) Videoüberwachung zum Einsatz kommen. → Rechtsgrundlage ist § 26 Abs. 1 Satz 2 BDSG. Zur Aufdeckung schwerer Pflichtverletzungen ist § 26 Abs. 1 Satz 1 BDSG die passende Rechtsgrundlage. Allerdings muss man sich auch hier an den hohen Anforderungen des § 26 Abs. 1 Satz 2 BDSG orientieren.
- **Videoüberwachung aus Sicherheitsgründen:** Das Unternehmen überwacht etwa aus Arbeitssicherheitsgründen gefährliche Arbeitsbereiche per Video, damit es bei Vorfällen schnell eingreifen kann. → Rechtsgrundlage bei Beschäftigten ist § 26 Abs. 1 Satz 1 BDSG; bei der Überwachung öffentlich zugänglicher Bereiche, z. B. Schrankenanlage der Betriebseisenbahn, ist dies Art. 6 Abs. 1 Buchst f DSGVO.

Kann man die Videoüberwachung auch auf die Einwilligung der Betroffenen stützen?

Zwar gelten alle Rechtsgrundlagen als gleichwertig, sodass man auch an die Einwilligung denken könnte. Doch diesen Ansatz sollten Sie am besten überhaupt nicht in Betracht ziehen. Denn es gibt gleich mehrere Haken. Nachfolgende Anforderungen lassen sich kaum umsetzen:

Die Einwilligung
- muss klar umrissen sein. Der Betroffene muss die Rahmenbedingungen kennen, damit er in Kenntnis der Sachlage für den konkreten Fall die Zustimmung erklärt.
- muss aktiv durch bestätigendes Handeln erklärt werden. Es reicht insbesondere nicht aus, dass man das Betreten eines überwachten Bereichs als Einwilligung wertet.
- ist ohne Wenn und Aber widerruflich. Wird die Einwilligung widerrufen, entfällt die Rechtsgrundlage für die Zukunft. Die verarbeiteten Daten müssten gelöscht werden.

Worauf ist zu achten, wenn Kameraattrappen zum Einsatz kommen?

Handelt es sich um Kameraattrappen, die zur Abschreckung eingesetzt werden, sind DSGVO und BDSG generell nicht anwendbar. Der Grund: Es kann rein praktisch keine Verarbeitung personenbezogener Daten stattfinden.

Schließlich fehlt es an der entsprechenden Technik. Allerdings haben Sie insbesondere im betrieblichen Umfeld oder bei Kameraausrichtung auf Nachbargrundstücke das Problem zu lösen, dass auch durch eine Kameraattrappe ein Überwachungsdruck bei den betroffenen Beschäftigten oder sonstigen Betroffenen erzeugt werden kann. Schließlich sieht man in der Regel der Kamera(attrappe) nicht an, ob diese funktionsfähig ist oder nicht. Im Zweifel können Betroffene annehmen, dass sie dauerhaft überwacht werden, was in letzter Konsequenz unverhältnismäßig und insgesamt unzulässig wäre. Raten Sie davon ab, Kameras entsprechend auszurichten.

Wonach bemisst sich die Aufzeichnungsdauer einer Videoüberwachung?

Generell können Sie sich an zwei datenschutzrechtlichen Anforderungen orientieren und damit eine individuelle Dauer festlegen:

- Einerseits gilt das Grundprinzip der Datenminimierung (Art. 5 Abs. 1 Buchst. c DSGVO), sprich, eine Verarbeitung muss im Hinblick auf den Zweck angemessen, erheblich sowie auf das notwendige Maß beschränkt sein. Das gilt auch für die Dauer der Aufzeichnung bzw. für die Aufbewahrung von aufgezeichnetem Bildmaterial.
- Andererseits gilt die Pflicht zur Löschung: Nach Art. 17 Abs. 1 Buchst. a DSGVO sind personenbezogene Daten zu löschen, wenn sie für die Zwekke nicht mehr notwendig sind, für die sie erhoben oder auf sonstige Weise verarbeitet wurden.

„Firma zu“ ist kein Argument

Heutzutage lassen sich Videoüberwachungsanlagen mit der entsprechenden Software sehr genau steuern. Generelle mehrwöchige Aufzeichnungsdauern lassen sich daher kaum noch rechtfertigen. Auch das Argument „Wir müssen länger speichern, weil die Firma über Weihnachten geschlossen ist“, zieht kaum noch. Schließlich kann auch nur für diesen beschränkten Zeitraum die Speicherfrist verlängert werden. Im Rest des Jahres reichen ggf. auch 72 Stunden.

Videoüberwachung nach BDSG? So prüfen Sie richtig

Auch wenn einzelne Gerichte und Datenschutzaufsichtsbehörden die deutsche Regelung zur Videoüberwachung für nicht anwendbar halten, man kann auch das Gegenteil vertreten: Es handelt sich um eine gesetzliche Regelung, die vom Bundestag beschlossen und nach juristischer Prüfung durch den Bundespräsidenten in Kraft getreten ist. Ihr Unternehmen kann sich daran orientieren.

Als Datenschutzbeauftragter können Sie selbstverständlich Ihre eigene Auffassung vertreten und § 4 Bundesdatenschutzgesetz (BDSG) aufgrund der in der Datenschutz-Grundverordnung (DSGVO) fehlenden Öffnungsklausel für nicht anwendbar halten. Schließlich sind Sie in der Ausübung Ihrer Aufgaben weisungsfrei (Art. 38 Abs. 3 Satz 1 DSGVO). Halten Ihre Unternehmensleitung und Sie die Regelung für anwendbar, können Sie für Ihre Beratung folgende Checkliste einsetzen:

CHECKLISTE: Videoüberwachung nach § 4 BDSG		
Schwerpunkte	**Geprüft?**	
Liegt eine umfassende Dokumentation der eingesetzten Technik vor? Eine Dokumentation ist ein Muss, denn nur so können Sie eine konkrete Prüfung vornehmen. Achten Sie hier auch darauf, dass ebenfalls beschrieben ist, welche Kameratypen (z. B. fest installiert, Dome-Kamera, mit Zoomfunktion) zum Einsatz kommen und wie bzw. wo die Daten gespeichert werden sollen. Denken Sie auch an Erfassungsbereiche.	❑ ja	❑ nein
Ist der Zweck der Videoüberwachung festgelegt und handelt es sich um einen der in § 4 Abs. 1 BDSG genannten zulässigen Zwecke, für deren Erreichung die Videoüberwachung erforderlich ist? Als zulässige Zwecke sind in § 4 Abs. 1 BDSG erwähnt: • zur Aufgabenerfüllung öffentlicher Stellen, • zur Wahrnehmung des Hausrechts oder • zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke.	❑ ja	❑ nein

CHECKLISTE: Videoüberwachung nach § 4 BDSG		
Schwerpunkte	**Geprüft?**	
Handelt es sich um einen in § 4 Abs. 1 Satz 2 BDSG privilegierten Bereich, bei welchem der Schutz von Leben, Gesundheit oder Freiheit als ein besonders wichtiges Interesse in der Abwägung zu berücksichtigen ist? Das sind: • öffentlich zugängliche großflächige Anlagen, wie insbesondere Sport-, Versammlungsund Vergnügungsstätten, Einkaufszentren oder Parkplätze, oder • Fahrzeuge und öffentlich zugängliche großflächige Einrichtungen des öffentlichen Schienen-, Schiffsund Busverkehrs.	❑ ja	❑ nein
Bestehen keine Anhaltspunkte, dass schutzwürdige Interessen der Betroffenen überwiegen? Als Interesse der Betroffenen kommt beispielsweise in Betracht, nicht Objekt einer Überwachung werden zu wollen. Dies insbesondere, wenn etwa der öffentliche Raum oder das Nachbargrundstück durch die Videoüberwachung erfasst werden soll. Bei einem privilegierten Bereich müssen Sie den Schutz von Leben, Gesundheit oder Freiheit als ein besonders wichtiges Interesse in Ihre Abwägung einfließen lassen. Dementsprechend kann die Interessenabwägung eher zugunsten des verfolgten Interesses ausfallen.	❑ ja	❑ nein
Ist für Betroffene frühestmöglich erkennbar, dass ein Bereich videoüberwacht ist und wer dies verantwortet? Idealerweise gibt es gut erkennbar angebrachte Hinweisschilder, beispielsweise das Video-Infozeichen nach DIN 33450. Außerdem muss für den Betroffenen erkennbar sein, wer für die Videoüberwachung verantwortlich ist. § 4 Abs. 2 BDSG schreibt mindestens den Namen und die Kontaktdaten des Verantwortlichen vor. Alternativ können Sie auf ein Muster der Datenschutzaufsichtsbehörden zurückgreifen.	❑ ja	❑ nein
Ist eine Verarbeitung (z. B. Erfassung, Speicherung, Aufzeichnung, Nutzung) der Bilddaten für die Erreichung des Zwecks erforderlich? Prüfen Sie insbesondere, ob die Aufzeichnung erforderlich ist, um den Zweck zu erreichen. Bei den nach § 4 Abs. 1 Satz 2 BDSG privilegierten Bereichen ist die Gewichtung der Schutzgüter Leben, Gesundheit oder Freiheit zu berücksichtigen. Die Verwendung für einen anderen Zweck ist nur zulässig, wenn dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist (§ 4 Abs. 3 Satz 3 BDSG).	❑ ja	❑ nein

CHECKLISTE: Videoüberwachung nach § 4 BDSG		
Schwerpunkte	**Geprüft?**	
Gibt es im Zusammenhang mit der Verwendung der Bilddaten Anhaltspunkte, die das schutzwürdige Interesse der Betroffenen überwiegen lassen? Auch im Zusammenhang mit der Aufzeichnung des Bildmaterials ist eine Interessenabwägung notwendig. Geht es um eine Videoaufzeichnung von nach § 4 Abs. 1 Satz 2 BDSG privilegierten Bereichen, müssen Sie den Schutz von Leben, Gesundheit oder Freiheit der sich in den Bereichen aufhaltenden Personen als ein besonders wichtiges Interesse in Ihrer Abwägung berücksichtigen.	❑ ja	❑ nein
Wann werden die Daten gelöscht? Prüfen Sie, ob die allgemeinen Vorgaben zur Löschung aus Art. 17 DSGVO umgesetzt sind. Beachten Sie außerdem § 4 Abs. 5 BDSG. Danach müssen die Daten unverzüglich gelöscht werden, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen. Will man eine längerfristige Datenspeicherung vornehmen, sollten Sie deutlich machen, dass dies auch mit datenschutzrechtlichen Grundprinzipien unvereinbar ist. Verstößt Ihr Unternehmen gegen das Gebot der Datenminimierung (Art. 5 Abs. 1 Buchst. c DSGVO), kann auch das zu einem Bußgeld führen.	❑ ja	❑ nein

Videoüberwachung per Betriebsvereinbarung regeln? So geht es richtig

Geht es um Videoüberwachung, ist vielen Unternehmen klar: Das geht nur mit der Zustimmung des Betriebsrats, und eine Betriebsvereinbarung muss her. Doch einfach nur einige Punkte zusammenschreiben ist keine gute Idee, gerade in datenschutzrechtlicher Hinsicht.

Bei alten Betriebsvereinbarungen heißt es Vorsicht! Auch wenn die Datenschutz-Grundverordnung (DSGVO) schon eine gefühlte halbe Ewigkeit gilt, ist manches noch nicht angekommen. So z. B. dass bei Betriebsvereinbarungen besondere Regeln gelten, wenn sie eine Rechtsgrundlage darstellen sollen. Die Betriebsvereinbarung kann die Erlaubnis für die Videoüberwachung schaffen. Allerdings müssen insbesondere die Mindeststandards aus Art. 88 Abs. 2 DSGVO eingehalten werden. So müssen angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Personen ergriffen sein. Ferner muss die Transparenz der Verarbeitung sichergestellt werden. Außerdem müssen die Maßnahmen auch hinsichtlich einer Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe und eventueller Überwachungssysteme am Arbeitsplatz angemessen sein.

Beachten Sie die üblichen Standards

Art. 88 Abs. 2 DSGVO beachten reicht so nicht. Es sind auch weitere Aspekte zu berücksichtigen, die bei allen Verarbeitungen personenbezogener Daten gelten. Denken Sie an:

- Grundsätze der Verarbeitung personenbezogener Daten (Art. 5 DSGVO)
- Umsetzung der Informationspflichten nach Art. 13 DSGVO
- risikoangemessene technische und organisatorische Schutzmaßnahmen (Art. 32 DSGVO)

Beraten Sie nur im Datenschutz

Wird Ihnen ein Entwurf einer Betriebsvereinbarung vorgelegt, sollten Sie ausschließlich unter Datenschutzaspekten beraten. Dabei können Sie sich an der folgenden Checkliste orientieren:

CHECKLISTE: Regelungsinhalte Betriebsvereinbarung Videoüberwachung			
Ihre Aufgabe	**Hinweise**	**Umgesetzt?**	
Ist definiert, für wen die Betriebsvereinbarung gelten soll?	Prüfen Sie unbedingt den Geltungsbereich und schauen Sie genau hin. Grundsätzlich ist zu überlegen, für wen die Betriebsvereinbarung gelten soll – in räumlicher (z. B. auf einen bestimmten Betrieb beschränkt) wie personeller Hinsicht (z. B. nur Mitarbeiter in der Produktion). Ist hier ungenau formuliert, fehlt für einen Teil der betroffenen Arbeitnehmer eventuell die erforderliche Rechtsgrundlage.	❑ ja	❑ nein
Geht klar aus der Betriebsvereinbarung hervor, dass diese eine Erlaubnis (Rechtsgrundlage) zur Videoüberwachung schaffen soll?	Empfehlen Sie, dass eine entsprechende Aussage enthalten ist. Das dient insbesondere dazu, Transparenz zu schaffen. Jeder Leser weiß damit sofort, was Ziel dieser Betriebsvereinbarung ist.	❑ ja	❑ nein
Sind die mit der Vereinbarung bzw. Videoüberwachung verfolgten Zwecke klar beschrieben?	Den oder die Zwecke konkret festzulegen ist von besonderer Bedeutung. Dies ist nicht nur für Sie wichtig, damit Sie etwa prüfen können, ob eine Videoüberwachung in einem bestimmten Umfang geeignet, erforderlich und angemessen, sprich: verhältnismäßig ist. Konkrete Zwecke dienen auch der Transparenz gegenüber den betroffenen Mitarbeitern. Sind Ziele zu allgemein formuliert, kann auch dies dazu führen, dass die Unternehmensleitung sich nicht auf die Betriebsvereinbarung als Rechtsgrundlage berufen kann.	❑ ja	❑ nein

CHECKLISTE: Regelungsinhalte Betriebsvereinbarung Videoüberwachung			
Ihre Aufgabe	**Hinweise**	**Umgesetzt?**	
Werden die zu verarbeitenden personenbezogenen Daten konkret aufgeführt?	Eine konkrete Beschreibung, welche personenbezogenen Daten verarbeitet werden, ist unerlässlich. Einfach nur von „Bilddaten" sprechen reicht unter Umständen nicht aus. Besser kann es sein, die Bilddaten in einen Zusammenhang zu stellen, etwa „Bilddaten vom Mitarbeiterparkplatz". Das lässt auch später weniger Interpretationsspielraum zu. Und außerdem werden Transparenz und Verständlichkeit gefördert.	❑ ja	❑ nein
Hat man die eingesetzten Systeme, Verarbeitungen und Prozesse beschrieben? Wie steht es um Technik und Kamerastandorte?	Nur von „Videoüberwachungsanlage" zu sprechen, wäre falsch. Machen Sie klar, dass das konkret formuliert werden muss. Die eingesetzten IT-Systeme und Datenverarbeitungsverfahren oder -prozesse müssen beschrieben sein. Auch etwa Kamerastandorte und Erfassungsbereiche. Denkbar ist, dies in die Betriebsvereinbarung selbst aufzunehmen. Unter Umständen ist es jedoch besser, wenn dies in eine Anlage zur Betriebsvereinbarung ausgelagert wird. So können Ergänzungen oder Aktualisierungen einfacher vorgenommen werden.	❑ ja	❑ nein
Ist die Sicherheit der Datenverarbeitung gewährleistet?	Art. 32 DSGVO darf nicht unter den Tisch fallen. Achten Sie darauf, dass ergriffene Schutzmaßnahmen beschrieben sind. Zwar müssen nicht alle Details offengelegt werden, allerdings muss erkennbar werden, wie ein angemessenes Schutzniveau erreicht wird. Denken Sie hier insbesondere an die Unterbringung der Speichertechnik der Videoüberwachungsanlage, etwa im Serverraum.	❑ ja	❑ nein
Gibt es Festlegungen zur Leistungsund Verhaltenskontrolle?	Gerade bei Videoüberwachung kann dies ein Problem sein: Häufig wird in Betriebsvereinbarungen jede Form der Leistungsund Verhaltenskontrolle ausgeschlossen. Hinterfragen Sie, ob man wirklich alles ausschließen will. Unter Umständen können dann interne Ermittlungen oder eine Datennutzung für andere legitime und zulässige Zwecke nicht mehr stattfinden.	❑ ja	❑ nein

CHECKLISTE: Regelungsinhalte Betriebsvereinbarung Videoüberwachung			
Ihre Aufgabe	**Hinweise**	**Umgesetzt?**	
Sind Berechtigungen oder Rollen konkret definiert?	Bestehen Sie auf konkrete Festlegungen dazu, wer wann auf welche (Bild-)Daten zugreifen darf. Genauso wichtig ist, wer dazu berechtigt ist, mit den Daten zu arbeiten oder diese auszuwerten. Gerade bei Auswertungen lohnt es sich, konkret zu werden. Häufig sind Auswertungen Grund für spätere Auseinandersetzungen zwischen Arbeitgeber, Mitarbeiter oder Betriebsrat.	❑ ja	❑ nein
Ist festgelegt, welche Befugnisse der Betriebsrat hat?	Auch der Betriebsrat darf mit personenbezogenen Daten nicht umgehen, wie es ihm beliebt. Daher ist es wichtig, dass die Beteiligten etwa die Rechte des Betriebsrats (z. B. zur Kontrolle, Einsicht, Auswertung) konkret festlegen.	❑ ja	❑ nein
Werden datenschutzrechtliche Grundprinzipien umgesetzt?	Prüfen Sie im Zusammenhang mit einer Betriebsvereinbarung stets, ob die in Art. 5 DSGVO enthaltenen Datenschutzgrundprinzipien eingehalten sind. Zweckbindung, Datenminimierung, Speicherbegrenzung und Vertraulichkeit spielen im Zusammenhang mit Betriebsvereinbarungen zur Videoüberwachung eine ganz besondere Rolle.	❑ ja	❑ nein
Wird den Informationspflichten aus Art. 13 DSGVO entsprochen?	Transparenz ist oberstes Gebot. Klar ist, dass die Videoüberwachung erkennbar sein muss, beispielsweise auch durch Hinweisschilder. Aber: Prüfen Sie auch, ob die notwendigen Informationen in der Betriebsvereinbarung oder auf andere geeignete Weise (z. B. Anlage zur Betriebsvereinbarung, Informationen im Intranet) gegeben werden.	❑ ja	❑ nein
Gibt es Festlegungen zur Aufbewahrung und Löschung von Daten?	Wichtig ist, dass es Vorgaben darüber gibt, wann personenbezogene Daten gelöscht werden müssen. Hinterfragen Sie stets, ob man sich wirklich auf das erforderliche Maß beschränkt. Hierzu sollten Sie sich am Zweck bzw. am verfolgten berechtigten Interesse orientieren.	❑ ja	❑ nein

CHECKLISTE: Regelungsinhalte Betriebsvereinbarung Videoüberwachung			
Ihre Aufgabe	**Hinweise**	**Umgesetzt?**	
Ist beschrieben, ob Dienstleister eingeschaltet bzw. ob Daten an Dritte weitergegeben werden dürfen?	Auch bei Videoüberwachung gibt es inzwischen Cloud-Lösungen. Es ist Verhandlungssache zwischen Arbeitgeber und Betriebsrat, ob das Unternehmen entsprechende Anbieter bzw. Dienstleister einbinden darf. Unter Umständen muss das Unternehmen weitergehende Vereinbarungen schließen, beispielsweise zur Auftragsverarbeitung (Art. 28 DSGVO) oder zum Transfer in Drittstaaten (z. B. USA) auf Basis sogenannter Standarddatenschutzklauseln (Art. 46 Abs. 2 Buchst. c DSGVO).	❑ ja	❑ nein
Wird dem betroffenen Mitarbeiter klar, wie er seine Rechte geltend machen kann?	Testen Sie beim Lesen selbst: Wird Ihnen klar, welche Rechte Sie haben und wie Sie etwa Ihre Rechte auf Auskunft oder Löschung geltend machen können?	❑ ja	❑ nein
Genügt die Betriebsvereinbarung insgesamt den Anforderungen aus Art. 88 Abs. 2 DSGVO?	Werfen Sie abschließend einen Blick auf die Anforderung aus Art. 88 Abs. 2 DSGVO: Lässt sich insgesamt sagen, dass angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Personen ergriffen sind? Ist insbesondere die Transparenz der Verarbeitung gegeben? Sind die Maßnahmen auch hinsichtlich einer Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe und eventueller Überwachungssysteme am Arbeitsplatz angemessen?	❑ ja	❑ nein
Wird mit der Betriebsvereinbarung nicht der Mindeststandard der DSGVO abgesenkt?	Die DSGVO gibt die Basis für den Datenschutz vor. Die enthaltenen Standards darf Ihr Unternehmen nicht unterschreiten. Betrachten Sie in diesem Zusammenhang unbedingt die Grundsätze zur Verarbeitung personenbezogener Daten aus Art. 5 DSGVO. Diese gelten für jede Verarbeitung personenbezogener Daten, gerade auch für die Videoüberwachung.	❑ ja	❑ nein

Kein Hexenwerk: So gelingt der Hinweis auf Videoüberwachung

Ein zentraler Regelungsaspekt der Datenschutz-Grundverordnung (DSGVO) ist Transparenz. Betroffene sollen jederzeit und insbesondere vor Beginn einer Verarbeitung personenbezogener Daten wissen können, welche Daten erfasst werden und was mit diesen passiert. Bei der Videoüberwachung ist das nicht anders. Setzen Sie auf folgende Tipps:

Tipp 1: Mehrstufige Information wohl am besten

Werfen Sie einen Blick in Art. 13 DSGVO, merken Sie in Zusammenhang mit Videoüberwachung schnell: Wenn man alle Informationen geben wollte, die Art. 13 DSGVO vorsieht, müsste das Informationsschild geradezu riesig ausfallen, wenn auf dem Schild noch irgendetwas lesbar sein soll. Dass riesige Hinweisschilder schlichtweg nicht praktikabel sind, ist auch den Datenschutzaufsichtsbehörden nicht entgangen.

Daher kann Ihr Unternehmen auch mehrstufig vorgehen: Beispielsweise an der Zufahrt zum Unternehmen gibt es einen Ersthinweis, sprich: in der ersten Stufe. Dieser umfasst natürlich den Hinweis auf die Videoüberwachung, beispielsweise durch ein Piktogramm, welches sich an der DIN 33450 (Video-Infozeichen) orientiert. Dazu gibt es noch einige Basisinformationen zur Transparenz (siehe Beispiel rechts), insbesondere

- zum Verantwortlichen,
- zum Datenschutzbeauftragten,
- zum Zweck,
- zur Rechtsgrundlage,
- zur Speicherdauer.

Der Betroffene kann auch ausführliche Informationen mit allen Angaben nach Art. 13 DSGVO erhalten, sprich: umfassende Informationen in der zweiten Stufe. Diese werden beispielsweise am Empfang als Aushang oder im Internet vorgehalten. Auch kann der Betroffene die vollständigen Informationen etwa per E-Mail anfordern.

Denken Sie auch an moderne Möglichkeiten

So kann auf dem Ersthinweis auch ein Kurzlink oder QR-Code angebracht werden, der zu einer ausführlichen Information auf der Webseite des Unternehmens führt. Das hat den Vorteil, dass sich der Betroffene mit dem Smartphone direkt vor Ort ausführlich informieren kann. QR-Codes lassen sich kostenlos im Internet erzeugen. Suchen Sie einfach nach „QR- Code-Generator“.

Tipp 2: Orientieren Sie sich an den Empfehlungen der Aufsichtsbehörden

Auch wenn es eigentlich viel gestalterische Freiheit gibt, unter Umständen will Ihr Unternehmen auf jeden Fall auf der sicheren Seite sein. Das geht einfacher, als Sie denken. Schauen Sie auf die Webseite der für Ihr Unternehmen zuständigen Datenschutzaufsichtsbehörde. Dort finden Sie in der Regel auch Informationen zum Thema Videoüberwachung und wahrscheinlich auch ein Muster.

Sie müssen kein Künstler sein

Bei manchen Aufsichtsbehörden finden Sie das rechts abge- bildete Hinweisschild als Beispiel zur Orientierung. Gibt es das Muster nur als PDF, schauen Sie beispielsweise auf die Seite der Aufsichtsbehörde in Niedersachsen. Unter folgendem Link finden Sie dort auch bearbeitbare Word-Dateien: https://www.lfd.niedersachsen.de/startseite/dsgvo/transparenzanforderungen-und-hinweisbeschilderung-bei-einer-videoueberwachung-nach-der-ds-gvo-158959.html.

Tipp 3: Sprechen Sie mit den zuständigen Personen

Wenn es um den Hinweis auf Videoüberwachung geht, sollten Sie nicht einfach festlegen, wie die Sache umzusetzen ist. Besser ist es, wenn Sie mit den zuständigen Stellen im Unternehmen sprechen. Das kann beispielsweise die Unternehmenssicherheit oder das Facility Management sein. Ferner sollten Sie sich mit der Unternehmensleitung abstimmen. Schließlich kann ein Hinweis auf Videoüberwachung auf verschiedene Weise erfolgen. Der Gestaltung sind kaum Grenzen gesetzt, soweit den Anforderungen aus Art. 13 DSGVO (bzw. § 4 Abs. 2 Bundesdatenschutzgesetz)

entsprochen und für Transparenz gesorgt wird. Insofern ist es auch nicht zwingend, dass es ein Kamerasymbol gibt. Auch ein „Achtung, Videoüberwachung!“ in großer Schrift kann ins Auge stechen.

Tipp 4: Zutreffende und vollständige Inhalte sind ein Muss

Steht das Design fest, sollten Sie zusehen, dass die Inhalte passen.Achten Sie insbesondere darauf, dass die zu machenden Angaben richtig und vollständig sind. Außerdem: Betrachten Sie die Informationen immer aus der Sicht eines Betroffenen und fragen Sie sich: Sind die Informationen inhaltlich verständlich? Dabei ist wichtig: Gehen Sie gerade bei der mehrstufigen Information in der ersten Stufe nicht zu sehr ins Detail. Denn dann kann bei gleicher Hinweisgröße die Schrift größer ausfallen.

Tipp 5: Achten Sie auf Erkennbarkeit und Lesbarkeit

Ganz wichtig ist: Der Betroffene muss frühestmöglich erkennen können, dass er sich vor einem Bereich mit Videoüberwachung befindet. Erkennt er das erst, wenn er sich schon im videoüberwachten Bereich befindet, ist es zu spät. Dann hat er nämlich nicht mehr die Möglichkeit, sich gegen eine Videoüberwachung zu entscheiden und den überwachten Bereich nicht zu betreten. Daher gilt: Der Hinweis muss so groß sein, dass er auch aus einiger Entfernung ins Auge fällt und die Inhalte lesbar sind. Apropos „ins Auge fallen“: Der Hinweis darf nicht irgendwo versteckt werden. Er muss leicht sichtbar angebracht werden, beispielsweise in Augenhöhe. Auch darf er sich nicht auf Türen befinden, sodass er nicht mehr sichtbar ist, wenn sich diese öffnen.

Tipp 6: Machen Sie die Probe aufs Exempel

Auch wenn vieles besprochen und abgestimmt wurde, beispielsweise zu Design, Inhalten und Anbringungsorten, sollten Sie ein Auge auf die tatsächliche Umsetzung haben. Möglicherweise sehen die Hinweisschilder doch etwas anders aus. Achten Sie gerade auch auf Art, Größe und Farbe der ausgewählten Schrift. Ab und an gibt es hier große Überraschungen, und das Schild ist schon aus kurzer Distanz nicht mehr lesbar. Außerdem: Manchmal werden fertige Schilder doch nicht oder an der falschen Stelle angebracht. Daher: Lassen Sie sich die Fertigstellung bestätigen und schauen Sie, wie die Umsetzung erfolgt ist.

Tipp 7: Schauen Sie auch später ab und an nach dem Rechten

Einmal sich mit dem Thema Information rund um die Videoüberwachung beschäftigen und dann das Thema vergessen, das geht nicht. Setzen Sie sich selbst Termine im Kalender, an denen Sie schauen, ob noch alles passt. So können Sie auch Ihrem Kontrollauftrag als Datenschutzbeauftragter aus Art. 39 Abs. 1 Buchst. b DSGVO nachkommen. Denn: Dass noch alles passt, ist keine Selbstverständlichkeit. So können sich Informationen zum Verantwortlichen ändern, beispielsweise die Anschrift oder Kontaktmöglichkeiten. Unter Umständen fehlen aus irgendwelchen Gründen angebrachte Schilder oder werden durch Bäume und Sträucher verdeckt. Auch die Sonne kann dafür sorgen, dass Schilder ausbleichen und der Informationspflicht nicht mehr genügt werden kann. Stellen Sie irgendwelche Defizite fest, geben Sie den zuständigen Personen einen Hinweis und bitten Sie, diese zu beheben.

Tipp 8: Die Welt brauchen Sie nicht retten

Auch wenn Sie Vorschläge zur Umsetzung machen und beispielsweise die Empfehlungen von Aufsichtsbehörden berücksichtigen, heißt das nicht automatisch, dass das auch so umgesetzt wird. Unter Umständen kommt es dazu, dass man sagt: „Es gibt schon Piktogramme. Das muss reichen. Basta." Nehmen Sie solche Entscheidungen und Statements nicht persönlich. Beherzigen Sie stets: Sie sind nicht der Retter der Welt. Gerade in schwierigen Zeiten kann die Unternehmensleitung die Prioritäten anders setzen. Machen Sie allerdings stets deutlich, dass die Verantwortung für die Einhaltung der Datenschutzbestimmungen beim Verantwortlichen und damit bei der Unternehmensleitung verbleibt. Und denken Sie an Folgendes: Dokumentieren Sie, dass und wie Sie beraten haben. Dann können Sie im Fall der Fälle belegen, dass Sie eine andere Empfehlung ausgesprochen haben.

So kann ein Ersthinweis zur Videoüberwachung aussehen

Kurz-Informationen gemäß Art. 13 DSGVO zur Videoüberwachung der Max Mustermann GmbH

ACHTUNG
VIDEOÜBERWACHUNG

Weitere Informationen für Sie:
- an unserem Empfang
- per Mail an info@mustermann-abc.xyz
- unter www.mustermann-abc.xyz/video

Name und Kontaktdaten des Verantwortlichen und ggf. seines Vertreters: Max Mustermann GmbH Musterstraße 123, 12345 Musterstadt
Tel. 012345/6789-0, E-Mail: empfang@mustermann-abc.xyz Geschäftsführer: Max Mustermann

Zwecke und Rechtsgrundlage der Datenverarbeitung: Schutz von Personen; Absicherung des Grundstücks, des Betriebsgeländes sowie von Gebäude und Flächen; Wahrnehmung des Hausrechts
Rechtsgrundlage: Art. 6 Abs. 1 Satz 1 Buchst. f DSGVO

Berechtigte Interessen, die verfolgt werden: Schutz vor und Verfolgung von Straftaten, beispielsweise Eigentumsdelikten, Hausfriedensbruch, Sachbeschädigung und Vandalismus; Sicherung von Beweisen

Speicherdauer oder Kriterien für die Festlegung der Dauer: automatische Löschung durch Überschreiben nach 72 Stunden, sofern kein konkreter Anlass zur weitergehenden Speicherung besteht (z. B. zur Verfolgung von Straftaten)

Kontaktdaten des Datenschutzbeauftragten (sofern vorhanden): Max Mustermann GmbH, Datenschutzbeauftragter (Anschrift wie oben) Tel. 012345/6789-0, E-Mail datenschutz@mustermann-abc.xyz

Fehler bei der Videoüberwachung: Vermeiden Sie die Top Ten der Stolperfallen

Stolperfallen gibt es überall, nicht nur im Alltag. Auch im Datenschutzrecht lauern Stolperfallen, die man auf den ersten Blick gar nicht als solche erkennt. Nehmen Sie z. B. das Thema Videoüberwachung: Häufig wird sie geplant, und man meint, alles richtig gemacht zu haben – auch im Datenschutz. Doch bei genauerem Hinsehen wird klar, dass manches im Argen liegt.

Helfen Sie beim Ausmachen und Vermeiden Manchmal erkennt man Stolperfallen erst, nachdem man gestolpert ist. Weiß man jedoch, wo die Stolperfalle ist, kann man ihr aus dem Weg gehen. Damit beim Thema Videoüberwachung die größten Stolperfallen kein Thema in Ihrem Unternehmen sind, können Sie die folgende Checkliste verwenden.

CHECKLISTE: Typische Stolperfallen bei der ideoüberwachung		
Aspekt	**Umgesetzt? Eingehalten?**	
1. Ist die Videoüberwachung dokumentiert? Die schriftliche Dokumentation des Systems, der eingesetzten Technik, der Standorte der Kameras, der verfolgten Zwecke, Berechtigungen und Löschfristen ist unerlässlich. Hier wird der Sollzustand beschrieben, gegen den Sie prüfen können. Auch kann damit der Dokumentationspflicht aus der DSGVO nachgekommen werden. Denken Sie hier auch an das Verzeichnis von Verarbeitungstätigkeiten.	❑ ja	❑ nein
2. Besteht eine Rechtsgrundlage? Ist die Videoüberwachung erforderlich bzw. ist der Verhältnismäßigkeitsgrundsatz gewahrt? Ohne Rechtsgrundlage keine Verarbeitung personenbezogener Daten. Soll die Videoüberwachung auf Art. 6 Abs. 1 Satz 1 Buchst. f DSGVO gestützt werden, muss eine Interessenabwägung stattfinden. Nur ein berechtigtes Interesse haben reicht nicht. Es müssen die Interessen der Betroffenen überwiegen. Dabei spielen Erforderlichkeit und Verhältnismäßigkeit eine wichtige Rolle.	❑ ja	❑ nein

CHECKLISTE: Typische Stolperfallen bei der ideoüberwachung		
Aspekt	**Umgesetzt? Eingehalten?**	
3. Ist die Videoüberwachung auf das eigene Grundstück bzw. eigene Bereiche beschränkt? Grundsätzlich darf Ihr Unternehmen nur innerhalb der eigenen Grundstücksgrenzen überwachen. Geht es nicht anders, darf der überwachte Bereich maximal 1 m über die Grenze hinausgehen.	❑ ja	❑ nein
4. Werden Bereiche, die nicht überwacht werden dürfen, verpixelt oder geschwärzt? Werden Bereiche erfasst, die nicht erfasst werden dürfen, müssen diese ausgeblendet, verpixelt oder geschwärzt werden. Das muss jedoch schon bei der Aufnahme passieren und nicht erst nachträglich. Prüfen Sie den Punkt durch Einsichtnahme ins gelieferte Bildmaterial.	❑ ja	❑ nein
5. Wo und wie werden Betroffene darüber informiert, dass sie sich einem Bereich mit Videoüberwachung nähern? Prüfen Sie selbst, ob Sie rechtzeitig problemlos erkennen können, dass Sie sich auf einen Bereich mit Videoüberwachung zubewegen. Ein Hinweisschild oder Piktogramm reicht in aller Regel nicht aus. Zumindest Basisangaben (z. B. Verantwortlicher, Kontaktdaten, weitere Informationsmöglichkeit) müssen gegeben werden.	❑ ja	❑ nein
6. Wurden für die Festlegung von technischen und organisatorischen Schutzmaßnahmen Risiken ausgemacht und bewertet? Sind Maßnahmen zur Risikobehandlung umgesetzt? Bevor den Anforderungen aus Art. 32 DSGVO entsprochen werden kann, bedarf es einer Risikoanalyse. Prüfen Sie, ob festgelegte Maßnahmen risikoangemessen sind und nicht nur auf dem Papier existieren.	❑ ja	❑ nein
7. Besteht ein Berechtigungskonzept und ist dieses Konzept auch tatsächlich umgesetzt? Vorab muss festgelegt sein, wer für welchen Zweck auf die aufgezeichneten Daten zugreifen darf. Achten Sie hier darauf, dass man sich auf das Erforderliche beschränkt, sprich: das „Need to Know"-Prinzip umsetzt.	❑ ja	❑ nein
8. Wurden Aufzeichnungsdauer und Löschfristen festgelegt und sind diese im System umgesetzt? Auch hier muss dem Grundsatz der Datenminimierung Rechnung getragen werden. Ist die Kenntnis der Daten für den verfolgten Zweck nicht mehr erforderlich, müssen sie gelöscht werden – egal, wie viel Speicherplatz man hat.	❑ ja	❑ nein

CHECKLISTE: Typische Stolperfallen bei der ideoüberwachung		
Aspekt	**Umgesetzt? Eingehalten?**	
9. Sind Festlegungen einer Betriebsvereinbarung umgesetzt? Betriebsvereinbarungen enthalten oft Vorgaben und Verbote. Prüfen Sie, ob diese Festlegungen in der Praxis auch umgesetzt sind. Gehen die Festlegungen über datenschutzrechtliche Anforderungen hinaus, brauchen Sie deren Sinnhaftigkeit nicht bewerten. Das haben Arbeitgeber und Betriebsrat selbst gemacht und die Regelung geschaffen.	❑ ja	❑ nein
10. Findet eine Prüfung statt, wenn Bilddaten für andere Zwecke verwendet werden sollen? Wasfüreinenbestimmten Zweckerhobenwurde,darfnichtfüreinenanderen Zweck verwendet werden. Ausnahmsweise ist das anders, wenn der neue Zweck mit dem ursprünglichen kompatibel ist. Hier muss Art. 6 Abs. 4 DSGVO berücksichtigt und geprüft werden.	❑ ja	❑ nein

© Egor – AdobeStock.com

PRIVACYXPERTS

ein Unternehmensbereich des VNR Verlags für die Deutsche Wirtschaft AG,
Theodor-Heuss-Str. 2–4, 53095 Bonn
Telefon: 02 28/9 55 01 50, Fax: 02 28/3 69 64 80
Internet: www.privacyxperts.de
E-Mail: kundendienst@privacyxperts.de

Vorstand: Richard Rentrop

Verantwortlicher i.S.d.P: Michael Jodda, Theodor-Heuss-Str. 2-4, 53095 Bonn

Autor: Andreas Würtz

Satz: Holger Hellendahl, Neuss

Alle Angaben wurden mit äußerster Sorgfalt ermittelt und überprüft. Sie basieren jedoch auf der Richtigkeit uns erteilter Auskünfte und unterliegen Veränderungen. Eine Gewähr kann deshalb nicht übernommen werden.

© 2020 by VNR Verlag für die Deutsche Wirtschaft AG, Bonn, Bukarest, Manchester, Warschau