

Videoüberwachung vs. Datenschutz

Digitale Absicherung kontra Privatsphäre

Kai-Oliver Detken

Unternehmen nutzen immer häufiger Videoüberwachung, um sich gegen unerwünschte Besucher zu schützen oder den täglichen Betrieb zu dokumentieren. Hierbei werden zum Teil auch Mitarbeiter in ihren Pausen überwacht. Dabei machen sich die wenigsten Unternehmen allerdings Gedanken darüber, ob der Einsatz von Videotechnik auch datenschutzkonform ist. Während man bei der Mitarbeiterüberwachung noch nachvollziehen kann, dass dies nicht der DSGVO entsprechen wird, trifft diese Problematik aber auch auf Kundenbesuche in der Firma zu. Wo und wie kann man also Videotechnik DSGVO-konform betreiben und welche technischen Möglichkeiten gibt es?

Bereiche einer Firma (z.B. das Lager) kontinuierlich per Video zu überwachen, ist der Wunsch vieler Unternehmer, um die eigenen Werte zu schützen. Die kleinen Videokameras sollen dabei vor Einbruch, Diebstahl oder Vandalismus schützen. Und die Umsetzung ist heute denkbar einfach, da einige Videokamerahersteller auf dieses Marktsegment aufgesprungen sind. Neben einer großen Auswahl an Lösungen bleiben dabei auch die Kosten überschaubar. Allerdings wurde sich vor dem Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) im Mai 2018 gar nicht und aktuell noch zu wenig mit dem Datenschutz auseinandergesetzt. Denn man greift mit so einer Überwachungslösung auch in die Privatsphäre der eigenen Mitarbeiter ein und dokumentiert eventuell regelmäßig z.B. deren Pausenverhalten. Kein Unternehmen sollte daher eine Videolösung einführen, ohne die DSGVO-Vorschriften einzubeziehen. Dieses Problem hat allerdings auch der Staat, der öffentliche Plätze aufgrund höherem Straftataufkommens überwachen lassen möchte oder dies bereits tut. Die Frage ist aber auch, wie viel uns die eigene Sicherheit gegenüber der Privatsphäre Wert ist.

Datenschutzvoraussetzung

Der Einsatz von Videosystemen zur Überwachung von öffentlichen Orten ist auch für Unternehmen nicht ohne weiteres gestattet. Die entsprechenden Rechtsvorschriften finden sich in der DSGVO wieder, obwohl diese sich nicht explizit mit der Videoüberwachung befasst. Es hat daher einer Beurteilung anhand der Generalklausel in Artikel 6 (Absatz 1, Seite 1 der DSGVO) zu erfolgen. Danach sind die Erfassung, die Verarbeitung oder die Speicherung personenbezogener Daten nur dann zulässig, wenn sie zur Wahrung der berechtigten Interessen

des Überwachenden oder Dritter erforderlich sind und die Interessen oder Grundrechte der betroffenen Personen nicht überwiegen. Daher müssen sowohl die Interessen des Unternehmens als auch die Interessen der Betroffenen (wie Kunden oder Mitarbeiter) sowie deren Grundrechte ermittelt und gegeneinander abgewogen werden.

Ein Grund für ein Unternehmen kann bestehen, wenn eine Gefahrenlage nachgewiesen werden kann. Beispielsweise lagert ein Unternehmen Wertgegenstände, die vor Einbruch geschützt werden müssen. Daher könnte hier für Abwehrmaßnahmen ein Videoüberwachungssystem installiert und die Videomitschnitte sicher archiviert werden, um ggf. eine Beweissicherung durchführen zu können. Das Verfahren der Videoüberwachung sollte dann aber in das DSGVO-Verzeichnis der Verarbeitungstätigkeit mit aufgenommen werden.

Die DSGVO fordert weiterhin von Unternehmen einen transparenten Umgang mit personenbezogenen Daten. Das heißt, ein Betroffener muss im Nachhinein nachvollziehen können, was im Detail mit seinen Daten geschehen ist. Konkret sind die folgenden Informationspflichten nach Artikel 13 (Absatz 1 und 2 der DSGVO) zu berücksichtigen bzw. darüber aufzuklären:

- Umstand der Beobachtung (Piktogramm, Kamerasymbol);
- Identität des Verantwortlichen (Name mit Kontaktdaten);
- Kontaktdaten des betrieblichen Datenschutzbeauftragten;
- Verarbeitungszweck und Rechtsgrundlage in Schlagworten;
- Angaben des berechtigten Interesses;
- Speicherdauer der Videodaten;
- Hinweis auf Zugang zu den weiteren Pflichtinformationen (z.B. Auskunftsrecht, Beschwerderecht).

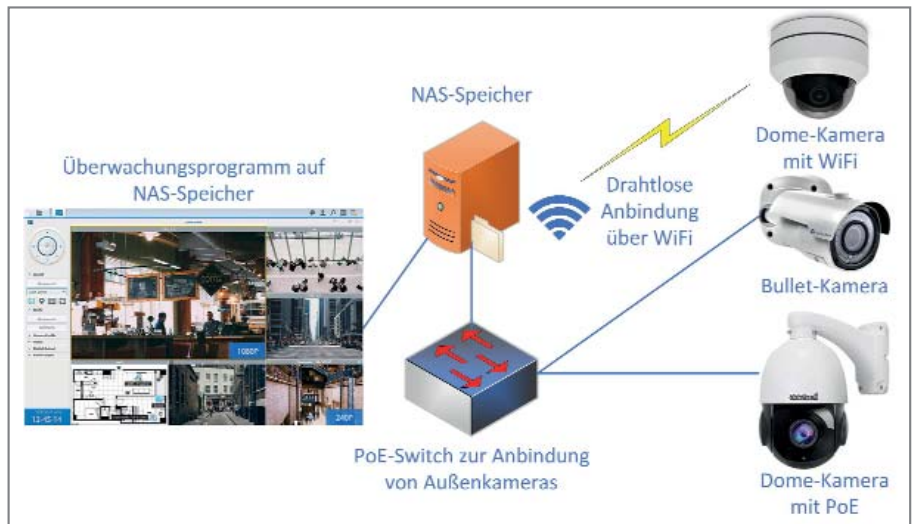
Zusätzlich zum Piktogramm sind diese Informationen am Ort der Videoüberwachung zur Verfügung zu stellen, indem man beispielsweise Informationsblätter auslegt.

Die technische Umsetzung kann unterschiedlich erfolgen und hängt unmittelbar mit der Speicherung zusammen. So kann man zwar Videolösungen ohne Speicherung der Daten nutzen, indem in Echtzeit die Überwachung des Kamerabildes stattfindet. Dies ist meistens aber nicht praktikabel und nur bei Einsatz eines Pförtners umsetzbar. Und selbst bei Unternehmen mit Pförtner findet meistens eine Datenspeicherung statt, da die Videolösung Tag und Nacht in Betrieb sein sollte. Daher muss vor einer Umsetzung überprüft werden, ob eine Datenspeicherung zulässig ist.

Zu unterscheiden sind laut DSGVO folgende Datenverarbeitungsmöglichkeiten:

- **Zulässigkeit der Speicherung:** Die Speicherung der Daten gilt als zulässig, wenn diese notwendig ist und ein konkreter Zweck damit verfolgt wird. Dabei müssen die schutzwürdigen Interessen der betroffenen Personen überwiegen.
- **Dauer der Speicherung:** Es besteht ein Lösungsgebot, d.h., die Videodaten müssen gelöscht werden, sobald man diese nicht mehr benötigt. Dies gilt auch, wenn die schutzwürdigen Interessen des Betroffenen gegen ein weiteres Speichern sprechen.
- **Datenverarbeitung für andere Zwecke:** Die Verarbeitung der Videodaten für andere Zwecke ist nicht gestattet. Ausnahmen sind nur zulässig, wenn die öffentliche oder staatliche Sicherheit gefährdet ist oder Unterstützung bei der Aufklärung von Straftaten geleistet werden kann.

Daraus lässt sich ableiten, dass der Staat in öffentlichen Bereichen zur Absicherung durchaus Videoüberwachungssysteme anbringen darf und diese auch von der Polizei auswerten lassen kann, da es sich dabei um die Aufklärung von Straftaten handelt. Ein Unternehmen hingegen kann nicht ohne weiteres öffentliche Bereiche überwachen oder in relevanten



Einbindung unterschiedlicher IP-Kameras auf zentralem NAS-Speicher

Unternehmensbereichen die Videodaten für andere Zwecke (z.B. Pausenüberwachung der Mitarbeiter) nutzen.

Technische Umsetzung

Die technische Umsetzung kann sehr einfach mit einer Einzelkamera erfolgen, aber auch aus einem komplexen System mit beliebig vielen Kameras und unterschiedlichen Speichermöglichkeiten bestehen. Dabei lassen sich heute Audio-, Video- und Bilddaten erfassen und on Premises oder in der Cloud ablegen. Während anfangs analoge Übertragungssysteme mit Koaxialkabel- oder Zweidrahttechnik verbaut wurden, die es immer noch gibt und angeboten werden, nutzt man heute bei reinen Digitalsystemen die Übertragung via IP. Dadurch kommt es zu keinen Medienbrüchen mehr, da auch die Kameras inzwischen mittels IP angesteuert werden, und die Daten von überall aus abrufbar sind. Die Kameras selbst sind fest montiert und können ggf. motorisch geschwenkt werden. Unterscheiden lassen sich verschiedene Bauformen, die vom Einsatzzweck abhängen:

- **Kameras mit Wandarm:** Überwachung von öffentlichen Plätzen, Parkanlagen und Gebäuden;
- **Dome-Kameras:** Überwachung von Parkhäusern, Supermärkten oder öffentlichem Personennahverkehr;
- **PTZ- (Pan Tilt Zoom) und steuerbare Kameras:** steuerbare Kameras, die in unterschiedliche Richtungen bewegt werden können; zur Erfassung

und Verfolgung von Personen, z.B. in Stadien und Flughäfen;

- **Minikameras:** kleine Kameras, die auf den ersten Blick nicht erkannt werden können; dienen der verdeckten Videoüberwachung, z.B. zur Gebäudesicherung;
- **getarnte Kameras:** dienen der verdeckten Videoüberwachung; sind z.B. in Bewegungsmeldern, Wanduhren oder Lampen enthalten.

Das Bild zeigt ein mögliches Videoüberwachungsszenario, in dem verschiedene Kameras mittels LAN oder WLAN an einen zentralen NAS-Speicher angebunden sind. Dieser enthält bereits eine entsprechende Überwachungssoftware und speichert alle Aufnahmen in seinem Festplattenarchiv. Das zentrale NAS-System kann über verschlüsselte VPN-Verbindungen sicher abgefragt werden oder alarmiert automatisch seinen Besitzer über E-Mail, falls Bewegungsdaten vorliegen. Das interne Speichersystem wird von den Videokameraherstellern auch Digital Video Recorder (DVR) genannt und so angeboten. Der Anschluss der Kameras kann drahtlos über Funk- oder Wifi-Technik sowie drahtgebunden über Ethernet bzw. Power over Ethernet (PoE) erfolgen. Wird PoE unterstützt, kann die separate Stromversorgung entfallen.

Videüberwachungssysteme

Videüberwachungssysteme gibt es in mannigfaltiger Ausführung. Daher kann an dieser Stelle nur eine Aus-

Hersteller	Netgear Arlo	Axis	Abus	Reolink	Berghoch	Hikvision	Bascom
HD-Auflösung (H.264, H.265)	ja	ja	ja	ja	ja	ja	ja
Nachtsicht/IR-Sperrfilter	ja/nein	ja/ja	ja/nein	ja/ja	ja/ja	ja/ja	ja/ja
App-Zugriff	ja	nein	ja	ja	ja	ja	ja
Bewegungsalarm	ja	ja	ja	ja	ja	ja	ja
Wireless-Anbindung	ja	nein	ja	nein	nein	ja	ja
PoE-Anschluss	nein	ja	ja	ja	ja	ja	ja
Mikrofon	ja	ja	nein	optional	nein	ja	ja
Dome-/Bullet-Kamera	nein/ja	ja/ja	ja/ja	ja/ja	ja/ja	ja/ja	ja/ja
wetterfest (IP66)	ja	ja	ja	ja	ja	ja	ja

Gegenüberstellung von Videüberwachungslösungen

wahl erfolgen, die aber einen guten Überblick über die Möglichkeiten geben soll. Es gibt auch bereits für den Privatanwender einige Lösungen, die allerdings einen etwas anderen Fokus (z.B. leichte Installation und App-Unterstützung) haben, als die Unternehmenslösungen (z.B. HD-Qualität der Aufnahmen, On-Premises-Datenspeicherung). Ausschlaggebend ist die Qualität der Kamera, die neben HD-Aufnahmen in hoher Auflösung (4 bis 20 Megapixel) auch Schwenk- und Drehfunktionen sowie automatische Bewegungserkennung besitzen sollte. Auch eine Nachtsichtfunktion wird oft zur Gebäudesicherung gefordert, da Einbrecher sich sicherlich nicht zur normalen Betriebszeit Zugang verschaffen wollen. Da die Kamera im Außenbereich angebracht wird, ist auch Wetterfestigkeit in die Anforderungen einzubeziehen sowie WLAN- bzw. Funktechnik, da nicht überall ein Netzanschluss verfügbar sein wird. Entscheiden muss man sich des Weiteren, ob es eine Dome-Kamera in Kugeloptik werden soll, die über Weitwinkel einen recht großen Bereich ohne Detailerkennung abdeckt oder eine Bullet-Kamera, die eventuell Zoom-Möglichkeiten anbietet. Ebenso spielt die Sichtbarkeit eine Rolle, da es inzwischen Kameras gibt, die so klein und handlich sind, dass sie sich unauffällig positionieren lassen. Auch Dome-Kameras lassen sich so in Deckenposition als Lampe tarnen. Ob dies bei den vorhandenen DSGVO-Vorschriften sinnvoll ist, ist allerdings

mehr als fragwürdig. Zusätzlich könnte die Sichtbarkeit auch eine abschreckende Wirkung erzielen. Viele Überwachungskameras lassen sich über Alarmanlagen steuern oder verbinden. Der Eigentümer wird dann über E-Mail oder SMS bei auftretenden Vorfällen benachrichtigt. Bei ausreichender Kameraqualität können die Aufnahmen bei Einbrüchen auch als Beweismittel herangezogen werden. Bei Nachtsichtkameras sollte auf ein Infrarotfilter geachtet werden, um kontrastreiche Bildaufnahmen zu ermöglichen. Ebenfalls immer häufiger anzutreffen sind verbaute Mikrofone in den Kameras. Die professionellen Anbieter setzen insgesamt auf Lösungen, die es ermöglichen, diverse Kameras miteinander zu koppeln, während Smart-Home-Systeme meistens nur für kleinere Setups geeignet sind. Auch bei der Bewegungsmeldung gibt es Unterschiede. Während die preisgünstigen Systeme alle Bewegungen von z.B. Katzen oder Bäumen registrieren, lösen die qualitativ besseren Systeme nur bei Menschen aus. Bei der Datenspeicherung muss man zwischen lokalem DVR-Gerät und Cloud-Servern unterscheiden. Der Hersteller Berghoch bietet z.B. einen exklusiven Zugriff auf die eigenen Server in Deutschland an. Bei anderen Herstellern ist der Cloud-Speicherort – falls vorhanden – hingegen nicht so eindeutig. Bei Cloud-Nutzung müssen allerdings die Anforderungen an den Datenschutz noch einmal separat betrachtet werden.

Die *Tabelle* zeigt eine Auswahl professioneller Videüberwachungslösungen sowie eine Smart-Home-Lösung von Netgear zum Vergleich. Es fällt auf, dass sich alle Varianten wenig voneinander unterscheiden. Einzige Unterschiede zwischen dem Smart-Home-System für Privatanwender und den anderen Lösungen ist die etwas schlechtere Nachtsichtqualität, der fehlende PoE-Anschluss, die Ausrichtung auf drahtlose Anbindung der Kameras und kein Einsatz von Dome-Kameras. Das heißt, das System kann so einfach wie möglich verlegt werden, benötigt aber Batterien für die Kameras. Bei den professionellen Systemen sind die Unterschiede marginal. Alle aufgeführten Hersteller bieten über verschiedene Bundle-Varianten fast alle notwendigen Leistungsmerkmale an. Hier wird allerdings mehr Wert auf feste Verkabelung mittels PoE gelegt, und Mikrofone an den Kameras sind eher die Ausnahme.

Fazit

Grundsätzlich muss man bei der Videüberwachung zwischen der Überwachung durch Unternehmen in öffentlich zugänglichen Bereichen (§ 6b BDSG) und nichtöffentlichen Bereichen (§ 28 BDSG) unterscheiden. Hinzu kommt die Videüberwachung von Beschäftigten (§ 32 Absatz 1 BDSG). In öffentlich zugänglichen Bereichen stehen dabei die Zweckbindung und Datensparsamkeit an erster Stelle. Das Bundesdatenschutzgesetz (BDSG) ist dabei ein Auffanggesetz, das durch die Datenschutzgesetze der Länder noch detaillierter geregelt wird. Aus diesem Grund sollte man sich mit den DSGVO-Richtlinien seines Bundeslandes unbedingt vertraut machen, bevor eine Videolösung installiert wird. Unternehmen sollten daher diese sensible Datenverarbeitung immer mit ihrem Datenschutzbeauftragten abstimmen, der bei über zehn Mitarbeitern sowieso Pflicht ist. Und es sollten nur schutzbedürftige Bereiche überwacht werden, so dass sowohl die Videüberwachung als auch der Datenschutz nicht zu kurz kommen. Deren Definition ist allerdings häufig Auslegungssache. (bk)