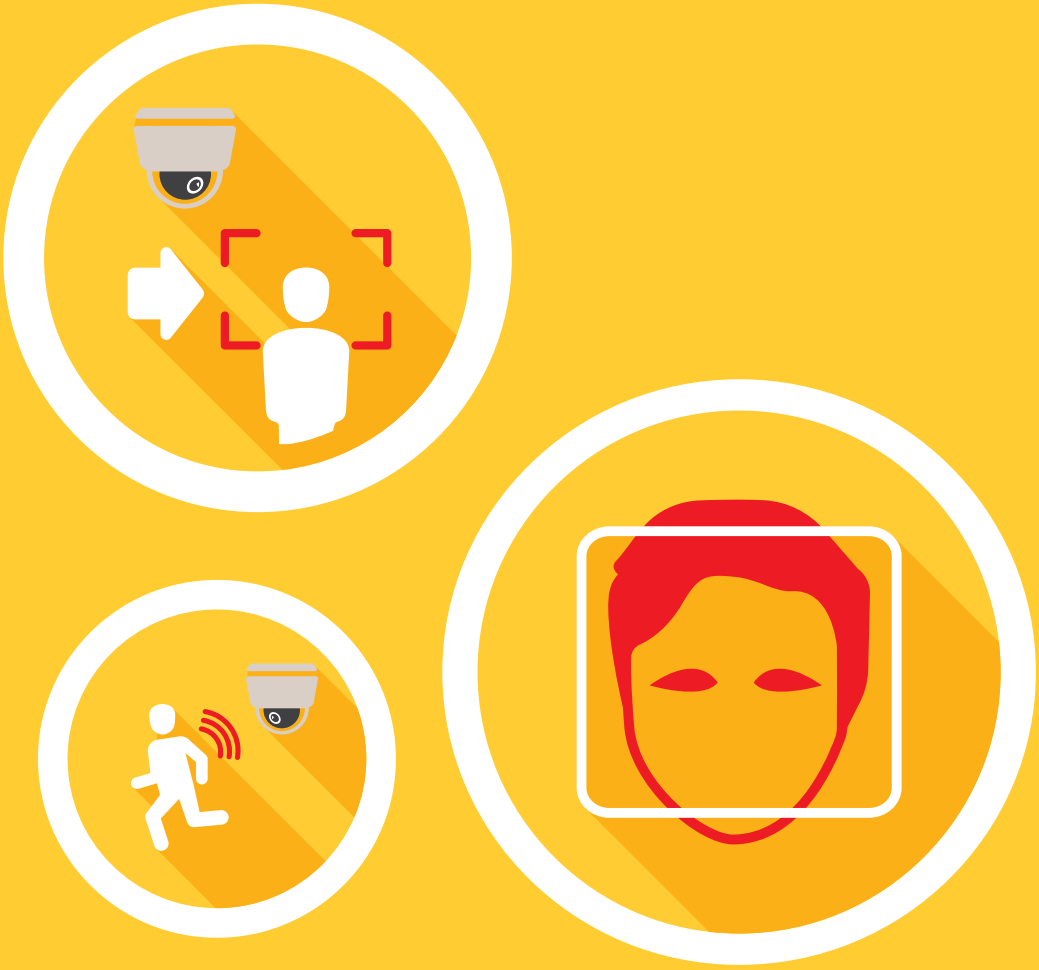
Korrekte **Anwendung der Datenschutzrichtlinien** in der Videoüberwachung

AXIS COMMUNICATIONS

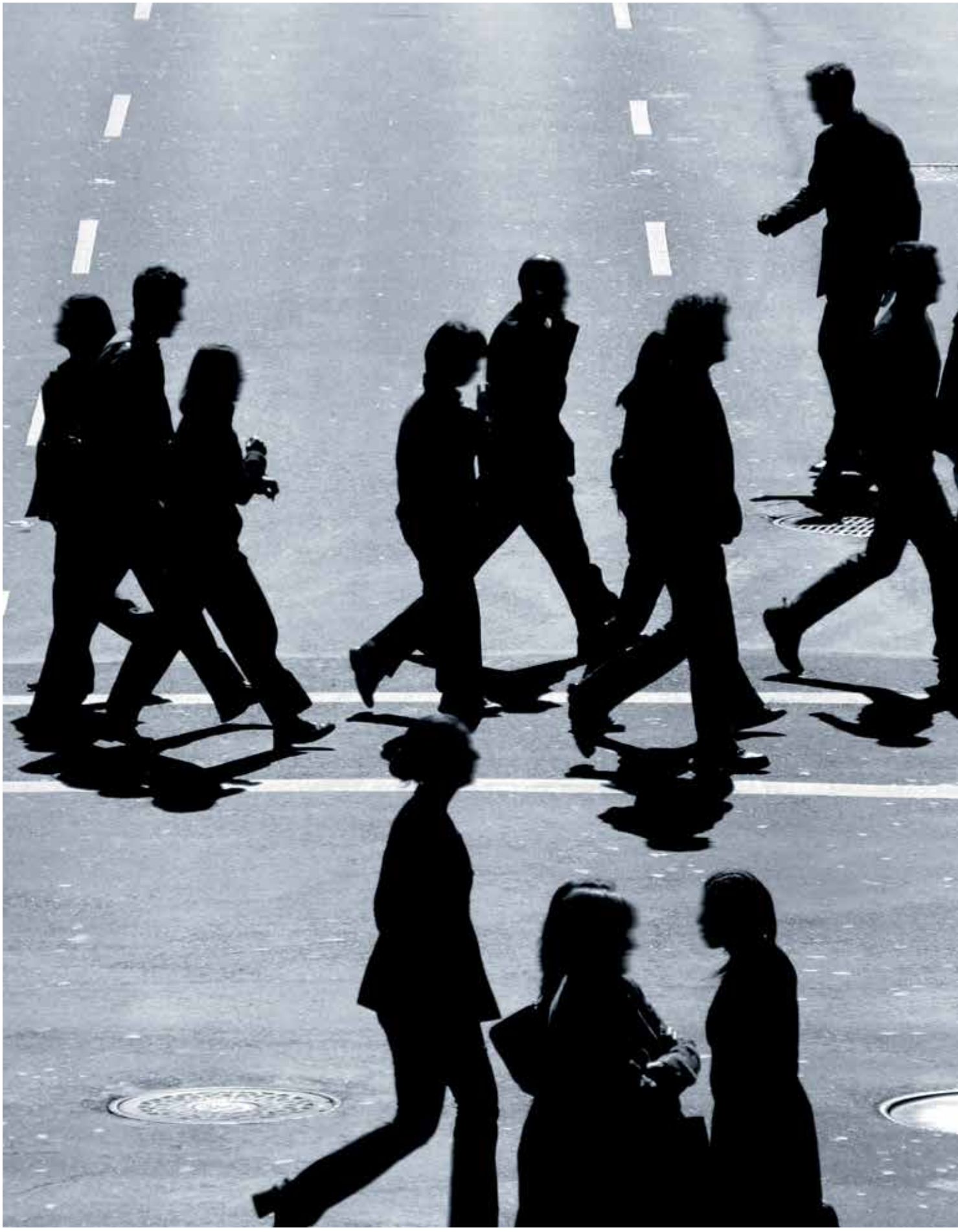
Datenschutz in der Video-überwachung.

Die Europäische Datenschutz-Grundverordnung (DSGVO) und ihre Auswirkungen auf die Videoüberwachung.



Hintergrund: seit dem 25. Mai 2018 ist die DSGVO auch in Deutschland geltendes Recht und muss von jedermann beachtet werden. Ziel dieser europaweit gültigen Verordnung ist es, natürliche Personen bei der Verarbeitung ihrer personenbezogenen Daten zu schützen. Da sie für jede Art der Verarbeitung gilt, unterliegen ihr auch Errichter (Installateure, Systemintegratoren) und Betreiber von Videoüberwachungsanlagen, soweit bei deren Einsatz personenbezogene Daten erfasst und verarbeitet werden.

Axis Communications hat sich von Beginn an dazu verpflichtet, die Privatsphäre von Personen zu respektieren und zu schützen. Daher steht Axis voll und ganz hinter der DSGVO. Während wir selbst darauf achten, die Anforderungen der Verordnung vollumfänglich einzuhalten, unterstützen wir auch Sie, unsere Kunden, um Ihnen deren Einhaltung bei der Planung und Durchführung von Videoüberwachungsmaßnahmen zu erleichtern.



Inhalts-verzeichnis

Die richtige Planung aus datenschutz-rechtlicher Sicht.

Worauf ist bei der Planung, Installation und anschließenden Auswertung bzw. Nutzung der aufgezeichneten Daten zu achten?

Was sollten Errichter im persönlichen Beratungsgespräch mit ihren Kunden (Betreiber) beachten? Was ist zulässig, was ist unzulässig?

Wer ist verantwortlich und kann im Zweifelsfall haftbar gemacht werden?

Mit dieser Broschüre wollen wir Ihnen ein Hilfsmittel an die Hand geben, das Sie in wichtigen Fragen hinsichtlich der Einhaltung der DSGVO unterstützt. Zahlreiche Themen, anschaulich grafisch aufgearbeitet, sollen Sie als Errichter (Installateur/ Systemintegrator) oder Betreiber bei der Planung und Installation von Überwachungssystemen sowie bei Fragen zu Auswertung und Weitergabe von Daten unterstützen. Darüber hinaus informieren wir Sie über generelle Fragen zum Thema Datenschutz.

Am Ende dieser Broschüre finden Sie ein beispielhaftes Szenario für eine Videoüberwachungslösung im Einzelhandel.

Skizzierung eines aus rechtlicher Sicht korrekten Planungs-ablaufs für alle Arten von Videoüber-wachungsanlagen.

Der Betreiber meldet Bedarf für eine Videoüberwachungsanlage an und kontaktiert den Errichter.

1

Betreiber und Errichter führen ein erstes Gespräch. In diesem konkretisiert der Betreiber seine Wünsche in Sachen Sicherheit. Der Errichter kann bereits auf rechtliche Rahmenbedingungen hinweisen und eine erste Machbarkeit prüfen.

2

Der Errichter skizziert den Überwachungsbedarf des Betreibers und schlägt konkrete technische Maßnahmen vor. Auf Basis dieser Informationen bindet der Betreiber seinen Datenschutzbeauftragten in die weitere Bearbeitung ein. Der Datenschutzbeauftragte kann entweder Mitarbeiter im Unternehmen sein oder seine Leistung kann als Dienstleistung eingekauft werden.

3

Der Datenschutzbeauftragte beleuchtet die datenschutzrechtlichen Aspekte der geplanten Installation und prüft sie auf rechtliche Zulässigkeit und Durchführbarkeit. Soweit rechtlich geboten, unterstützt er den Betreiber bei der Durchführung einer Datenschutz-Folgenabschätzung. Diese dient der Bewertung von Risiken und deren möglichen Folgen für die persönlichen Rechte und Freiheiten der Betroffenen und definiert die Maßnahmen, die zum Schutz der erhobenen Bilddaten zu treffen sind.

4

Der Betreiber übermittelt die Datenschutz-Folgenabschätzung an den Errichter, damit dieser die dortigen Vorgaben bei der weiteren Planung berücksichtigt. Zur vollständigen Absicherung empfiehlt sich für den Betreiber eine abschließende Rechtsberatung. So wird sichergestellt, dass sämtliche überwachungsrelevanten Punkte berücksichtigt sind. Wurden beispielsweise Gebäudeeigentümer/ Vermieter/Hausverwaltung informiert?
Werden sämtliche Vorgaben hinsichtlich Arbeitnehmerdaten-schutz und Schutz der Privatsphäre eingehalten?

5

Erst nachdem all diese Schritte berücksichtigt wurden, kann die wirkliche Planung und Durchführung des Überwachungsprojektes beginnen.

6

Generelle Fragen zum Thema Datenschutz.

1. Was ist die DSGVO?

Die seit dem 25.05.2018 geltende Datenschutz-Grundverordnung (DSGVO im Deutschen, GDPR im Englischen) ist ein europaweit gültiges Regelwerk. Sie gilt für die vollständige oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. In der Regel umfasst dies alle Formen der Verarbeitung personenbezogener Daten, die ein Unternehmen durchführt. Die Regelungen der DSGVO dienen dazu, natürliche Personen bei der Verarbeitung personenbezogener Daten zu schützen. Dazu gewährt sie diesen eine Reihe von Rechten (insbesondere auf Auskunft und Information) und erlegt Unternehmen, die personenbezogene Daten verarbeiten, entsprechende Pflichten auf. Für die Einhaltung dieser Pflichten sind die Unternehmen als sog. „Verantwortliche" rechenschaftspflichtig.

2. In welchem Verhältnis steht dazu das BDSG?

Die DSGVO ermöglicht es den Mitgliedstaaten, bei gewissen Sachverhalten ergänzende nationale Regeln zu erlassen. Davon hat der deutsche Gesetzgeber in dem ebenfalls seit dem 25.05.2018 geltenden neuen Bundesdatenschutzgesetz (BDSG) Gebrauch gemacht. Diese Regeln sind von den Unternehmen (und sonstigen Adressaten) ergänzend zu beachten. Soweit dem nationalen Gesetzgeber durch die DSGVO keine Regelungskompetenzen eingeräumt wurden, gehen deren Vorschriften dem BDSG vor.

3. Unter welchen Bedingungen ist eine Videoüberwachung rechtskonform?

Eine Videoüberwachung ist rechtskonform, wenn die Anlage den Vorgaben der DSGVO entspricht. Dabei sind die Grundsätze für die Verarbeitung personenbezogener Daten in Art. 5 sowie die speziellen Zulässigkeitsvoraussetzungen in Art. 6 zu beachten. Abgesehen von der Zustimmung des Betroffenen ist eine Verarbeitung in der Regel dann zulässig, wenn diese zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, nicht überwiegen (vgl. Art. 6 Abs. 1 f DSGVO). Da die Videoüberwachung in der DSGVO nicht explizit geregelt ist, hat der Europäische Datenschutzausschuss (EDSA) im Sommer 2019 Leitlinien zum datenschutzkonformen Einsatz von Videoüberwachung aufgestellt, der konkrete Anwendungsbeispiele enthält und dessen Beachtung deshalb sowohl Errichtern als auch Betreibern von Videoüberwachungsanlagen zu empfehlen ist.

Ähnliche Vorgaben in Bezug auf die Zulässigkeit finden sich in § 4 des neuen BDSG, der mit der Vorgängernorm § 6b des bisherigen BDSG inhaltlich weitgehend identisch ist. Danach ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) zulässig, wenn diese der Wahrnehmung des Hausrechtes oder der Wahrnehmung konkret festgelegter Zwecke des Verantwortlichen dient und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Nach Auffassung der Datenschutzbehörden sowie aktueller Rechtsprechung erlaubt die DSGVO den Mitgliedstaaten aber keine weitergehende Regelung in Bezug auf die Videoüberwachung durch private Verantwortliche, so dass § 4 BDSG keine direkte Anwendung finden soll. Gleichwohl können Gerichtsentscheidungen zur Vorgängernorm (§ 6b) aufgrund der inhaltlichen Übereinstimmungen mit den Vorgaben des Art. 6 Abs. 1 f DSGVO weiterhin als Auslegungshilfe herangezogen werden.

4. Was sind personenbezogene Daten?

Nach europäischem Recht und Bundesdatenschutzgesetz sind personenbezogene Daten all jene Informationen, die sich auf eine natürliche Person beziehen oder zumindest beziehbar sind und so Rückschlüsse auf deren Persönlichkeit erlauben. Besonders schützenswert sind dabei Daten, die Informationen über die ethnische und kulturelle Herkunft, politische, religiöse und philosophische Überzeugungen, Gesundheit, Sexualität und Gewerkschaftszugehörigkeit enthalten sowie genetische und biometrische Daten zur eindeutigen Identifizierung einer Person. Deren Verarbeitung ist nur unter engen Voraussetzungen erlaubt. Dabei hat der Verantwortliche stets die Persönlichkeitsrechte der Betroffenen sowie deren Recht auf informationelle Selbstbestimmung zu beachten, welches das Bundesverfassungsgericht aus den Persönlichkeits- und Freiheitsrechten des Grundgesetzes abgeleitet hat.

5. Was bedeutet „berechtigtes Interesse“?

Ein berechtigtes Interesse folgt den vom Betreiber konkret festgelegten Zwecken – z.B. dem Schutz vor Diebstahl oder Vandalismus, dem Schutz von Mitarbeitern und Kunden oder der Beweissicherung. Die Überwachungsmaßnahme darf nur zur Erfüllung der genannten Zwecke eingesetzt werden und muss erforderlich sein, um diese Zwecke zu erfüllen. Nach Auffassung der Datenschutzbehörden muss eine konkrete Bedrohungslage vorliegen und es darf keine anderen Mittel geben, die genauso zweckmäßig sind, aber weniger in die Persönlichkeitsrechte der Betroffenen eingreifen, als die beabsichtigte Videoüberwachung.

6. Was bedeutet öffentlicher Raum, öffentlich zugänglicher Raum, privater Raum?

> **Öffentlicher Raum** bezeichnet Straßen, Wege und Plätze, die dem öffentlichen Verkehr dienen – z.B. das öffentliche Straßenland (einschließlich Bürgersteige), Parks, Plätze, etc.

> Unter **öffentlich zugänglichem Raum** versteht man Räume innerhalb und außerhalb von Gebäuden, die nach dem erkennbaren Willen des Berechtigten von jedermann genutzt oder betreten werden können, unabhängig davon, wer der Eigentümer ist. Dies können z.B. Verkaufsflächen im Einzelhandel, Einkaufszentren, Parkgaragen, Schalterräume, Gasträume von Gaststätten oder Hotelfoyers sein, Eingangsbereiche von Unternehmen oder Behörden bzw. öffentliche Einrichtungen wie Museen, Sportanlagen, Bibliotheken, etc.

> Ein **nicht öffentlich zugänglicher (**oder auch **privater) Raum** ist ein Bereich, der nur von einem bestimmten Personenkreis oder aufgrund gesonderter Erlaubnis betreten werden darf und eindeutig abgegrenzt ist (z.B. Privatwohnung/-haus, Unternehmen, Büro- und Geschäftsräume, Produktionsbereiche, Lager, Landwirtschaftlicher Betrieb, Autowerkstatt usw.).

> Da Artikel 6 der DSGVO in Bezug auf die Zulässigkeit einer Datenverarbeitung nicht zwischen öffentlich zugänglichen und privaten Räumlichkeiten unterscheidet und § 4 BDSG keine Anwendung mehr finden soll (s.o.), bedarf es in Bezug auf die Zulässigkeit einer Videoüberwachung künftig nicht mehr dieser Differenzierung.

7. Wo beginnt, wo endet der öffentliche Raum?

Öffentlicher Raum beginnt/endet in der Regel an privaten Grundstücksgrenzen – an den Grenzen zu öffentlich zugänglichen oder privaten Bereichen.

8. Muss schriftlich darauf hingewiesen werden, dass Videoüberwachung eingesetzt wird? Wenn ja, wo soll der Hinweis hängen und welche Informationen muss dieser beinhalten?

Ja, es muss schriftlich darauf hingewiesen werden, dass Videoüberwachung eingesetzt wird. Diese Information muss so angebracht sein, dass sie gesehen werden kann, bevor eine Person in den Erfassungsbereich einer Kamera gelangt. Sie muss Name und Kontaktdaten des Verantwortlichen enthalten sowie weitere Informationen, die sich aus Art. 13 der DSGVO ergeben (z.B. die Verarbeitungszwecke, die verfolgten Interessen und die Rechtsgrundlage der Verarbeitung). Die Betreiber sollten sich dabei an dem Musterhinweisschild orientieren, auf das sich die Landesdatenschutzbeauftragten verständigt haben und welches auf ihren Internetseiten veröffentlicht ist. Dort finden sich auch Hinweise, welche Informationen auf ein vorgelagertes Hinweisschild gehören und welche weitergehenden Informationen gegebenenfalls an einer Pforte, in einem gesonderten Aushang oder im Internet hinterlegt werden können.

9. Wer trägt welche Verantwortung für die DSGVO-konforme Videoüberwachung?

Planer und Errichter haben so genannte „Sachwalterpflichten", sie müssen die Rechtsgrundlagen der Videoüberwachung kennen und den Auftraggeber auf mögliche Risiken hinweisen. Eine rechtliche Beratung muss nicht erfolgen. Planer oder Errichter sollten jedoch dem Auftraggeber empfehlen, sich rechtlich kompetent beraten zu lassen. Anderenfalls kann der Auftraggeber den Planer/Errichter im Falle von Sanktionen in Regress nehmen. Darüber hinaus haben Planer/Errichter für eigene Verstöße einzustehen, die im Rahmen einer möglichen Auftragsverarbeitung begangen werden.
Der Betreiber hat als sog. Verantwortlicher die Pflicht, geltendes Datenschutzrecht einzuhalten. Er muss i.d.R. einen Datenschutzbeauftragten einsetzen und vor Planung und Installation eine Datenschutz-Folgenabschätzung erstellen lassen. Er hat für die Sicherheit der erhobenen Daten zu sorgen (Security by design und Security by default) und ist gegenüber den Betroffenen informations-und auskunftspflichtig. Er ist schließlich dafür verantwortlich, dass Daten gelöscht werden, wenn deren Speicherung nicht mehr erforderlich ist.
Ein Sicherheitsdienst, der sich ggf. als externer NSL-Dienst auf die Kameras zuschaltet (z.B. Hosted Video), haftet nach den Grundsätzen der Auftragsverarbeitung (Art. 28 DSGVO). Er muss danach für die datenschutzkonforme Behandlung solcher Daten einstehen, deren Bearbeitung ihm vom Betreiber durch einen gesondert abzuschließenden Vertrag über Auftragsverarbeitung übertragen wurde (z.B. Auswertung der übertragenen Livebilder).

10. Was ist eine Datenschutz-Folgenabschätzung?

Die Datenschutz-Folgenabschätzung ist eine Vorabkontrolle und wird vom Betreiber unter Einbindung seines Datenschutzbeauftragten erstellt. Sie ist grundsätzlich vor der Planung und Installation von Überwachungssystemen durchzuführen. Eine Datenschutz-Folgenabschätzung ist immer dann erforderlich, wenn die Verarbeitung aufgrund der Art, des Umfanges, der Umstände und der Zwecke voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Die DSGVO nennt hier als Beispiel ausdrücklich die „systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche". Entspricht die geplante Videoüberwachung diesen Vorgaben (was nach Auffassung einiger Aufsichtsbehörden bei stationären Videoüberwachungsanlagen mit mehreren Kameras immer der Fall ist), dann sind die möglichen datenschutzrechtlichen Risiken zu prüfen und ggfs. Maßnahmen zu benennen, um diese Risiken beherrschbar zu machen. Dabei hat der Betreiber den Rat seines Datenschutzbeauftragten (DSB) einzuholen, wenn ein solcher bestellt wurde.

11. Wann ist ein Datenschutzbeauftragter zu bestellen?

Nach dem BDSG ist ein DSB zu bestellen, wenn im Unternehmen mindestens zehn Personen mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Finden im Unternehmen allerdings Verarbeitungen statt, die einer Datenschutz-Folgenabschätzung unterliegen, ist ein DSB unabhängig von der Zahl der mit der Datenverarbeitung befassten Mitarbeiter zu berufen. Ist mit anderen Worten eine (systematische und umfangreiche) Videoüberwachung geplant, wird der Betreiber um die Bestellung eines DSB nicht herumkommen. Bietet sich hierfür kein festangestellter Mitarbeiter an, kann die Leistung eines Datenschutzbeauftragten als Dienstleistung eingekauft werden.

12. Was sind die Folgen/Sanktionen bei Verstößen gegen die DSGVO?

Die zuständigen Aufsichtsbehörden (Landesdatenschutzbeauftragten) können Verletzungen der datenschutzrechtlichen Pflichten in Zukunft mit hohen Bußgeldern belegen. Beispielsweise kann bei Nichtdurchführung einer Datenschutz-Folgenabschätzung oder bei einem fehlenden Verfahrensverzeichnis eine Geldbuße von bis zu 10 Mio. Euro oder bei einem Unternehmen von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt werden. Zuwiderhandlungen gegen die Grundsätze der Datenverarbeitung oder die Zulässigkeitsvoraussetzungen können Geldbußen von bis zu 20 Mio. Euro und im Falle eines Unternehmens von bis zu 4 % Prozent des gesamten weltweit erzielten Jahresumsatzes zur Folge haben. Nachdem die deutschen Aufsichtsbehörden mit der Verhängung namhafter Bußgelder bisher zurückhaltend waren, wollen sie ab 2020 ein Bußgeldkonzept anwenden, welches auf umsatzabhängigen „Tagessätzen" basiert, die je nach Schwere des Verstoßes mit entsprechenden Faktoren multipliziert werden. Außerdem können Betroffene in Zukunft Schadensersatzansprüche gegen den Verantwortlichen geltend machen, wenn sie aufgrund eines Verstoßes gegen die DSGVO einen materiellen oder immateriellen Schaden erlitten haben. Auch Verbandsklagen sind möglich.

13. Wer ist berechtigt, Verstöße zu ahnden und Strafen zu verhängen?

Verstöße werden durch die zuständigen Aufsichtsbehörden – die Landesdatenschutzbeauftragten – geahndet. Unterstützung hinsichtlich technischer Fragen gibt das Bundesamt für Sicherheit in der Informationstechnologie (BSI).

14. Können festangestellte Mitarbeiter eines Unternehmens datenschutzrechtlich belangt werden?

Handelt der festangestellte Mitarbeiter im Auftrag seines Unternehmens, kann er von den Datenschutzbehörden nicht direkt rechtlich belangt werden. Hat er allerdings vorsätzlich oder grob fahrlässig gegen datenschutzrechtliche Pflichten verstoßen, die ihm arbeitsvertraglich auferlegt wurden, kann er von seinem Arbeitgeber in Regress genommen werden. Betreiber sind daher gut beraten, ihre Mitarbeiter auf das Datengeheimnis zu verpflichten und ihnen – je nach Aufgabenstellung – besondere Sorgfaltspflichten vertraglich aufzuerlegen.

15. Wie kann der Errichter seine Rechte zum Thema DSGVO sichern?

Der Errichter sollte seinen Kunden stets darauf hinweisen, dass er für die datenschutzkonforme Installation und vor allem für den datenschutzkonformen Betrieb der Videoüberwachungsanlage keine Gewähr übernehmen kann. Rechtsfragen sind durch den Kunden selbst (ggfs. mit Unterstützung durch Rechtsberater und Datenschutzbeauftragte) zu prüfen, da dieser als Betreiber die datenschutzrechtliche Verantwortung trägt. Diese Hinweise sollten aus Beweiszwecken schriftlich erfolgen und sind auch in die Allgemeinen Geschäftsbedingungen des Errichters aufzunehmen. Fordert der Kunde eine erkennbar datenschutzwidrige Installation, dann sollte dies durch den Errichter nicht befolgt werden, jedenfalls aber Gegenstand eines gesonderten Bedenkenhinweises sein. So kann er sich im Verhältnis zum Kunden gegen mögliche Regressansprüche absichern.

16. Können Planer/Errichter datenschutzrechtlich belangt werden?

Die Hauptverantwortung für die datenschutzkonforme Konfiguration und den datenschutzkonformen Betrieb der Videoüberwachungsanlage liegt beim Auftraggeber als Betreiber der Anlage und nicht beim Planer bzw. Errichter. Diese sollten den Auftraggeber auf dessen datenschutzrechtliche Pflichten hinweisen und die Einholung kompetenten Rechtsrates empfehlen und ansonsten Bedenken anmelden; dann dürfte ein Regress durch den Auftraggeber schwerlich durchsetzbar sein. Daneben obliegen den Planern/ Errichtern eigene datenschutzrechtliche Pflichten in Bezug auf ihr Unternehmen (z.B. Führung eines Verfahrensverzeichnisses, Bestellung eines Datenschutzbeauftragten, etc.). Findet im Rahmen der Auftragsdurchführung (oder bei daran anschließenden Wartungs-und Servicearbeiten) eine Bearbeitung der durch die Videoüberwachung erhobenen Bilddaten durch den Auftragnehmer statt (z.B. beim Parametrieren oder Testen der Anlage), dann handelt es sich nach Auffassung der Datenschutzbehörden um eine Auftragsverarbeitung gemäß Art. 28 DSGVO, die eines gesonderten Vertrages mit dem Auftraggeber bedarf. Die in diesem Zusammenhang übertragenen datenschutzrechtlichen Pflichten muss der Auftragnehmer einhalten, sonst setzt er sich Sanktionen der Aufsichtsbehörden und Schadensersatzansprüchen der Betroffenen aus.

17. Wie ist der Schutz des Arbeitnehmers hinsichtlich Videoüberwachung geregelt? Ist Videoüberwachung am Arbeitsplatz zulässig?

Videoüberwachung am Arbeitsplatz darf grundsätzlich eingesetzt werden, wenn sie den Vorgaben des Art. 6 Abs. 1 f DSGVO entspricht, also zweckmäßig, erforderlich und verhältnismäßig ist und darüber hinaus entsprechend § 26 Abs. 1 BDSG für die Durchführung des Beschäftigungsverhältnisses als erforderlich angesehen werden kann. Hierzu gehören beispielsweise Maßnahmen, die der Sicherheit der Beschäftigten am Arbeitsplatz dienen oder der Authentifikation oder Autorisierung. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten von Beschäftigen nur verarbeitet werden, wenn der begründete Verdacht vorliegt, dass die betroffene Person eine Straftat im Arbeitsumfeld begangen hat (vgl. § 26 Abs. 1 Satz 2 BDSG).

18. Welche Bereiche darf der Arbeitgeber per Videoüberwachung einsehen?

Ein Mitarbeiter kann sich – anders als z.B. ein Kunde oder Besucher – einer permanenten Videoüberwachung in der Arbeitsumgebung kaum entziehen. Deshalb darf diese keinen unzumutbaren Überwachungs- und Anpassungsdruck ausüben. Überwachungskameras an der Kasse sind deshalb z.B. so auszurichten, dass sie dem Mitarbeiter über die Schulter und nicht ins Gesicht sehen. Darüber hinaus ist die Überwachung der Privatsphäre (z.B. Raucherecken, Pausenräume, etc.) zu unterlassen, das Filmen in der Intimsphäre (z.B. Sanitär- oder Umkleideräume) ist absolut tabu.

19. Muss der Arbeitgeber stets das Einverständnis seiner Mitarbeiter einholen?

Das ist nur erforderlich, wenn die Maßnahmen nicht bereits aus anderen Gründen zulässig sind (z.B. weil die Interessen des Arbeitgebers überwiegen). Der Arbeitgeber muss wissen, dass eine Zustimmung nur wirksam ist, wenn der Arbeitnehmer vorher ausreichend über die Maßnahme und ihre Folgen aufgeklärt wurde und wenn er seine Zustimmung absolut freiwillig abgegeben hat. Das ist aufgrund der Abhängigkeiten in einem Anstellungsverhältnis nur unter engen Voraussetzungen der Fall, etwa wenn die Zustimmung mit einem Vorteil für den Arbeitnehmer verbunden ist oder wenn Arbeitgeber und Arbeitnehmer gemeinsame Interessen verfolgen. Außerdem kann eine Einwilligung stets mit Wirkung für die Zukunft widerrufen werden. Deshalb sollte der Betreiber auf Installationen setzen, die auch ohne Zustimmung der Arbeitnehmer zulässig sind.

20. Welche Bedeutung haben Betriebsvereinbarungen?

Nach dem Bundesdatenschutzgesetz ist die Verarbeitung personenbezogener Daten für Zwecke des Beschäftigungsverhältnisses auf der Grundlage von Betriebsvereinbarungen zulässig. Solche werden in Unternehmen, welche dem Betriebsverfassungsgesetz unterliegen, mit den Arbeitnehmervertretern (Betriebsrat) abgeschlossen. Diese Vereinbarungen (z.B. über die Videoüberwachung oder Zutrittskontrolle) sind dann für alle Beteiligten verbindlich. Sie können sogar die Verarbeitung von besonders schützenswerten Daten nach Art. 9 DSGVO umfassen. Damit lassen sich z.B. auch Zutrittskontrollsysteme, die mit biometrischen Daten arbeiten, legitimieren, was sonst nur mit dem ausdrücklichen (freiwilligen!) Einverständnis der Beschäftigten möglich ist.


M18
REDLITHIUM-ION
3.0 Ah

Planung & Installation eines Überwachungs-systems.

1. Muss jede Kamera vor Betrieb separat datenschutzrechtlich abgenommen werden?

Ja. In Bezug auf jede Kamera ist zu prüfen, ob sie datenschutzrechtlich zulässigen Zwecken dient, ob deren Einsatz (zu welchen Zeiten und in Bezug auf welche Erfassungsbereiche) erforderlich ist und ob die schützenswerten Interessen der Betroffenen nicht überwiegen (z.B. in deren Privat- oder Intimsphäre). Dabei muss die Überwachung zur Zweckerfüllung geeignet sein und darf auch nur zur Erfüllung des genannten Zwecks eingesetzt werden. Handelt es sich um eine systematische und umfangreiche Überwachung, kann diese Prüfung im Rahmen einer Datenschutz-Folgenabschätzung durchgeführt werden. Diese Prüfung kann im Ergebnis dazu führen, dass der Erfassungsbereich und/oder zeitliche Einsatz der Kamera auf ein datenschutzrechtlich zulässiges Maß beschränkt wird.

2. In welchen Bereichen ist eine Videoüberwachung grundsätzlich zulässig, in welchen Bereichen nicht?

Nach der Rechtsprechung hat stets eine Abwägung zwischen den schutzwürdigen Interessen der Betroffenen (Persönlichkeitsrechte) einerseits und den Interessen des Betreibers stattzufinden. Das Ergebnis einer solchen Abwägung hängt davon ab, in welcher Sphäre eine Überwachung stattfindet. In der sog. Sozial- oder Geschäftssphäre geraten die Menschen eher beiläufig oder nur kurzfristig in überwachte Zonen Dies gilt etwa für Schalterräume von Banken, Verkaufsflächen in Einkaufsmärkten, Tankstellen, Parkplätzen etc. Hier überwiegt in der Regel das Interesse des Betreibers am Schutz seiner Einrichtungen, Waren und sonstigen Sachen. In der sog. Privatsphäre sieht es hingegen anders aus. Hier überwiegt in der Regel das Interesse der

Betroffenen, unbeobachtet zu sein. Dies gilt insbesondere für Räumlichkeiten, in denen Kommunikation bzw. soziale Interaktion stattfindet, wie z.B. in Gasträumen, Raucherecken, Besucherzimmern, etc. In der sog. Intimsphäre ist eine Bilddatenerhebung absolut tabu, hierzu zählen Umkleidekabinen, Sanitärräume, Ruheräume, etc.

Für die Arbeitsumwelt bedeutet dies: wird z.B. eine Verkaufsfläche in einem Warenhaus zur Diebstahlprävention und/oder zur Beweissicherung überwacht und umfasst diese Überwachung gleichzeitig die Arbeitsplätze der Mitarbeiter, so ist dies zulässig und die Mitarbeiter müssen das i.d.R. zulassen, solange die Kamera nicht auf die Gesichter der Mitarbeiter an einem festen Arbeitsplatz (z.B. an der Kasse) ausgerichtet ist. Eine Überwachung der Raucherecke hingegen ist nicht zulässig, da sich die Mitarbeiter dort privat austauschen. Gänzlich untersagt ist das Filmen in Räumen, in denen sich die Mitarbeiter umziehen oder ausruhen.

Videoüberwachung im öffentlichen Bereich (z.B. im Straßenraum) ist NICHT erlaubt, es sei denn, der Betreiber ist eine Stadt/Gemeinde/Sicherheitsbehörde und es besteht ein berechtigtes Interesse an einer Überwachung – z.B. Unfallprävention an vielbefahrenen Kreuzungen, Beobachtung von Kriminalitätsschwerpunkten, usw.

3. Dürfen im Eingangsbereich (öffentlich zugänglich bzw. privat) Kameras installiert werden? Welchen Einfluss haben Bildwinkel und Schutzziel? Unter welchen Bedingungen ist der Betrieb der AXIS Türstation erlaubt?

Bildwinkel und Schutzziel (Auflösung) bestimmen, wie weit die Kamera reicht und wie viel auf dem Videobild zu sehen ist. Im Eingangsbereich (z.B. eines Kaufhauses) dürfen Kameras installiert werden, solange diese keine Flächen erfassen, die dem öffentlichen Verkehr gewidmet sind (z.B. Fußgängerweg oder öffentliche Straßen). Allerdings ist nach der Rechtsprechung die Überwachung der Fassade eines Gebäudes zulässig, soweit sich der Erfassungsbereich auf einen Meter entlang der Gebäudehülle beschränkt. Der Betrieb einer AXIS Türstation ist daher gestattet, solange dieser äußere Erfassungsbereich nicht überschritten wird.

4. Wie unterscheidet sich die Videoüberwachung mit optischen oder Thermalkameras aus rechtlicher Sicht?

Wärmebildkameras nutzen zur Bildgebung die von Objekten wie Fahrzeugen oder Personen abgestrahlte Wärme. Eine Wärmebildkamera kann bei schwierigen Lichtverhältnissen wie Schatten, Gegenlicht, Dunkelheit und auch bei getarnten Objekten Bilder liefern, anhand derer der Bediener verdächtige Aktivitäten feststellen kann. Solange sich Personen aufgrund einer geringen Auflösung nicht erkennen bzw. identifizieren lassen, ist der Datenschutz nicht einschlägig. Diese Frage ist im Rahmen der Datenschutz-Folgenabschätzung zu klären. Handelt es sich um moderne Thermalkameras mit hoher Auflösung, sieht die Sache anders aus. Solche Kameras liefern derart gute Bilder, dass Personen in der Regel erkannt und durch Abgleich mit Bewegungsmustern auch identifiziert werden können. In diesen Fällen gelten für Thermalkameras die gleichen Regeln, wie für normale Videokameras.

5. Dürfen nur bestimmte Typen von Kameras in Unternehmen/ Krankenhäusern/Altersheimen usw. eingesetzt werden?

Grundsätzlich kommt es nicht auf die Kameratechnik als solche, sondern auf den konkreten Einsatz im Einzelfall an. Dabei hat stets die bereits erwähnte datenschutzrechtliche Abwägung stattzufinden. In diesem Zusammenhang stellt sich schnell heraus, dass z.B. Hochleistungskameras in bestimmten Bereichen nicht erforderlich sind, sondern dass einfache Kameras mit starrer Ausrichtung und festem Bildwinkel völlig ausreichen. Das gilt insbesondere für Standardanwendungen in Unternehmen, öffentlichen Einrichtungen, etc. Auch sollte bei der Auswahl der Kameras darauf geachtet werden, bei potentiell betroffenen Personen so wenig Protest wie möglich auszulösen. Dies könnte z.B. bei Dome-Kameras mit verdunkelter Kuppel der Fall sein - hier ist die Ausrichtung der Linse nicht zu erkennen.

6. Dürfen PTZ-Kameras zur Videoüberwachung eingesetzt werden?

Hier gilt das oben gesagte entsprechend. PTZ-Kameras dürfen zur Überwachung eingesetzt werden, wenn der Überwachungszweck den Einsatz besonders leistungsfähiger Systeme rechtfertigt (z.B. das Verfolgen von Straftaten), und die Persönlichkeitsrechte der Betroffenen in der Abwägung mit den berechtigten Interessen des Betreibers nicht unzumutbar beeinträchtigt werden.

Betrieb, Auswertung, Weitergabe.

1. Ist eine Datenaufzeichnung grundsätzlich zulässig?

Erhobene Daten dürfen vom Verantwortlichen auch gespeichert und verwertet werden, wenn dies den Zwecken dient, für die sie erhoben worden sind (z.B. für die Beweissicherung). Das gilt nur, wenn die Persönlichkeitsrechte der Betroffenen dadurch nicht in unzumutbarer Weise beeinträchtigt werden, und die Bilddaten nur so lange gespeichert bleiben, wie es für die Zwecke, für die sie erhoben wurden, erforderlich ist.

2. Was darf ich aufzeichnen?

Grundsätzlich gilt: was live beobachtet werden darf (sog. Monitoring), darf auch aufgezeichnet werden. Dabei ist stets eine Abwägung zwischen den berechtigten Interessen des Betreibers und den schutzwürdigen Interessen der Betroffenen vorzunehmen (s.o.). Zusätzlich muss der Betreiber dafür sorgen, dass die gespeicherten Bilddaten vor dem Zugriff unbefugter Personen und einer missbräuchlichen Verwendung geschützt sind. Diesbezüglich sind nach den Vorgaben der DSGVO geeignete technische und organisatorische Maßnahmen zu ergreifen (s.u.).

3. Wie lange dürfen/sollen Aufzeichnungen gespeichert werden?

Das aufgezeichnete Material muss unverzüglich gelöscht werden, sobald der Zweck der Aufzeichnung erreicht ist oder schutzwürdige Interessen der Betroffenen gegen eine weitere Speicherung sprechen. Es gibt keine starren gesetzlichen Fristen, trotzdem geben die Datenschutzbehörden bestimmte Leitlinien vor, wie z.B. 72 Stunden bei Aufnahmen, die zur Beweissicherung von Diebstählen im Einzelhandel gespeichert werden. Es ist dann Sache des Betreibers, gute Argumente für eine längere Speicherdauer zu finden.

4. Unter welchen Bedingungen ist die Nutzung von Video- und Audioanalytik rechtskonform?

Rechtskonform ist die Nutzung von Video- und Audioanalytik nur dann, wenn keine Rückschlüsse auf konkrete Personen möglich sind und die Daten nicht aufgezeichnet werden. Mit den AXIS ACAP Modulen ist eine Video- und Audiodatenanalyse direkt auf der Kamera möglich, diese erfolgt nicht über den Live-Stream. Somit ist eine Speicherung der Daten zur Auswertung nicht notwendig.

5. Wie müssen die Zugriffe auf die gespeicherten Daten datenschutzrechtlich geregelt sein, wie sollten Videodaten geschützt werden?

Der Betreiber muss geeignete technische und organisatorische Maßnahmen für ein entsprechendes Schutzniveau ergreifen (sog. TOM's). Diese Maßnahmen schließen u.a. die Pseudonymisierung und Verschlüsselung personenbezogener Daten ein. So sollten Kamerasysteme eingesetzt werden, bei denen die Übertragung der Bilddaten auf den Server in verschlüsselter Form erfolgt, damit diese nicht während der Übertragung von außen eingesehen werden können. Bei gespeicherten Videodaten findet der Schutz üblicherweise in drei Stufen statt. Zuallererst muss der physische Schutz des Datenspeichers sichergestellt sein – er muss diebstahlsicher untergebracht sein und nur autorisierte Personen dürfen darauf zugreifen. Darüber hinaus muss es einen Zugriffsschutz über eine Benutzer-Authentifizierung (individueller Benutzername, komplexes Kennwort) geben. Zusätzlich kann eine Verschlüsselung des Datenträgers eine sinnvolle Erweiterung des Schutzes darstellen.

6. Wer hat (wie) Zugriff auf die Videoaufzeichnung/Datenspeicher?

Zugriff auf Videoaufzeichnungen oder auf den Datenspeicher darf nur berechtigten Personen gewährt werden. Wer eine Berechtigung erhält, ist abhängig von der Aufgabenstellung im Unternehmen und vom Zweck der Überwachungsmaßnahme. Zugriff haben neben dem Betreiber ausgewählte Mitarbeiter (z.B. der Administrator und ggf. eine Bedienkraft), welche auf die Einhaltung des Datenschutzes zu verpflichten sind. Details dazu sind in der Datenschutz-Folgenabschätzung bzw. im Verfahrensverzeichnis festzuhalten.

7. Unter welchen Bedingungen dürfen Bilddaten weitergegeben werden?

Die Weitergabe von Aufzeichnungen (Übermittlung) ist nach dem BDSG nur zu Zwecken der polizeilichen Prävention und/ oder Strafverfolgung zulässig. Dies sollte aber nicht „auf Zuruf" erfolgen, sondern nur, wenn eine entsprechende staatsanwaltschaftliche oder richterliche Anordnung vorliegt. Darüber hinaus kann der Betreiber zum Zwecke der Beweissicherung gespeicherte Sequenzen zur Durchsetzung rechtlicher Ansprüche z.B. vor Gericht verwenden. Die zweckwidrige Übermittlung von Aufzeichnungen an Dritte (z. B. zur Auswertung für Marketingmaßnahmen) ist hingegen unzulässig.

8. Welche Rechte haben Privatpersonen in Bezug auf Videoaufnahmen?

Sowohl das BDSG als auch die DSGVO räumen den von der Datenverarbeitung betroffenen Personen weitgehende Informations- und Auskunftsrechte ein (vgl. Artikel 12 ff DSGVO). Dies beginnt damit, dass der Betreiber über die Tatsache der Videoüberwachung und weitere Einzelheiten der Verarbeitung auf geeigneten Hinweisschildern informieren muss, bevor eine Person in den Erfassungsbereich der Kameras gelangt (s.o.). Darüber hinaus können die Betroffenen Auskunft über die Verarbeitungszwecke und den weiteren Umgang mit den personenbezogenen Daten verlangen (Art. 15) und Ansprüche auf Berichtigung (Art. 16), auf Löschung („Recht auf Vergessenwerden", Art. 17), auf Einschränkung der Verarbeitung (Art. 18) und auf Datenübertragbarkeit (Art. 20) geltend machen. Darüber hinaus können sie Widerspruch gegen die Verarbeitung der sie betreffenden personenbezogenen Daten einlegen (Art. 21). Näheres hierzu lässt sich den genannten Artikeln sowie den Veröffentlichungen der Datenschutzbehörden entnehmen. Der Betreiber sollte in seinem Hause ein qualifiziertes Informations- und Auskunftsmanagement in Bezug auf die Verarbeitung personenbezogener Daten einrichten, um hier keine bußgeldpflichtigen Verstöße zu begehen.

9. Dürfen KFZ-Kennzeichen aufgezeichnet werden?

KFZ-Kennzeichen sind personenbezogene Daten – somit gelten auch hier die Rahmenbedingungen der DSGVO. KFZ-Kennzeichen dürfen grundsätzlich nicht aufgezeichnet werden, solange kein vorrangiges berechtigtes Interesse des Betreibers besteht. Dies kann der Fall sein bei parkenden bzw. querenden Fahrzeugen auf privatem oder öffentlich zugänglichem Gelände, etwa zur Wahrung des Hausrechts oder zu Zwecken der Beweissicherung.

10. Dürfen die Videodaten an einen Speicherort ausgelagert werden, der von einem Dritten (Hoster) bereitgestellt wird?

Grundsätzlich ja. Es liegt in der Verantwortung des Auftraggebers, einen entsprechend qualifizierten Dienstleister für Datenspeicherung und -verarbeitung zu beauftragen. Dieser Dienstleister muss Maßnahmen zum Schutz der Daten, vor ungewollten Zugriffen oder Manipulation durch Dritte ergreifen und sich nachweislich an den Vorgaben der DSGVO hinsichtlich Datensicherheit orientieren. Der Dienstleister ist hierzu in einem Vertrag über Auftragsverarbeitung gemäß Art. 28 DSGVO vom Betreiber zu verpflichten.

11. Wo darf/muss der Server stehen?

Maßgeblich ist grundsätzlich nicht, wo der Server eines Video-Management-Systems steht, sondern wer darauf Zugriff hat. Zugriff auf Videoaufzeichnungen oder auf den Datenspeicher darf nur berechtigten Personen gewährt werden, dies ist im Verfahrensverzeichnis und ggf. in der Datenschutz-Folgenabschätzung festzuhalten. Der physische Schutz des Datenspeichers muss sichergestellt sein – er muss diebstahlsicher untergebracht sein und lediglich autorisierte Personen (die auf die Einhaltung des Datenschutzes zu verpflichten sind) dürfen darauf zugreifen. Darüber hinaus muss es einen Zugriffsschutz über eine Benutzer-Authentifizierung geben, optional auch eine Verschlüsselung des Datenträgers. Wenn die Datenübertragung im Wege des Cloud-Computing erfolgt, muss sichergestellt sein, dass die Datenbearbeitung und -übertragung nur durch Dienstleister erfolgt, die ihren Sitz in einem Mitgliedstaat der Europäischen Union haben und dem europäischen Datenschutz unterworfen sind.

12. Was muss beim Einsatz sogenannter Web-Attraction-Cameras beachtet werden? (Kameras um z.B. einen Hafen, eine Landschaft, Stadtmitte auf einer Webseite live aus Tourismuszwecken darzustellen).

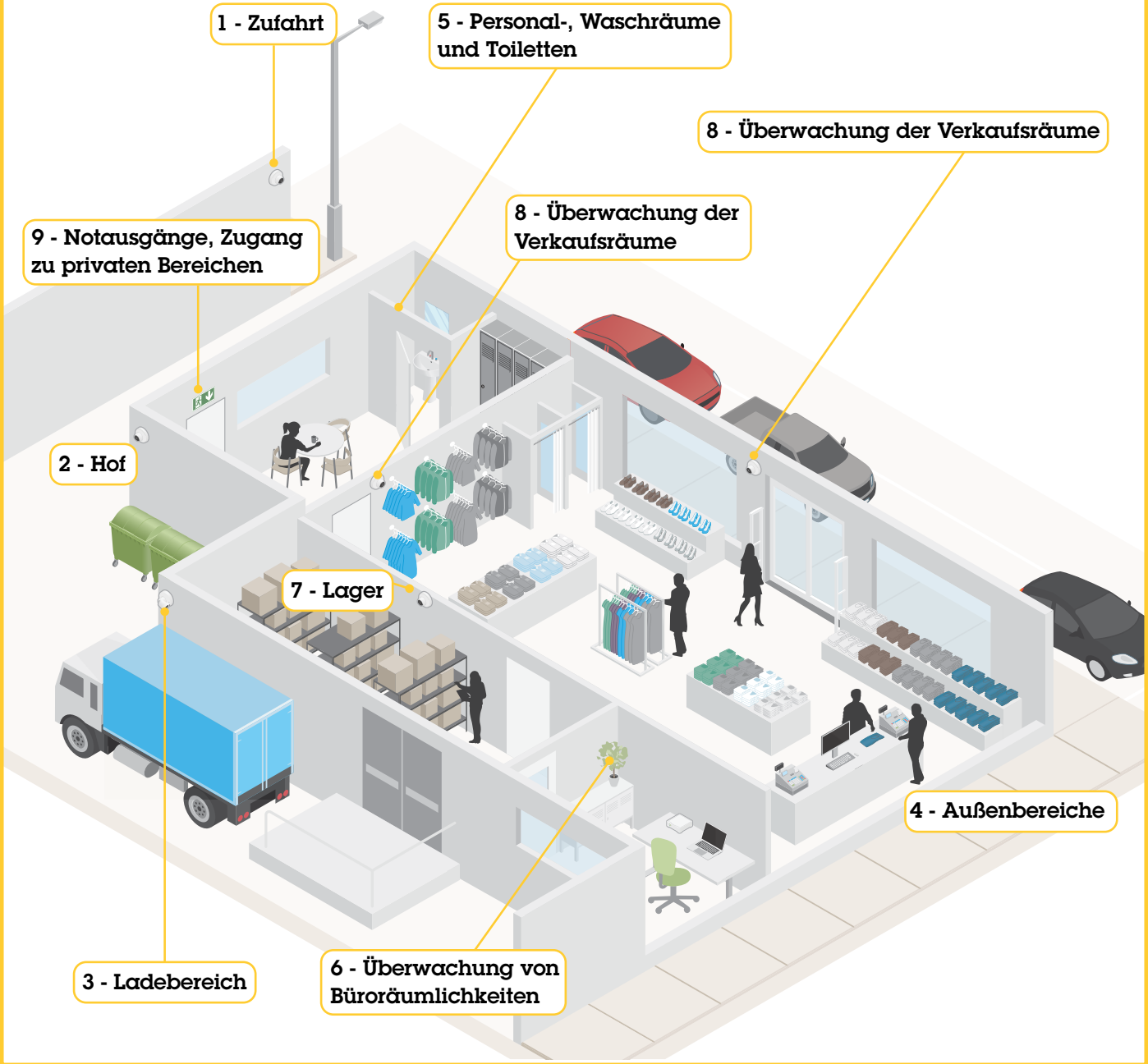
Solange auf den von Webcams erzeugten Bildern keine Personen erkennbar sind, stellen sich auch keine datenschutzrechtlichen Fragen. So liefern Panoramakameras i.d.R. keine Details, die Personen identifizierbar machen. Das ändert sich, wenn die Bildauflösung ausreicht, so dass die abgebildeten Personen zumindest durch Bekannte wiedererkannt werden können. Dann sind in jedem Fall die Vorschriften des Kunsturhebergesetzes betroffen, die eine unautorisierte Verbreitung von Bildnissen eines Menschen verbieten, solange dessen Abbildung nicht lediglich ein unbedeutendes Beiwerk einer Landschaft oder sonstigen Örtlichkeit darstellt. Des Weiteren ist der Datenschutz einschlägig, wenn sich z.B. durch Verknüpfung anderer Daten (z.B. KFZ-Kennzeichen) auf eine bestimmte natürliche Person schließen lässt. In solchen Fällen unterliegt dann der Einsatz von Webcams der vollen Bandbreite der einschlägigen datenschutzrechtlichen Vorschriften, die bisher erörtert wurden.

13. Wofür dürfen generierte Daten eingesetzt werden? Können sie auch zu Marketing- oder Vertriebszwecken eingesetzt werden?

Bilddaten aus Überwachungskameras dürfen nur für die vorher vom Betreiber festzulegenden Zwecke verwendet werden, soweit diese aus einem berechtigten Interesse abgeleitet wurden. Hierbei handelt es sich beispielsweise um den Schutz vor Diebstahl oder Vandalismus, Schutz von Mitarbeitern und Kunden oder um die Beweissicherung. Über dieses berechtigte Interesse ist der Betroffene in geeigneter Weise zu informieren. Jegliche andere Verwendung der generierten Daten ist unzulässig (etwa zu Marketing- oder Vertriebszwecken), es sei denn, der Betroffene hat hierin ausdrücklich (schriftlich) eingewilligt.

Überwachungsszenario am Beispiel eines Fashionstores.

An den markierten Stellen befinden sich Kameras. Unter der jeweiligen Ziffer finden Sie auf der rechten Seite die entsprechende Erläuterung.



Außenbereich - privat und öffentlich zugänglich:

1. Zufahrt: Kameras zeigen an, wenn Fahrzeuge Ladezufahrten und Rettungswege versperren oder sich unbefugte Personen in schlecht einsehbaren Bereichen aufhalten.

2. Hof: Kameras zeigen an, wenn sich unbefugte Personen dort aufhalten, sich auffällig verhalten oder sich an im Außenbereich abgestellter Ware/Eigentum zu schaffen machen.

3. Ladebereich: Kameras geben einen Überblick über die Laderampe - halten sich dort unbefugte Personen auf oder befindet sich dort noch Ware?

4. Außenbereiche: Kameras können direkt an den öffentlichen Bereich angrenzende Zäune, Tore, Außenfassaden oder Schaufensterbereiche überblicken. Sie dürfen hier innerhalb einer Toleranzzone von 1 m aufzeichnen. Ordnungswidrigkeiten, Vandalismus, Einbruch oder andere Straftaten lassen sich häufig durch eine Früherkennung vermeiden. Die Videoüberwachung ergänzt in Außenbereichen den klassischen physischen Schutz (Zäune, Mauern, Tore, Schranken) und erlaubt eine automatische Erkennung (Bewegungs- und Audioanalytik) und visuelle Verifizierung. Die Wahrung des Hausrechts und die Vereitelung von Straftaten in privaten und öffentlich zugänglichen Zonen kann hier eine Begründung darstellen.

In privaten und öffentlich zugänglichen Teilen der Innenbereiche sind Kameras an den folgenden Stellen sinnvoll und gemäß DSGVO erlaubt bzw. nicht erlaubt:

5. Personal: Waschräume und Toiletten: Häufig gibt es Übergangsbereiche, in denen eine Unterscheidung von Angestellten und unautorisierten Personen schwierig aber notwendig ist (z.B. Zugänge zu Kundentoiletten/ Waschräumen). Der Schutz der Privatsphäre und die Wahrung des Hausrechts können hier im Widerspruch stehen. Trotzdem ist eine Überwachung nur in Ausnahmefällen erlaubt. In den Sanitärräumen selbst sind Kameras absolut tabu.

6. Büro: Befinden sich in einem Bürobereich wertvolle Dinge oder/und geschäftssensible Informationen, kann zusätzlich zur physischen Sicherung eine Videoüberwachung eingesetzt werden. Besonders außerhalb der Arbeitszeiten sieht man so, wer sich Zutritt zu den Räumlichkeiten verschafft. Auf die Persönlichkeitsrechte der Arbeitnehmer ist bei Ausrichtung der Kameras Rücksicht zu nehmen, etwaige Betriebsvereinbarungen sind zu beachten.

7. Lager: Im Warenlager sollten sich nur autorisierte Personen aufhalten. Es sollte nachvollziehbar sein, wer den Raum betreten, was er dort getan und wann er ihn wieder verlassen hat. Gerade bei direktem Zugang aus einem öffentlich zugänglichen Bereich heraus ist dies sinnvoll, um fremde Personen, die sich unautorisiert Zutritt verschafft haben, im Nachgang identifizieren zu können. Die permanente Überwachung stationärer Arbeitsplätze im Lager ist zu vermeiden.

8. Verkaufsräume: Da es sich um einen öffentlich zugänglichen Bereich handelt, kann jeder die Räumlichkeiten betreten. Unerwünschte Personen und Vorgänge im Verkaufsraum oder Überfälle sind aber denkbare Szenarien. Die Vorgänge an den Verkaufstheken oder vor den Regalen und Warenauslagen können im Fokus einer Kameraüberwachung stehen, um Manipulationen oder Diebstähle erfassen, erkennen und dokumentieren zu können. Außerhalb der Öffnungszeiten sollte sich im Verkaufsraum niemand aufhalten. Damit ändert sich unter Umständen der Fokus und damit die Begründung für die Überwachung.

9. Notausgänge, Zugang zu privaten Bereichen: Nicht nur außerhalb der Öffnungszeiten ist es wichtig, den Überblick über die eigenen Räumlichkeiten zu haben. Unerwünschte Personen oder auch das Personal nutzen gerne einmal Durchgänge, die nicht dafür gedacht sind, oder halten Türen (Notausgang/Brandschutz) geöffnet. Das kann auch zur Vorbereitung eines Einbruchs, Diebstahls oder einer anderen Straftat dienen.

73439/DE/R1/1912

Über Axis Communications

Axis ermöglicht eine smarte und sichere Welt durch die Entwicklung von Netzwerklösungen. Diese bieten Erkenntnisse, um die Sicherheit und Geschäftsmethoden zu verbessern. Als Technologieführer im Bereich Netzwerk-Video bietet Axis Produkte und Dienstleistungen für Videoüberwachung und -analyse sowie Zutrittskontrolle und Audiosysteme. Das 1984 gegründete schwedische Unternehmen beschäftigt mehr als 3.500 engagierte Mitarbeiter in über 50 Ländern. Gemeinsam mit seinen Partnern auf der ganzen Welt bietet das Unternehmen kundenspezifische Lösungen an.

Weitere Informationen über Axis finden Sie unter www.axis.com

AXIS COMMUNICATIONS