Brüssel, 17. März 2010

LEITLINIEN DES EUROPÄISCHEN DATENSCHUTZBEAUFTRAGTEN ZUR VIDEOÜBERWACHUNG

Inhalt

Vorwort

Die vorliegenden Leitlinien enthalten eine Reihe von praktischen Empfehlungen für Organe und Einrichtungen der Europäischen Union zu der Frage, wie sie ihre Videoüberwachungssysteme konzipieren und betreiben sollen. Sachgerecht konzipierte und selektiv eingesetzte Videoüberwachungssysteme sind leistungsstarke Werkzeuge zur Lösung von Sicherheitsproblemen. Schlecht ausgelegte Systeme dagegen vermitteln lediglich ein falsches Sicherheitsgefühl, dringen in unsere Privatsphäre ein und wirken sich negativ auf andere Grundrechte aus.

Grundrechte und Sicherheit müssen sich aber nicht gegenseitig ausschließen. Wenn Videoüberwachungssysteme pragmatisch auf der Basis der beiden Grundsätze der Selektivität und der Verhältnismäßigkeit eingesetzt werden, können sie den Sicherheitserfordernissen gerecht werden und zugleich unsere Privatsphäre achten. Kameras können und sollten intelligent und ausschließlich zur Lösung genau ermittelter Sicherheitsprobleme eingesetzt werden, um auf diese Weise das Zusammentragen von Bildmaterial, das nicht von Belang ist, auf ein Mindestmaß zu reduzieren. Damit werden nicht nur Eingriffe in die Privatsphäre auf ein Minimum reduziert, sondern es ist zugleich auch gewährleistet, dass die Videoüberwachung zielgerichteter und letztendlich auch effizienter eingesetzt werden kann.

Innerhalb der vom Datenschutzgesetz vorgegebenen Grenzen verfügt jedes Organ und jede Einrichtung über einen gewissen Ermessensspielraum bei der Konzeption seines bzw. ihres eigenen Systems. Zugleich muss jedes Organ auch nachweisen, dass es Verfahren zur Einhaltung der Datenschutzanforderungen eingerichtet hat. Zu den empfohlenen organisatorischen Verfahren gehören u. a. eine Reihe von Datenschutzgarantien, die in der Videoüberwachungsstrategie des Organs oder der Einrichtung beschrieben werden, sowie regelmäßige Audits zur Überprüfung der Vereinbarkeit.

In Fällen, in denen die Risiken der Verletzung von Grundrechten besonders hoch sind (etwa im Fall einer verdeckten Überwachung oder einer dynamisch-präventiven Überwachung), sollte auch eine datenschutzrechtliche Folgenabschätzung durchgeführt und dem EDSB zur Vorabkontrolle vorgelegt werden. Von diesen Ausnahmen einmal abgesehen ist es allerdings nicht notwendig, den EDSB in den Entscheidungsprozess über die Konzeption eines besonderen Systems eng einzubinden.

Datenschutz sollte nicht als eine vom Gesetz auferlegte Hürde, als „Compliance-Kästchen“ gesehen werden, das „abgehakt“ werden muss, sondern sollte vielmehr Teil einer Organisationskultur und einer gesunden Struktur der guten Verwaltungsführung sein, bei der die Leitung eines jeden Organs Entscheidungen auf der Grundlage der Ratschläge der entsprechenden Datenschutzbeauftragten und von Beratungen mit allen betroffenen Interessengruppen trifft.

Wir hoffen, dass Ihnen unsere Leitlinien bei Ihren Bemühungen um Vereinbarkeit eine Hilfestellung geben können.

(gezeichnet)

Giovanni Buttarelli
Stellvertretender Europäischer Datenschutzbeauftragter

1 Ziel der Leitlinien

Diese Leitlinien („**Leitlinien**“) wurden vom Europäischen Datenschutzbeauftragten („**EDSB**“) in Ausübung der ihm aufgrund von Artikel 47 der Verordnung Nr. 45/2001[1] zum Schutz personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft übertragenen Befugnisse („**Verordnung**“) erstellt.

Die Leitlinien sollen den Organen und Einrichtungen der Europäischen Union (vormals: der Europäischen Gemeinschaft) („**Organe**“)[2], die Videoüberwachungsausrüstungen betreiben, praktische Orientierungshilfen zu der Frage geben, wie sie die Verordnung einhalten und die Videoüberwachung verantwortungsvoll zusammen mit effizienten Schutzvorkehrungen einsetzen. Darin sind auch die Grundsätze bei der Beurteilung der Frage dargelegt, ob der Einsatz der Videoüberwachung tatsächlich notwendig ist, und es werden Handlungshilfen angeboten, wie Videoüberwachung so durchgeführt wird, dass die Auswirkungen auf die Privatsphäre und auf andere Grundrechte möglichst gering gehalten werden.

Die Leitlinien richten sich an diejenigen, die entscheiden, ob Videoüberwachungssysteme installiert werden, und die für ihren Betrieb zuständig sind (der Sprachenregelung des Datenschutzes zufolge werden diese Personen als „für die Verarbeitung Verantwortliche“ bezeichnet[3]). Darunter fallen typischerweise die Sicherheitsabteilungen der Organe, aber auch die oberste Leitung, die letztendlich für die Entscheidungsfindung zuständig ist. Darüber hinaus sollen die Leitlinien aber auch Lieferanten oder anderen Auftragnehmern, die bei der Installation und beim Betrieb behilflich sind (von denen einige als „**Auftragsverarbeiter**[4]“ fungieren), sowie den behördlichen Datenschutzbeauftragten der Organe („**DSB**“)[5], Personalvertretern und der Öffentlichkeit als Orientierungshilfe dienen.

Die Leitlinien sind keine endgültigen Gesetzesaussagen. Sie geben vielmehr Empfehlungen an die Hand und schlagen bewährte praktische Lösungen vor, während zugleich anerkannt wird, dass es Ausnahmen von der Regel geben könnte

---

[1] Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, ABl. L 8 vom 12.01.2001, S. 1.

[2] Seit Inkrafttreten des Lissabon-Vertrags haben sich die rechtlichen Rahmenbedingungen in der Europäischen Union erheblich geändert. Eine der auffälligsten Änderungen war die Abschaffung der Säulenstruktur und damit die Eingliederung der Politikbereiche der dritten Säule in den Bereich der ehemaligen ersten Säule. Diese Änderungen haben Folgen für die Arbeit des EDSB und werfen Fragen zum Geltungsbereich der bestehenden Datenschutzvorschriften für europäische Organe und Einrichtungen auf. Unbeschadet einer weiteren Auslegung oder einer möglichen Änderung von Artikel 3 Absatz 1 der Verordnung unterstützt und berät der EDSB bei Bedarf bereits heute alle Organe und empfiehlt ihnen die Einhaltung dieser Leitlinien.

[3] Siehe Artikel 2 Buchstabe d der Verordnung.

[4] Siehe Artikel 2 Buchstabe e der Verordnung.

[5] Siehe Artikel 24 der Verordnung.

und dass jedes Organ innerhalb der datenschutzrechtlichen Grenzen über einen gewissen Ermessensspielraum bei der Konzeption seines eigenen Systems verfügt. Die Leitlinien sind flexibel: sie sind so konzipiert, dass sie eine benutzerspezifische Anpassung ermöglichen. Mit dieser Flexibilität soll verhindert werden, dass eine starre oder bürokratische Auslegung von Datenschutzbelangen berechtigten Sicherheitserfordernissen oder anderen legitimen Zielen im Weg steht.

Vor diesem Hintergrund ist die Einhaltung der Empfehlungen häufig die effizienteste Art und Weise zur Einhaltung des Gesetzes. Damit werden aber auch die Effizienz und die Sicherheit der Systeme verbessert, und das Vertrauen der Mitarbeiter und der Öffentlichkeit in die Organisation wird gestärkt. Außerdem sind die Leitlinien mehr als nur eine unverbindliche Sammlung bewährter Verfahren. Denn sie enthalten eine maßgebliche Auslegung des Rechts durch den EDSB. Der EDSB wird der Vereinbarkeit mit den Leitlinien für den Fall, dass er von seinen Durchsetzungsbefugnissen Gebrauch macht, Rechnung tragen. Dies kann sich also darauf auswirken, ob ein Organ oder eine Einrichtung einer Kontrolle und anderen Durchsetzungsmaßnahmen unterzogen wird, einschließlich

- Ermahnung und Verwarnung,[6]
- Anordnung der Löschung von Daten,[7]
- Verbot der Verarbeitung[8] oder
- Befassung der „Hierarchie“ des Organs, des Parlaments, des Rates, der Kommission oder des Europäischen Gerichtshofs.[9]

2 Geltungsbereich der Leitlinien

2.1 Geltungsbereich

Die Leitlinien finden Anwendung auf eine Videoüberwachung, die von den Organen oder Einrichtungen oder einer anderen Partei in ihrem Auftrag für Zwecke durchgeführt wird, bei denen Kameras personenbezogene Daten gemäß Definition in der Verordnung erfassen.

Im Mittelpunkt der Leitlinien steht eine Videoüberwachung für typische Sicherheitszwecke einschließlich der Zugangskontrolle. Die Leitlinien gelten aber auch für

- komplexere oder spezifischere Sicherheitsmaßnahmen,
- eine Videoüberwachung bei internen Ermittlungen (unabhängig davon, ob

[6] Artikel 47 Absatz 1 Buchstabe d der Verordnung.

[7] Artikel 47 Absatz 1 Buchstabe e.

[8] Artikel 47 Absatz 1 Buchstabe f.

[9] Artikel 47 Absatz 1 Buchstabe g und h.

diese sicherheitsrelevant sind oder nicht) und
- eine Videoüberwachung für alle anderen Zwecke.

2.2 Ausschlüsse vom Geltungsbereich

Die Leitlinien gelten nicht für

- Videoanrufe und Videokonferenzen,
- videoüberwachte Eingänge ohne Aufzeichnung,[10]
- Kameras, die für künstlerische oder journalistische Zwecke eingesetzt werden (etwa für das Filmschaffen oder für die Aufzeichnung oder Ausstrahlung von aktuellen Veranstaltungen),[11]
- Kameras, die für wissenschaftliche Zwecke in kontrollierten Laborumgebungen eingesetzt werden, sofern sie lediglich Prozesse (z. B. physikalische oder chemische Prozesse) und keine Menschen überwachen,
- die Aufzeichnung oder Ausstrahlung von Veranstaltungen wie Konferenzen, Seminare, Sitzungen oder Schulungsmaßnahmen für Dokumentations-, Fortbildungs- oder ähnliche Zwecke und
- die Aufzeichnung oder Übertragung von Sitzungen der Entscheidungsorgane der EU im Hinblick auf eine verstärkte Transparenz (z. B. Live-Übertragungen der Plenarsitzungen des Europäischen Parlaments).

Diese und weitere potenzielle Einsatzmöglichkeiten fallen zwar möglicherweise in den Geltungsbereich der Verordnung und erfordern damit entsprechende Datenschutzvorkehrungen, werden jedoch in diesen Leitlinien nicht näher erörtert. Die erforderliche Einhaltung muss daher von den Organen in jedem einzelnen Fall geklärt werden.

2.3 Erläuterungen zum Geltungsbereich

2.3.1. Erstrecken sich die Leitlinien auf andere Systeme als Videokameraüberwachungssysteme („CCTV-Systeme“)?

Für die Zwecke dieser Leitlinien wird der Begriff Videoüberwachung definiert als die Überwachung eines bestimmten Bereichs, einer bestimmten Veranstaltung, Aktivität oder Person mithilfe eines elektronischen Geräts oder Systems zur visuellen Überwachung. Typischerweise betreiben die Organe sogenannte CCTV-Systeme,

---

[10] Darunter verstehen wir ein einfaches System, mit dessen Hilfe ein Rezeptionist oder Sicherheitsbediensteter ferngesteuert eine geschlossene Tür (z. B. Haupteingang oder Garagentor) öffnen und Besucher einlassen kann, die keine Zutrittsausweise für einen automatischen Zugang besitzen. Das System wird von den Besuchern selbst beim „Klingeln“ aktiviert. Diese Ausnahmeregelung sollte im engen Sinne ausgelegt werden und nicht auf komplexere Systeme oder auf Systeme Anwendung finden, bei denen sich die Besucher auch dann, wenn die Systeme nichts aufzeichnen, im Erfassungsbereich von Sicherheitskameras befinden, ohne dass sie selbst den Kontakt auslösen. Dem steht das in Punkt 2.3.4 genannte Beispiel gegenüber.

[11] Die Leitlinien finden jedoch Anwendung auf die Übertragung von Bildmaterial aus der Videoüberwachung, das für einen anderen Zweck erhoben wurde, an die Medien. Ein allgemeiner Rahmen für Übertragungen ist in Abschnitt 10 beschrieben.

dies bedeutet „Videoüberwachungssysteme“ („closed circuit television systems“), einschließlich einer Reihe von Kameras zur Überwachung eines bestimmten geschützten Bereichs und zusätzlicher Geräte für die Übertragung, Betrachtung und/oder Speicherung und Weiterverarbeitung des Bildmaterials aus der Videoüberwachung. Doch auch die Verwendung anderer fester oder transportabler elektronischer Geräte oder Systeme fällt in den Geltungsbereich der Leitlinien, sofern diese in der Lage sind, Bilddaten zu erfassen. Beispiele hierfür sind tragbare Videokameras, Kameras, die Standbilder aufnehmen, Webcams, Infrarotkameras und Wärmeerkennungsgeräte.

2.3.2. Was sind personenbezogene Daten?

Der Begriff personenbezogene Daten wird in der Verordnung definiert als „alle Informationen über eine bestimmte oder bestimmbare natürliche Person“. In der Verordnung heißt es weiter: „als bestimmbar wird eine Person angesehen, die direkt *oder indirekt* identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind.“[12] Was bedeutet dies in der Praxis?

Zunächst sind erkennbare Gesichtsbilder immer personenbezogene Daten. Dies gilt selbst dann, wenn die Personen den Betreibern des Systems nicht bekannt oder von ihnen nicht bestimmbar sind.

Beispiel:

Ihr Organ oder Ihre Einrichtung installiert Videokameras zur Überwachung eines verschlossenen Archivraums in der Nacht und an Wochenenden, um erkennbare Gesichtsbilder zu erfassen und Unbefugte zu identifizieren. Die Leitlinien gelten auch dann, wenn Sie lediglich die Bilder aufzeichnen, sich jedoch die Aufzeichnungen niemals ansehen.

Häufig müssen jedoch noch nicht einmal erkennbare Gesichtsbilder erfasst werden, damit die Leitlinien Anwendung finden. Auch bei weniger deutlichen Bildern einer Person kann es sich um personenbezogene Daten handeln, sofern die Personen direkt oder indirekt (zusammen mit anderen Informationen) identifiziert werden können. Ob eine Person als indirekt bestimmbar angesehen werden kann, hängt von den jeweiligen Umständen ab, einschließlich der Zweckbestimmung der Videoüberwachung und der Wahrscheinlichkeit, dass das Organ (oder andere potenzielle Empfänger) in der Lage ist, alle erforderlichen Anstrengungen zu unternehmen, um die von der Kamera erfassten Personen zu erkennen.

[12] Siehe Artikel 2 Buchstabe a der Verordnung und Stellungnahme 4/2007 der Artikel-29-Datenschutzgruppe zum Begriff „personenbezogene Daten“, Seite 16 und 21.

Beispiel:

Auf dem Dach eines Gebäudes werden Kameras mit begrenzter Auflösung zur Überwachung der Umgebung zu Sicherheitszwecken bei besonderen Veranstaltungen angebracht. Auch wenn die Kameraaufnahmen nicht unbedingt immer erkennbare Gesichtsbilder liefern, ist die Polizei, die eine schwere Straftat untersucht, möglicherweise in der Lage, die von den Kameras erfassten Personen indirekt anhand von Informationen aus dem Bildmaterial (beispielsweise Kleidung, Figur, mitgeführte Gegenstände) zusammen mit anderen Informationen, die während der Ermittlungen festgestellt werden (zum Beispiel mithilfe von Zeugen oder anhand anderer Bildaufnahmen), zu identifizieren. Unter solchen Umständen finden die Leitlinien Anwendung.

Des Weiteren gilt auch Bildmaterial, auf dem Gegenstände zu sehen sind, die mit einer bestimmten Person in Verbindung gebracht werden können, als personenbezogene Daten, je nach den spezifischen Umständen des Falls.

Beispiel:

Ein Videokameraüberwachungssystem (CCTV), das Kfz-Kennzeichen überwacht, ist an eine Datenbank mit Daten über Kfz-Kennzeichen angeschlossen. Es ist außerdem mit Software ausgestattet, die Kennzeichen lesen und diese mit den Personen abgleichen kann, in deren Namen das Fahrzeug angemeldet ist. Dieses System fällt auch dann in den Geltungsbereich der Leitlinien, wenn keine Personen, sondern nur Kfz-Kennzeichen aufgenommen werden.

Und schließlich gelten die Leitlinien auch dann, wenn ein Organ nicht beabsichtigt, Aufnahmen zu machen, die zur Erkennung der aufgenommenen Personen führen, sofern die bestimmbaren Personen tatsächlich von den Kameras erfasst werden.

Beispiel:

Zu Werbezwecken wird an einem Urlaubsort eine Webcam installiert. Die Leitlinien gelten, selbst wenn der Betreiber der Kamera nicht die Absicht hatte, die von den Kameras aufgezeichneten Personen zu identifizieren.

2.3.3. Fallen nur ständige Videoüberwachungssysteme in den Geltungsbereich der Leitlinien?

Nein, die Leitlinien gelten auch dann, wenn die Kameras nur auf einer Ad-hoc-Basis verwendet werden.

Beispiel:

Nach wiederholten Diebstählen wird am Eingang eines zuvor nicht überwachten Lagerraums für einen begrenzten Zeitraum (eine Woche) eine Videokamera angebracht, die Diebe abschrecken oder untersuchen soll, ob trotz der angebrachten Kameras weiter gestohlen wird. Trotz ihres vorübergehenden und Ad-hoc-Charakters fällt die Videoüberwachung in den Geltungsbereich der Leitlinien.

2.3.4. Gelten die Leitlinien auch dann, wenn kein Bildmaterial aufgezeichnet wird?

Ja, die Live-Videoüberwachung oder Live-Videoübertragung fällt ebenfalls in den Geltungsbereich der Verordnung und der Leitlinien.

Beispiel:

Sicherheitskameras überwachen Ausgänge und Eingänge eines Gebäudes: Das Bildmaterial wird nicht aufgezeichnet, sondern vom Sicherheitspersonal in einem Kontrollraum oder im Empfangsbereich des Gebäudes angesehen. Die Leitlinien finden Anwendung.

Tatsächlich können Risiken für das Recht auf Privatsphäre und für die Sicherheit auch dann auftreten, wenn kein Bildmaterial aufgezeichnet und dieses Bildmaterial lediglich live über ein internes Netzwerk an die dafür vorgesehenen Empfänger übertragen wird. Zu den Risiken gehört beispielsweise die Tatsache, dass die Bilder von Hackern abgefangen oder auch von einem der Empfänger aufgezeichnet und später für unzulässige Zwecke verwendet werden könnten. Wichtig in diesem Zusammenhang ist, dass die Verletzung der Privatsphäre und die Auswirkungen auf das Verhalten der Menschen, die beobachtet werden, häufig mit der Verletzung der Privatsphäre durch Aufzeichnungen und mit den damit verbundenen Auswirkungen vergleichbar sind. Im Allgemeinen nehmen die Risiken für die Privatsphäre und den Datenschutz mit steigender Zahl der Empfänger zu und sind dann besonders groß, wenn das Videomaterial ins Internet gestellt wird.

2.3.5. Was geschieht, wenn die Überwachung von einem ausgegliederten Unternehmen durchgeführt wird?

Auch wenn ein Organ seine Videoüberwachungsaktivitäten ganz oder teilweise an Dritte (ein „**Auftragsverarbeiter**“) fremdvergibt, haftet es nach wie vor für die Einhaltung der Verordnung als „für die Verarbeitung Verantwortlicher“.

Beispiel:

Die Sicherheitsbediensteten, die im Empfangsbereich eines Organs live Videoaufnahmen überwachen, arbeiten für ein Privatunternehmen, an welches das

Organ die Live-Überwachung fremdvergeben hat. In diesem Fall muss das Organ gewährleisten, dass die Sicherheitsbediensteten ihre Aufgaben im Einklang mit der Verordnung und den Leitlinien wahrnehmen.

Weitere Handlungsempfehlungen für die Fremdvergabe sind in Abschnitt 14.1 zu finden.

3 „Privacy by design“ (eingebauter Datenschutz)

3.1 Einbau des Datenschutzes bei der Konzeption eines Systems

In die Spezifikationen für die Konzeption der von den Organen eingesetzten Technologie sowie in ihre organisatorischen Verfahren[13] sollten auch Datenschutzgarantien und Vorkehrungen zum Schutz der Privatsphäre eingebaut werden.

3.2 Frühzeitige Klärung datenschutzrechtlicher Fragen

Bei der Installation oder Aufrüstung eines Videoüberwachungssystems sollte mit Unterstützung des behördlichen Datenschutzbeauftragten eine erste Datenschutzbewertung durchgeführt werden, und zwar weit im Vorfeld einer Ausschreibung für Neuanschaffungen bzw. des Eingehens finanzieller Verpflichtungen. Damit lassen sich kostspielige Fehler vermeiden.

Beispiel:

Als Leiter der Sicherheitsabteilung Ihres Organs erkennen Sie die Notwendigkeit, das vorhandene Videoüberwachungssystem aufzurüsten, was die Anschaffung und Installation zusätzlicher Kameras und neuer Software erforderlich macht. Es ist wichtig, dass Sie frühzeitig zumindest eine vorläufige Analyse durchführen, was nicht nur dazu führen könnte, dass besondere Datenschutzgarantien verabschiedet werden, sondern auch, dass das Leistungsverzeichnis für die Lieferanten geändert wird. Möglicherweise lässt sich damit sogar der Umfang der vorgeschlagenen Investitionen reduzieren.

3.3 Folgenabschätzung

Der EDSB empfiehlt vor der Installation und Implementierung von

[13] Stellungnahme 168 der Artikel-29-Datenschutzgruppe vom 1. Dezember 2009 zur Zukunft des Schutzes der Privatsphäre, gemeinsamer Beitrag der Artikel-29-Datenschutzgruppe und der Arbeitsgruppe Polizei und Justiz zu der Konsultation der Europäischen Kommission zu dem Rechtsrahmen für das Grundrecht auf den Schutz der personenbezogenen Daten. Siehe insbesondere Kapitel 4.

Videoüberwachungssystemen immer dann die Durchführung einer datenschutzrechtlichen Folgenabschätzung, wenn dies für die Bemühungen des Organs um Vereinbarkeit mit einem zusätzlichen Nutzen verbunden ist.[14] Mit dieser Folgenabschätzung soll ermittelt werden, welche Auswirkungen das vorgeschlagene System auf das Recht auf Privatsphäre und andere Grundrechte der betroffenen Personen hat und wie nachteilige Auswirkungen gemindert oder ganz vermieden werden können.

Es hängt von den jeweiligen Umständen ab, welcher Aufwand in eine Folgenabschätzung investiert wird. Ein Videoüberwachungssystem mit den damit verbundenen erheblichen Risiken oder ein System, das komplizierte oder neuartige Probleme aufwirft, rechtfertigt einen viel größeren Aufwand als ein System mit vergleichsweise begrenzten Auswirkungen auf das Recht auf Privatsphäre und andere Grundrechte, wie etwa ein konventionelles statisches Videokameraüberwachungssystem (CCTV-System), das für typische Sicherheitszwecke betrieben wird, für die in den Leitlinien bereits angemessene Schutzvorkehrungen vorgesehen sind.

Jedenfalls müssen die Organe in allen Fällen, unabhängig davon, ob es sich um eine offizielle Folgenabschätzung oder um etwas anderes handelt, prüfen und begründen, ob und weshalb sie eine Videoüberwachung in Anspruch nehmen wollen, wie sie den Standort für ihre Systeme bestimmen, wie sie diese Systeme auswählen und konfigurieren und wie die in den Leitlinien vorgeschlagenen Datenschutzvorkehrungen umgesetzt werden sollen.

Darüber hinaus sind aber auch Fälle denkbar, in denen ein Organ ein nicht handelsübliches System vorschlägt. In einem solchen Fall sollte das Organ sorgfältig die geplanten Abweichungen von den in den Leitlinien dargelegten üblichen Verfahren und Empfehlungen prüfen, diese mit seinem behördlichen Datenschutzbeauftragten und anderen Akteuren besprechen und diese Prüfung schriftlich dokumentieren, entweder in Form einer offiziellen Folgenabschätzung oder auf anderem Weg. Bei der Prüfung des Systems durch das Organ (siehe Abschnitt 13) sollte man sich auch mit der Frage befassen, ob die benutzerspezifische Anpassung des Systems rechtmäßig ist.

Und schließlich empfiehlt der EDSB aufgrund der Komplexität, der Neuartigkeit, der Besonderheit oder der inhärenten Risiken dringend die Durchführung einer Folgenabschätzung in folgenden Fällen:

- Videoüberwachung zu anderen als Sicherheitszwecken (einschließlich zu Ermittlungszwecken, siehe Abschnitt 5.8),
- Überwachung von Mitarbeitern (Abschnitt 5.9),
- Webcams (Abschnitt 5.10),
- Überwachung im Hoheitsgebiet der Mitgliedstaaten und in Drittländern

[14] Für Systeme, die zum Zeitpunkt des Inkrafttretens dieser Leitlinien bereits in Betrieb sind, sollte die Folgenabschätzung rückwirkend erfolgen. Nähere Angaben zu den Übergangsbestimmungen und zur Frage, wie die Vereinbarkeit für bereits in Betrieb befindliche Systeme gewährleistet werden kann, siehe Abschnitt 15.

(Abschnitte 6.5-6.6),
- besondere Datenkategorien (Abschnitt 6.7),
- Bereiche, in denen verstärkte Erwartungen an den Schutz der Privatsphäre gestellt werden (Abschnitt 6.8),
- Hightech- und/oder intelligente Videoüberwachung (Abschnitt 6.9),
- Verbundsysteme (Abschnitt 6.10),
- verdeckte Überwachung (Abschnitt 6.11),
- Tonaufzeichnungen und Videokameras mit Lautsprechern („talking CCTV“) (Abschnitt 6.12).

Die Folgenabschätzung kann entweder intern oder durch einen unabhängigen Auftragnehmer durchgeführt werden. Sie sollte in einem Frühstadium des Projekts stattfinden. Aufgrund der Ergebnisse der Folgenabschätzung kann ein Organ beschließen,

- auf die geplante Überwachung zu verzichten oder diese abzuändern und/oder
- zusätzliche Schutzvorkehrungen zu ergreifen, die über die in diesen Leitlinien genannten hinausgehen.

Die Folgenabschätzung sollte hinreichend dokumentiert werden. Grundsätzlich sollte ein Bericht zur Folgenabschätzung klar auf die Risiken für das Recht auf Privatsphäre und/oder andere Grundrechte, die von dem Organ aufgezeigt wurden, sowie auf die vorgeschlagenen zusätzlichen Schutzvorkehrungen hinweisen.

Beispiel:

Ihr Organ zieht die Installation eines komplexen dynamisch-präventiven Videoüberwachungssystems in Betracht. Möglicherweise ist dies nur dann zulässig, wenn das Organ eine umfassende datenschutzrechtliche Folgenabschätzung durchführt (und alle anderen Schutzvorkehrungen eingehalten werden, die in diesen Leitlinien dargelegt werden bzw. vom EDSB im Rahmen eines Vorabkontrollverfahrens empfohlen wurden).

3.4 Einsatz einer „privatsphärenfreundlichen“ Technologie

Nach Möglichkeit sollten technologische Lösungen gewählt werden, die der Privatsphäre förderlich sind. Auftragnehmer sollten bei der Bestellung des Systems und der Erstellung des Leistungsverzeichnisses aufgefordert werden, solche Lösungen anzubieten, und es sollten ihnen entsprechende Anreize angeboten werden.

Beispiele:

- Durch Verschlüsselung der Daten lassen sich potenzielle Schäden im Fall eines unbefugten Zugriffs auf die Bilder reduzieren. Siehe hierzu auch Abschnitt 9.
- Durch das Maskieren oder Verwürfeln von Bildern kann die Überwachung

bestimmter Bereiche, die für Ihr Überwachungsziel nicht von Belang sind, ausgeschaltet werden. Diese Technik ist auch dann von Nutzen, wenn bei der Gewährung des Zugriffs auf die Bilder eines Betroffenen die Bilder von Dritten herausredigiert werden sollen. Zum Nutzen dieser Technik zum Schutz von Gesichtsbildern oder von Informationen zu Kfz-Kennzeichen bei Einsatz einer Webcam siehe Abschnitt 5.10.

3.5 Vorausplanung einer Ad-hoc-Überwachung

Und schließlich wird auch eine Vorausplanung für den Fall empfohlen, dass ein Organ den Einsatz der Videoüberwachung auf Ad-hoc-Basis plant (etwa dann, wenn hochkarätige Veranstaltungen ausgerichtet werden, oder bei internen Ermittlungen). In diesem Fall sollten der notwendige Rahmen und die erforderlichen Datenschutzstrategien mit einem ausreichenden zeitlichen Vorlauf vor Einsatz der Videoüberwachung an sich festgelegt werden.

Beispiele:

- *Ihr Organ richtet regelmäßig hochkarätige Veranstaltungen wie z. B. Zusammenkünfte von Staats- und Regierungschefs mit erhöhten Sicherheitserfordernissen aus.*
- *Sie können absehen, dass von Zeit zu Zeit bei internen Ermittlungen Kameras an bestimmten Stellen für einen begrenzten Zeitraum auf Ad-hoc-Basis installiert und eingesetzt werden müssen.*

4 Wer sollte zu dem neuen System angehört werden?

Die Anhörung und Rücksprache mit den Akteuren und zuständigen Behörden ist von maßgeblicher Bedeutung, um alle wichtigen Anliegen und Belange des Datenschutzes zu ermitteln. Bei der Entscheidung, ob eine Videoüberwachung in Anspruch genommen und die erforderlichen Rahmenbedingungen und Strategien für den Datenschutz festgelegt werden sollen, müssen möglicherweise einige oder alle der nachstehend aufgeführten Personen oder Organisationen hinzugezogen werden:

- der behördliche Datenschutzbeauftragte des Organs,
- Personalvertreter,
- andere Akteure (in manchen Fällen einschließlich der Kommunalbehörden),
- der EDSB und
- nationale (oder regionale) Datenschutzbehörden.

4.1 Behördlicher Datenschutzbeauftragter

Zuallererst sollten Pläne zur Installation oder Aufrüstung eines Videoüberwachungssystems dem behördlichen Datenschutzbeauftragten des Organs mitgeteilt werden. Dieser sollte in allen Fällen angehört und in alle Phasen der Entscheidungsfindung einbezogen werden.

Beispiele:

- *Der behördliche Datenschutzbeauftragte sollte einbezogen werden, wenn erstmals entschieden wird, ob die Videoüberwachungstechnologie gemäß Abschnitt 3.2 zum Einsatz gelangen soll.*
- *Der behördliche Datenschutzbeauftragte sollte als fachkundiger Berater bei der Entwicklung von datenschutzfreundlichen Verfahren hinzugezogen werden.*
- *Er sollte ebenfalls hinzugezogen werden, um eine Stellungnahme zum Entwurf der Videoüberwachungsstrategie (einschließlich Anlagen) des Organs abzugeben, Fehler zu berichtigen und Verbesserungsvorschläge zu unterbreiten.*
- *Ferner sollte er auch für Mitteilungen an den EDSB und die nationalen (oder regionalen) Datenschutzbehörden hinzugezogen werden.*

4.2 Mitarbeiter und andere Akteure

Der EDSB empfiehlt dringend, das Personal in allen Fällen anzuhören, in denen Videoaufnahmen von Mitarbeitern gemacht werden könnten. Eine solche Anhörung wird auch dann empfohlen, wenn der Zweck der Verarbeitung nicht die Überwachung oder Beurteilung der Leistung der Mitarbeiter ist. Eine Anhörung ist gleichfalls zwingend erforderlich, wenn dies aufgrund des anwendbaren Rechts gesetzlich vorgeschrieben ist. Die Mitarbeiter können typischerweise über die Personalausschüsse der Organe angehört werden; andere Formen (etwa öffentliche Anhörungen und Workshops) können jedoch ebenso wirksam sein.

Beispiel:

Das Personal sollte auch dann angehört werden, wenn der Zweck der Datenverarbeitung der Sicherheit und Zugangskontrolle dient und die Kameras nur an den Eingängen und Ausgängen der Gebäude und anderer strategisch wichtiger Räumlichkeiten wie z. B. Archive installiert werden.

Anhörung bedeutet nicht, dass die Leitung des Organs auf alle Fälle eine Einigung mit den Personalvertretern in Bezug auf das Ausmaß der Überwachung herbeiführen muss. Der EDSB hält jedoch eine echte Anhörung für eine besonders wichtige Schutzvorkehrung, damit sichergestellt ist, dass die installierte Videoüberwachung die Privatsphäre nicht stärker verletzt als unbedingt nötig und dass angemessene Schutzvorkehrungen getroffen werden, um eine Gefährdung der Privatsphäre und anderer schutzwürdiger Interessen und Grundrechte auf ein Mindestmaß zu reduzieren.

Für den Fall, dass aufgrund des Standortes oder der Besonderheit der Videoüberwachung weitere Akteure anwesend sind, sollte das Organ dafür Sorge tragen, dass diese Akteure bzw. ihre Vertreter ebenfalls so umfassend wie möglich

angehört werden. Dies umfasst auch die Anhörung von Kommunalverwaltungen, der Polizei oder anderer Behörden in den in den Abschnitten 6.5 und 6.6 genannten Fällen.

Beispiel:

Eltern sollten auch dann angehört werden, wenn sich die Videoüberwachung auch auf Kinderbetreuungseinrichtungen Ihres Organs erstreckt.

4.3 Vorabkontrolle durch den EDSB

In manchen Fällen muss der behördliche Datenschutzbeauftragte des Organs dem EDSB eine Vorabkontrollmeldung vorlegen.[15] Mit diesem Verfahren soll das Organ bei der Einführung zusätzlicher Datenschutzvorkehrungen in Fällen unterstützt werden, in denen seine Aktivitäten über die üblichen Vorgänge hinausgehen, für welche in den Leitlinien bereits ausreichende Schutzgarantien vorgesehen sind. Bei den Vorabkontrollverfahren kann auch die Einhaltung der Empfehlungen in diesen Leitlinien durch das Organ überprüft werden.

Der EDSB hält derzeit eine Vorabkontrollmeldung in folgenden Fällen für erforderlich:

- Videoüberwachung zu Ermittlungszwecken (Abschnitt 5.8),
- Überwachung von Mitarbeitern (Abschnitt 5.9),
- Verarbeitung besonderer Datenkategorien (Abschnitt 6.7),
- Überwachung von Bereichen, in denen verstärkte Erwartungen an den Schutz der Privatsphäre gestellt werden (Abschnitt 6.8),
- Hightech- und/oder intelligente Videoüberwachung (Abschnitt 6.9),
- Verbundsysteme (Abschnitt 6.10),
- verdeckte Überwachung (Abschnitt 6.11),
- Tonaufzeichnungen und Videokameras mit Lautsprechern („talking CCTV“) (Abschnitt 6.12).

Der Meldung sind auch der Bericht zur Folgenabschätzung (oder sonstige sachdienliche Unterlagen zur Folgenabschätzung), die Videoüberwachungsstrategie und der Auditbericht (siehe Abschnitt 13) beizufügen.

4.4 Nationale Datenschutzbehörden

Es gelten die Bestimmungen der Verordnung[16], und der EDSB ist für die Überwachung der gesamten durch oder im Namen der Organe durchgeführten

[15] Siehe Artikel 27 der Verordnung, wo es heißt: „Verarbeitungen, die aufgrund ihres Charakters, ihrer Tragweite oder ihrer Zweckbestimmungen besondere Risiken für die Rechte und Freiheiten der betroffenen Personen beinhalten können, werden vom Europäischen Datenschutzbeauftragten vorab kontrolliert.“

[16] Siehe Artikel 3 Absatz 1 und Artikel 41 Absatz 2 der Verordnung.

Videoüberwachung zuständig, unabhängig davon, ob dabei Bilder innerhalb oder außerhalb der Gebäude der Organe aufgenommen werden. Die Datenschutzbehörden des Mitgliedstaats, in dem das Organ seinen Sitz hat, haben also möglicherweise ein Interesse an einer Überwachung, die außerhalb der Gebäude stattfindet. In diesem Fall ist die Anwendbarkeit des nationalen Datenschutzgesetzes durch die Vorrechte und Befreiungen der Organe gemäß Artikel 291 EG-Vertrag und Protokoll (Nr. 36) über die Vorrechte und Befreiungen der Europäischen Gemeinschaften (1965)[17] eingeschränkt. Der EDSB wird bei Bedarf mit den Datenschutzbehörden in den Mitgliedstaaten zusammenarbeiten.[18]

In Abschnitt 6.5 wird eine Reihe von Empfehlungen abgegeben, um die Überwachung im Hoheitsgebiet der Mitgliedstaaten auf ein Mindestmaß zu reduzieren. Diese Empfehlungen sollten bewährte Verfahren zum Datenschutz fördern, zugleich jedoch auch Doppelarbeit sowie die Unsicherheit verhindern oder minimieren, die sich aus der gleichzeitigen Anwendbarkeit von zwei Datenschutzregelungen sowie dem zeitgleichen Tätigwerden von zwei Überwachungsbehörden ergeben.

Neben diesen äußerst wichtigen Empfehlungen empfiehlt der EDSB aus verfahrensrechtlichen Gründen den Organen außerdem, dass sie der nationalen Datenschutzbehörde (und/oder gegebenenfalls der regionalen oder lokalen Datenschutzbehörde) zumindest ein kurzes Schreiben während des vorläufigen Konsultationsprozesses zukommen lassen. In diesem Schreiben sollte das Organ die Behörde davon in Kenntnis setzen, dass es in seinen Gebäuden aus Sicherheitsgründen und zum Zweck der Zugangskontrolle ein Videoüberwachungssystem betreibt und das System auch in der Nähe der Gebäude Aufnahmen macht. In dem Schreiben sollte bestätigt werden, dass diese Verfahren im Einklang mit diesen Leitlinien und der Verordnung stehen und dem EDSB in seiner Funktion als Kontrollinstanz vorgelegt wurden (und gegebenenfalls durch den EDSB vorab kontrolliert werden). Eine Ausfertigung bzw. ein Link zu den Leitlinien sollte ebenfalls beigefügt werden. Falls die nationale Datenschutzbehörde weitere Angaben wünscht, sollte das Organ vertrauensvoll mit ihr zusammenarbeiten. Im Interesse einer guten Praxis kann die abschließende Stellungnahme zur Vorabkontrolle des EDSB ebenfalls der zuständigen Datenschutzbehörde übermittelt werden.

5 Entscheidung darüber, ob eine Videoüberwachung eingesetzt werden soll oder nicht

Die Entscheidung über den Einsatz von Videoüberwachungssystemen sollte nicht leichtfertig getroffen werden und setzt eine sorgfältige Prüfung der potenziellen Vorteile und der Auswirkungen auf das Recht auf Privatsphäre und andere

[17] Amtsblatt C 321E vom 29.12.2006, S. 318-324. Es wird darauf hingewiesen, dass es in einigen der sogenannten „Sitzabkommen“ zwischen den Organen und ihren Gastländern konkret heißt, dass die nationalen Datenschutzgesetze nicht für das Organ gelten. Dies ist beispielsweise bei der Europäischen Zentralbank der Fall.

[18] Siehe Artikel 28 Absatz 6 der Richtlinie und Artikel 46 Buchstabe f der Verordnung.

Grundrechte und legitimen Interessen derjenigen voraus, die sich im Erfassungsbereich des Videoüberwachungssystems befinden. Die Entscheidung sollte nach Möglichkeit schriftlich dokumentiert und mithilfe von Nachweisen wie statistischen Daten zur genauen Zahl der eingetretenen Sicherheitsvorfälle sowie zur Effizienz von in der Vergangenheit eingesetzten Kameras bei der Abwehr, Verhütung, Ermittlung oder Verfolgung solcher Vorfälle hinlänglich belegt werden. Während des Audits (siehe Abschnitt 13) sollte überprüft und bewertet werden, ob eine schriftliche Begründung des Einsatzes und der Angemessenheit der Videoüberwachung vorliegt und angemessen ist.

Diese Analyse muss jedoch nicht unbedingt umfangreich oder zeitaufwändig sein. Der Umfang der Prüfung richtet sich nach der Größe des vorgeschlagenen Systems und dessen voraussichtlichen Auswirkungen auf die Privatsphäre von Menschen und auf andere legitime Interessen oder Grundrechte. Die Organe müssen sich dabei mit folgenden Fragen befassen:

- Welche Vorteile sind mit der Videoüberwachung verbunden und überwiegen sie die Nachteile?
- Ist der Zweck des Systems eindeutig und genau beschrieben und rechtmäßig? Gibt es für die Videoüberwachung eine rechtmäßige Begründung?
- Wird die Notwendigkeit des Einsatzes der Videoüberwachung eindeutig nachgewiesen? Ist sie ein wirksames Werkzeug zur Erreichung des Verwendungszwecks oder gibt es Alternativen, die weniger stark in die Privatsphäre eingreifen?

Mithilfe der in diesem Dokument angebotenen Handlungshilfen können die Organe besser entscheiden, ob die Videoüberwachung tatsächlich ein geeignetes Werkzeug darstellt. Für bereits vorhandene Systeme[19] werden viele Organe möglicherweise feststellen, dass sie lediglich deutlicher und transparenter vorgehen müssen, und ihre bereits bestehenden bewährten Verfahren schriftlich bestätigen.

5.1 Zweckbestimmung des Systems

Bevor das Organ beschließt, ein neues System zu installieren, muss es zunächst die Zweckbestimmung der Videoüberwachung festlegen und sicherstellen, dass diese Zweckbestimmung rechtmäßig ist.[20]

5.1.1 Drücken Sie sich klar, konkret und genau aus. Vage, zweideutige oder ganz einfach zu allgemein gefasste Beschreibungen reichen nicht aus. Wenn Organe den Zweck der Videoüberwachung konkret beschreiben, kann ihnen dies bei der Einhaltung des Gesetzes, der Bewertung des Erfolgs ihres Systems und der Erklärung der Notwendigkeit eines solchen Systems gegenüber ihren Mitarbeitern und der Öffentlichkeit behilflich sein.

---

[19] Siehe Abschnitt 15 „Übergangsbestimmungen“.

[20] Siehe Artikel 4 Buchstabe b der Verordnung.

5.1.2. Information der Öffentlichkeit über den Zweck. Die Zweckbestimmungen des Systems müssen der Öffentlichkeit in Form eines kurzen Überblicks sofort und dann ausführlicher beispielsweise über die öffentliche Online-Fassung der Videoüberwachungsstrategie des Organs[21] mitgeteilt werden.

5.1.3. Zweckentfremdung und schleichende Funktionsübertretung.[22] Die Grenzen bei der Verwendung der Daten müssen klar festgelegt werden, insbesondere dann, wenn dies von Personalvertretern oder anderen Interessengruppen gefordert wird.

Ferner muss gewährleistet sein, dass die Daten später nicht für unvorhergesehene Zwecke verwendet oder unvorhergesehenen Empfängern gegenüber offengelegt werden, die sie zu weiteren, mit dem eigentlichen Zweck nicht zu vereinbarenden Zwecken verwenden („**schleichende Funktionsübertretung**"). Zu den mit dem ursprünglichen Zweck nicht zu vereinbarenden Zweckbestimmungen gehören nicht nur neue Zweckbestimmungen, die in keinem Verhältnis zum ursprünglichen Zweck stehen, sondern auch alle Zweckbestimmungen, die von der überwachten Person berechtigterweise nicht erwartet werden. Eine weiter gefasste Definition des Zwecks auf hohem Niveau ist keine Begründung für eine weitere Nutzung der Daten zu nicht näher bezeichneten Zwecken.

Beispiel:

Wenn ein Videoüberwachungssystem zu Sicherheitszwecken installiert wird und den Mitarbeitern auch als solches angekündigt wurde, sollten die Aufzeichnungen nicht dazu verwendet werden, zu beurteilen, wie gut die Mitarbeiter ihre Arbeit erledigen oder ob sie rechtzeitig zur Arbeit kommen. Sie sollten auch nicht zu Ermittlungszwecken oder als Beweismittel bei internen Untersuchungen oder Disziplinarverfahren herangezogen werden, es sei denn, es handelt sich um einen physischen Sicherheitsvorfall oder in Ausnahmefällen auch um strafbares Verhalten.

5.2 Gibt es eine rechtmäßige Begründung für die Videoüberwachung?[23]

Für den Fall, dass ein Organ die Videoüberwachung für typische Sicherheits- und Zugangskontrollzwecke nutzt, kann diese für die Verwaltung und das Funktionieren

[21] Weitere Handlungshilfen zu der Frage, wie die Öffentlichkeit informiert werden kann, siehe Abschnitt 11 und Anhang 1 und 2.

[22] Siehe Artikel 4 Buchstabe b der Verordnung über einen Zweck, der mit den ursprünglichen Zwecken nicht zu vereinbaren ist.

[23] Siehe Artikel 5 der Verordnung.

dieser Organe als *potenziell* erforderlich erachtet werden. Für das Videoüberwachungssystem muss daher nach Maßgabe der Verordnung eine rechtmäßige Begründung vorliegen.[24]

Trifft dies nicht zu, dann stellt sich die Frage, ob es andere mögliche rechtmäßige Gründe für die Videoüberwachung gibt. Beispiele für mögliche rechtmäßige Gründe können Situationen sein, in denen eine Videoüberwachung gesetzlich vorgeschrieben ist oder in denen die Betroffenen ohne jeden Zweifel ihre Einwilligung gegeben haben.[25]

5.3 Ist die Erforderlichkeit des Einsatzes der Videoüberwachung klar nachgewiesen?

Sobald die Zweckbestimmung des Videoüberwachungssystems genau festgelegt ist und eine rechtmäßige Begründung für seinen Einsatz vorliegt, sollte man begründen, dass die Nutzung der Kameras angesichts der konkreten Umstände, in denen sich das Organ befindet, tatsächlich *erforderlich* ist.[26]

5.4 Ist die Videoüberwachung ein wirksames Werkzeug, um den damit angestrebten Zweck zu erfüllen?

Es sollten keine Systeme installiert werden, die nicht effizient genug sind, um ihren Zweck zu erfüllen, etwa dann, wenn sie nur die Illusion von mehr Sicherheit vermitteln.

Beispiel:

Falls Ihr System dazu eingesetzt wird, den Zugang zu verschiedenen Teilen eines großen Gebäudes zu kontrollieren, die nicht physisch durch geschlossene Türen oder andere Zugangskontrollsysteme voneinander getrennt sind, werden Ihnen hundert Kameras, die Bildmaterial aufzeichnen und von einem Kontrollraum ferngesteuert von zwei Bedienern der Videoüberwachungskameras aus angesehen werden, nicht helfen, einen unbefugten Zutritt zu verhindern, sondern bestenfalls bei der Untersuchung eines Sicherheitsvorfalls, nachdem dieser eingetreten ist.

[24] Siehe Artikel 5 Buchstabe a und Erwägungsgrund 27 der Verordnung.

[25] Siehe Artikel 5 Buchstabe b und d.

[26] Siehe Verordnung Artikel 5 Buchstabe a, b, c. und e (falls der Einsatz der Videoüberwachung an eine Einwilligung geknüpft ist, müssen Sie sicherstellen, dass die Videoüberwachung nicht über das hinausgeht, was zur Erfüllung des Zwecks, für den die Betroffenen ihre Einwilligung gegeben haben, erforderlich ist).

5.5 Gibt es Alternativen, die die Privatsphäre weniger stark verletzen?

Das Organ muss außerdem prüfen, ob es eine Methode gibt, mit der der Verwendungszweck ebenso erfüllt werden kann und die weniger in die Privatsphäre eingreift, ohne dass Kameras eingesetzt werden. Die Videoüberwachung sollte nicht eingesetzt werden, wenn angemessene Alternativen zur Verfügung stehen. Eine Alternative gilt als angemessen, es sei denn, sie ist nicht machbar oder erheblich ineffizienter als die Videoüberwachung oder wäre mit unverhältnismäßig hohen Kosten verbunden.

Die Tatsache an sich, dass eine Technologie zu relativ geringen Kosten verfügbar ist, reicht als Begründung für den Einsatz der Videotechnologie noch nicht aus. Man sollte davon Abstand nehmen, sich einfach nur für die kostengünstigste, einfachste und schnellste Alternative zu entscheiden, wenn dabei die Auswirkungen auf die legitimen Interessen der Betroffenen und auf ihre Grundrechte nicht berücksichtigt werden.

Beispiel:

Sie sollten zur Überwachung des Bereichs Ihrer Info-Center, in denen Besucher einen Internetanschluss haben, rein zum Zweck der Überwachung der verfügbaren Computerplätze kein Videoüberwachungssystem installieren. Alternativ dazu können Sie eine Software installieren, die in jedem Info-Center jederzeit die Anzahl der ein- und ausgeloggten Computer rückverfolgt.

5.6 Überwiegen die Vorteile die Nachteile?[27]

Und schließlich sollte ein Organ, das zu der Schlussfolgerung gelangt, dass ein eindeutiger Bedarf am Einsatz einer Videoüberwachung besteht und es keine anderen Methoden gibt, die weniger stark in die Privatsphäre eingreifen, diese Technologie nur dann nutzen, wenn die Vorteile der Videoüberwachung ihre negativen Auswirkungen überwiegen.

Es liegt auf der Hand, dass die Videoüberwachung nicht verwendet werden sollte, wenn ihre Nachteile ihre Vorteile eindeutig überwiegen.

Beispiel:

Sie sollten in der Gemeinschaftsküche und im gemeinsamen Pausenraum keine

[27] Siehe Artikel 4 Absatz 1 Buchstabe c der Verordnung und Artikel 8 und 52 der Charta der Grundrechte der Europäischen Union. Weitere einschlägige Bestimmungen zu Grundrechten sind u. a. Artikel 7, 11, 12, 21 und 45 der Charta. Vergleiche hierzu auch die Europäische Menschenrechtskonvention, insbesondere Artikel 8, 10 und 11 und das Protokoll Nr. 4 Artikel 2 sowie Artikel 13 des Vertrags zur Gründung der Europäischen Gemeinschaften.

Kamera installieren, um diejenigen davon abzuhalten oder ausfindig zu machen, die sich mit Produkten „bedienen“, die andere Mitarbeiter im Kühlschrank oder in den Schränken gelassen haben. Dies gilt auch dann, wenn i) ein entsprechender Hinweis angebracht wird, ii) dies ein Problem ist, das immer wieder auftritt, und iii) andere Mittel, um Abhilfe zu schaffen, nicht greifen.

In vielen Fällen ist die Analyse jedoch viel komplizierter, und die legitimen Interessen und Grundrechte der überwachten Personen müssen möglicherweise sehr sorgfältig gegen die Vorteile der Überwachung abgewogen werden.

5.7 Sicherheitszwecke

Wenn die Videoüberwachung zu Sicherheitszwecken durchgeführt wird, sollten die Organe die Risiken sorgfältig prüfen, anstatt lediglich zu erklären, dass der Zweck darin bestünde, „Unregelmäßigkeiten innerhalb des Sicherheitsbereichs zu beobachten“ oder „sich mit Sicherheitsvorfällen zu befassen“. So sollten die Organe nicht nur eine allgemeine Vorstellung von dem Zweck haben, zu dem sie ihr System einsetzen wollen, sondern auch die Arten sicherheitsrelevanter Ereignisse genau beschreiben können, die möglicherweise in dem überwachten Bereich auftreten könnten und die sie mithilfe der Kameras abwehren, verhüten, untersuchen oder verfolgen wollen.

Die Organe sollten bei der Definition des Zwecks generell klarstellen, dass das Videoüberwachungssystem bei der Kontrolle des Zugangs zu den Gebäuden hilft und einen Beitrag dazu leistet, die Sicherheit der Gebäude, der Mitarbeiter und Besucher sowie des Grundstücks und der in den Räumlichkeiten befindlichen oder gespeicherten Informationen zu gewährleisten.

Sie sollten außerdem angeben, ob das Videoüberwachungssystem zur Verhütung, Abwehr, Untersuchung und/oder Verfolgung von Sicherheitsvorfällen (durch Sicherstellung von Beweismitteln) konzipiert wurde.[28]

Sie sollten nicht einfach nur potenzielle Sicherheitsrisiken erkennen, sondern müssen auch realistisch und auf nachvollziehbare Art und Weise begründen, dass solche Risiken vorhanden sind, und in welchem Umfang (konkrete Gefahren, Kriminalitätsraten usw.). Die reine „Wahrnehmung“ eines Risikos, Spekulation oder anekdotische Evidenz reichen zur Begründung der Notwendigkeit einer Videoüberwachung nicht aus. Diese Risikoanalyse sollte schriftlich dokumentiert werden und vorhandene Risiken genau bezeichnen und beurteilen. Die Organe müssen die Art der Sicherheitsrisiken in dem unter Beobachtung gestellten Bereich nachweisen, indem sie zeigen, welche Sicherheitsvorfälle dort in der Vergangenheit aufgetreten sind bzw. in Zukunft auftreten könnten.

[28] Videoüberwachung kann bisweilen bei der Verhütung von Sicherheitsvorfällen helfen, indem entweder potenzielle Täter abgeschreckt werden oder schnell auf Notsituationen reagiert werden kann. In der Praxis dient die Videoüberwachung allerdings weniger der Verhütung von Sicherheitsvorfällen, sondern lediglich der Untersuchung von Sicherheitsvorfällen im Nachhinein und der Beweissicherung in einem solchen Fall. Sie müssen sehr präzise und klar zum Ausdruck bringen, was Sie mit der Videoüberwachung bezwecken.

Beispiele:

Sie sollten den potenziellen Einsatz der Videoüberwachung für jede einzelne der nachstehend genannten Arten von Sicherheitsvorfällen, sofern zutreffend, spezifisch und im Einzelnen prüfen und beurteilen:

- *unberechtigter physischer Zugang zu besonders gesicherten Räumlichkeiten und geschützten Räumen (z. B. Räume, in denen kritische IT-Infrastruktur untergebracht ist oder sensible operative Informationen gespeichert werden);*
- *Diebstahl persönlicher Habe von Mitarbeitern (z. B. Laptops, Mobiltelefone, Handtaschen oder Jacken, die unbeaufsichtigt in Einzelbüros oder in Sitzungsräumen zurückgelassen werden);*
- *Fahrraddiebstähle oder Autoeinbrüche auf Ihrem Parkplatz;*
- *Bedrohungen für die Sicherheit bei internationalen Gipfeln und anderen Sonderveranstaltungen;*
- *Ausrüstungen in Kernforschungsanlagen, die versagen;*
- *tätliche Angriffe auf Ihre Gebäude (Werfen von Steinen, Einbrüche, Vandalismus usw.) bei Protestveranstaltungen und Demonstrationen;*
- *physische Übergriffe auf Ihr Sicherheitspersonal am Haupteingang bei Protestveranstaltungen und Demonstrationen.*

Diese Liste dient nur zur Veranschaulichung.

Nach der Ermittlung der Risiken muss eine ganze Reihe von Fragen gestellt werden, und zwar nicht nur, um konkrete Gefährdungen nachzuweisen, sondern auch, um zu belegen, dass eine Videoüberwachung tatsächlich das Richtige ist, um diesen Gefährdungen entgegenzutreten. Wie bereits in den Abschnitten 5.4 bis 5.6 ausgeführt, muss nachgewiesen werden, dass die Videoüberwachung ein effizientes Werkzeug zur Erreichung dieses Zwecks ist, dass es keine anderen Alternativen gibt, die die Privatsphäre weniger verletzen, und dass die Vorteile die Nachteile überwiegen. Wichtig hierbei ist, dass vor der Entscheidung für die Videoüberwachung alle anderen Alternativen, die weniger aufdringlich sind, sorgsam geprüft werden. Hierzu könnten beispielsweise Kontrollen durch Sicherheitspersonal, die Aufrüstung von Alarmsystemen, Zugangskontrollsysteme, die Panzerung und Verstärkung von Pforten, Türen und Fenstern und eine bessere Beleuchtung gehören. Man sollte sich nur dann für eine Videoüberwachung entscheiden, wenn Lösungen der genannten Art nachweislich unzureichend sind.

5.8 Ermittlungszwecke

Wenn ein System für typische Sicherheitszwecke eingerichtet wird, können Videoaufzeichnungen zu Ermittlungszwecken bei physischen Sicherheitsvorfällen verwendet werden, die beispielsweise in Fällen des unbefugten Zugangs zu Grundstücken oder geschützten Räumen, von Diebstahl, Vandalismus, Feuer oder tätlichen Übergriffen auf Personen auftreten. Neben der Abschreckung und Verhütung dient das Videoüberwachungssystem in nahezu allen Fällen auch der

Ermittlung des Sachverhalts nach Eintreten eines Sicherheitsvorfalls und der Sicherung von Beweismitteln zur Verfolgung des Täters. Videoüberwachungssysteme sollten jedoch grundsätzlich nicht für interne Untersuchungen installiert oder konzipiert werden, wenn diese über physische sicherheitsrelevante Ereignisse der vorstehend beschriebenen Art hinausgehen.

Vor diesem Hintergrund kann nicht ausgeschlossen werden, dass die Technologie der Videoüberwachung in Ausnahmefällen trotz alledem auch für Ermittlungszwecke eingesetzt werden kann, auch wenn die Ursache dafür nicht unmittelbar ein physischer Sicherheitsvorfall ist. Um zu entscheiden, ob solche Anwendungszwecke zulässig sind oder nicht und ob sie zusätzliche Schutzvorkehrungen erfordern, die nicht in diesen Leitlinien vorgesehen sind, muss in jedem Einzelfall eine Analyse durchgeführt werden. Daher müssen Sie in Ihrer Strategie bezüglich eines solchen vorgeschlagenen Einsatzes einer Videoüberwachung eine Folgenabschätzung durch Ihr Organ und eine Vorabkontrolle durch den EDSB veranlassen.

Beispiele:

- *In einem verschlossenen Archivraum werden zu Sicherheits- und Zugangskontrollzwecken Kameras installiert, und das Bildmaterial wird direkt von einem Sicherheitsbediensteten im Empfangsbereich überwacht. Das Bildmaterial wird von den Kameras auch aufgezeichnet. Um 16.00 Uhr geht die Alarmanlage an und meldet einen unbefugten Zugang. Die Ermittlung des Sicherheitsvorfalls mithilfe des Bildmaterials aus der Videoüberwachung im Anschluss daran ergibt, dass am Vortag die Klimaanlage des Archivraums repariert worden war, wobei ein Fenster geöffnet und versehentlich offen gelassen worden war. Eine solche Untersuchung ist angemessen und fällt in den Geltungsbereich eines typischen Sicherheitszwecks.*

- *Sie wollen das Videoüberwachungssystem gezielt zur Untersuchung der täglichen Arbeit von Herrn X verwenden, eines Bediensteten Ihres Organs, der im Verdacht steht, Beschaffungsbetrug oder Leistungsbetrug begangen, eine Arbeitskollegin belästigt zu haben oder betrunken zur Arbeit gekommen zu sein. Dies würde über den Sicherheits- und Zugangskontrollzweck hinausgehen und sowohl eine Folgenabschätzung als auch eine Vorabkontrolle voraussetzen.*

5.9 Überwachung von Mitarbeitern

Überwachungsmaßnahmen, die zu stark in die Privatsphäre eindringen, können unnötigen Stress für die Mitarbeiter verursachen und außerdem das Vertrauen innerhalb der Organisation untergraben. Der Einsatz der Videoüberwachung ausschließlich zu dem Zweck der Überwachung, wie die Mitarbeiter ihre Arbeit ausführen, sollte daher vermieden werden, von Ausnahmefällen abgesehen, in denen ein Organ nachweist, dass es ein großes Interesse an einer solchen Überwachung hat.

Jeder Vorschlag zum Einsatz der Videoüberwachung setzt daher voraus, dass das betreffende Organ eine Folgenabschätzung durchführt. Das Organ muss außerdem seine Vorhaben dem EDSB zur Vorabkontrolle vorlegen. Wenn das Organ vorschlägt, die Videoüberwachungstechnologie zur Überwachung der Arbeit seiner Mitarbeiter einzusetzen, legt der EDSB ein ganz besonderes Augenmerk auf die Ansichten und Bedenken der Personalvertreter des Organs und darauf, ob diesen Ansichten auch Rechnung getragen wurde.

Eine Überwachung der Mitarbeiter im Zusammenhang mit der Arbeit des Organs ist im Allgemeinen dann nicht gerechtfertigt, wenn sie der Verwaltung der Produktivität am Arbeitsplatz, der Qualitätskontrolle, der Stärkung der Strategien des Organs oder der Beweissicherung zur Beilegung von Konflikten dienen soll.

Beispiel:

Sie sollten Ihr bereits vorhandenes Videoüberwachungssystem nicht zur Überwachung der Effizienz des ausgegliederten Reinigungspersonals einsetzen, das in den frühen Morgenstunden zum Einsatz gelangt, auch wenn ein diesbezüglicher Hinweis erfolgte und wenn wiederholt Beschwerden bezüglich der Qualität der Arbeit laut wurden.

Ferner sollten auch Verfahren vermieden werden, bei denen Mitarbeiter unter ständiger Beobachtung (ständig im Blickfeld von Videoüberwachungskameras) stehen.

Beispiel:

Sie sollten Videoüberwachungskameras nicht zur ständigen Überwachung des Kassierers und der Registrierkasse in der Kantine während der Öffnungszeiten einsetzen, auch wenn der Kassierer diesbezüglich einen angemessenen Hinweis erhalten hat.

Wie auch im Fall der Überwachung aufgrund von Sicherheitsproblemen oder Problemen im Bereich des Arbeits- und Gesundheitsschutzes oder ähnlichen triftigen Gründen in Ausnahmefällen wird der EDSB solche Begründungen von Fall zu Fall prüfen.

5.10 Webcams

Zu den Zwecken dieser Leitlinien ist unter einer Webcam ein mit dem Internet verbundenes digitales Videoerfassungsgerät zu verstehen, das allen Besuchern der Website dieser Webcam die Möglichkeit der Einsichtnahme in die von der Webcam auf die Website übertragenen Bilder gibt. Auch Geräte, die mit dem Intranet des Organs oder mit Websites verbunden sind, die nicht der Öffentlichkeit, sondern nur einem bestimmten Publikum (etwa den Teilnehmern einer Veranstaltung) zugänglich sind, gelten im Sinne dieser Leitlinien als Webcams.

Webcams bieten beispielsweise die Möglichkeit der Förderung von Bildung, Kommunikation und Freizeit. Webcams können jedoch auch bestimmte Risiken im Zusammenhang mit dem Datenschutz verursachen. Viele dieser Risiken gehen auf die mangelnde Kontrolle durch den Betreiber der Webcam zurück, der nicht kontrolliert, wer die Bilder ansehen und nutzen kann und zu welchen Zwecken. Webcams erfassen und übertragen digitale Bilder, die unmittelbar an eine Vielzahl von Empfängern übertragen werden. Diese Bilder können von jedem dieser Empfänger problemlos aufgezeichnet, kopiert und weiter übertragen werden. Die digitalen Aufzeichnungen mit fortlaufenden, ausführlichen Informationen können auch bequem gespeichert, gesucht und mit einem Index versehen und damit unendlich häufig wiedergegeben und analysiert werden. Die heute aufgezeichneten Videos sind möglicherweise noch viele Jahre lang einsehbar – sie enthalten den „digitalen Fußabdruck" der Menschen. Und schließlich ist auch ein erhöhtes Risiko aufgrund eines möglichen Missbrauchs der Bilder gegeben.

Im Vergleich zu den Vorteilen des Einsatzes einer Webcam – die häufig nur wenig mehr sind als reine „Unterhaltung" – sind diese Risiken häufig nicht gerechtfertigt. Oft gibt es auch andere Alternativen, die jederzeit einsatzbereit sind und weniger stark in die Privatsphäre eingreifen und mit denen genau dieselben Ziele erreicht werden können. Aus diesen Gründen muss die Installation von Webcams stets sehr genau geprüft werden. Webcams sollten normalerweise nicht leichtfertig oder zu Zwecken der Werbung für Freizeiteinrichtungen des Organs oder eines Touristenorts eingesetzt werden (z. B. Besucherzentrum, Fitnessstudio, Cafeteria oder die Besuchergalerie in einem Sitzungsraum).

In Ausnahmefällen können Webcams jedoch trotz alledem zulässig sein, sofern jeder Nutzer der Einrichtung entsprechend unterrichtet wurde und seine Einwilligung persönlich erteilt hat. Den Ansichten und Bedenken von Personalvertretern und/oder anderen Interessengruppen sollte ein besonderes Augenmerk gelten.

Beispiel:

Sie wollen Werbung für das neue Besucherzentrum machen und installieren hierzu eine Videokamera auf dem Gelände; die Bilder werden live an die Website des Organs übertragen. Der EDSB rät von einer solchen Vorgehensweise ab, da viele Nutzer das Vorhandensein der Kameras als ein Eindringen in ihre Privatsphäre empfinden könnten. Falls ein Großteil der Nutzer jedoch trotz alledem Interesse daran bekundet, gefilmt zu werden, können Sie so vorgehen, allerdings nur unter der Voraussetzung, dass jeder einzelne Nutzer entsprechend in Kenntnis gesetzt wird und persönlich seine Einwilligung erteilt. Die Nutzer der Einrichtung sollten eine echte Wahlmöglichkeit bekommen, ob sie den von den Kameras erfassten Teil des Geländes nutzen oder lieber außer Schussweite bleiben, die Einrichtungen jedoch unter den gleichen Bedingungen nutzen wollen.

In der Praxis setzt dies voraus, dass a) nur ein (kleiner) Teil der Einrichtung beworben werden sollte, der dann auch von den Kameras erfasst wird, b) andere Nutzer in anderen Bereichen der Einrichtung selbige unter denselben Bedingungen nutzen können wie in dem beworbenen Bereich und c) in diesem Bereich ein gut sichtbarer und absolut unübersehbarer Hinweis angebracht wird. Wenn dafür in diesem Fall der speziell ausgeschilderte Bereich der Einrichtung genutzt wird,

könnte dies einem stillschweigenden Einverständnis gleichkommen.

Ein weiterer wichtiger Faktor, der bei der Konzeption eines Systems berücksichtigt werden sollte, ist das Ausmaß, in dem Personen bestimmbar sind: Die Aufnahme eines Gebäudes aus der Vogelperspektive mit einer niedrigen Auflösung greift weit weniger in die Privatsphäre ein als Bilder, auf denen die Gesichter von Personen zu erkennen sind. Die negativen Auswirkungen auf die Privatsphäre lassen sich manchmal auch mithilfe einer Software reduzieren, die Einzelheiten auf den Bildern maskiert, die zur Erkennung einer Person beitragen könnten (z. B. Gesichter oder Kfz-Kennzeichen). Auch wenn keine dieser Schutzvorkehrungen an sich den Einsatz von Webcams legitimieren kann, sollten Sie sie bei der Prüfung der Frage, ob Sie Webcams einsetzen sollen, berücksichtigen.

6 Auswahl und Konfiguration des Videoüberwachungssystems und Wahl des Standorts

In diesem Abschnitt werden Handlungshilfen zu der Frage gegeben, wie ein System ausgewählt und konfiguriert und wie sein Standort bestimmt werden sollte. Das Leitprinzip in Verbindung mit allen in diesem Abschnitt (und auch im Rest der Leitlinien) angesprochenen Fragen sollte lauten, negative Auswirkungen auf das Recht auf Privatsphäre und andere Grundrechte und schutzwürdige Interessen von überwachten Personen auf ein Mindestmaß zu reduzieren.[29] Während des Audits (siehe Abschnitt 13) sollte jede Entscheidung auf ihre Angemessenheit überprüft und bewertet werden.

6.1 Standorte von Kameras und Bildwinkel

Die Standorte von Kameras sollten so gewählt werden, dass die Betrachtungspositionen, die für den Verwendungszweck nicht von Belang sind, so klein wie möglich gehalten werden.

Beispiele:

- *Wenn eine Kamera zur Überwachung eines Notausgangs auf einem Dach installiert wird, sollte man darauf achten, dass die Kamera nicht so aufgestellt wird, dass nebenbei auch die Terrasse eines privaten Nachbargebäudes mit aufgezeichnet wird.*
- *Ebenso sollte man dann, wenn eine Kamera zur Überwachung des Eingangs eines besonders geschützten Raums innerhalb eines Gebäudes aufgestellt wird, darauf achten, dass die Kamera nicht so positioniert wird, dass nebenbei auch der Eingang des angrenzenden Privatbüros mit aufgezeichnet wird.*

[29] Siehe Artikel 4 Absatz 1 Buchstabe c der Verordnung.

Im Regelfall gilt, dass das Organ dann, wenn zum Schutz von Vermögenswerten (Grundstück oder Informationen) des Organs oder zur Gewährleistung der Sicherheit der Mitarbeiter und Besucher ein Videoüberwachungssystem installiert werden soll, die Überwachung beschränken sollte auf

- sorgfältig ausgewählte Bereiche mit sensiblen Informationen, hochwertigen Gegenständen oder anderen Vermögenswerten, die aus einem bestimmten Grund einen höheren Schutz erforderlich machen,
- Eingänge und Ausgänge der Gebäude (einschließlich Notausgänge, Fluchtwege und Mauern oder Zäune rund um das Gebäude bzw. Grundstück) und
- Eingänge und Ausgänge im Gebäude, die verschiedene Bereiche mit unterschiedlichen Zugangsrechten, die durch verschlossene Türen oder andere Zugangskontrollmechanismen voneinander getrennt sind, miteinander verbinden.

Beispiele:

- *Sie können am Eingang eines verschlossenen Archivraums, in dem Sie wichtige Unterlagen Ihres Organs aufbewahren und der nur gelegentlich von autorisiertem Personal zur Ablage oder zum Auffinden von Unterlagen betreten wird, Kameras anbringen.*
- *Sie vermieten die oberste Etage Ihres Gebäudes an ein anderes Organ. Die Etage ist mit einer Tür gesichert, die immer verschlossen ist und nur mithilfe der Zutrittsausweise der Mitarbeiter geöffnet werden kann, die auf dieser Etage arbeiten. Sie können im Fahrstuhlbereich dieser Etage eine Kamera anbringen, die alle Personen erfasst, die diese Etage verlassen oder von anderen Gebäudebereichen aus betreten.*

Es kann nicht ausgeschlossen werden, dass aufgrund der Sicherheitserfordernisse eine umfangreichere Überwachung in bestimmten Gebäuden gerechtfertigt ist. Sollte dies der Fall sein, sollten derartige Vorhaben im Rahmen der Videoüberwachungsstrategie konkret dargelegt werden, und das Organ sollte die Notwendigkeit und Verhältnismäßigkeit einer solchen zusätzlichen Überwachung (im Rahmen einer Folgenabschätzung oder auf anderem Weg) nachweisen.

6.2 Zahl der Kameras

Die Zahl der zu installierenden Kameras richtet sich nach der Größe der Gebäude und nach den Sicherheitserfordernissen, die wiederum von einer Vielzahl von Faktoren abhängen. Dieselbe Zahl und derselbe Typ Kamera können für ein Organ angemessen, für ein anderes jedoch völlig unverhältnismäßig sein. Allerdings ist bei sonst gleichen Bedingungen die Zahl der Kameras ein guter Indikator für die Komplexität und Größe eines Überwachungssystems, der auf erhöhte Risiken für die Privatsphäre und andere Grundrechte hindeuten kann. Mit steigender Zahl der Kameras nimmt auch die Wahrscheinlichkeit zu, dass diese Kameras nicht effizient

eingesetzt werden und eine Informationsüberflutung droht. Der EDSB empfiehlt daher, die Zahl der Kameras auf das zu beschränken, was für die Erreichung der Ziele des Systems unbedingt erforderlich ist. Die Zahl der Kameras ist in der Videoüberwachungsstrategie aufzuführen.

6.3 Zeiten der Überwachung

Man sollte die Zeiten, in denen die Kameras zur Aufzeichnung eingeschaltet werden, genau festlegen, um die Überwachung in Zeiten, die für den Verwendungszweck nicht von Belang sind, auf ein Mindestmaß zu reduzieren. Falls die Zweckbestimmung der Videoüberwachung die Sicherheit ist, sollte das System so weit wie möglich nur in Zeiten eingeschaltet werden, in denen die Wahrscheinlichkeit, dass die angeblichen Sicherheitsprobleme auftreten, höher ist.

Beispiel:

Wiederholte Fälle von Diebstahl finden nachts und an Wochenenden in einem geschlossenen Lagerbereich abseits von einem stark frequentierten Treppenhaus statt. Sie können in der Nähe des Eingangs des Lagerbereichs eine Kamera installieren, um herauszufinden, wer den Diebstahl begangen hat, oder um einen weiteren Diebstahl zu verhindern (sofern ein entsprechender Hinweis erfolgt). Die Kameras sollten nur außerhalb der Bürozeiten eingeschaltet werden.

6.4 Auflösung und Bildqualität

Man sollte sich für eine angemessene Auflösung und Bildqualität entscheiden. Unterschiedliche Zweckbestimmungen erfordern unterschiedliche Bildqualitäten. Wenn beispielsweise die Erkennung der betroffenen Personen von maßgeblicher Bedeutung ist, sollten die Auflösung der Kameras, die Einstellungen für die Bildkompression in einem digitalen System, der Standort, die Beleuchtung und andere Faktoren allesamt berücksichtigt und ausgewählt oder aber abgeändert werden, damit die sich daraus ergebende Bildqualität ausreicht, um erkennbare Gesichtsbilder zu liefern. Wenn dagegen eine Erkennung nicht notwendig ist, sollten die Kameraauflösung und andere veränderbare Faktoren so gewählt werden, dass keine erkennbaren Gesichtsbilder erfasst werden.

Beispiel:

In manchen Situationen ist die Erkennung von Personen nicht notwendig, und es reicht aus, wenn die Bildqualität die Erkennung von Bewegungen von Menschen oder des Verkehrsflusses ermöglicht.

6.5 Überwachung im Hoheitsgebiet der Mitgliedstaaten

Bei nachweislichen Sicherheitserfordernissen kann ein Organ die Bereiche überwachen, die unmittelbar an seine Gebäude im Hoheitsgebiet der Mitgliedstaaten angrenzen. Dabei ist jedoch zu gewährleisten, dass eine solche Überwachung auf

das absolute Mindestmaß beschränkt wird, das zur Durchsetzung der Sicherheitserfordernisse des Organs notwendig ist. Dies kann Eingänge und Ausgänge einschließlich von Notausgängen und Fluchtwegen sowie Mauern oder Zäune rund um das Gebäude bzw. Grundstück einschließen.

Beispiel:

Am Eingang eines Gebäudes werden Kameras angebracht, die Personen filmen, die das Gebäude betreten und verlassen, und dabei nebenbei auch einige Quadratmeter der öffentlichen Anlagen rund um das Gebäude (und meist Bilder von Passanten auf einer verkehrsreichen Straße liefern). Diese Vorgehensweise ist zulässig. Die Überwachung der Fenster eines Wohnblocks gegenüber ist allerdings zu vermeiden. Der Standort bzw. die Richtung der Kameras sollten geändert und die Bilder maskiert oder verwürfelt werden, oder es sind ähnliche Maßnahmen zu ergreifen.

In allen Fällen, in denen mehr als nur die Eingänge und Ausgänge überwacht werden, sollte eine Folgenabschätzung durchgeführt werden. Eine solche zusätzliche Überwachung kann nur im Fall nachweislicher Sicherheitserfordernisse und nur bei Annahme zusätzlicher Datenschutzgarantien stattfinden. Hierzu gehören u. a.:

- Beschränkung der Überwachung von angrenzendem *privatem* Raum (z. B. über das Maskieren oder Verwürfeln von Bildern),
- nach Möglichkeit kurze Aufbewahrungsfristen von maximal 48 Stunden (oder nur Live-Überwachung),
- Beschränkung der Zoom-Möglichkeiten der Kameras oder aber eine Kameraauflösung, bei der nur der umliegende öffentliche Raum erfasst wird,
- nach Möglichkeit Beschränkung der Überwachung auf Zeiten mit erhöhten Sicherheitserfordernissen (z. B. internationale Gipfel oder andere Sonderveranstaltungen) und
- angemessene Schulung der Bediener des Videoüberwachungssystems, damit die Privatsphäre von Passanten oder anderen Personen, die von den Kameras aufgenommen werden, nicht unverhältnismäßig stark verletzt wird.

Die Meinung der nationalen (oder regionalen) Datenschutzbehörden und anderer zuständiger Behörden und Interessengruppen sollte ebenfalls berücksichtigt werden.

Man sollte sich jedenfalls vor Augen halten, dass die Zweckbestimmung einer Videoüberwachung in aller Regel keine Verbrechensverhütung allgemein oder die Aufrechterhaltung von Recht und Ordnung im Hoheitsgebiet der Mitgliedstaaten sein kann. Dies sind die Vorrechte bestimmter staatlicher Behörden oder Organisationen in den Mitgliedstaaten, die entsprechende Schutzgarantien nach Maßgabe des innerstaatlichen Rechts voraussetzen. So sind etwa Kommunalverwaltungen und/oder die örtliche Polizei möglicherweise als Einzige hierzu berechtigt. Daher kann im Allgemeinen kein Organ legitim Videoüberwachungssysteme für derartige Zwecke konzipieren und installieren.

Dies bedeutet jedoch nicht, dass das Organ sein Videoüberwachungssystem nicht zu

solchen Zwecken einsetzen kann, wenn dies unter Mitwirkung der örtlichen Polizei (und/oder gegebenenfalls der örtlichen Kommunalverwaltung) und anderweitig im Einklang mit dem geltenden innerstaatlichen Recht erfolgt. In diesem Fall empfiehlt der EDSB, eine entsprechende schriftliche Vereinbarung zu schließen. Zu jeder vorgeschlagenen Videoüberwachung sollte das Organ eine Folgenabschätzung durchführen.

Beispiel:

In einem (hypothetischen) Land, in dem sich Ihr Gebäude befindet, darf eine Videoüberwachung von öffentlichen Anlagen wie z. B. Stadtparks und Straßen nur von der örtlichen Polizei durchgeführt werden und bedarf außerdem der Genehmigung der Kommunalverwaltung. Bei Ihnen gehen wiederholt Beschwerden ein, wonach Bedienstete von EU-Organen überfallen werden, wenn sie spät abends durch den kleinen Park direkt neben Ihrem Gebäude nach Hause kommen. Sie sollten zur Abwehr dieser Überfälle nicht in Eigeninitiative Kameras anbringen, mit denen Sie den ganzen Park überblicken können. Sie können jedoch, sofern dies laut Kommunalrecht zulässig ist, mit der örtlichen Polizei zusammenarbeiten und, was ebenfalls der vorherigen Genehmigung der Kommunalverwaltung bedarf, eine Reihe von Kameras installieren und betreiben, beispielsweise, um den Hauptweg durch den Park von der Dämmerung bis zum Tagesanbruch zu überwachen. Sie sollten außerdem zusammen mit der nationalen Datenschutzbehörde prüfen, ob Sie zusätzliche Datenschutzgarantien einhalten müssen.

Sollte eine Vorabkontrollmeldung erforderlich sein, sollte die EU-Kommission dem EDSB im Namen aller Kommissionsvertretungen in den Mitgliedstaaten eine einzige Vorabkontrollmeldung vorlegen.

6.6 Überwachung in Drittländern

Die in Abschnitt 6.5 genannten Bedingungen sollten sinngemäß auch für Überwachungstätigkeiten außerhalb des Hoheitsgebiets der Europäischen Union Anwendung finden. Da sich Sicherheitsrisiken und Datenschutzvorschriften außerhalb der Europäischen Union deutlich unterscheiden, fordert der EDSB die Delegationen der Kommission in Drittländern dringend auf, unabhängig ihre Sicherheitserfordernisse selbst zu prüfen und ihre Videoüberwachungssysteme dementsprechend zu konzipieren. Außerdem sollten sie mit den örtlichen Kommunalbehörden im Rahmen des Machbaren zusammenarbeiten, solange ihre Sicherheit durch eine solche Zusammenarbeit nicht gefährdet wird.

Immer dann, wenn eine Vorabkontrollmeldung erforderlich ist, sollte die EU-Kommission dem EDSB im Namen aller EU-Delegationen in Drittländern eine einzige Vorabkontrollmeldung vorlegen.

6.7 Besondere Datenkategorien

Videoüberwachungssysteme sollten nicht zur Erfassung von Bildern (etwa durch

Zoomen oder genaues Anvisieren) oder anderweitige Formen der Verarbeitung (z. B. Indexierung, Profilierung) eingesetzt werden, aus denen sogenannte „besondere Datenkategorien“ hervorgehen, etwa die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit sowie Daten über Gesundheit oder Sexualleben.[30]

Auch Bereiche, in denen die Wahrscheinlichkeit höher ist, dass die Kameras Bilder aufnehmen, aus denen besondere Datenkategorien hervorgehen, sollten nicht überwacht werden, auch wenn die Erhebung solcher besonderer Datenkategorien gar nicht beabsichtigt ist.[31]

Beispiele:

Sie sollten keine Demonstranten oder Warteräume des medizinischen Dienstes filmen oder ein Videoüberwachungssystem installieren, bei dem zufällig Warteräume oder Bereiche erfasst werden, in denen Demonstranten protestieren. Auch sollten Sie im Eingangsbereich eines Gewerkschaftsbüros keine Kamera aufstellen oder den Bereich überwachen, der an eine religiöse Einrichtung außerhalb Ihres Gebäudes grenzt.

Für den Fall, dass ein Organ von diesen Vorschriften abweichen möchte, ist eine Folgenabschätzung durchzuführen. Eine Überwachung kann nur stattfinden, wenn zusätzliche Schutzgarantien vorgesehen werden.

Im Fall einer Überwachung, die bei Demonstrationen für Sicherheit sorgen soll, können diese zusätzlichen Schutzgarantien u. a. Folgendes umfassen:

- die Überwachung friedlicher Protestaktionen kann nur erfolgen, wenn dies für die Sicherheit nachweislich erforderlich ist;
- die Kameras sollten nicht auf die Gesichter von Personen gerichtet werden, und es sollte nicht versucht werden, mithilfe der Kameras Personen zu erkennen, es sei denn, die öffentliche Sicherheit ist unmittelbar bedroht oder es handelt sich um ein gewalttätiges strafbares Verhalten (z. B. Vandalismus oder tätliche Übergriffe);
- wenn kein sicherheitsrelevantes Ereignis festgestellt wurde, löschen Sie die Aufzeichnungen aller friedlichen Proteste innerhalb von zwei Stunden nach dem Ende der Protestaktion (oder aber Sie prüfen, ob Sie sich nur auf die Live-Überwachung beschränken wollen);
- die Bilder werden nicht für die gezielte Datensuche (Data Mining) verwendet;

[30] Siehe Artikel 10 der Verordnung.

[31] In der Regel (z. B. dann, wenn ein Organ die Eingänge und Ausgänge seines Gebäudes überwacht) hat die Tatsache an sich, dass aus dem Gesichts- oder Körperbild einer Person oder der Kleidung oder Accessoires, die sie trägt, ihre rassische oder ethnische Herkunft und vielleicht ihr Gesundheitszustand hervorgehen, an sich noch nicht zur Folge, dass die Videoüberwachung mit einer Verarbeitung besonderer Datenkategorien verbunden ist.

und

- die Bediener des Videoüberwachungssystems werden angemessen geschult, damit die Privatsphäre und andere Grundrechte der aufgenommenen Teilnehmer einschließlich – und dies ist wichtig – ihrer Versammlungsfreiheit nicht unverhältnismäßig stark verletzt werden.

Jede Überwachung, bei der besondere Datenkategorien verarbeitet werden, muss durch den EDSB vorab kontrolliert werden.

6.8 Bereiche, in denen verstärkte Erwartungen an den Schutz der Privatsphäre gestellt werden

Bereiche, in denen verstärkte Erwartungen an den Schutz der Privatsphäre gestellt werden, sollten nicht überwacht werden. Hierzu gehören typischerweise Einzelbüros (einschließlich von Büros, in denen zwei oder mehr Personen arbeiten, und Großraumbüros mit Arbeitsnischen), Freizeitbereiche (Kantinen, Cafeterias, Bars, Kochnischen, Imbissstuben, Aufenthaltsbereiche, Wartezimmern usw.), Toiletten, Duschräume und Umkleideräume.

Für den Fall, dass ein Organ von diesen Vorschriften abweichen möchte, ist eine Folgenabschätzung durchzuführen. Außerdem ist eine Vorabkontrolle durch den EDSB erforderlich.

6.9 Hightech- und/oder intelligente Videoüberwachung

Die Einführung von „Hightech-Videoüberwachungswerkzeugen“ oder „intelligenten Videoüberwachungssystemen“ ist nur zulässig, wenn eine Folgenabschätzung durchgeführt wird. Sie setzt außerdem eine Vorabkontrolle voraus. Der EDSB prüft in jedem einzelnen Fall die Zulässigkeit des eingesetzten Verfahrens und kann bei Bedarf besondere Datenschutzgarantien anordnen.

Unter diese Kategorie fallen u. a. folgende Werkzeuge:

- Koppelung des Videoüberwachungssystems an biometrische Daten (z. B. Fingerabdrücke für die Zugangskontrolle) oder an jede andere Datenbank, biometrischer oder anderer Art (z. B. eine Datenbank mit Fotos von Verdächtigen für die Gesichtserkennung oder Kfz-Zulassungsdaten für die automatische Erkennung des Kfz-Kennzeichens);
- Indexierung der Daten auf den Bildern für automatisierte Suchvorgänge und Alarmmeldungen (z. B. zur Verfolgung von natürlichen Personen);
- Gesichts- oder andere Bilderkennungs- oder Gangerkennungssysteme;
- jede Art von dynamisch-präventiver Überwachung (z. B. mithilfe von Softwareanwendungen zur automatischen Verhaltensanalyse, die automatisierte Alarmmeldungen aufgrund von vorher festgelegten verdächtigen Verhaltensmustern, Bewegungen, Kleidung oder Körpersprache erstellen);
- ein Netzwerk von installierten Kameras samt Tracking-Softwareanwendung, die bewegliche Gegenstände oder Menschen in einem ganzen Bereich verfolgen kann;
- audiogestützte Alarmsysteme (die durch Veränderungen der Lärmmuster wie z. B. plötzliche Schreie ausgelöst werden);

- Infrarot- oder Nahinfrarotkameras, Wärmebildgeräte und andere Spezialkameras, die Bilder im Dunklen oder bei schlechten Lichtverhältnissen aufnehmen, durch Wände hindurchsehen und unter der Kleidung suchen können (wie z. B. Ganzkörper-Scanner), und
- Spezialkameras mit verbesserten optischen und digitalen Zoom-Fähigkeiten.

Bitte beachten Sie, dass die folgenden Merkmale an und für sich keine Folgenabschätzung oder Vorabkontrolle erfordern:

- Bewegungsmelder, mit denen Videosignale auf Ereignisse beschränkt werden sollen, die der Beobachtung und Aufzeichnung wert sind;
- Konfiguration eines Bewegungsmeldesystems, damit Sicherheitsbedienstete Alarmmeldungen erhalten, wenn das System erkennt, dass jemand den zugangsbeschränkten Raum betritt (z. B. ein verschlossener IT-Raum außerhalb der Bürozeiten);
- handelsübliches Schwenken, Neigen und beschränkte optische und digitale Zoom-Fähigkeiten.

Wenn Sie sich nicht sicher sind, ob eine Vorabkontrolle erforderlich ist, wenden Sie sich im Zweifelsfall bitte an uns.

6.10 Zusammenschaltung von Videoüberwachungssystemen

Die Zusammenschaltung des Videoüberwachungssystems eines Organs mit dem Videoüberwachungssystem eines anderen Organs oder von Dritten erfordert eine Folgenabschätzung. Eine Folgenabschätzung ist auch dann erforderlich, wenn ein einzelnes Organ mehrere voneinander unabhängige Systeme betreibt (etwa Systeme in verschiedenen Städten oder Systeme am gleichen Standort, die jedoch zu unterschiedlichen Zwecken verwendet werden) und diese zusammenschalten möchte. In diesem Fall ist auch eine Vorabkontrollmeldung erforderlich.

6.11 Verdeckte Überwachung

Zu den Zwecken dieser Leitlinien ist unter dem Begriff der verdeckten Videoüberwachung eine Überwachung mithilfe von Kameras zu verstehen, die

- entweder absichtlich uneinsehbar sind oder
- anderweitig installiert werden, ohne dass die Öffentlichkeit einen entsprechenden Hinweis erhält, sodass
- berechtigterweise davon ausgegangen werden kann, dass sich die überwachten Personen der Kameras nicht bewusst sind.

Wenn Kameras in Bereichen installiert werden, in denen verstärkte Erwartungen an den Schutz der Privatsphäre gestellt werden (siehe Abschnitt 6.8), ohne dass die beiden nachstehenden Voraussetzungen gleichzeitig erfüllt werden, spricht man von einer verdeckten Videoüberwachung, und zwar auch dann, wenn am Eingang des Gebäudes ein allgemeiner Hinweis angebracht ist, dass das Gebäude videoüberwacht wird:

- Unmittelbar vor Ort (z. B. an der Tür eines Einzelbüros) ist ein konkreter und gut sichtbarer Hinweis angebracht und
- in einer öffentlich zugänglichen Videoüberwachungsstrategie im Einklang mit den Empfehlungen in Abschnitt 11 sind weitere konkrete Erläuterungen der Möglichkeit einer Überwachung in diesen Bereichen (z. B. Einzelbüros) enthalten.

Die verdeckte Überwachung ist aufgrund ihrer heimlichtuerischen Natur hochgradig aufdringlich. Darüber hinaus hat sie kaum oder gar keine Präventivwirkung und wird häufig nur als eine Art Falle zur Beweissicherung eingebaut. Sie sollte daher nicht eingesetzt werden.

Vorgeschlagene Ausnahmen sind schlüssig zu begründen und erfordern eine Folgenabschätzung und eine Vorabkontrolle durch den EDSB, der bei Bedarf besondere Datenschutzgarantien vorschreiben kann.

Grundsätzlich wird der EDSB nur dann eine befürwortende Stellungnahme zur Vorabkontrolle abgeben, wenn alle nachstehend aufgeführten Bedingungen erfüllt sind:

- Eine verdeckte Überwachung wird zur Untersuchung einer hinlänglich schweren Straftat im Rahmen einer förmlichen, gesetzlich vorgeschriebenen oder rechtlich zulässigen Ermittlung durch die Polizei eines Mitgliedstaats oder andere zuständige Strafverfolgungsbeamte oder durch die zuständigen Ermittlungsbehörden der EU durchgeführt;
- der Einsatz der verdeckten Überwachung steht im Einklang mit dem Gesetz und wurde offiziell genehmigt a) durch einen Richter oder einen anderen Beamten, der kraft Gesetzes des Mitgliedstaats, der den Einsatz der verdeckten Überwachung in dem Organ beantragt hat, entsprechend befugt ist, oder b) durch das zuständige oberste Entscheidungsgremium des Organs nach Maßgabe der schriftlichen und öffentlich zugänglichen Strategie des Organs in Bezug auf den Einsatz der verdeckten Überwachung (z. B. ein hochrangiges Leitungsgremium);
- es wird über alle Genehmigungen dieser Art und alle Fälle, in denen die verdeckte Überwachung eingesetzt wurde, ein Register geführt; dieses Register muss dem behördlichen Datenschutzbeauftragten und dem EDSB auf Verlangen zur Prüfung vorgelegt werden;
- die Kameras werden nur für einen streng begrenzten Zeitraum und an streng begrenzten Standorten aufgestellt; und es muss gewährleistet sein, dass
- es für eine erfolgreiche Untersuchung des Falles keine anderen Alternativen zum Einsatz der verdeckten Überwachung gibt und
- die sich daraus ergebenden Vorteile die Verletzung der Privatsphäre der beobachteten Personen überwiegen würden.

6.12 Tonaufzeichnungen und Videoüberwachungskameras mit Lautsprechern („talking CCTV“)[32]

Aufgrund ihres aufdringlichen Charakters sind Tonaufzeichnungen und der Einsatz von Videoüberwachungskameras mit Lautsprechern („talking CCTV“) grundsätzlich ebenfalls verboten, es sei denn, sie werden als Sicherungssystem für die Zugangskontrolle außerhalb der Bürozeiten eingesetzt (als Bildtelefon, um mit dem Sicherheitspersonal, welches das System ferngesteuert bedient, Kontakt aufzunehmen, um sich Zugang zu verschaffen).

Wird das System als Sicherungssystem für die Zugangskontrolle eingesetzt, sollte ein klarer Hinweis darauf gegeben werden, und die Kameras sollten nur dann Ton übermitteln oder aufzeichnen, a) wenn sie von der Person selbst aktiviert wurden, die versucht hat, sich Zugang zu verschaffen, oder b) nach einer genau festgelegten Zahl von Fehlversuchen, um sich Zugang zu verschaffen

Vorgeschlagene weitere Ausnahmen sind schlüssig zu begründen und erfordern eine Folgenabschätzung und eine Vorabkontrolle.

7 Wie lange sind die Aufzeichnungen aufzubewahren?

7.1 Aufbewahrungsfrist

7.1.1 Allgemeine Grundsätze. Aufzeichnungen dürfen nicht länger aufbewahrt werden, als es für die konkreten Zwecke, für die sie gemacht wurden, notwendig ist.[33] Dabei ist auch zu berücksichtigen, ob die Aufzeichnung überhaupt notwendig ist und ob eine Live-Überwachung ohne Aufzeichnung nicht ausreichen würde.

Wenn sich ein Organ für eine Aufzeichnung entscheidet, muss es den Zeitraum der Aufbewahrung genau angegeben. Nach Ablauf dieser Frist müssen die Aufzeichnungen gelöscht werden. Der Löschvorgang sollte wenn möglich automatisiert werden, etwa durch automatisches und regelmäßiges Überschreiben der Datenträger nach dem FIFO-Prinzip (die ältesten Daten zuerst). Sobald die Datenträger nicht mehr länger verwendbar sind (nach vielen Einsatzzyklen), müssen sie sicher so entsorgt werden, dass die darauf verbleibenden Daten für immer und unwiderruflich gelöscht sind (z. B. durch Schreddern oder ähnliches).

Falls die Videoüberwachung zu Zwecken der Sicherheit und der Zugangskontrolle eingesetzt werden soll und ein Sicherheitsvorfall eintritt und festgestellt wird, dass die Aufzeichnungen für die weitere Untersuchung des Vorfalls notwendig sind oder als

---

[32] Im Sinne dieser Leitlinien bedeutet „Videoüberwachungskameras mit Lautsprechern („talking CCTV“)“ eine Videoüberwachungskonfiguration, bei der in dem überwachten Bereich Lautsprecher eingesetzt werden, wobei die Bediener des Systems die beobachteten Bürger „ansprechen“ können (z. B. „der Herr in der braunen Lederjacke – heben Sie bitte den Müll, den Sie gerade fallen gelassen haben, wieder auf“).

[33] Artikel 4 Absatz 1 Buchstabe e der Verordnung.

Beweismittel dienen könnten, kann das entsprechende Bildmaterial über die normale Aufbewahrungsfrist hinaus so lange aufbewahrt werden, wie es diese Zwecke erfordern. Anschließend müssen die Aufzeichnungen jedoch ebenfalls gelöscht werden.

Beispiel:

Eine Agentur ist mit einem Videoüberwachungssystem für die Sicherheit und Zugangskontrolle ausgestattet. Die Agentur muss genau den Zeitraum angeben, zum Beispiel drei Kalendertage, nach dessen Ablauf die Aufzeichnungen automatisch überschrieben werden.

Wenn während dieser drei Tage, solange die Aufzeichnungen verfügbar sind, ein Sicherheitsvorfall eintritt, etwa ein Feuer, das im Parkhaus des Gebäudes ausbricht, kann das entsprechende Bildmaterial aufbewahrt werden, bis die Untersuchungen des Zwischenfalls abgeschlossen sind.

7.1.2 Aufbewahrungsfrist für typische Sicherheitszwecke: eine Woche. Wenn Kameras zu Sicherheits- und Zugangskontrollzwecken installiert werden, sollte eine Woche in den meisten Fällen mehr als ausreichend sein, damit das Sicherheitspersonal in voller Kenntnis der Sachlage eine Entscheidung darüber treffen kann, ob Bildmaterial länger aufbewahrt werden soll, um einen Sicherheitsvorfall weiter zu untersuchen, oder ob dieses Bildmaterial als Beweis dienen kann. Diese Entscheidungen können normalerweise binnen weniger Stunden getroffen werden. Organe sollten daher eine Aufbewahrungsfrist von maximal sieben Kalendertagen festlegen.[34] In den meisten Fällen dürften auch kürzere Fristen ausreichen.

7.1.3 Hoheitsgebiet der Mitgliedstaaten oder von Drittländern: 48 Stunden. Falls sich die Überwachung auf einen Bereich außerhalb der Gebäude im Hoheitsgebiet eines Mitgliedstaats (oder Drittlandes) (typischerweise Bereiche in der Nähe der Eingangs- und Ausgangsbereiche) erstreckt und es sich nicht vermeiden lässt, dass Passagiere oder vorbeifahrende Fahrzeuge von den Kameras erfasst werden, empfiehlt der EDSB, die Aufbewahrungsfrist auf 48 Stunden zu verkürzen oder, sofern dies möglich ist, Bedenken, die vor Ort entstehen, anderweitig Rechnung zu tragen.

Beispiel:

Agentur A und B sind beide mit einem Videoüberwachungssystem für die Sicherheit und Zugangskontrolle ausgestattet.

Agentur A befindet sich abgelegen in einer ländlichen Gegend, in deren Umgebung es keinen Fußgänger- oder Autoverkehr gibt. Das Gelände ist umzäunt, dahinter

[34] Siehe Stellungnahme 4/2004 der Artikel-29-Datenschutzgruppe zum Thema Verarbeitung personenbezogener Daten aus der Videoüberwachung, Teil 7, Buchstabe E, Seite 20.

befinden sich offene Felder. Agentur A kann ihre Aufzeichnungen länger als 48 Stunden aufbewahren (maximal jedoch sieben Kalendertage). Sie kann beispielsweise dieselbe Aufbewahrungszeit von drei Kalendertagen für die Überwachung der Bereiche auf ihrem Gelände und der angrenzenden Bereiche außerhalb ihres Anwesens wählen.

Agentur B ist inmitten eines verkehrsreichen Stadtzentrums mit einem Bahnhof in der Nähe und starkem Fußgängerverkehr auf den Bürgersteigen der Straßen außerhalb ihrer Gebäude gelegen. Agentur B sollte dafür Sorge tragen, dass die Aufbewahrungszeit der Aufnahmen der Anlagen von außerhalb ihrer Gebäude auf höchstens 48 Stunden beschränkt wird. Sie sollte außerdem prüfen, ob eine kürzere Aufbewahrungszeit oder auch eine Live-Überwachung nicht ausreichen würden.

7.1.4 Kürzere Aufbewahrungsfristen. Der EDSB kann kürzere Aufbewahrungszeiten oder eine Live-Überwachung nur dann empfehlen, wenn die Verletzung des Rechts auf Privatsphäre und anderer Grundrechte und schutzwürdiger Interessen derjenigen, die sich im Schwenkbereich der Kamera befinden, auf ein Mindestmaß reduziert wird.

Beispiel:

Häufig finden politische Protestaktionen vor Ihren Gebäuden statt. Sie reichen Ihre Vorabkontrolle aufgrund dessen ein, dass besondere Datenkategorien verarbeitet werden könnten (siehe Abschnitt 6.7). Aufgrund der gegebenen Umstände in diesem Fall kann der EDSB empfehlen, dass Sie dann, wenn kein Sicherheitsvorfall festgestellt wurde, die Aufzeichnungen jeder einzelnen friedlichen Protestaktion innerhalb von spätestens zwei Stunden nach dem Ende der Aktion löschen (oder aber Sie prüfen, ob Sie nicht einfach nur eine Live-Überwachung vornehmen).

7.2 Register von Aufzeichnungen, die über die Aufbewahrungszeit hinaus gespeichert werden

Es sollte ein Register – möglichst in elektronischer Form – geführt werden, in dem alle Aufzeichnungen, die über die normale Aufbewahrungszeit hinaus gespeichert werden, zurückverfolgt werden können. Dieses Register sollte folgende Angaben enthalten:

- Datum und Uhrzeit des Bildmaterials und Standort der Kamera,
- Kurzbeschreibung des Sicherheitsvorfalls,
- Grund, weshalb das Bildmaterial aufbewahrt werden muss, und
- voraussichtliches Datum, an dem überprüft wird, ob das Bildmaterial noch länger aufbewahrt werden muss.

Beispiel eines Eintrags in das Register:

- *Datum und Uhrzeit des Bildmaterials: 1. Oktober 2009, 10.00 bis 12.00 Uhr*
- *Standort der Kamera: Kamera Nr. 5 (Standort in der Nähe des Fahrstuhleingangsbereichs im Parkhaus)*
- *Kurzbeschreibung des Sicherheitsvorfalls: Im Abfalleimer neben dem Fahrstuhleingang im Parkhaus ist ein Feuer ausgesprochen. Keine Personenschäden und keine Körperverletzung.*
- *Grund, weshalb das Bildmaterial aufbewahrt werden muss: Der Vorfall muss von der Sicherheitsabteilung anhand des Bildmaterials aus der Videoüberwachung weiter untersucht werden, um herauszufinden, weshalb das Feuer ausgebrochen ist. Damit sollen entsprechende Erkenntnisse gewonnen und mögliche Schutzmaßnahmen ergriffen werden*
- *Voraussichtliches Datum, an dem überprüft wird, ob das Bildmaterial noch länger aufbewahrt werden muss: 15. Oktober 2009.*

8 Wem sollte Zugriff auf die Bilder gewährt werden?

8.1 Eine kleine Zahl von klar bestimmten Personen gemäß dem Grundsatz „Kenntnis nur, wenn nötig“

Die Rechte auf Zugriff müssen auf eine kleine Zahl von klar bestimmten Personen streng gemäß dem Grundsatz „Kenntnis nur, wenn nötig“ beschränkt werden. Außerdem ist zu gewährleisten, dass autorisierte Nutzer ausschließlich auf die personenbezogenen Daten zugreifen können, auf die sich ihre Zugriffsberechtigung erstreckt.[35] Es sollten Strategien für die Zugriffskontrolle nach dem Prinzip der minimalen Zugriffsrechte formuliert werden, d. h., die Zugriffsberechtigung der Nutzer sollte nur für solche Ressourcen gewährt werden, die zur Wahrnehmung ihrer Aufgaben unbedingt erforderlich sind.

Lediglich der „für die Verarbeitung Verantwortliche“, der Systemadministrator oder andere Mitarbeiter, die vom für die Verarbeitung Verantwortlichen speziell zu diesem Zweck benannt werden, sollten in die Lage versetzt werden, Personen Zugriffsberechtigungen zu gewähren und diese abzuändern oder aufzuheben. Die Gewährung, Änderung oder Aufhebung von Zugriffsberechtigungen muss nach den Kriterien erfolgen, die in der Videoüberwachungsstrategie des Organs verankert sind.

Zugriffsberechtigte müssen Personen sein, die jederzeit eindeutig bestimmbar sind.

Beispiel:

Es sollten keine allgemeinen oder gängigen Nutzernamen oder Passwörter an eine ausgegliederte Sicherheitsfirma vergeben werden, die mehrere Personen beschäftigt, die für Ihr Organ tätig sind.

[35] Bezüglich des letztgenannten Aspekts siehe Artikel 22 Absatz 2 Buchstabe e der Verordnung.

In der Videoüberwachungsstrategie muss eindeutig ausgeführt und dokumentiert werden, wer Zugriff auf das Bildmaterial aus der Videoüberwachung und/oder die technische Architektur des Videoüberwachungssystems besitzt, zu welchem Zweck, und woraus diese Zugriffsberechtigungen bestehen. Insbesondere muss genau beschrieben werden, wer berechtigt ist,

- das Bildmaterial in Echtzeit anzusehen,
- die PTZ-Kameras (schwenk-, neig- und zoombare Kameras) zu bedienen,
- das aufgezeichnete Bildmaterial anzusehen oder
- zu kopieren,
- herunterzuladen,
- zu löschen oder
- Bildmaterial zu verändern.

Unterschiede zwischen den Zugriffsberechtigungen verschiedener Personenkategorien müssen genau beschrieben werden.

So nehmen beispielsweise diejenigen,

- die die Bilder live betrachten,
- für die technische Wartung des Systems zuständig sind oder
- Sicherheitsvorfälle untersuchen,

unterschiedliche Aufgaben wahr und sollten daher auch unterschiedliche Zugriffsberechtigungen auf das System haben.

Eigenes Personal und externe Auftragnehmer nehmen ebenfalls unterschiedliche Aufgaben wahr und sollten daher auch unterschiedliche Zugriffsberechtigungen bekommen.

Die Zugriffsberechtigungen sollten technisch in das System eingebaut sein. So kann beispielsweise das Nutzerprofil einer Person das Kopieren von aufgezeichnetem Bildmaterial erlauben, während das Profil eines anderen nur das Prüfen von Rechten gestattet.

Darüber hinaus muss in der Zugriffsstrategie aber auch klar beschrieben werden, unter welchen Bedingungen die Zugriffsrechte wahrgenommen werden können. Zum Beispiel, in welchen Fällen eine Person, die aufgrund ihres Profils zum Kopieren oder Löschen berechtigt ist, tatsächlich auch berechtigt ist, Bildmaterial zu kopieren oder zu löschen.

Falls die Videoüberwachung zu Sicherheits- und Zugangskontrollzwecken durchgeführt wird, sollten Zugriffsberechtigungen nur internem Personal und ausgegliedertem Sicherheitspersonal sowie den für die technische Wartung des Systems zuständigen Personen erteilt werden.

Beispiel:

Ausgegliederte Sicherheitsbedienstete, die in Ihrem Kontrollraum arbeiten, können in technischer Hinsicht berechtigt sein, das Bildmaterial in Echtzeit anzusehen, die PTZ-Kameras zu bedienen (d. h. einen Gegenstand heranzuzoomen) oder aufgezeichnetes Bildmaterial online anzusehen, sollten jedoch keinen technischen Zugriff auf Merkmale wie Kopieren, Herunterladen, Löschen oder Verändern des Bildmaterials bekommen.

Während von den Sicherheitswachen erwartet wird, dass sie das Bildmaterial in Echtzeit überwachen und die PTZ-Kameras so bedienen, wie es ihre Überwachungsaufgaben erfordern, sollten sie darüber hinaus angewiesen werden, die PTZ-Kameras nicht zum Heranzoomen eines Ziels einzusetzen, etwa einer Gruppe von Personen, die vor dem Gebäude friedlich demonstrieren, oder von zwei Mitarbeitern, die gerade vorbeigehen, wenn dies nicht unbedingt erforderlich ist, um die Sicherheit und Zugriffskontrolle, für welche die Überwachung durchgeführt wird, zu gewährleisten.

8.2 Schulungen in datenschutzrechtlichen Fragen

Alle Mitarbeiter mit Zugriffsberechtigungen, einschließlich ausgegliederten Personals, das für die täglichen Videoüberwachungen oder die Wartung des Systems zuständig ist, sollte in datenschutzrechtlichen Fragen geschult und mit den Bestimmungen dieser Leitlinien insofern vertraut sein, als diese für ihre Aufgaben von Belang sind. Bei diesen Schulungen sollte ein besonderes Augenmerk darauf gelenkt werden, dass die Weitergabe von Bildmaterial aus der Videoüberwachung an andere als die autorisierten Personen verhindert werden muss.

Schulungen sollten dann stattfinden, wenn ein neues System installiert wird, wenn größere Änderungen am System vorgenommen werden, wenn ein neuer Mitarbeiter seine Stelle antritt, sowie in regelmäßigen Abständen im Anschluss daran. Für bereits bestehende Systeme sollte eine erste Schulung in der Übergangszeit vor dem 1. Januar 2011 stattfinden.

8.3 Vertraulichkeit

Alle Mitarbeiter mit Zugriffsberechtigungen, einschließlich ausgegliederten Personals, das für die täglichen Videoüberwachungen oder die Wartung des Systems zuständig ist, einschließlich der ausgegliederten Firmen selbst, sollten Vertraulichkeitserklärungen unterzeichnen, um zu gewährleisten, dass sie den Inhalt von Bildmaterial aus der Videoüberwachung nicht übertragen, zeigen oder anderweitig an andere als die autorisierten Personen weitergeben.

9 Welche Sicherheitsmaßnahmen sind zum Schutz der Daten zu ergreifen?[36]

Zuallererst muss eine interne Analyse der Sicherheitsrisiken durchgeführt werden, um festzulegen, welche Sicherheitsmaßnahmen zum Schutz des Videoüberwachungssystems einschließlich der mit diesem System verarbeiteten personenbezogenen Daten erforderlich sind.

In allen Fällen sind Maßnahmen zu ergreifen, welche die Sicherheit gewährleisten in Bezug auf

- die Übertragung,
- die Speicherung (etwa in Computer-Datenbanken) und
- den Zugriff (etwa Zugriff auf Computersysteme und Räume).

Eine Übertragung muss über sichere Kommunikationskanäle erfolgen und abhörsicher sein. Die Abhörsicherheit ist besonders wichtig, wenn ein drahtloses Übertragungssystem verwendet oder wenn Bildmaterial über das Internet übertragen wird. In diesen Fällen müssen die Daten verschlüsselt übertragen werden oder es ist ein gleichwertiger Schutz vorzusehen.

In anderen Fällen sind auch eine Verschlüsselung oder andere technische Möglichkeiten für einen entsprechenden Schutz während der Übertragung und Speicherung in Betracht zu ziehen, sofern dies aufgrund der internen Analyse der Sicherheitsrisiken gerechtfertigt ist. Dies kann beispielsweise dann der Fall sein, wenn das Bildmaterial besonders sensibel ist.

Alle Räumlichkeiten, in denen Bildmaterial aus der Videoüberwachung gespeichert und auch angesehen wird, sind zu sichern. Der physische Zugang zum Kontrollraum und zu dem Raum, in dem das Bildmaterial aus der Videoüberwachung gespeichert wird, muss geschützt werden. Dritte (z. B. Reinigungs- oder Wartungspersonal) sollten keinen unbeaufsichtigten Zugang zu diesen Räumlichkeiten haben.

Der Standort von Bildschirmen ist so zu wählen, dass unbefugtes Personal sie nicht einsehen kann. Wenn Bildschirme in der Nähe des Empfangsbereichs aufgestellt werden müssen, dann sind sie so zu platzieren, dass nur das Sicherheitspersonal sie einsehen kann.

Es muss ein zuverlässiges digitales Datenerfassungssystem vorhanden sein, damit sich bei einem Audit jederzeit feststellen lässt, wer wann und wo Zugriff auf das System hatte. Das Datenerfassungssystem muss in der Lage sein zu ermitteln, wer Bildmaterial aus der Videoüberwachung angesehen, gelöscht, kopiert oder geändert hat. Diesbezüglich, aber auch anderweitig muss den Schlüsselfunktionen und den Befugnissen der Systemadministratoren sowie der Notwendigkeit, diese mit einer angemessenen Überwachung und mit entsprechenden Schutzvorkehrungen in ein Gleichgewicht zu bringen, besondere Aufmerksamkeit zuteilwerden.

---

[36] Siehe Artikel 22 der Verordnung.

Außerdem muss ein Prozess eingerichtet werden, mit dem angemessen auf eine unbeabsichtigte Weitergabe personenbezogener Daten reagiert werden kann. Dies sollte nach Möglichkeit auch die Meldung einer Verletzung an diejenigen umfassen, deren Daten versehentlich weitergegeben wurden, sowie an den behördlichen Datenschutzbeauftragten des Organs.

Die Sicherheitsanalyse sowie die Maßnahmen zum Schutz des Bildmaterials aus der Videoüberwachung müssen angemessen dokumentiert und dem EDSB auf Wunsch zur Einsichtnahme vorgelegt werden.

Und schließlich muss das Organ mit der gebührenden Sorgfalt bei der Auswahl und Beaufsichtigung ausgegliederter Mitarbeiter vorgehen.

10 Übermittlung und Weitergabe von Daten

10.1 Allgemeiner Rahmen

Für die Übermittlung sieht die Verordnung drei Faustregeln vor, je nachdem, ob die gespeicherten Daten (i) an einen Empfänger innerhalb des Organs oder bei einem anderen Organ, (ii) an andere Empfänger innerhalb der Europäischen Union oder (iii) außerhalb der Europäischen Union übermittelt werden.[37]

Für den ersten Fall sieht die Verordnung vor, dass die gespeicherten Daten an andere Empfänger innerhalb des Organs oder eines anderen Organs übermittelt werden dürfen, falls dies für die rechtmäßige Erfüllung der Aufgaben, die in den Zuständigkeitsbereich des Empfängers fallen, erforderlich ist (nähere Angaben und Beispiele dazu siehe Abschnitt 10.3.).

Für den zweiten Fall (Übermittlung an Empfänger außerhalb der Organe, jedoch innerhalb der Europäischen Union) ist eine Übermittlung dann möglich, wenn dies für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder zur Ausübung der öffentlichen Gewalt gehört, bzw. dann erforderlich ist, wenn der Empfänger auf anderem Wege nachweist, dass die Übermittlung notwendig ist und kein Grund zu der Annahme besteht, dass die berechtigten Interessen derjenigen, deren Bilder übermittelt werden, beeinträchtigt werden könnten (nähere Angaben und Beispiele dazu siehe Abschnitt 10.4.).

Drittens sind Übermittlungen außerhalb der Europäischen Union möglich, (i) wenn dies ausschließlich im Interesse der Wahrnehmung der Aufgaben des Organs geschieht[38] und (ii) nur dann, wenn zusätzliche Erfordernisse gegeben sind, in erster

---

[37] Daten dürfen nur nach Maßgabe von Artikel 7, 8 oder 9 der Verordnung übermittelt werden. Diese Artikel sollten zusammen mit anderen Bestimmungen der Verordnung gelesen werden, insbesondere mit Artikel 4, 5, 6 und 10. Darüber hinaus können die gespeicherten Daten auch der betroffenen Person übermittelt werden, damit diese ihr Auskunftsrecht gemäß Artikel 13 der Verordnung geltend machen kann (siehe Abschnitt 12 dieser Leitlinien).

[38] Von dieser Vorschrift gibt es eine Reihe von Ausnahmen gemäß Artikel 9 Absatz 6, wo es u. a. heißt, dass die Übermittlung möglich ist, wenn sie „zur Feststellung … von Rechtsansprüchen vor Gericht“ erforderlich ist. Dies wiederum sollte so ausgelegt werden, dass auch Anträge der Polizei im Zusammenhang mit Strafverfolgungen darunter fallen.

Linie, um für einen angemessenen Schutz der Daten im Ausland zu sorgen (nähere Angaben und Beispiele dazu siehe Abschnitt 10.4.)

Bei der Beurteilung der Rechtmäßigkeit einer Übermittlung sind jedoch noch viele weitere Bestimmungen der Verordnung zu beachten, in denen zusätzliche Voraussetzungen definiert werden, bevor eine Übermittlung stattfinden kann. Wichtig ist, dass eine Übermittlung zu Zwecken, die mit dem ursprünglich beschriebenen Zweck eines Videoüberwachungssystems nicht in Einklang stehen, meist nicht stattfinden darf.

Beispiel:

Wenn das Videoüberwachungssystem zu Sicherheitszwecken installiert wird und auch als solches angekündigt wurde, dürfen die gespeicherten Daten nicht an den Vorgesetzten des Mitarbeiters übermittelt werden, der diese Daten als Beweismittel anfordert, um nachzuweisen, dass der Betroffene zu spät zur Arbeit erschienen ist.

Von dieser Regel gibt es eine Reihe wichtiger Ausnahmen.[39] Die wichtigste Ausnahme greift dann, wenn die Polizei die Übermittlung der Daten für die Verhütung und Verfolgung von Straftaten verlangt (siehe Abschnitt 10.4)

10.2 Ad-hoc- und systematische Übermittlungen

Die Frage, ob eine Übermittlung möglich ist, setzt häufig voraus, dass zwischen den Rechten der Person und den Rechten oder Interessen derjenigen, die das Bildmaterial anfordern, sorgfältig abgewogen wird. Jede Übermittlung muss von Fall zu Fall sorgfältig geprüft werden.

Im Fall einer Ad-hoc-Übermittlung sollte immer der Rat des behördlichen Datenschutzbeauftragten eingeholt werden, um zu klären, ob die Übermittlung nach Maßgabe der Verordnung rechtmäßig ist. Werden jedoch ähnliche Übermittlungen wiederholt durchgeführt, kann auch die datenschutzrechtliche Folgenabschätzung ähnlich ausfallen. Solche typischen Übermittlungen sollten in der Videoüberwachungsstrategie des Organs beschrieben werden. Sobald eine solche Strategie in Bezug auf derartige Übermittlungen feststeht, ist es nicht erforderlich, den behördlichen Datenschutzbeauftragten für jede einzelne Routineübermittlung um Rat zu bitten, obwohl es immer empfehlenswert ist, ihn im Zweifelsfall hinzuzuziehen.

Beispiel:

Die Kameras in der Nähe Ihres Haupteingangs erfassen auch den angrenzenden Abstellplatz für Fahrräder. Alle paar Monate beantragt die örtliche Polizei die Übermittlung entsprechender Aufzeichnungen für die Verfolgung von

[39] Siehe Artikel 20 der Verordnung.

Fahrraddiebstählen. Sie sollten über eine Strategie verfügen, die Ihnen die Frage beantwortet, wie Sie solche Anträge beantworten. In diesem Fall müssen Sie nicht jedes Mal Ihren behördlichen Datenschutzbeauftragten hinzuziehen

10.3 Übermittlungen an EU-Ermittlungsbehörden

Vorbehaltlich der vorstehend beschriebenen Einzelfallanalyse und in Anbetracht der ursprünglichen Zweckbestimmungen der Aufzeichnung kann das entsprechende Bildmaterial (beispielsweise Bildmaterial, das als Beweismittel dienen kann) in Ausnahmefällen übermittelt werden, wenn dies beantragt wird

- vom Europäischen Amt für Betrugsbekämpfung („**OLAF**“) im Rahmen einer Untersuchung des OLAF,
- vom Untersuchungs- und Disziplinaramt der Kommission („**IDOC**“) im Rahmen eines disziplinarrechtlichen Verfahrens gemäß den Vorschriften in Anhang IX des Statuts der Beamten der Europäischen Union oder
- von denjenigen, die ein förmliches Untersuchungs- oder Disziplinarverfahren innerhalb des Organs durchführen,

sofern berechtigterweise davon ausgegangen werden kann, dass die Übermittlungen bei der Untersuchung oder Verfolgung eines hinlänglich schweren Disziplinarverstoßes oder einer Straftat helfen. Anträgen auf gezielte Datensuche (Data Mining) sollte nicht stattgegeben werden.

Die Leitung, die Personalabteilung oder andere Beteiligte sollten keine Kopien oder einen anderweitigen Zugriff auf Bildmaterial aus der Videoüberwachung außerhalb der genannten förmlichen Verfahren erhalten. Im Zweifelsfall sollte zunächst der behördliche Datenschutzbeauftragte hinzugezogen werden.

Beispiel:

Ein Mitarbeiter reicht Beschwerde gegen seinen unmittelbaren Vorgesetzten wegen Mobbing ein, der wiederum ein Verfahren wegen unzulänglicher fachlicher Leistungen gegen seinen Mitarbeiter einleitet. Außerhalb dieser Verfahren bittet der Vorgesetzte Sie informell, sich nach verdächtigem Bildmaterial des Mitarbeiters „umzusehen“, etwa Aufsuchen des Büros außerhalb der Bürozeiten, zu spätes Erscheinen bei der Arbeit oder Betreten des Büros anderer Personen ohne Aufsicht. Derartigen Ersuchen sollten Sie auf keinen Fall nachkommen.

Und schließlich kann Bildmaterial aus der Videoüberwachung auch an den EDSB übermittelt werden, beispielsweise dann, wenn der EDSB eine Kontrolle vor Ort durchführt oder eine Beschwerde untersucht.

10.4 Übermittlungen an nationale Behörden

Abhängig von der vorstehend beschriebenen Einzelfallanalyse und auch unter

Berücksichtigung der ursprünglichen Zweckbestimmungen der Aufzeichnung kann der nationalen Polizei, Gerichten oder anderen nationalen Behörden in manchen Fällen auch Zugriff auf Bildmaterial aus der Videoüberwachung gewährt werden.

Falls die nationale Polizei, ein Gericht oder andere nationale Behörden die Weiterleitung der gespeicherten Daten verlangen, sollte das Organ darauf bestehen, dass gemäß den Anforderungen des geltenden nationalen Rechts im Hinblick auf Form und Inhalt ein formeller schriftlicher Antrag gestellt wird. Außerdem sollte das Organ die Aufzeichnungen nur dann weitergeben, wenn bei einer anderen in diesem Land niedergelassenen Organisation ebenfalls ein Antrag gestellt worden wäre oder wenn sie zumindest unter ähnlichen Umständen die Genehmigung zur Weiterleitung dieser Daten erhalten hätte.

Unabhängig von den nationalen Anforderungen sollte das Organ nach Möglichkeit eine richterliche Verfügung, einen von einem Polizeibeamten von ausreichend hohem Rang unterzeichneten schriftlichen Antrag oder einen ähnlichen formellen Antrag verlangen. In diesem Antrag sollte der Grund, weshalb das Bildmaterial aus der Videoüberwachung benötigt wird, möglichst genau beschrieben werden, ebenso Ort, Datum und Uhrzeit der Aufnahme des angeforderten Bildmaterials.

Das Organ kann in den meisten Fällen Anträgen der nationalen Polizei stattgeben, wenn die Aufzeichnungen für die Untersuchung oder Verfolgung von Straftaten benötigt werden, sofern die Daten im Rahmen einer konkreten kriminalpolizeilichen Ermittlung angefordert werden. Allgemeinen Anträgen zum Zweck einer gezielten Datensuche (Data Mining) sollte jedoch nicht stattgegeben werden.

Beispiel:

Vor Ihrem Gebäude findet eine Demonstration statt, an der auch illegale Zuwanderer teilnehmen, weil sie auf die Notwendigkeit aufmerksam machen wollen, ihre Situation zu legalisieren. Am Ende dessen, was sich als friedliche Demonstration ohne Sicherheitsvorfälle erwiesen hat, verlangt die nationale Polizei ohne Verweis auf eine konkrete kriminalpolizeiliche Ermittlung von Ihnen, dass Sie Ihr gesamtes Bildmaterial aus der Videoüberwachung, das Sie aufgenommen haben, übergeben, da sie dieses Bildmaterial zur Identifizierung illegaler Zuwanderer nutzen und deren Bilder gegebenenfalls für mögliche zukünftige Gelegenheiten aufbewahren möchte. Einem solchen Antrag sollten Sie nicht stattgeben.

Bitte beachten Sie auch, dass die Polizei eines Mitgliedstaats oder eine andere nationale Organisation, die während eines ordentlichen Verfahrens einen Antrag auf Zugriff stellt, zunächst verpflichtet ist, die Aufhebung der Immunität zu beantragen, falls das Bildmaterial einen EU-Bediensteten betrifft.

10.5 Register der Übermittlung und Weitergabe von Daten

Die Organe sollten ein Register – nach Möglichkeit in elektronischer Form – der übermittelten und weitergegebenen Daten führen. Darin sollte jede Übermittlung an

Dritte erfasst werden (Dritte sind auch alle Personen innerhalb eines Organs, an die Daten von denjenigen übermittelt werden, die zunächst Zugriff auf die gespeicherten Daten haben. Darunter fällt typischerweise auch jede Übermittlung an Empfänger außerhalb der Sicherheitsabteilung). In das Register sollten darüber hinaus alle Fälle eingetragen werden, in denen die Aufzeichnungen Dritten gezeigt wurden, auch wenn keine Kopie des Bildmaterials aus der Videoüberwachung übermittelt wurde, oder in denen Dritten der Inhalt der Aufzeichnungen auf anderem Wege offengelegt wurde.

Das Register sollte mindestens folgende Angaben enthalten:

- Datum der Aufzeichnungen,
- Antrag stellende Partei (Name, Titel und Organisation),
- Name und Titel der Person, die die Übermittlung genehmigt hat,
- kurze Beschreibung des Inhalts der Aufzeichnungen,
- Grund für den Antrag und Grund für dessen Bewilligung und
- ob eine Kopie des Bildmaterials übermittelt, das Bildmaterial gezeigt oder verbal darüber Auskunft erteilt wurde.

Der DSB sowie der EDSB können von dem Organ jederzeit die Vorlage einer Kopie des Registers zur Kontrolle verlangen.

11 Wie ist die Öffentlichkeit zu informieren?

11.1 Mehrstufiger Ansatz

Die Öffentlichkeit muss effizient und umfassend über die Videoüberwachung informiert werden.[40] In den Leitlinien wird ein mehrstufiger Ansatz empfohlen, der auf einer Kombination der folgenden beiden Methoden beruht:

- Hinweise vor Ort, mit denen die Öffentlichkeit unmittelbar darauf aufmerksam gemacht wird, dass eine Überwachung stattfindet, und ihr die wesentlichen Informationen über das Vorgehen mitgeteilt werden, und
- eine detaillierte Datenschutzerklärung, die in das Intranet des Organs und ins Internet für all diejenigen eingestellt werden, die mehr wissen möchten (zur Vermeidung von Doppelarbeit kann das Organ die öffentliche Fassung seiner Videoüberwachungsstrategie ins Internet stellen, anstatt eine gesonderte Datenschutzerklärung zu erstellen).

Diese beiden Methoden können durch weitere Methoden ergänzt werden. So können beispielsweise Ausdrucke der Datenschutzerklärung am Empfang ausgelegt und auf Wunsch bei der Sicherheitsabteilung angefordert werden, und außerdem sollte das Organ auch eine Telefonnummer und eine E-Mail-Adresse für weitere Anfragen bereitstellen. Ausführlichere Informationen im Intranet oder Internet (sowie

[40] Die gesetzlich vorgeschriebene Liste der Angaben, die in Ihrem Hinweis enthalten sein müssen, siehe Artikel 12 der Verordnung.

Merkblätter und Informationen auf anderen Wegen) sind jedoch kein Ersatz für Hinweise vor Ort.

11.2 Hinweise vor Ort

Hinweise vor Ort sollten ein Piktogramm (z. B. das ISO-Piktogramm oder das Piktogramm, das normalerweise am Standort des Gebäudes verwendet wird) und alle in Artikel 12 vorgesehenen Angaben umfassen, die den Umständen entsprechend angemessen sind. Der Hinweis muss folgende Angaben enthalten:

- die Identität des „für die Verarbeitung Verantwortlichen“ (normalerweise genügt der Name des Organs);
- es ist der Zweck der Überwachung anzugeben (normalerweise genügt es, „für Ihre Sicherheit“ anzugeben);
- es muss klar ersichtlich sein, ob die Bilder gespeichert werden;
- Kontaktangaben und einen Link zur Online-Videoüberwachungsstrategie;
- wenn Bereiche außerhalb des Gebäudes überwacht werden, sollte darauf ausdrücklich aufmerksam gemacht werden. Wenn in einem solchen Fall nur ein Hinweis erfolgt, dass *das Gebäude* videoüberwacht wird, könnte dies irreführend sein.

Das Sicherheits- und Empfangspersonal muss in datenschutzrechtlichen Aspekten der Videoüberwachung geschult und in die Lage versetzt werden, auf Wunsch sofort Kopien der ausführlichen Datenschutzerklärung (Videoüberwachungsstrategie) vorzulegen. Es muss außerdem in der Lage sein, der Öffentlichkeit zu erklären, an wen sie sich bei weiteren Fragen oder bei dem Wunsch, Zugriff auf die sie betreffenden Daten zu bekommen, wenden soll.

Die Hinweistafeln müssen so aufgestellt werden und groß genug sein, dass die betroffenen Personen sie bemerken, bevor sie den überwachten Bereich betreten, und sie problemlos lesen können. Dies bedeutet nicht, dass neben jeder einzelnen Kamera ein Hinweis angebracht werden muss.

Beispiel:

Ihr Organ beschäftigt 50 Mitarbeiter und ist in einem kleinen Gebäude in einem dicht bebauten Stadtgebiet untergebracht. Möglicherweise wollen Sie Hinweistafeln in der Größe A3 am Haupteingang des Gebäudes, ein etwas größeres Schild an der Parkhauseinfahrt (so, dass es vom Fahrersitz aus sichtbar ist) und weitere Hinweistafeln in der Größe A3 neben den Fahrstuhltüren im Parkhaus und im Erdgeschoss anbringen. Falls es weitere Eingänge gibt, sollten dort ebenfalls Schilder angebracht werden.

Die innerhalb des Gebäudes angebrachten Hinweisschilder müssen in der Sprache (bzw. in den Sprachen) abgefasst sein, die das Personal und die meisten Besucher in der Regel auch verstehen. Hinweisschilder außerhalb der Gebäude (falls auch Außenbereiche überwacht werden) müssen ebenfalls in der Landessprache (bzw. den Landessprachen) abgefasst sein.

Falls Kameras in Bereichen angebracht werden, in denen von den dort anwesenden Personen verstärkte Erwartungen an den Schutz der Privatsphäre gestellt werden (siehe Abschnitt 6.8) oder in denen man ansonsten keine Kameras erwartet würde und die Personen deshalb völlig überrascht reagieren, muss ein zusätzlicher Hinweis vor Ort in unmittelbarer Nähe des überwachten Bereichs (etwa an der Tür eines überwachten Einzelbüros) angebracht werden.[41]

Anhang 2 enthält ein Muster für einen Hinweis vor Ort, der von den Organen entsprechend ihren jeweiligen Erfordernissen angepasst werden kann.

11.3 Videoüberwachungsstrategie online

Wenn Sie eine Videoüberwachungsstrategie beschließen und diese in Ihr Intranet oder ins Internet einstellen, kommen Sie damit auch Ihrer Verpflichtung nach, eine ausführliche Datenschutzerklärung vorzulegen. Dementsprechend müssen Sie auch keine separate Online-Datenschutzerklärung erstellen und ins Netz stellen.

Damit Ihre Videoüberwachungsstrategie auch als Datenschutzerklärung fungieren kann, muss sie folgende Angaben in einer benutzerfreundlichen Sprache und einem entsprechenden Format enthalten:

- Identität des „für die Verarbeitung Verantwortlichen“ (z. B. Organ, Generaldirektion, Direktion und Referat)
- Kurzbeschreibung des Erfassungsbereichs des Videoüberwachungssystems (z. B. Eingänge und Ausgänge, Computerräume, Archivräume)
- Rechtsgrundlage für die Videoüberwachung,
- erfasste Daten und Zweck der Videoüberwachung (Einschränkungen der zulässigen Verwendungszwecke sollten ebenfalls genau beschrieben werden)
- Wer hat Zugang zum Bildmaterial aus der Videoüberwachung und an wen dürfen die Bilder weitergegeben werden?
- Wie werden die Daten geschützt und gesichert?
- Wie lange werden die Daten aufbewahrt?
- Wie können die betroffenen Personen die sie betreffenden Daten (einschließlich Kontaktangaben für weitere Fragen und Informationen darüber, wie sie intern Beschwerde einlegen können) überprüfen, abändern oder löschen?
- Recht, den EDSB jederzeit hinzuziehen zu können.

Die Videoüberwachungsstrategie sollte darüber hinaus Hyperlinks enthalten zu:

- den Leitlinien des EDSB zum Thema Videoüberwachung,
- dem/den Auditbericht/-en des Organs,
- dem/den Bericht/-en des Organs über die Folgenabschätzung/-en,
- ggf. der Stellungnahme des EDSB zur Vorabkontrolle.

[41] Siehe auch Abschnitt 6.11 zum Thema verdeckte Videoüberwachung.

Anhang 1 enthält ein Muster für eine Videoüberwachungsstrategie (die auch als Online-Datenschutzerklärung fungieren kann) für ein handelsübliches Videoüberwachungssystem. Diese Strategie kann benutzerspezifisch angepasst werden

11.4 Individuelle Hinweise

Natürliche Personen müssen auch individuell darauf aufmerksam gemacht werden, dass sie von einer Kamera identifiziert wurden (etwa vom Sicherheitspersonal bei einer Sicherheitsuntersuchung), sofern eine oder mehrere der nachstehenden Bedingungen ebenfalls erfüllt sind:

- Die Identität der Person wird in Dateien bzw. Unterlagen festgehalten,
- die Videoaufnahme wird gegen die Person verwendet,
- die Videoaufnahme wird über die vorschriftsmäßige Aufbewahrungszeit hinaus gespeichert,
- die Videoaufnahme wird an Empfänger außerhalb der Sicherheitsabteilung übermittelt *oder*
- die Identität der Person wird jemandem außerhalb der Sicherheitsabteilung offengelegt.

Solche Hinweise können zuweilen vorübergehend zurückgestellt werden, etwa dann, wenn dies für die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten erforderlich ist.[42] Falls eine solche Situation eintritt, ziehen Sie bitte Ihren behördlichen Datenschutzbeauftragten zurate.

12 Wie kann Anträgen der Öffentlichkeit auf Zugriff stattgegeben werden?

Wenn eine natürliche Person die Anfrage stellt, welche Daten das Organ über sie verarbeitet, muss diese Anfrage zeitnah und so ausführlich beantwortet werden, wie es in Anbetracht der Anliegen des Antragstellers angemessen ist.

Ist die Anfrage sehr allgemein gehalten, reicht ein Verweis auf die Videoüberwachungsstrategie aus.

Beispiel:

Eine Person in einem Mitgliedstaat A, in dem sich Ihr Gebäude befindet, schickt Ihnen eine E-Mail mit folgendem Inhalt: „Ich mache mir Sorgen aufgrund der Videoüberwachung außerhalb Ihres Gebäudes, an dem ich jeden Tag vorbeigehe. Bitte lassen Sie mir ausführlichere Informationen über die Videoüberwachung und die von Ihnen verarbeiteten mich betreffenden Daten zukommen“. Eine allgemeine Antwort, in der auf Ihre Videoüberwachungsstrategie verwiesen wird, reicht in diesem Fall aus.

[42] In Ausnahmefällen greifen auch andere Ausnahmen gemäß Artikel 20 der Verordnung.

Bei anderen, spezifischeren Anfragen ist eine ausführlichere Antwort erforderlich. Falls dies konkret gefordert wird, muss Zugang zu den Aufzeichnungen gewährt werden, damit sich die betreffende Person die Aufzeichnungen ansehen kann, oder sie muss eine Kopie davon erhalten. In diesem Fall müssen die Rechte Dritter, die ebenfalls mit aufgezeichnet wurden, sorgfältig geprüft und bei Bedarf geschützt werden (etwa, indem die Einwilligung für die Weitergabe oder Bearbeitung der Bilder wie Maskieren oder Verwürfeln eingeholt wird). Der Schutz der Rechte Dritter sollte jedoch nicht als Vorwand benutzt werden, um die berechtigten Forderungen natürlicher Personen auf Zugriff auf ihre Daten abzuwehren, insbesondere, wenn die Aufzeichnungen als Beweismittel dienen.

Beispiele:

Ein Mitarbeiter, gegen den ein Disziplinarverfahren wegen Mobbing läuft, fragt, ob Sie im Zusammenhang mit dem Verfahren ihn betreffendes Bildmaterial aus einer Videoüberwachung durchgesehen und der Leitung, der Polizei oder anderen Personen übermittelt haben. Falls dies nicht der Fall ist, würde als Antwort ein einfaches „Nein“ genügen.

Sollten Sie jedoch Daten übermittelt haben, sollten Sie dies auch zugeben und genau angeben, was auf diesem Bildmaterial zu sehen war, wann und wo es aufgenommen wurde und wem es aus welchen Gründen übermittelt wurde.

Sie sollten, sofern der Mitarbeiter konkret darum gebeten hat, vorbehaltlich der Rechte anderer Personen, die auf diesem Bildmaterial ebenfalls zu sehen sind, und je nach den Umständen des Falles dem Mitarbeiter die Möglichkeit geben, das übermittelte Bildmaterial anzusehen, oder ihm eine Kopie davon zur Verfügung stellen.

Der Zugang zu den Mindestangaben gemäß Artikel 13 der Verordnung ist kostenlos zu gewähren. Die Bereitstellung eines kostenfreien Zugangs sollte aber auch eine Standardregelung sein für den Fall, dass ausführlichere Informationen oder der Zugang zu Aufzeichnungen aus der Videoüberwachung gewünscht werden. Falls die Zahl der Anträge auf Zugriff auf solche Daten erheblich steigt, kann die Standardregelung allerdings durch eine begründete Entscheidung geändert werden, um zu versuchen, lästige oder unseriöse Anfragen zu verhindern. In diesem Fall kann man zunächst einen *angemessenen Betrag* für die Bereitstellung von Kopien der Aufzeichnungen oder für die Möglichkeit, sich die Aufzeichnungen anzusehen, zur Deckung der entstandenen Kosten in Verbindung mit der Bereitstellung des Zugangs in Rechnung stellen. Die Kosten dürfen nicht zu hoch sein, und sie dürfen auch nicht zur Abwehr berechtigter Anträge auf Einsichtnahme in die Daten benutzt werden. In der Videoüberwachungsstrategie muss darauf hingewiesen werden, dass eine Gebühr für die Bereitstellung des Zugangs erhoben wird.

Anträge auf Zugang müssen zeitnah beantwortet werden. Es sollte nach Möglichkeit ein Zugang gewährt oder, falls dies nicht möglich ist, innerhalb von 15 Kalendertagen eine andere aussagekräftige Antwort (und nicht nur eine Empfangsbestätigung)

erteilt werden.

Beispiel:

Ein Mitarbeiter beantragt den Zugriff auf eine Aufzeichnung und gibt die Uhrzeit und den Ort dieser Aufzeichnung an. Eile ist seinen Aussagen zufolge nicht geboten, und er gibt auch nicht an, aus welchem Grunde er den Antrag stellt und ob er eine Kopie wünscht oder sich lediglich die Aufzeichnung ansehen möchte. Ansonsten macht er alle erforderlichen Angaben (Identitätsnachweis, Foto). Innerhalb von wenigen Tagen nach Eingang des Antrags machen Sie die Aufzeichnung ausfindig. Darauf sind mehrere andere Personen im Hintergrund zu sehen. Innerhalb weniger weiterer Tage redigieren Sie die Bilder der Personen im Hintergrund heraus und schicken dem Mitarbeiter eine E-Mail, in der Sie ihn bitten, einen Termin zu vereinbaren, an dem er die Bilder in Ihren Räumlichkeiten ansehen kann. Wenn der Mitarbeiter, der die Einsichtnahme beantragt hat, schnell darauf antwortet, kann ihm der Zugang zu den Bildern innerhalb von zwei Wochen gewährt werden.

In komplexeren Fällen kann eine Bestätigung zusammen mit weiteren Informationen zur Ursache der Verzögerung und zu dem Datum, an dem in dem Verfahren voraussichtlich weitere Schritte ergriffen werden, verschickt werden. Die Gewährung des Zugangs (oder eine endgültige, aussagekräftige Antwort, mit der der Zugang verweigert wird) darf jedoch auch unabhängig von der Komplexität des Falles um maximal drei Monate gemäß dem in der Verordnung[43] genannten Zeitraum hinausgezögert werden. In den meisten Fällen sollte der Zugang sehr viel eher gewährt werden.

Dringliche Anträge müssen so bald wie möglich beantwortet werden, und es müssen – sofern machbar – alle aufgrund der Umstände des Falles erforderlichen oder ersichtlichen Fristen eingehalten werden.

Sollten Sie Zweifel bezüglich der Frage haben, wie Sie einen besonderen Antrag auf Zugang beantworten sollen, so wenden Sie sich bitte an den DSB. Besteht zwischen dem Organ und der Person, die den Zugang beantragt, ein Dissens, sollte Ihnen ein einfaches und effizientes internes Prüf- oder Beschwerdeverfahren zur Verfügung stehen. Dieses sollte nicht nur den Bediensteten, sondern auch Dritten, die einen Zugang beantragen, offenstehen.

Die Öffentlichkeit muss sowohl im Rahmen der Videoüberwachungsstrategie als auch in der Antwort auf den Antrag auf Zugang über dieses Prüfverfahren unterrichtet werden.

13 Rechenschaftspflicht: Gewährleistung, Überprüfung und

[43] Siehe Artikel 13 der Verordnung.

Nachweis einer guten Verwaltungspraxis

Organe müssen Strategien und Verfahren einrichten, die gewährleisten, dass sie die Videoüberwachung im Einklang mit der Verordnung einsetzen.[44] Im Sinne von Transparenz und guter Verwaltungspraxis und als Nachweis gegenüber seinen Mitarbeitern, dem EDSB sowie anderen Interessengruppen,[45] dass es die Vorgaben einhält, sollte jedes Organ die Einhaltung seiner Verfahren mit den Bestimmungen dieser Leitlinien überprüfen und dokumentieren.

Der EDSB empfiehlt insbesondere nachdrücklich, dass jedes Organ

- eine Videoüberwachungsstrategie beschließt,
- in regelmäßigen Abständen Audits durchführt und deren Ergebnisse in Auditberichten dokumentiert.

Darüber hinaus sollte in den in Abschnitt 3.2 genannten Fällen auch eine Folgenabschätzung durchgeführt und in einem Bericht zur Folgenabschätzung dokumentiert werden.

13.1 Videoüberwachungsstrategie

Die Videoüberwachungsstrategie sollte

- einen Überblick über das Videoüberwachungssystem geben und dessen Zweckbestimmungen beschreiben,
- beschreiben, wie das System betrieben wird, welche personenbezogenen Daten verwendet werden und welche Datenschutzvorkehrungen eingerichtet wurden,
- ausdrücklich die Übereinstimmung und Vereinbarkeit mit der Verordnung und den Leitlinien bestätigen,
- Abweichungen von den in den Leitlinien empfohlenen üblichen Verfahren beschreiben und die Gründe dafür erläutern,
- erforderliche Umsetzungsmaßnahmen darstellen.

Bei der Videoüberwachungsstrategie handelt es sich um ein Dokument, das mehreren Zwecken dient und das die folgenden Anforderungen an eine gute Verwaltungspraxis erfüllen soll:

- Die Verabschiedung dieses Dokuments ist häufig erforderlich, um die Rechtsgrundlage zu vervollständigen und genau darzulegen und damit eine rechtmäßige Begründung für die Videoüberwachung anzuführen.[46]

---

[44] Artikel 22 Absatz 1 der Verordnung.

[45] Stellungnahme 168 der Artikel-29-Datenschutzgruppe vom 1. Dezember 2009 zum Thema „Die Zukunft des Datenschutzes“, auf die in Fußnote 13 Bezug genommen wird. Siehe insbesondere Kapitel 6 zum Thema „Stärken der Verantwortung des für die Datenerarbeitung Verantwortlichen“.

[46] Artikel 5 Buchstabe a der Verordnung. Siehe auch Artikel 8 Absatz 2 der Charta der Grundrechte der Europäischen Union und die damit verbundene Rechtsprechung.

- Durch die schriftliche Darstellung vorhandener bewährter Verfahren und gründliche Überlegungen darüber, welche weiteren Maßnahmen ergriffen werden müssen, können die Verfahren verbessert und eine bessere Vereinbarkeit gewährleistet werden.
- Die Annahme einer Strategie, die der Öffentlichkeit zugänglich gemacht wird, hilft ebenfalls dabei, der Verpflichtung aus der Verordnung nachzukommen, der Öffentlichkeit die notwendigen Informationen mitzuteilen, um eine Verarbeitung nach Treu und Glauben zu gewährleisten.
- In der Strategie wird eine Reihe von Regeln festgelegt, anhand derer die Vereinbarkeit gemessen werden kann (z. B. bei einem Audit).
- Und schließlich können Organe durch die Verbesserung der Transparenz und den Nachweis ihrer Bemühungen um Vereinbarkeit
    - Vertrauen bei ihren Mitarbeitern und bei Dritten schaffen,
    - die Anhörung von Interessengruppen erleichtern und
    - die wechselseitigen Beziehungen mit dem EDSB vereinfachen.

Die Organe sollten ihre Videoüberwachungsstrategien in ihrem Intranet und auf ihren Internet-Seiten der Öffentlichkeit zugänglich machen. Falls dieses Dokument vertrauliche Informationen enthält, sollte eine nicht vertrauliche Fassung für die Öffentlichkeit bereitgestellt werden.

Beispiele:

Falls erforderlich, Sicherheitsmaßnahmen zum Schutz Ihres Videoüberwachungssystems; die ausführliche Karte mit dem genauen Standort der Kameras und mit Spezifikationen; oder aber, es können bestimmte spezielle Überwachungsmaßnahmen in Verbindung mit dem Kampf gegen Terrorismus in Form einer Übersicht zusammengefasst werden, damit die Sicherheit oder die Effizienz des Systems nicht gefährdet wird und hochgradig sensible Daten oder Verschlusssachen nicht preisgegeben werden.

Anhang 1 enthält eine Mustervorlage für eine Videoüberwachungsstrategie, die von den Organen benutzerspezifisch anpassen werden kann.

13.2 Datenschutzaudit

Jedes Organ sollte überprüfen und in einem Datenschutzaudit („**Audit**“) dokumentieren, ob seine Verfahren mit den Bestimmungen der Verordnung, mit diesen Leitlinien und mit seiner eigenen Videoüberwachungsstrategie in Einklang stehen. Die Ergebnisse sollten in einem schriftlichen Auditbericht („**Auditbericht**“) zusammengefasst werden.

Mit dem Audit werden zwei Ziele verfolgt:

- Es soll überprüft werden, ob es eine dokumentierte und aktualisierte Videoüberwachungsstrategie gibt und ob diese Strategie mit der Verordnung und den Leitlinien übereinstimmt („**Angemessenheitsaudit**“), und
- es soll geprüft werden, ob die Organisation tatsächlich im Einklang mit ihrer

Videoüberwachungsstrategie arbeitet („**Konformitätsaudit**“). Dazu gehört auch eine Überprüfung, ob sich das Personal dieser Strategie bewusst ist, sie versteht, ihre Bestimmungen einhält und ob die Strategie tatsächlich funktioniert und wirksam ist.

In einem Angemessenheitsaudit geht es an erster Stelle darum, dass eine dokumentierte Strategie zu der Frage vorhanden ist, wie mit datenschutzrechtlichen Fragen umgegangen wird und dass sich diese Strategie tatsächlich hinlänglich mit allen Anforderungen der Verordnung und der Leitlinien befasst. Bei einem Konformitätsaudit geht es um die Frage, wie die Strategie in Wirklichkeit genutzt wird und wie wirksam sie ist.

Das Audit ist u. a. mit folgenden Vorteilen verbunden:

- Es erleichtert die Einhaltung der Datenschutzvorschriften;
- es schärft das Problembewusstsein für datenschutzrechtliche Fragen bei Leitung und Mitarbeitern;
- es liefert Impulse im Hinblick auf die notwendige Überprüfung der Videoüberwachungsstrategie und
- es verringert die Wahrscheinlichkeit von Fehlern, die zu einer Beschwerde führen.

Der Auditbericht sollte

- Aufschluss geben über Datum, Umfang und Mitglieder des Auditteams usw.,
- die wichtigsten Ergebnisse des Audits und die dabei festgestellten Fälle von Nichtübereinstimmung zusammenfassen,
- Vorschläge für Korrekturmaßnahmen dokumentieren und
- Aufschluss über die Art und den zeitlichen Rahmen vereinbarter Folgemaßnahmen geben.

Ein Teil des Angemessenheitsaudits kann extern anhand von schriftlichen Unterlagen erstellt werden. Für ein vollständiges Audit ist es jedoch von zentraler Bedeutung, Besuche vor Ort durchzuführen, Software und Hardware für die Videoüberwachung sowie vor Ort ausgehängte Datenschutzerklärungen, Register der Aufbewahrung und Übermittlung von Daten, Protokolldateien, Anträge auf Zugang und andere Unterlagen über die Nutzung des Systems zu begutachten und Gespräche mit der Leitung und mit Mitarbeitern zu führen.

Das Audit kann intern (Selbstaudit) durchgeführt werden, oder aber es werden unabhängige Dritte mit seiner Durchführung beauftragt (Drittaudit). Der Drittprüfer kann beispielsweise ein anderes Organ sein, wenn Audits gegenseitig erstellt werden. In diesem Fall prüfen die Organisationen gegenseitig ihre Verfahren, was Leistungsvergleichen und der Annahme bewährter Verfahren zugutekommen kann.

Es sollte nach Möglichkeit gewährleistet werden, dass die Prüfer unabhängig von der Funktion sind, die geprüft wird (typischerweise die Sicherheitsabteilung). Außerdem empfiehlt der EDSB dringend, dass der DSB des Organs eine maßgebliche Rolle sowohl bei der Konzeption als auch bei der Umsetzung der Prüfverfahren des Organs spielen sollte und dass ihm hierfür ausreichende Ressourcen zur Verfügung

gestellt werden sollten. Für Selbstaudits empfiehlt der EDSB, dass nach Möglichkeit die internen Prüfer des Organs in das Auditteam einbezogen und angemessen in datenschutzrechtlichen Fragen und den Leitlinien geschult werden sollten. Das Prüfverfahren darf auf keinen Fall die Unabhängigkeit der behördlichen Datenschutzbeauftragten gefährden. Die behördlichen Datenschutzbeauftragten und ihre Mitarbeiter sollten bei dem Audit und bei seiner Weiterverfolgung eine aktive Rolle spielen, unabhängig davon, ob sie offiziell Mitglieder des Auditteams sind oder nicht.

Der EDSB kann zur Durchführung von Audits beratend tätig sein. Diese Beratung kann auch Checklisten zur Vereinbarkeit sowie weitere Beratung zur Methodik umfassen, die beim Audit zugrunde gelegt wird.

Ein Audit sollte vor Inbetriebnahme des Videoüberwachungssystems, aber auch in regelmäßigen Abständen danach stattfinden, mindestens jedoch alle zwei Jahre, und außerdem jedes Mal, wenn eine wichtige Änderung der Umstände eine Überprüfung rechtfertigt. Bei einem wichtigen Systemausbau ist normalerweise eine Überprüfung ebenfalls gerechtfertigt.

14 Ausgliederung und Dritte

14.1 Ausgliederung der Videoüberwachung

Auch wenn das Organ einen Teil seiner Videoüberwachung ausgliedert, haftet es weiterhin als „für die Verarbeitung Verantwortlicher“. Daher ist bei der Auswahl der Auftragnehmer die gebührende Sorgfalt walten zu lassen, und bei der Überprüfung der Vereinbarkeit muss ein proaktiver Ansatz gewählt werden.

Die datenschutzrechtlichen Verpflichtungen des Auftragsverarbeiters sind in Schriftform und rechtsverbindlich niederzulegen. Dies bedeutet normalerweise, dass zwischen dem Organ und der ausgegliederten Firma ein schriftlicher Vertrag geschlossen werden muss. Die ausgegliederte Firma muss auch mit ihren Unterauftragnehmern einen schriftlichen Vertrag schließen.

Der Vertrag sowie die Leistungsbeschreibung sollten beinhalten, dass der Auftragnehmer die Bestimmungen

- der Verordnung,
- dieser Leitlinien,
- der Videoüberwachungsstrategie des Organs und
- Ratschläge des ESDB, etwa bei einer möglichen Vorabkontrolle oder einem Beschwerdeverfahren oder infolge einer Kontrolle oder Anhörung,

einhalten sollte.

Der Vertrag sowie die Leistungsbeschreibung müssen außerdem einen klaren und konkreten Verweis enthalten auf die Verpflichtungen des Vertragsunternehmens im Hinblick auf

- Sicherheit,
- Vertraulichkeit und
- auf seine Verpflichtung, ausschließlich auf Anweisung des Organs tätig zu werden.[47]

Das Vertragsunternehmen muss außerdem sein Personal entsprechend schulen, einschließlich in datenschutzrechtlichen Fragen. Jeder direkte oder indirekte Unterauftragnehmer unterliegt denselben Verpflichtungen wie der direkte Auftragnehmer. Das Organ sollte in der Lage sein, gegen die Wahl der Unterauftragnehmer Einspruch zu erheben, falls begründete Zweifel in Bezug auf deren Fähigkeit aufkommen, die datenschutzrechtlichen Anforderungen zu erfüllen.

Falls erforderlich, sollten dem Auftragsverarbeiter ausführliche Anweisungen erteilt werden, um die Einhaltung der Schutzgarantien in der Verordnung und in diesen Leitlinien zu gewährleisten. Diesbezüglich sollte man besonders darauf achten, dass gewährleistet ist, dass der Öffentlichkeit und den Mitarbeitern des Organs angemessene Datenschutzerklärungen vorgelegt werden.

14.2 Videoüberwachung durch Dritte

Gelegentlich wird eine Videoüberwachung nicht vom Organ oder von einem Auftragnehmer in dessen Auftrag, sondern vielmehr vom Vermieter der Räumlichkeiten des Organs oder von einem Auftragnehmer im Namen des Vermieters durchgeführt. In manchen Fällen besteht sogar ein komplexes vertragliches System aus mehreren Miet- und Untermietverträgen und/oder mehreren Auftragnehmern und Unterauftragnehmern, und das Organ hat nur geringen oder gar keinen vertraglichen Einfluss auf den Betreiber des Videoüberwachungssystems.

Beispiel:

Organ A hat eine Etage in einem großen Gebäude von Organ B angemietet, das die übrigen Etagen des Gebäudes bezogen hat. Organ B wiederum mietet die Räumlichkeiten vom Besitzer des Gebäudes, Unternehmen C. Unternehmen C hat die Wartung des Gebäudes an Firma D fremdvergeben. Firma D wiederum hat die Wartung der Sicherheitstechnik, einschließlich des Betriebs eines Videoüberwachungssystems, an eine Fachfirma, Firma E, fremdvergeben. In diesem Fall besteht das Vertragsverhältnis zwischen dem Organ und der Firma, die die Videoüberwachung tatsächlich durchführt, aus vier Ebenen.

Auch wenn das Organ in derartigen Situationen meist nicht als „für die Verarbeitung Verantwortlicher“ angesehen wird, sollte es trotzdem eine proaktive Rolle spielen und entsprechende Anstrengungen unternehmen, um zu gewährleisten, dass sich der für die Verarbeitung Verantwortliche bei der Videoüberwachung an diese Leitlinien hält. So sollte es beispielsweise mit dem Vermieter (oder ggf. anderen Beteiligten) verhandeln, damit die Einhaltung wichtiger Schutzvorkehrungen in der Verordnung

[47] Siehe Artikel 22 und 23 der Verordnung.

gewährleistet ist (z. B., dass Hinweise vor Ort angebracht und ausführlichere Informationen in das Intranet und die Websites des Organs eingestellt werden).

15 Übergangsbestimmungen und zukünftige Aktualisierungen

Die Leitlinien gelten sowohl für bereits eingerichtete als auch für noch zu installierende Videoüberwachungssysteme und zukünftige Aktivitäten. Jedes Organ hat bis zum 1. Januar 2011 Zeit, seine bestehenden Verfahren mit den Leitlinien in Einklang zu bringen. Die Vereinbarkeit für bestehende Systeme herstellen bedeutet, dass die Organe bis zu diesem Datum

- überprüfen sollten, welche Verfahren es bei ihnen gibt,
- aufzeigen sollten, welche weiteren Schritte auf dem Weg zu einer uneingeschränkten Vereinbarkeit erforderlich sind, und
- alle notwendigen Maßnahmen im Hinblick auf eine uneingeschränkte Vereinbarkeit ergreifen sollten.

Diese Ex-post-Überprüfung muss in den meisten Fällen gar nicht kompliziert oder aufwändig sein, und sie sollte auf keinen Fall mit unnötigem Verwaltungsaufwand verbunden sein. Viele Organe, die in der Vergangenheit mit ihren behördlichen Datenschutzbeauftragten über ihre Videoüberwachungssysteme gesprochen haben, stellen möglicherweise fest, dass ihre bestehenden Verfahren den Empfehlungen in diesen Leitlinien bereits weitgehend entsprechen und sie diese daher meist nur noch überprüfen und schriftlich bestätigen müssen. Darüber hinaus - und dies ist ein wichtiger Punkt - können die Organe aufgrund der Überprüfung auch gezielte, konkrete Anpassungen vornehmen, um den Grad der Vereinbarkeit weiter zu verbessern.

Im Sinne einer möglichst effizienten Durchführung dieser Ex-post-Überprüfung empfiehlt der EDSB einen umfassenden Ansatz, bei dem jedes Organ nur einen einzigen Schritt durchführt, bei dem

- es (entweder im Rahmen eines förmlichen Audits oder einer informellen Bestandsaufnahme) die Angemessenheit und Vereinbarkeit der bestehenden Verfahren mit der Verordnung und den Leitlinien überprüft,
- die Videoüberwachungsstrategie des Organs erstellt (oder aktualisiert) und schließlich
- die überprüften Verfahren anhand der überarbeiteten Strategie, der Leitlinien und der Verordnung im Rahmen eines förmlichen Angemessenheits- und Konformitätsaudits prüft.

Im Rahmen dieser Prüfung sollte, sofern dies notwendig oder hilfreich ist, auch eine Ex-post-Folgenabschätzung durchgeführt werden.

15.1. Ex-post-Überprüfung des Compliance-Status und Ex-post-

Vorabkontrolle[48]

Zugleich muss jeder DSB dem EDSB den Compliance-Status seines Organs mitteilen. Dies kann in Form eines einfachen Schreibens an den EDSB erfolgen. Dieses Schreiben muss folgende Angaben enthalten:

- Bestätigung, dass das Organ eine Videoüberwachungsstrategie beschlossen und
- ein Audit durchgeführt hat;
- Angaben zu der Frage, ob das Organ eine Folgenabschätzung durchgeführt hat und
- ob das Organ der Auffassung ist, dass eine Ex-post-Vorabkontrolle erforderlich ist, und wenn ja, weshalb.

Dem Schreiben sind folgende Unterlagen beizufügen:

- die Videoüberwachungsstrategie (zusammen mit ihren Anhängen),
- der Auditbericht und
- ggf. der Bericht zur Folgenabschätzung.

Wenn trotz aller Bemühungen eines Organs die Vereinbarkeit bestimmter, spezifischer Punkte bis zum Stichtag 1. Januar 2011 nicht hergestellt werden kann, sollte das Organ einen Plan verabschieden, in dem es sich selbst verpflichtet, Schritt für Schritt die vollständige Vereinbarkeit herbeizuführen. In diesem Plan sollten die Gründe für die Verzögerung bei der Herbeiführung der uneingeschränkten Vereinbarkeit erläutert und die weiteren Schritte und Fristen dargelegt werden, die geplant sind, um so bald wie möglich die uneingeschränkte Vereinbarkeit herzustellen. Der Plan sollte dem EDSB bis spätestens 1. Januar 2011 zusammen mit den übrigen vorstehend genannten Unterlagen vorgelegt werden.

In Anbetracht dessen, dass diese Unterlagen bereits alle Punkte enthalten sollten, die normalerweise im Vordruck des EDSB für die Vorabkontrollmeldung enthalten sind, ist es zur Vermeidung von Doppelarbeit nicht erforderlich, dem EDSB ein weiteres Formular für eine Vorabkontrollmeldung vorzulegen. Das Organ muss allerdings in seinem Schreiben deutlich machen, ob ein Ex-post-Vorabkontrolle erforderlich ist, und wenn ja, weshalb. Eine rasche Einhaltung und Mitteilung des Compliance-Status vor der Schlussfrist sind zu begrüßen.

Im Zweifelsfall steht der EDSB in allen Fragen, die während der Übergangszeit auftreten, beratend zur Verfügung.

Ab 1. Januar 2011 und nach Erhalt der erforderlichen Unterlagen erstellt der EDSB einen Plan für die Bearbeitung der Ex-post-Vorabkontrollmeldungen. Je nach Zahl und Qualität der bei ihm eingegangenen Ex-post-Vorabkontrollmeldungen, der Bandbreite der gestellten Fragen und anderer wichtiger Faktoren kann der EDSB

[48] „Ex-post"-Vorabkontrolle bezieht sich auf die Überprüfung bereits vorhandener Systeme, während sich eine „echte" Vorabkontrolle im Sinne von Artikel 27 der Verordnung auf die Überprüfung neuer Systeme (oder die Aufrüstung bestehender Systeme) bezieht, die noch nicht eingerichtet wurden.

einzelne Stellungnahmen oder aber gemeinsame Stellungnahmen an mehrere Organe und/oder zu mehreren Fragen abgeben. Das Verfahren kann auch Kontrollen vor Ort oder Inspektionen umfassen.

Im Anschluss daran oder aber parallel zur Bearbeitung der Vorabkontrollmeldungen kann der EDSB Untersuchungen und/oder Kontrollen der Verfahren einiger oder aller Organe einleiten, auch wenn diese keine Vorabkontrolle erforderlich machen. Je nach dem von den Organen erreichten Grad der Vereinbarkeit, der Bandbreite der gestellten Fragen und anderer wichtiger Faktoren kann der EDSB weitere Empfehlungen aussprechen, und zwar entweder einzeln an bestimmte Organe oder aber gemeinsam an mehrere Organe zu Fragen, die sie alle betreffen.

15.2. Ausstehende Ex-post-Vorabkontrollmeldungen

Aufgrund der Änderungen, die die Organe vornehmen müssen, um ihre Verfahren in Einklang mit den Leitlinien zu bringen, wird der EDSB alle Ex-post-Vorabkontrollverfahren abschließen, zu denen die Meldungen vor Erscheinen dieser Leitlinien eingegangen sind und die bis zur Verabschiedung der vorliegenden Leitlinien noch anhängig waren. Die Organe, deren Vorabkontrollmeldungen dementsprechend abgeschlossen wurden, sollten dem EDSB ihren Compliance-Status entsprechend den allgemeinen Regelungen und innerhalb der allgemein anerkannten Frist mitteilen.

Der EDSB kann zur weiteren Unterstützung dieser Organe bei ihren Bemühungen um Herstellung der Vereinbarkeit auf besonderen Wunsch vorläufige Empfehlungen auf der Grundlage der Vorabkontrollmeldung und anderer, von dem Organ in der Vergangenheit vorgelegter Unterlagen abgeben. Diese Empfehlungen beruhen ausschließlich auf den eingereichten Unterlagen; es geht ihnen keine gründliche Untersuchung voraus.

15.3. Vorabkontrollmeldungen für neue Systeme

Wie auch bei den „echten“ Vorabkontrollmeldungen für neue Systeme sollten diese während der Planungsphase so bald wie möglich und ohne Berücksichtigung der Übergangsfrist oder des Plans für die Ex-post-Überprüfung eingereicht werden. Der EDSB wird sie als dringliche Angelegenheit bearbeiten.

15.4. Überprüfung der Leitlinien

Wenn wichtige Änderungen der Umstände dies erfordern, kann der EDSB überarbeitete Fassungen dieser Leitlinien herausgeben. Zu den Umständen, die zu einer Überprüfung führen können, gehören u. a.:

- Veränderungen der Verfahren der Organe und auf internationaler Ebene bei der Videoüberwachung einschließlich technologischer Veränderungen,
- Weiterentwicklung internationaler Regelungen der Videoüberwachung,
- Erkenntnisse aus der Anwendung dieser Leitlinien und eingegangene Kommentare.

Anhang 1: Muster für eine Videoüberwachungsstrategie

[Agentur] Videoüberwachungsstrategie

Angenommen durch Beschluss des Direktors vom **[31. Mai 2010]**

1. Ziel und Umfang der Videoüberwachungsstrategie der Agentur

Für die Sicherheit ihrer Gebäude, Vermögenswerte, Mitarbeiter und Besucher betreibt unsere Agentur ein Videoüberwachungssystem. Die vorliegende Videoüberwachungsstrategie nebst Anlagen enthält eine Beschreibung des Videoüberwachungssystems der Agentur und der Schutzvorkehrungen, die von der Agentur zum Schutz personenbezogener Daten, der Privatsphäre und anderer Grundrechte und schutzwürdiger Interessen der von den Kameras erfassten Personen getroffen werden.

2. Wie stellen wir sicher, dass unser Videoüberwachungssystem unter Berücksichtigung datenschutzrechtlicher Belange konzipiert wurde und mit dem Datenschutzrecht in Einklang steht?

2.1. Überprüfung des bestehenden Systems. Bereits vor Herausgabe der Leitlinien des Europäischen Datenschutzbeauftragten zur Videoüberwachung („**Leitlinien**“) am ____ 2010 hat unsere Agentur ein Videoüberwachungssystem betrieben. Unsere Verfahren wurden jedoch seither überarbeitet, um sie mit den Empfehlungen in den Leitlinien (Leitlinien, Abschnitt 15) in Einklang zu bringen. **[Hyperlink zu den Leitlinien auf der Website des EDSB]**

2.2. Compliance-Status. Die Agentur verarbeitet Bilder sowohl im Einklang mit den Leitlinien als auch mit der Verordnung (EG) Nr. 45/2001 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft. **[Abweichungen von den Empfehlungen in den Leitlinien sind klar in Ihrer Videoüberwachungsstrategie auszuführen und zu begründen.]**

2.3. Selbstaudit. Das System wurde im Rahmen eines Selbstaudits geprüft. **Der Auditbericht** ist als **Anlage 1 beigefügt.**

2.4. Mitteilung des Compliance-Status an den EDSB. Angesichts des begrenzten Umfangs des Systems war die Durchführung einer förmlichen Folgenabschätzung (Leitlinien, Abschnitt 3.2) oder die Einreichung einer Vorabkontrollmeldung an den EDSB (Leitlinien, Abschnitt 4.3) nicht erforderlich. **[Bitte beachten Sie, dass Sie im Fall der Durchführung einer Folgenabschätzung den entsprechenden Bericht ebenfalls Ihrer Videoüberwachungsstrategie beifügen und die wichtigsten Punkte und Ergebnisse in der Strategie selbst aufführen sollten. Ebenso sollte für den Fall, dass der EDSB eine Stellungnahme zu einer**

Vorabkontrollmeldung abgibt, diese Stellungnahme ebenfalls beigefügt werden, und die wichtigsten Empfehlungen des EDSB sowie die von Ihnen ergriffenen Folgemaßnahmen zu diesen Empfehlungen sollten in der Strategie selbst zusammengefasst werden.]

Gleichzeitig haben wir mit der Annahme dieser Videoüberwachungsstrategie dem EDSB auch unseren Compliance-Status mitgeteilt; hierzu haben wir ihm ein Exemplar unserer Videoüberwachungsstrategie sowie unseren ersten Auditbericht übermittelt.

2.5. Kontakte zu den zuständigen Datenschutzbehörden in den Mitgliedstaaten. Die zuständige Datenschutzbehörde in **[bitte das Land einfügen]** wurde unterrichtet, und ihre Bedenken und Empfehlungen wurden berücksichtigt. Der Hinweis vor Ort und die Videoüberwachungsstrategie liegen insbesondere auch in **[Landessprache(n)]** vor.

2.6. Entscheidung des Direktors und Anhörung. Die Entscheidung über den Einsatz des derzeitigen Videoüberwachungssystems und die Annahme der in dieser Videoüberwachungsstrategie beschriebenen Schutzvorkehrungen wurde vom Direktor der Agentur nach Anhörung folgender Parteien getroffen:

- Leiter der Sicherheitsabteilung der Agentur,
- behördlicher Datenschutzbeauftragter der Agentur,
- Personalausschuss.

Die Agentur hat im Laufe dieses Entscheidungsprozesses

- die Notwendigkeit eines Videoüberwachungssystems gemäß Vorschlag in dieser Strategie nachgewiesen und dokumentiert,
- Alternativen erörtert und ist zu der Schlussfolgerung gelangt, dass die Wartung des derzeit im Einsatz befindlichen Videoüberwachungssystems nach der Annahme der Datenschutzvorkehrungen gemäß Vorschlag in dieser Strategie notwendig und den in Abschnitt 1 beschriebenen Zwecken (siehe Leitlinien, Abschnitt 5) angemessen ist, und
- sich mit den Anliegen des behördlichen Datenschutzbeauftragten und des Personalausschusses (siehe Leitlinien, Abschnitt 4) auseinandergesetzt.

2.7 Transparenz. Die Videoüberwachungsstrategie liegt in zwei Fassungen vor: eine Fassung, die nur für einen bestimmten Nutzerkreis bestimmt ist, und diese öffentliche Fassung, die auf unseren Internet- und Intranetseiten unter **[Internet- und Intranet-Adressen]** einsehbar ist. Diese öffentliche Fassung der Videoüberwachungsstrategie kann Kurzinformationen zu bestimmten Themen oder Anlagen enthalten. Wenn dies der Fall ist, ist auch immer klar darauf hinzuweisen. In der für die Öffentlichkeit bestimmten Version werden nur dann Informationen ausgelassen, wenn die Wahrung des Datengeheimnisses aus zwingenden Gründen absolut notwendig ist (z. B. aus Sicherheitsgründen oder zur Wahrung der Vertraulichkeit wirtschaftlich sensibler Informationen oder zum Schutz der Privatsphäre natürlicher Personen).

2.8. Regelmäßige Überprüfungen. Die Sicherheitsabteilung führt regelmäßig alle zwei Jahre eine Datenschutzüberprüfung durch, erstmals am 31. Mai 2012. Bei diesen regelmäßigen Überprüfungen werden wir erneut prüfen, ob

- die Notwendigkeit eines Videoüberwachungssystems nach wie vor gegeben ist,
- das System weiterhin sein erklärtes Ziel verfolgt und
- weiterhin keine angemessenen Alternativen bestehen.

Bei den regelmäßigen Überprüfungen werden aber auch alle anderen Themen aufgegriffen, die im ersten Bericht angesprochen werden, insbesondere die Frage, ob unsere Videoüberwachungsstrategie nach wie vor mit der Verordnung und den Leitlinien übereinstimmt (Angemessenheitsaudit) und ob sie in der Praxis eingehalten wird (Konformitätsaudit). Dieser Videoüberwachungsstrategie werden in **Anlage 1** auch Ausfertigungen der regelmäßigen Berichte beigefügt.

2.9. Technologische „privatsphärenfreundliche“ Lösungen. Wir haben auch technologische Lösungen implementiert, die dem Schutz des Rechts auf Privatsphäre förderlich sind (siehe Leitlinien, Abschnitt 3.4):

[Auflistung und Beschreibung der implementierten Lösungen]

3. Welche Bereiche werden überwacht?

Das Videoüberwachungssystem besteht aus **[sieben fest stehenden Kameras]. Eine Karte mit den Standorten der Kameras** ist in **Anlage 2** beigefügt.

[Sechs der sieben Kameras] befinden sich an den Eingängen und Ausgängen unseres Gebäudes, einschließlich am Haupteingang, an den Notausgängen und Fluchtwegen und an der Einfahrt zum Parkhaus. Darüber hinaus ist auch am Eingang zum Treppenhaus im Parkhaus eine Kamera aufgestellt.

Ansonsten wurden inner- oder außerhalb des Gebäudes keine weiteren Kameras installiert. Wir überwachen auch keine Bereiche, in denen verstärkte Erwartungen an den Schutz der Privatsphäre gestellt werden, etwa Einzelbüros, Freizeitbereiche, Toilettenräume und andere (siehe Leitlinien, Abschnitt 6.8). Die Standorte der Kameras wurden gewissenhaft geprüft, um die Überwachung derjenigen Bereiche, die für die Verwendungszwecke nicht von Belang sind, auf ein Mindestmaß zu reduzieren (Leitlinien, Abschnitt 6.1).

Die Überwachung außerhalb unseres Gebäudes im Hoheitsgebiet **[bitte den Namen des Mitgliedstaats einfügen, in dem Sie niedergelassen sind]** ist gemäß den Empfehlungen in Abschnitt 6.5 der Leitlinien auf ein absolutes Minimum beschränkt.

4. Welche personenbezogenen Daten erheben wir und für welchen Zweck?

4.1. Kurzbeschreibung und ausführliche technische Spezifikationen des Systems. Das Videoüberwachungssystem ist ein konventionelles statisches System. Es nimmt digitale Bilder auf und ist mit Bewegungsmeldern ausgestattet. Es erfasst jede Bewegung, die von den Kameras in dem überwachten Bereich festgestellt wird, zusammen mit Uhrzeit, Datum und Ort. Alle Kameras sind 24 Stunden am Tag und sieben Tage die Woche in Betrieb. In den meisten Fällen ist es aufgrund der Bildqualität möglich, die Personen zu identifizieren, die sich im Erfassungsbereich der Kamera befinden (siehe Leitlinien, Abschnitt 6.4). Die Kameras sind alle fest montiert (keine schwenk-, neig- und zoombaren Kameras) und können daher von den Bedienern nicht zum Heranzoomen eines Ziels oder zur Verfolgung von Personen eingesetzt werden.

Wir setzen keine Hightech- oder intelligente Videoüberwachungstechnologie ein (siehe Abschnitt 6.9 der Leitlinien), wir schalten unser System auch nicht mit anderen Systemen zusammen (Abschnitt 6.10) und wir verwenden keine verdeckte Überwachung (Abschnitt 6.11), Tonaufzeichnungen oder „talking CCTV“ (Abschnitt 6.12). **Die technischen Spezifikationen** der Kameras und **des Videoüberwachungssystems als Ganzes** (einschließlich Software und Hardware) sind **Anlage 3** zu entnehmen.

4.2. Zweckbestimmung der Überwachung. Die Agentur setzt ihr Videoüberwachungssystem einzig und allein zu Sicherheitszwecken und zum Zweck der Zugangskontrolle ein. Das Videoüberwachungssystem hilft bei der Zugangskontrolle zu unserem Gebäude und gewährleistet die Sicherheit des Gebäudes unserer Mitarbeiter und Besucher sowie des Grundstücks und der in unseren Räumlichkeiten befindlichen oder gespeicherten Informationen. Es ergänzt andere physische Sicherheitssysteme, wie z. B. Zugangskontrollsysteme und physische Einbruchmeldesysteme. Es ist Teil der Maßnahmen zur Förderung unserer Sicherheitsstrategien im weiteren Wortsinne und unterstützt die Verhütung, Abwehr und ggf. die Untersuchung unbefugten physischen Zutritts, einschließlich des unbefugten Zutritts zu Sicherheitsräumen und geschützten Räumen, zur IT-Infrastruktur oder zu operativen Informationen. Darüber hinaus hilft die Videoüberwachung bei der Verhütung, Erkennung und Untersuchung von Diebstählen von Ausrüstungsgegenständen oder Vermögenswerten, die sich im Besitz der Agentur, von Besuchern oder Mitarbeitern befinden, sowie bei der Verhütung, Erkennung und Untersuchung von Gefahren für die Sicherheit der Besucher oder des im Büro tätigen Personals (z. B. Brand, tätliche Übergriffe).

4.3. Eingrenzung der Zweckbestimmung. Das System wird nicht zu anderen Zwecken eingesetzt; so wird es nicht zur Überwachung der Arbeit der Mitarbeiter oder zur Überwachung der Anwesenheit eingesetzt. Auch wird es nicht zur Ermittlung verwendet (mit Ausnahme von Untersuchungen physischer Sicherheitsvorfälle wie Diebstähle oder unbefugter Zutritt). Nur in Ausnahmefällen können die Bilder im Rahmen eines förmlichen Disziplinarverfahrens oder eines strafrechtlichen Ermittlungsverfahrens gemäß Beschreibung in Abschnitt 6.5 (siehe Abschnitte 5.7, 5.8 und 10.3 der Leitlinien) an Ermittlungsbehörden übermittelt

werden.

4.4. Es ist keine Ad-hoc-Überwachung geplant. Wir planen derzeit keine Ad-hoc-Überwachung (siehe Leitlinien, Abschnitt 3.5).

4.5. Webcams. Wir setzen keine Webcams ein (siehe Abschnitt 5.10 der Leitlinien).

4.6. Es werden keine besonderen Datenkategorien erhoben. Wir erheben keine besonderen Datenkategorien (Abschnitt 6.7 der Leitlinien).

5. Auf welcher rechtmäßigen Begründung und auf welcher Rechtsgrundlage beruht die Videoüberwachung?

Wir müssen unser Videoüberwachungssystem für die Leitung und den reibungslosen Betrieb unserer Agentur (zum Zweck der Sicherheit und der Zugangskontrolle gemäß Beschreibung in Abschnitt 4.2) einsetzen. Es gibt daher eine rechtmäßige Begründung für die Videoüberwachung (siehe Abschnitt 5.2 der Leitlinien). Eine ausführlichere und konkretere Rechtsgrundlage für die Videoüberwachung ist in dieser Videoüberwachungsstrategie enthalten. Diese Strategie wiederum ist Teil der Sicherheitsstrategien unserer Agentur im weiteren Sinne.

6. Wer hat Zugriff auf die Informationen, und an wen werden sie weitergegeben?

6.1. Internes Sicherheitspersonal und ausgegliederte Sicherheitsbedienstete. Videoaufnahmen sind ausschließlich unserem internen Sicherheitspersonal zugänglich. Auf Live-Videoaufnahmen haben auch die diensthabenden Sicherheitsbediensteten Zugriff. Diese Sicherheitsbediensteten arbeiten für eine ausgegliederte Sicherheitsfirma. Der **Vertrag mit dieser Sicherheitsfirma** ist in **Anlage 4** beigefügt.

6.2. Zugangsrechte. In der Sicherheitsstrategie der Agentur im Bereich der Videoüberwachung (siehe Abschnitt 7 und Anlage 7) ist klar ausgeführt und dokumentiert, wer Zugang zu dem Bildmaterial aus der Videoüberwachung und/oder zu der technischen Architektur des Videoüberwachungssystems besitzt, zu welchem Zweck und woraus diese Zugangsrechte bestehen. In dem Dokument wird genau ausgeführt, wer berechtigt ist,

- das Bildmaterial in Echtzeit anzusehen,
- das aufgezeichnete Bildmaterial anzusehen oder
- zu kopieren,
- herunterzuladen,
- zu löschen oder
- Bildmaterial zu verändern.

6.3. Schulungen in datenschutzrechtlichen Fragen. Alle Mitarbeiter, die Zugangsrechte besitzen, einschließlich der ausgegliederten Sicherheitsbediensteten,

wurden am **[15. Mai 2010]** erstmals in datenschutzrechtlichen Fragen geschult. Jeder neue Mitarbeiter wird geschult, und es finden regelmäßig mindestens alle zwei Jahre für alle Mitarbeiter mit Zugangsrechten Workshops zu Themen in Verbindung mit der Einhaltung der Datenschutzvorschriften statt (siehe Abschnitt 8.2 der Leitlinien).

6.4. Vertraulichkeitserklärungen. Nach der Schulung hat jeder Mitarbeiter außerdem eine Vertraulichkeitserklärung unterzeichnet. Diese Erklärung wurde auch von der ausgegliederten Firma unterzeichnet. Kopien dieser **Vertraulichkeitserklärungen** sind als **Anlage 5** (siehe Abschnitt 8.3 der Leitlinien) beigefügt.

6.5. Übermittlung und Weitergabe von Daten. Jede Übermittlung und Weitergabe von Daten außerhalb der Sicherheitsabteilung wird dokumentiert und setzt eine gründliche Prüfung der Notwendigkeit einer solchen Übermittlung sowie der Vereinbarkeit der Zwecke der Übermittlung mit dem ursprünglichen Ziel der Verarbeitung zu Sicherheits- und Zugangskontrollzwecken voraus (siehe Abschnitt 10 der Leitlinien). **Das Register der Aufbewahrung und Übermittlung von Daten** ist in **Anlage 6** beigefügt (siehe Abschnitt 10.5 und 7.2 der Leitlinien). Der behördliche Datenschutzbeauftragte der Agentur wird in jedem einzelnen Fall hinzugezogen. **[Falls Sie Routineübermittlungen ohne Hinzuziehung des DSB durchführen, beschreiben Sie bitte Ihre diesbezügliche Strategie ausführlich in dieser Videoüberwachungsstrategie.]**

Der Leitung oder der Personalabteilung wird kein Zugriff gewährt. **[Falls dies nicht zutrifft, nennen Sie bitte zum besseren Verständnis anschauliche Beispiele für solche Übermittlungen. Beschreiben Sie bitte auch Ihre Vorschriften, in denen geregelt ist, was an wen und unter welchen Umständen übermittelt werden darf.]**

Zur Untersuchung oder Verfolgung von Straftaten kann der örtlichen Polizei ggf. ein Zugriff gewährt werden. In der Vergangenheit wurde der Polizei nur in wenigen Fällen der Zugriff auf Bildmaterial gewährt, als sie einen Fahrraddiebstahl im Bereich der Abstellplätze an der Einfahrt zur Garage untersuchte. In den letzten **[fünf Jahren]** wurde der Polizei kein weiterer Zugriff gewährt. **[Auch hier gilt: falls es andere Fälle gegeben hat, nennen Sie bitte zum besseren Verständnis anschauliche Beispiele für solche Übermittlungen. Beschreiben Sie bitte auch Ihre Vorschriften, in denen geregelt ist, was an wen und unter welchen Umständen übermittelt werden darf.]**

In Ausnahmefällen kann auch folgenden Parteien Zugriff gewährt werden:

- dem Europäischen Amt für Betrugsbekämpfung („**OLAF**“) im Rahmen einer Untersuchung des OLAF,
- dem Untersuchungs- und Disziplinaramt der Kommission („**IDOC**“) im Rahmen eines disziplinarrechtlichen Verfahrens gemäß den Vorschriften in Anhang IX des Statuts der Beamten der Europäischen Union, oder
- denjenigen, die ein förmliches Untersuchungs- oder Disziplinarverfahren

innerhalb des Organs durchführen,

sofern berechtigterweise davon ausgegangen werden kann, dass die Übermittlungen die Untersuchung oder Verfolgung von ausreichend schweren Disziplinarvergehen oder Straftaten voranbringen. Anträgen auf gezielte Datensuche (Data Mining) wird nicht stattgegeben. In den letzten **[fünf Jahren]**, in denen wir die Datenübermittlungen protokolliert haben, haben wir keine Übermittlung aus den vorstehend genannten Gründen genehmigt.

7. Wie schützen und sichern wir die Informationen?

Zum Schutz der Sicherheit des Videoüberwachungssystems, einschließlich der personenbezogenen Daten, wurde eine Reihe von technischen und organisatorischen Maßnahmen ergriffen. Diese sind in der verarbeitungsspezifischen Sicherheitsstrategie („**Sicherheitsstrategie für die Videoüberwachung**“), die als **Anlage 7** beigefügt ist, im Einzelnen beschrieben.

Die Sicherheitsstrategie der Agentur für die Videoüberwachung wurde im Einklang mit Abschnitt 9 der Leitlinien des EDSB zur Videoüberwachung festgelegt.

Es wurden u. a. folgende Maßnahmen ergriffen:

- Durch physische Sicherheitsmaßnahmen geschützte Sicherheitsräume, in denen sich die Server mit den gespeicherten Aufnahmen befinden; Netzwerk-Firewalls schützen den logischen Perimeter der IT-Infrastruktur; und die wichtigsten Computersysteme, mit denen die Daten gehalten werden, sind sicherheitsgehärtet.
- Zu den verwaltungstechnischen Maßnahmen gehören die Verpflichtung für das gesamte ausgegliederte Personal, das Zugriff auf das System besitzt (einschließlich der für die Wartung der Ausrüstung und Systeme zuständigen Mitarbeiter), eine individuelle Sicherheitsüberprüfung zu durchlaufen.
- Das gesamte Personal (extern und intern) hat Vertraulichkeits- und Geheimhaltungsvereinbarungen unterzeichnet.
- Zugriffsrechte für Nutzer werden nur denjenigen gewährt, die zur Erfüllung ihrer Aufgaben einen Zugriff unbedingt benötigen.
- Nur der vom für die Verarbeitung Verantwortlichen speziell hierzu benannte Systemadministrator ist in der Lage, Personen Zugangsrechte zu gewähren oder diese abzuändern oder aufzuheben. Die Gewährung, Änderung oder Aufhebung von Zugangsrechten erfolgt gemäß den in der Sicherheitsstrategie für die Videoüberwachung ausgeführten Kriterien (siehe Anlage 7).
- Die Sicherheitsstrategie für die Videoüberwachung umfasst eine aktualisierte Liste aller Personen, die jederzeit Zugang zum System besitzen, und beschreibt ihre Zugangsrechte im Einzelnen.

8. Wie lange bewahren wir die Daten auf?

Die Bilder werden höchstens 48 Stunden lang aufbewahrt. Anschließend werden alle Bilder gelöscht. Wenn Bilder für weitere Untersuchungen oder als Beweismittel bei Sicherheitsvorfällen gespeichert werden müssen, können sie so lange aufbewahrt

werden, wie dies notwendig ist. Ihre Aufbewahrung ist genau zu dokumentieren und die Notwendigkeit der Aufbewahrung muss regelmäßig überprüft werden. Eine Kopie des **Registers der Aufbewahrung und Übermittlung von Daten** ist in **Anlage 6** (siehe Abschnitt 7 der Leitlinien) beigefügt.

Das System wird außerdem live vom Sicherheitsbediensteten im Empfangsgebäude im Erdgeschoss 24 Stunden am Tag überwacht.

9. Wie informieren wir die Öffentlichkeit?

9.1. Mehrstufiger Ansatz. Die Öffentlichkeit wird effizient und umfassend über die Videoüberwachung informiert (siehe Leitlinien, Abschnitt 11). Hierzu empfehlen wir einen mehrstufigen Ansatz, der auf einer Kombination der folgenden beiden Methoden beruht:

- Hinweise vor Ort, mit denen die Öffentlichkeit unmittelbar darauf aufmerksam gemacht wird, dass eine Überwachung stattfindet, und ihr die wesentlichen Informationen über das Vorgehen mitgeteilt werden;
- diese Videoüberwachungsstrategie stellen wir in unser Intranet und in unsere Websites für all diejenigen ein, die mehr über die Verfahren unseres Organs im Bereich der Videoüberwachung wissen möchten.

Ausdrucke dieser Videoüberwachungsstrategie sind auch bei unserem Empfang erhältlich und können auf Wunsch bei unserer Sicherheitsabteilung angefordert werden. Für weitere Anfragen stellen wir außerdem eine Telefonnummer und eine E-Mail-Adresse bereit.

Außerdem bringen wir Hinweise vor Ort neben den überwachten Bereichen an. Wir haben einen Hinweis in der Nähe des Haupteingangs, des Fahrstuhleingangs im Parkhaus und an der Einfahrt zum Parkhaus angebracht.

Die Datenschutzerklärung der Agentur, die vor Ort ausgehängt wird, ist als **Anlage 8** beigefügt.

9.2. Spezifische individuelle Hinweise. Natürliche Personen müssen auch individuell darauf aufmerksam gemacht werden, dass sie von einer Kamera identifiziert wurden (etwa vom Sicherheitspersonal bei einer Sicherheitsuntersuchung), sofern eine oder mehrere der nachstehenden Bedingungen erfüllt sind:

- Die Identität der Person wird in Dateien bzw. Unterlagen festgehalten,
- die Videoaufnahme wird gegen die Person verwendet,
- die Videoaufnahme wird über die vorschriftsmäßige Aufbewahrungszeit hinaus gespeichert,
- die Videoaufnahme wird an Empfänger außerhalb der Sicherheitsabteilung übermittelt *oder*
- die Identität der Person wird jemandem außerhalb der Sicherheitsabteilung

offengelegt.

Solche Hinweise können zuweilen vorübergehend zurückgestellt werden, etwa dann, wenn dies für die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten erforderlich ist.[49] Der behördliche Datenschutzbeauftragte des Organs wird in derartigen Fällen hinzugezogen, um zu gewährleisten, dass die Rechte der Person gewahrt werden.

10. Wie kann die Öffentlichkeit die sie betreffenden Daten überprüfen, ändern oder löschen? Die Öffentlichkeit hat das Recht auf Zugang zu den von uns gehaltenen, sie betreffenden Daten sowie das Recht, diese Daten zu berichtigen oder zu vervollständigen. Anträge auf Zugriff, Berichtigung, Sperrung und/oder Löschung personenbezogener Daten sind an Herrn/Frau _____, Leiter/-in des Referats __, **[E-Mail-Adresse und Telefonnummer]**, zu richten. Sie können auch dann Kontakt mit ihr/ihm aufnehmen, wenn Sie andere Fragen zur Verarbeitung personenbezogener Daten haben.

Die Sicherheitsabteilung beantwortet Anfragen nach Möglichkeit in der Sache innerhalb von 15 Kalendertagen. Falls dies nicht möglich ist, wird der Antragsteller binnen zwei Wochen über die nächsten Schritte und den Grund für die Verzögerung informiert. Auch in sehr komplexen Fällen muss innerhalb von spätestens drei Monaten der Zugang gewährt oder aber eine definitive Antwort gegeben werden, in der begründet wird, weshalb der Antrag abgelehnt wird. Das Referat muss sich bemühen, die Anfrage früher zu beantworten, insbesondere dann, wenn der Antragsteller die Dringlichkeit seines Antrags nachgewiesen hat.

Eine Betrachtung der Bilder kann veranlasst werden, sofern dies konkret beantragt wird; der Antragsteller kann aber auch eine Kopie der Aufnahmen auf einer DVD oder einem anderen Datenträger bekommen. Falls ein solcher Antrag gestellt wird, müssen Antragsteller ihre Identität zweifelsfrei nachweisen (z. B. sollten sie zur Betrachtung Personalausweise mitbringen) und außerdem nach Möglichkeit auch Datum, Uhrzeit, Ort und die Umstände angeben, unter denen sie gefilmt wurden. Außerdem müssen sie ein Foto neueren Datums von sich mitbringen, damit das Sicherheitspersonal sie anhand der überprüften Bilder erkennen kann.

Gegenwärtig stellen wir Antragstellern, die die Betrachtung oder eine Kopie ihrer Aufnahmen beantragen, keine Gebühren in Rechnung. Wir behalten uns jedoch vor, eine angemessene Gebühr zu berechnen, falls die Zahl solcher Anträge auf Zugang zunimmt.

Ein Antrag auf Zugang kann abgelehnt werden, wenn eine Ausnahme gemäß Artikel 20 Absatz 1 der Verordnung Nr. 45/2001 in einem bestimmten Fall zum Tragen kommt. So ist es denkbar, dass wir beispielsweise nach einer Einzelfallevaluierung zu dem Schluss gelangen, dass der Zugang zum Schutz der Untersuchung einer Straftat eingeschränkt werden muss. Eine solche Einschränkung

[49] In Ausnahmefällen können auch weitere Ausnahmen gemäß Artikel 20 der Verordnung zum Tragen kommen.

kann sich auch dann als notwendig erweisen, wenn die Rechte und Freiheiten anderer geschützt werden müssen, etwa, wenn auch andere Menschen auf den Bildern zu sehen sind und es nicht möglich ist, ihre Einwilligung zur Weitergabe der sie betreffenden personenbezogenen Daten zu bekommen oder die Bilder entsprechend zu bearbeiten, weil sie ihre Einwilligung nicht erteilen.

11. Recht, sich an den Europäischen Datenschutzbeauftragten zu wenden

Jede Person hat das Recht, sich an den Europäischen Datenschutzbeauftragten (edps@edps.europa.eu) zu wenden, wenn sie der Auffassung ist, dass ihre Rechte aus der Verordnung Nr. 45/2001 aufgrund der Verarbeitung der sie betreffenden personenbezogenen Daten durch die Agentur verletzt wurden. Vorher empfehlen wir den Betroffenen jedoch, sich hierfür zunächst zu wenden an:

- den Leiter der Sicherheitsabteilung (Kontaktangaben siehe oben) und/oder
- den Datenschutzbeauftragten der Agentur **[bitte Name, Telefonnummer und E-Mail-Adresse einfügen]**

Mitarbeiter können nach Maßgabe von Artikel 90 des Statuts von ihrer Anstellungsbehörde auch eine Überprüfung des Sachverhalts verlangen.

[Angaben zum internen Beschwerdeverfahren, einschließlich Fristen und Kontaktangaben]

* * *

Anlagen zur Videoüberwachungsstrategie:

- **Der Auditbericht** liegt als **Anlage 1** bei. Anhang 1 enthält auch die **regelmäßigen Überprüfungen.**
- Eine Karte mit den Standorten der Kameras ist in **Anlage 2** enthalten.
- Die **technischen Spezifikationen** für die Kameras und für das Videoüberwachungssystem als Ganzes (einschließlich Software und Hardware) sind in **Anlage 3** beigefügt.
- Der **Vertrag mit der ausgegliederten Sicherheitsfirma** ist in **Anlage 4** beigefügt
- Kopien der **Vertraulichkeitserklärungen** liegen als **Anlage 5** bei (siehe Abschnitt 8.3 der Leitlinien).
- **Das Register der Aufbewahrung und Übermittlung von Daten** ist in **Anlage 6** beigefügt (siehe Abschnitte 10.5 und 7.2 der Leitlinien).
- Zum Schutz der Sicherheit des Videoüberwachungssystems einschließlich der darin enthaltenen personenbezogenen Daten wurde eine Reihe von technischen und organisatorischen Maßnahmen ergriffen. Diese sind in der verarbeitungsspezifischen Sicherheitsstrategie („**Sicherheitsstrategie für die Videoüberwachung**“), die als **Anlage 7** beigefügt ist, im Einzelnen beschrieben.
- Die **Datenschutzerklärung** der Agentur, die **vor Ort** ausgehängt wird, ist als **Anlage 8** beigefügt.

Anhang 2: Muster für eine Datenschutzerklärung vor Ort

[Bitte fügen Sie das für Ihre Videoüberwachung verwendete Piktogramm ein: Sie könnten hierzu beispielsweise das ISO-Piktogramm oder das Piktogramm verwenden, das Sie normalerweise an Ihrem Standort verwenden.]

Zu Ihrer Sicherheit werden dieses Gebäude und seine unmittelbare Umgebung videoüberwacht. Es werden keine Bilder aufgezeichnet. **[Alternative: Die Aufnahmen werden 48 Stunden lang gespeichert.]**

Weitere Auskünfte erhalten Sie unter der Adresse www.domainnameofyourinstitution/cctv. Sie können sich aber auch mit der Sicherheitsabteilung der Agentur unter **[Telefonnummer und E-Mail-Adresse]** in Verbindung setzen.

[Bitte fügen Sie ggf. mehrsprachige Fassungen bei.]