Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte

Version 2.0

Angenommen am 29. Januar 2020

Versionsverlauf

Version 2.0	29. Januar 2020	Annahme der Leitlinien nach öffentlicher Konsultation
Version 1.0	10. Juli 2019	Annahme der Leitlinien zur öffentlichen Konsultation

Inhaltsverzeichnis

Der Europäische Datenschutzausschuss –

gestützt auf Artikel 70 Absatz 1 Buchstabe e der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (im Folgenden „DSGVO“),

gestützt auf das Abkommen über den Europäischen Wirtschaftsraum, insbesondere auf Anhang XI und das Protokoll 37 in der durch den Beschluss des Gemeinsamen EWR-Ausschusses Nr. 154/2018 vom 6. Juli 2018 geänderten Fassung,[1]

gestützt auf Artikel 12 und Artikel 22 seiner Geschäftsordnung –

HAT DIE FOLGENDEN LEITLINIEN ANGENOMMEN:

1 EINLEITUNG

1. Die verstärkte Nutzung von Videogeräten hat einen erheblichen Einfluss auf das Verhalten der Bürgerinnen und Bürger. Der großflächige Einsatz solcher Anwendungen in vielen Lebensbereichen des Menschen setzt sie zusätzlich unter Druck, Verhaltensweisen zu vermeiden , die als ungewöhnlich angesehen werden könnten. De facto können diese Technologien die Möglichkeit beschränken, sich anonym zu bewegen und anonym Dienstleistungen in Anspruch zu nehmen, und generell die Möglichkeit einschränken, unbemerkt zu bleiben. Es bestehen massive Auswirkungen auf den Datenschutz.

2. Während manche Menschen beispielsweise mit Videoüberwachung, die für einen bestimmten Sicherheitszweck eingerichtet wurde, durchaus leben können, müssen Garantien vorgesehen werden, um jeglichen Missbrauch für völlig andere und – für die betroffene Person – unerwartete Zwecke (z. B. Marketing, Leistungsüberwachung von Mitarbeitern usw.) zu verhindern. Darüber hinaus kommen heutzutage viele Anwendungen zum Einsatz, um die aufgenommenen Bilder auszuwerten und aus herkömmlichen Kameras intelligente („smarte“) Kameras zu machen. Die Menge der durch Videoaufnahme generierten Daten erhöht in Kombination mit diesen Tools und Techniken sowohl das das Risiko des Missbrauchs als auch das einer sekundären Nutzung (Letzteres gilt unabhängig davon, ob diese mit dem ursprünglich dem System zugewiesenen Zweck in Zusammenhang steht oder nicht.). Die allgemeinen Grundsätze der DSGVO (Artikel 5) müssen bei der Videoüberwachung stets sorgfältig berücksichtigt werden.

3. Videoüberwachungsanlagen verändern in vielerlei Hinsicht die Art und Weise, wie Akteure aus dem privaten und dem öffentlichen Sektor agieren, um an privaten oder öffentlichen Orten die Sicherheit zu erhöhen, Publikumsanalysen zu erhalten, personalisierte Werbung zu betreiben usw. Durch den zunehmenden Einsatz intelligenter Videoanalysen ist die Videoüberwachung äußerst leistungsfähig geworden. Diese Techniken können mehr (z. B. komplexe biometrische Technologien) oder weniger in

[1] Soweit in dieser Stellungnahme auf „Mitgliedstaaten“ Bezug genommen wird, ist dies als Bezugnahme auf „EWR-Mitgliedstaaten“ zu verstehen.

die Privatsphäre eindringen (z. B. einfache Zählalgorithmen). Generell wird es immer schwieriger, anonym zu bleiben und die Privatsphäre zu wahren. Die in der jeweiligen Situationen zu beantwortenden Datenschutzfragen können stark voneinander variieren, ebenso wie die rechtliche Analyse bei der Verwendung der einen oder anderen Technologie.

4. Neben Datenschutzproblemen treten auch Risiken im Zusammenhang mit möglichen Fehlfunktionen dieser Geräte und den durch sie verursachten Verzerrungen auf. Forscher berichten, dass Software, die für die Gesichtsidentifizierung, -erkennung oder -analyse verwendet wird, je nach Alter, Geschlecht und ethnischer Zugehörigkeit der Person, die sie identifiziert, unterschiedlich funktioniert. Algorithmen können auf der Grundlage unterschiedlicher demografischer Daten funktionieren, sodass Voreingenommenheit bei der Gesichtserkennung die Vorurteile der Gesellschaft verstärken könnte. Deshalb müssen Verantwortliche auch dafür sorgen, dass die Verarbeitung biometrischer Daten, die sich aus der Videoüberwachung ergibt, regelmäßig auf ihre Relevanz und auf ausreichende Garantien hin überprüft wird.

5. Eine Videoüberwachung ist nicht zwangsläufig erforderlich, wenn es andere Mittel gibt, um den zugrundeliegenden Zweck zu erreichen. Andernfalls laufen wir Gefahr, dass sich die gesellschaftlichen Normen dahingehend ändern, dass der Mangel an Privatsphäre von vornherein akzeptiert wird.

6. Diese Leitlinien sollen Hilfestellung bei der Anwendung der DSGVO in Bezug auf die Verarbeitung personenbezogener Daten durch Videogeräte geben. Die Beispiele sind nicht abschließend, die allgemeine Grundsätze können auf alle potenziellen Anwendungsbereiche angewandt werden.

2 ANWENDUNGSBEREICH[2]

2.1 Personenbezogene Daten

7. Die systematische automatisierte Überwachung eines bestimmten Bereichs mit optischen oder audiovisuellen Mitteln, vor allem zum Schutz von Eigentum oder zum Schutz des Lebens und der Gesundheit des Einzelnen, hat in letzter Zeit stark an Bedeutung gewonnen. Dies ist in der Regel mit dem Erfassen und Speichern bildlicher oder audiovisueller Informationen über alle Personen verbunden, die den überwachten Bereich betreten und anhand ihres Aussehens oder anderer spezifischer Merkmale identifizierbar sind. Mit Hilfe dieser Merkmale kann die Identität der betroffenen Personen festgestellt werden. Möglich ist ferner die Weiterverarbeitung personenbezogener Daten in Bezug auf den Aufenthalt und das Verhalten der Personen in dem betreffenden Bereich. Das potenzielle Risiko des Missbrauchs dieser Daten wächst mit der Größe des überwachten Bereichs und der Zahl der den Bereich frequentierenden Personen. Dies ergibt sich aus Artikel 35 Absatz 3 Buchstabe c, dem zufolge im Falle einer systematischen umfangreichen Überwachung eines öffentlich zugänglichen Bereichs eine Datenschutz-Folgenabschätzung durchzuführen ist, sowie aus Artikel 37 Absatz 1 Buchstabe b, wonach Auftragsverarbeiter einen Datenschutzbeauftragten benennen müssen, wenn der Verarbeitungsvorgang aufgrund seiner Art eine regelmäßige und systematische Überwachung der betroffenen Personen beinhaltet.

8. Die Verordnung gilt jedoch nicht für die Verarbeitung von Daten, die keinen Bezug zu einer Person haben, z. B. wenn eine Person weder direkt noch indirekt identifiziert werden kann.

> Beispiel: Die DSGVO gilt nicht für Kamera-Attrappen (d. h. für Kameras, die nicht als Kamera funktionieren und somit keine personenbezogenen Daten verarbeiten). *In einigen Mitgliedstaaten könnten dazu jedoch nationale Rechtsvorschriften existieren.*
>
> Beispiel: Aufzeichnungen aus großer Höhe fallen nur dann in den Anwendungsbereich der DSGVO, wenn die verarbeiteten Daten im jeweiligen Einzelfall mit einer bestimmten Person in Verbindung gebracht werden können.
>
> Beispiel: Eine Videokamera ist als Einparkhilfe in ein Auto eingebaut. Wenn die Kamera so eingebaut oder eingestellt ist, dass sie keine Informationen über eine natürliche Person erfasst (z. B. Kennzeichen oder Informationen, mit denen Passanten identifiziert werden könnten), findet die DSGVO keine Anwendung.

9.

2.2 Anwendung der Strafverfolgungsrichtlinie (EU 2016/680)

10. Die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Untersuchung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, fällt unter die Richtlinie EU 2016/680.

2.3 Ausnahmeregelung für Privathaushalte

[2] Der EDSA weist darauf hin, dass in Fällen, in denen die DSGVO dies zulässt, besondere Anforderungen in nationalen Rechtsvorschriften gelten können.

11. Gemäß Artikel 2 Absatz 2 Buchstabe c fällt die Verarbeitung personenbezogener Daten durch eine natürliche Person zur Ausübung rein persönlicher oder rein familiärer Tätigkeiten, zu der auch Online-Tätigkeiten gehören können, nicht in den Anwendungsbereich der DSGVO.[3]

12. Diese Bestimmung – die so genannte Haushaltsausnahme – muss im Zusammenhang mit der Videoüberwachung eng ausgelegt werden. Nach Auffassung des Europäischen Gerichtshofs ist die so genannte Haushaltsausnahme *„somit dahin auszulegen, dass mit ihr nur Tätigkeiten gemeint sind, die zum Privat- oder Familienleben von Einzelpersonen gehören, was offensichtlich nicht der Fall ist bei der Verarbeitung personenbezogener Daten, die in deren Veröffentlichung im Internet besteht, sodass diese Daten einer unbegrenzten Zahl von Personen zugänglich gemacht werden.“*[4] Darüber hinaus kann eine Videoüberwachung, soweit sie die ständige Aufzeichnung und Speicherung personenbezogener Daten umfasst und sich *„auch nur teilweise auf den öffentlichen Bereich erstreckt und dadurch auf einen Bereich außerhalb der privaten Sphäre desjenigen gerichtet ist, der die Daten auf diese Weise verarbeitet, nicht als eine ausschließlich „persönliche oder familiäre“ Tätigkeit im Sinne von Artikel 3 Absatz 2 zweiter Gedankenstrich der Richtlinie 95/46 angesehen werden“.*[5]

13. Videogeräte, die innerhalb der Grundstücksgrenzen einer Privatperson betrieben werden, können unter die Ausnahmeregelung für Privathaushalte fallen. Dies hängt jedoch von mehreren Faktoren ab, die vorab geprüft werden müssen. Abgesehen von den oben genannten Elementen, die der EuGH in seinen Urteilen festgestellt hat, muss die Anwenderin oder der Anwender von Videoüberwachung im Privathaushalt berücksichtigen, ob eine persönliche Beziehung zur betroffenen Person besteht, ob der Umfang oder die Häufigkeit der Überwachung auf eine Art beruflicher Tätigkeit seinerseits hindeuten, und ob die Überwachung möglicherweise nachteilige Auswirkungen auf die betroffenen Personen haben kann. Die Existenz eines einzelnen der genannten Umstände bedeutet nicht zwangsläufig, dass die Verarbeitung nicht unter die Haushaltsausnahme fällt; für diese Entscheidung ist eine Gesamtbewertung erforderlich.

> Beispiel: Ein Tourist nimmt Videos sowohl mit seinem Mobiltelefon als auch mit einem Camcorder auf, um seinen Urlaub zu dokumentieren. Er zeigt das Filmmaterial Freunden und der Familie, macht es aber nicht für eine unbestimmte Zahl von Menschen zugänglich. Dies würde unter die Haushaltsausnahme fallen.
>
> Beispiel: Eine Mountain-Bikerin möchte ihre Abfahrt mit einer Action-Cam aufzeichnen. Sie fährt in einem abgelegenen Gebiet und plant, die Aufzeichnungen nur für ihre persönliche Unterhaltung zu Hause zu nutzen. Dies würde auch dann unter die Ausnahmeregelung für Privathaushalte fallen, wenn in gewissem Umfang personenbezogene Daten verarbeitet werden.
>
> Beispiel: Jemand überwacht seinen eigenen Garten und macht Aufzeichnungen. Das Grundstück ist eingezäunt, und nur der Betreiber selbst und seine Familie betreten den Garten regelmäßig. Dies würde unter die Haushaltsausnahme fallen, sofern sich die Videoüberwachung nicht teilweise auf einen öffentlichen Bereich oder ein angrenzendes Grundstück erstreckt.

14.

[3] Vgl. auch Erwägungsgrund 18.

[4] Europäischer Gerichtshof, Urteil in der Rechtssache C-101/01, *Bodil Lindqvist*, 6. November 2003, Rn. 47.

[5] Europäischer Gerichtshof, Urteil in der Rechtssache C-212/13, *František Ryneš* gegen *Úřad pro ochranu osobních údajů*, 11. Dezember 2014, Rn. 33.

3 RECHTMÄßIGKEIT DER VERARBEITUNG

15. Vor dem Einsatz einer Videoüberwachung sind die Verarbeitungszwecke im Einzelnen festzulegen (Artikel 5 Absatz 1 Buchstabe b). Eine Videoüberwachung kann unterschiedlichen Zwecken dienen, z. B. dem Schutz von Eigentum und anderen Vermögenswerten, dem Schutz des Lebens und der körperlichen Unversehrtheit von Einzelpersonen, der Erhebung von Beweismitteln zur Durchsetzung zivilrechtliche Ansprüche.[6] Diese Überwachungszwecke sollten schriftlich dokumentiert werden (Artikel 5 Absatz 2) und müssen für jede eingesetzte Überwachungskamera spezifiziert werden. Kameras, die von einem einzigen Verantwortlichen für denselben Zweck verwendet werden, können gemeinsam dokumentiert werden. Darüber hinaus müssen betroffene Personen gemäß Artikel 13 über den/die Zweck(e) der Verarbeitung informiert werden *(siehe Abschnitt 7, Transparenz- und Informationspflichten).* Die Angabe des Zwecks „Sicherheit“ oder „zu Ihrer Sicherheit“ , ist nicht spezifisch genug (Artikel 5 Absatz 1 Buchstabe b. Darüber hinaus verstößt sie gegen den Grundsatz, dass personenbezogene Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden müssen (vgl. Artikel 5 Absatz 1 Buchstabe a).

16. Grundsätzlich kann jede Variante des Artikel 6 Absatz 1 eine Rechtsgrundlage für die Verarbeitung von Videoüberwachungsdaten bieten. So findet beispielsweise Artikel 6 Absatz 1 Buchstabe c nur dann Anwendung, wenn das nationale Recht eine Verpflichtung zur Videoüberwachung vorsieht.[7] In der Praxis werden jedoch im Regelfall folgende Bestimmungen als Rechtsgrundlagen für eine Videoüberwachung heranzuziehen sein:

- Artikel 6 Absatz 1 Buchstabe f (berechtigtes Interesse),
- Artikel 6 Absatz 1 Buchstabe e (Notwendigkeit der Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt).

In seltenen Ausnahmefällen könnte der Verantwortliche Artikel 6 Absatz 1 Buchstabe a (Einwilligung) als Rechtsgrundlage heranziehen.

3.1 Berechtigtes Interesse, Artikel 6 Absatz 1 Buchstabe f

17. Die rechtliche Bewertung von Artikel 6 Absatz 1 Buchstabe f sollte sich im Einklang mit Erwägungsgrund 47 auf folgende Kriterien stützen.

3.1.1 Das Bestehen berechtigter Interessen

18. Videoüberwachung ist rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen (Artikel 6 Absatz 1 Buchstabe f). Berechtigte Interessen eines Verantwortlichen oder eines Dritten können rechtliche[8], wirtschaftliche oder immaterielle Interessen sein.[9] Der Verantwortliche sollte jedoch berücksichtigen, dass er, sollte die betroffene Person gemäß Artikel 21 Widerspruch einlegen, die Videoüberwachung dieser betroffenen Person nur vornehmen kann, wenn es sich um ein *zwingendes* berechtigtes Interesse handelt, das

[6] Die Vorschriften für die Erhebung von Beweismitteln für zivilrechtliche Ansprüche sind in den Mitgliedstaaten unterschiedlich.

[7] In diesen Leitlinien werden nationale Rechtsvorschriften, die von Mitgliedstaat zu Mitgliedstaat unterschiedlich sein können, weder analysiert noch näher ausgeführt.

[8] Europäischer Gerichtshof, Urteil in der Rechtssache C-13/16, *Rīgas satiksme*, 4. Mai 2017.

[9] Vgl. Artikel-29-Datenschutzgruppe, WP217.

gegenüber den Interessen, Rechte und Freiheiten der betroffenen Person überwiegt, oder wenn die Videoüberwachung für die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist.

19. Der Zweck, Eigentum vor Einbruch, Diebstahl oder Vandalismus zu schützen, kann ein legitimes Interesse an einer Videoüberwachung darstellen, wenn eine tatsächliche Gefährdungslage vorliegt.

20. Das berechtigte Interesse muss tatsächlich und aktuell bestehen (d. h. es darf nicht fiktiv oder spekulativ sein)[10] . Bevor mit der Überwachung begonnen wird, muss eine reale Gefährdungslage vorliegen, z. B. Schäden oder schwere Vorfälle in der Vergangenheit können darauf hindeuten. Angesichts des Grundsatzes der Rechenschaftspflicht sind Verantwortliche gut beraten, relevante Vorfälle (Datum, Art und Weise, finanzieller Schaden) und damit verbundene strafrechtliche Tatvorwürfe zu dokumentieren. Diese dokumentierten Vorfälle können ein starkes Indiz für das Bestehen eines berechtigten Interesses sein. Ob ein berechtigtes Interesse besteht und ob die Überwachung notwendig ist, sollte in regelmäßigen Abständen überprüft werden (z. B. einmal jährlich, je nach den Umständen im Einzelfall).

> Beispiel: Ein Ladeninhaber möchte ein neues Geschäft eröffnen und zur Verhinderung von Vandalismus eine Videoüberwachungsanlage installieren. Er kann mit Statistiken belegen, dass in der näheren Nachbarschaft durchaus mit Vandalismus zu rechnen ist. Auch Erfahrungen benachbarter Geschäfte sind nützlich. Es ist nicht erforderlich, dass der betreffende Verantwortliche bereits einen Schaden erlitten hat. Solange Schäden in der Nachbarschaft auf eine Gefahr oder Ähnliches hindeuten, kann dies ein Hinweis auf ein berechtigtes Interesse sein. Es reicht jedoch nicht aus, nationale oder allgemeine Kriminalitätsstatistiken vorzulegen, ohne das betreffende Umfeld oder die Gefahren für dieses spezifische Ladengeschäft zu analysieren.

21.

22. Gefährdungslagen können bestimmten Orten auch immanent sein, so dass regelmäßig ein berechtigtes Interesse anzunehmen ist, z. B bei Banken oder Geschäften, die wertvolle Waren (z. B. Schmuck) verkaufen, oder Orte, an denen immer wieder Eigentumsdelikte begangen werden (z. B. Tankstellen).

23. Behörden können ihre in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung nicht auf ein berechtigtes Interesse stützen (Artikel 6 Absatz 1 Satz 2).

3.1.2 Erforderlichkeit der Verarbeitung

24. Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“); vgl. Artikel 5 Absatz 1 Buchstabe c. Vor der Installation einer Videoüberwachungsanlage sollte der Verantwortliche stets kritisch prüfen, ob diese Maßnahme erstens geeignet ist, das angestrebte Ziel zu erreichen, und zweitens dem Zweck angemessen und erforderlich ist. Videoüberwachungsmaßnahmen sollten nur dann gewählt werden, wenn der Zweck der Verarbeitung nach vernünftigem Ermessen nicht durch andere Mittel erreicht werden kann, die weniger in die Grundrechte und Grundfreiheiten der betroffenen Person eingreifen.

25. Möchte ein Verantwortlicher Eigentumsdelikte verhindern, könnte er statt einer Videoüberwachungsanlage auch alternative Sicherheitsmaßnahmen ergreifen, wie z. B. Umfriedung

[10] Vgl. Artikel-29-Datenschutzgruppe, WP217, S. 24f. Vgl. ferner EuGH, Rechtssache C-708/18, Rn. 44.

des Grundstücks, regelmäßige Rundgänge des Sicherheitspersonals, Einsatz von Pförtnern, bessere Beleuchtung, Einbau von Sicherheitsschlössern, einbruchsicheren Fenstern und Türen oder Anbringung von Anti-Graffiti-Beschichtungen oder -Folien an Wänden. Solche Maßnahmen können gegen Einbruch, Diebstahl und Vandalismus genauso wirksam sein wie Videoüberwachungsanlagen. Der Verantwortliche muss im Einzelfall prüfen, ob solche Maßnahmen eine vernünftige Lösung darstellen können.

26. Vor der Inbetriebnahme eines Kamerasystems muss der Verantwortliche prüfen, wo und wann Videoüberwachungsmaßnahmen unbedingt erforderlich sind. In der Regel dürfte ein Überwachungssystem, das nachts sowie außerhalb der regulären Arbeitszeiten betrieben wird, den Bedürfnissen des Verantwortlichen entsprechen, Gefahren für sein Eigentum abzuwenden.

27. Im Allgemeinen endet die Erforderlichkeit der Videoüberwachung zum Schutz der Räumlichkeiten der Verantwortlichen an den Grundstücksgrenzen.[11] Es gibt jedoch Fälle, in denen die Überwachung des Grundstücks für einen wirksamen Schutz nicht ausreicht. In einigen Einzelfällen kann es erforderlich sein, die Videoüberwachung bis zur unmittelbaren Umgebung der Räumlichkeiten auszuweiten. In diesem Zusammenhang sollte der Verantwortliche physische und technische Mittel in Betracht ziehen, z. B. das Einschränken des Erfassungsbereichs mit einer Blende oder das Verpixeln nicht relevanter Bereiche.

> Beispiel: Eine Buchhandlung möchte ihr Grundstück vor Vandalismus schützen. Grundsätzlich sollten Kameras nur die Räumlichkeiten selbst filmen, da es nicht notwendig ist, benachbarte Grundstücke oder öffentliche Bereiche in der Umgebung der Buchhandlung zu diesem Zweck einzusehen.

28.

29. Fragen zur Erforderlichkeit der Verarbeitung stellen sich auch in Bezug auf die Art und Weise, wie das Filmmaterial aufbewahrt wird. Mitunter kann es erforderlich sein, „Black-Box"-Lösungen zu verwenden, bei denen das Filmmaterial nach Ablauf einer bestimmten Speicherfrist automatisch gelöscht und nur im Falle eines Vorkommnisses eingesehen wird. In anderen Fällen ist es vielleicht gar nicht notwendig, Videomaterial aufzuzeichnen, sondern eher angebracht, Echtzeitüberwachung (sog. Live-Monitoring) vorzunehmen. Die Wahl zwischen „Black-Box"-Lösung und Echtzeitüberwachung sollte auch mit Blick auf den verfolgten Zweck getroffen werden. Wenn beispielsweise der Zweck der Videoüberwachung in der Beweissicherung besteht, ist ein Live-Monitoring in der Regel nicht geeignet. Mitunter kann eine Echtzeitüberwachung auch stärker in die Privatsphäre eingreifen als die Speicherung und das automatische Löschen von Material nach einer bestimmten Frist. (Wenn z. B. jemand ständig den Monitor beobachtet, könnte dies stärker in die Privatsphäre eingreifen, als wenn es überhaupt keinen Monitor gibt und das Material direkt in einer Black Box gespeichert wird). In diesem Zusammenhang ist der Grundsatz der Datenminimierung zu beachten (Artikel 5 Absatz 1 Buchstabe c). Es sollte auch bedacht werden, dass der Verantwortliche anstelle von Videoüberwachung möglicherweise Sicherheitspersonal einsetzen könnte, das sofort reagieren und eingreifen kann.

3.1.3 Interessenabwägung

30. Auch wenn die Videoüberwachung zum Schutz der berechtigten Interessen eines Verantwortlichen erforderlich ist, darf eine Videoüberwachungsanlage nur in Betrieb genommen werden, wenn die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person nicht die berechtigten

[11] Dies könnte in einigen Mitgliedstaaten auch nationalen Rechtsvorschriften unterliegen.

Interessen des Verantwortlichen oder eines Dritten (z. B. Schutz des Eigentums oder der körperlichen Unversehrtheit) überwiegen. Der Verantwortliche muss erstens prüfen, inwieweit die Überwachung die Interessen, Grundrechte und Grundfreiheiten natürlicher Personen beeinträchtigt, und zweitens, ob dies zu Verletzungen der Rechte der betroffenen Person oder zu negativen Folgen für diese führt. Eine Interessenabwägung ist zwingend vorgeschrieben. Die Grundrechte und Grundfreiheiten einerseits und die berechtigten Interessen des Verantwortlichen andererseits müssen sorgfältig bewertet und gegeneinander abgewogen werden.

Beispiel: Ein privater Parkplatzbetreiber hat wiederholt Probleme mit Diebstählen aus abgestellten Fahrzeugen dokumentiert. Der Parkplatz ist ein offener, für jeden zugänglicher Bereich, ist aber eindeutig mit Schildern und Umfriedungen rund um die Parkfläche versehen. Der Parkplatzbetreiber hat ein berechtigtes Interesse (Verhinderung von Diebstählen aus den Autos der Kunden) daran, die Fläche während der Zeiten, in welchen es erfahrungsgemäß Probleme gibt, zu überwachen. Betroffene Personen werden in einem begrenzten Zeitraum überwacht; sie verbringen dort nicht ihre Freizeit, und es liegt auch in ihrem eigenen Interesse, dass Diebstähle verhindert werden. In diesem Fall überwiegt das berechtigte Interesse des Verantwortlichen gegenüber dem Interesse der betroffenen Personen am Ausschluss der Überwachung.

Beispiel: Ein Restaurant beschließt, in den Sanitäranlagen Videokameras zu installieren, um deren Sauberkeit zu kontrollieren. In diesem Fall überwiegen die Rechte der betroffenen Personen eindeutig den Interessen des Verantwortlichen, sodass dort keine Kameras installiert werden können.

31.

3.1.3.1 Einzelfallentscheidungen

32. Da die Interessenabwägung gemäß der Verordnung zwingend vorgeschrieben ist, muss eine Entscheidung im Einzelfall getroffen werden (siehe Artikel 6 Absatz 1 Buchstabe f). Die Bezugnahme auf abstrakte Situationen oder der Vergleich mit ähnlichen Fällen ist nicht ausreichend. Der Verantwortliche muss die Risiken des Eingriffs in die Rechte der betroffenen Person bewerten; entscheidend ist hier die Intensität des Eingriffs in die Rechte und Freiheiten des Einzelnen.

33. Die Intensität kann unter anderem durch die Art der erhobenen Informationen (Informationsgehalt), den Umfang (Häufigkeit, Größe und räumliche Ausdehnung des Erfassungsbereichs), die Anzahl der betroffenen Personen (absolut oder in Relation zu der relevanten Personengruppe), die tatsächlichen Interessen der Gruppe betroffener Personen, andere eingesetzte Mittel sowie durch die Art und den Umfang der Datenauswertung bestimmt werden.

34. Wichtige Abwägungsfaktoren können die Größe des überwachten Bereichs und die Zahl der überwachten betroffenen Personen sein. Die Nutzung der Videoüberwachung in einem abgelegenen Gebiet (z. B. zur Beobachtung von Wild oder zum Schutz kritischer Infrastrukturen wie einer privaten Funkantenne) muss anders bewertet werden als die Videoüberwachung in einer Fußgängerzone oder einem Einkaufszentrum.

Beispiel: Wer eine Dash Cam installiert (z. B. für die Beweiserhebung im Falle eines Unfalls), muss unbedingt sicherstellen, dass diese Kamera nicht ständig den Verkehr oder Personen aufzeichnet, die sich in der Nähe einer Straße befinden. Andernfalls kann das Interesse an Videoaufnahmen als Nachweis im theoretischen Fall eines Verkehrsunfalls diesen schwerwiegenden Eingriff in die Rechte der betroffenen Personen nicht rechtfertigen.[11]

35.

3.1.3.2 Vernünftigen Erwartungen der betroffenen Personen

36. Gemäß Erwägungsgrund 47 muss das Vorliegen eines berechtigten Interesses sorgfältig geprüft werden. Hier sind die vernünftigen Erwartungen der betroffenen Person zum Zeitpunkt und im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten zu berücksichtigen. Bei einer systematischen Überwachung kann das Verhältnis zwischen betroffener Person und Verantwortlichem erheblich variieren und sich auf die vernünftigen Erwartungen auswirken, die die betroffene Person haben könnte. Die Auslegung des Begriffs der vernünftigen Erwartung orientiert sich dabei nicht ausschließlich an den subjektiven Erwartungen der betroffenen Person. Entscheidendes Kriterium ist vielmehr, ob ein objektiver Dritter vernünftigerweise in der konkreten Situation erwarten bzw. schlussfolgern kann, dass er überwacht wird.

37. So erwartet beispielsweise ein Arbeitnehmer an seinem Arbeitsplatz in den meisten Fällen nicht, von seinem Arbeitgeber überwacht zu werden.[12] Auch im eigenen Garten, in Wohnräumen oder in Untersuchungs- und Behandlungsräumen erwartet man nicht, überwacht zu werden. Ebenso kann davon ausgegangen werden, dass in sanitären Anlagen oder Saunen eine Überwachung nicht zu erwarten ist – die Überwachung solcher Bereiche ist ein intensiver Eingriff in die Rechte der betroffenen Person. Betroffene Personen können berechtigterweise erwarten, dass in diesen Bereichen keine Videoüberwachung stattfindet. Andererseits könnte der Kunde einer Bank erwarten, dass er in der Bank oder am Geldautomaten überwacht wird.

38. Betroffene Personen können auch davon ausgehen, dass sie in öffentlich zugänglichen Bereichen nicht überwacht werden, vor allem, wenn diese Bereiche typischerweise für Erholungs-, Entspannungs- und Freizeitaktivitäten genutzt werden, sowie an Orten, an denen sich Personen aufhalten und/oder kommunizieren, wie z. B. Sitzbereiche, Tische in Restaurants, Parks, Kinos und Fitnesseinrichtungen. Hier überwiegen häufig die Interessen oder Rechte und Freiheiten der betroffenen Person die berechtigten Interessen des Verantwortlichen.

> Beispiel: In Toilettenräumen erwarten betroffene Personen, dass sie nicht überwacht werden. Eine Videoüberwachung beispielsweise zur Verhütung von Unfällen ist nicht verhältnismäßig.

39.

40. Hinweisschilder, die über die Videoüberwachung informieren, sind für die Bestimmung dessen, was eine betroffene Person objektiv in einer bestimmten Situation erwarten kann, unerheblich. Wird z. B. am Eingang eines Ladengeschäfts über die Videoüberwachung informiert, hat dies alleine keine Auswirkungen auf die *objektiv* vernünftigen Erwartungen der Betroffenen.

3.2 Die Verarbeitung ist erforderlich für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde (Artikel 6 Absatz 1 Buchstabe e).

41. Personenbezogene Daten könnten im Wege der Videoüberwachung nach Artikel 6 Absatz 1 Buchstabe e verarbeitet werden, wenn die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt.[13] Für

[12] Siehe auch: Artikel-29-Datenschutzgruppe, Stellungnahme 2/2017 zur Datenverarbeitung am Arbeitsplatz, WP249, angenommen am 8. Juni 2017.

[13] Die Rechtsgrundlage für die genannte Verarbeitung „wird festgelegt durch Unionsrecht oder das Recht der Mitgliedstaaten“ und „die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde“ (Artikel 6 Absatz 3).

den Fall, dass die Videoüberwachung nicht für die Ausübung öffentlicher Gewalt erforderlich ist, besteht für öffentliche Stellen darüber hinaus die Möglichkeit, ihre Videoüberwachung auf andere Rechtsgrundlagen zu stützen. Das kann insbesondere bei einer Videoüberwachung zum Schutz der Sicherheit und der Gesundheit der Beschäftigten und der Besucher jeweiligen öffentlichen Stelle der Fall sein, wobei den Pflichten nach der DSGVO und den Rechten der betroffenen Personen stets Rechnung getragen werden muss.

42. Die Mitgliedstaaten können spezifische nationale Rechtsvorschriften für die Videoüberwachung beibehalten oder einführen, um die Anwendung der Vorschriften der DSGVO anzupassen, indem sie spezifischere Anforderungen für die Verarbeitung festlegen, solange diese den in der DSGVO festgelegten Grundsätzen entsprechen (z. B. Speicherbegrenzung, Verhältnismäßigkeit).

3.3 Einwilligung, Artikel 6 Absatz 1 Buchstabe a

43. Die Einwilligung muss gemäß der Leitlinien in Bezug auf die Einwilligung ohne Zwang, für den konkreten Fall, in Kenntnis der Sachlage und unmissverständlich erteilt werden.[14]

44. Bei systematischer Überwachung kann die Einwilligung der betroffenen Person nur in Ausnahmefällen als Rechtsgrundlage gemäß Artikel 7 (siehe Erwägungsgrund 43) dienen. Es liegt in der Natur der Überwachung, dass diese Technologie eine unbekannte Anzahl von Personen gleichzeitig überwacht. Der Verantwortliche wird kaum nachweisen können, dass die betroffene Person vor der Verarbeitung ihrer personenbezogenen Daten ihre Einwilligung gegeben hat (Artikel 7 Absatz 1). Angenommen, die betroffene Person widerruft ihre Einwilligung, dürfte es für den Verantwortlichen schwierig sein, nachzuweisen, dass personenbezogene Daten nicht mehr verarbeitet werden (Artikel 7 Absatz 3).

> Beispiel: Sportler können bei einzelnen Übungen gefilmt werden, damit sie ihre Techniken und Leistungen analysieren können. Wenn hingegen ein Sportverein beschließt, eine ganze Mannschaft für denselben Zweck zu überwachen, ist die Einwilligung häufig nicht wirksam, da sich die einzelnen Sportler unter Umständen unter Druck gesetzt fühlen, ihre Einwilligung zu erteilen, damit sich ihre Weigerung nicht nachteilig auf die Teammitglieder auswirkt.

45.

46. Will sich der Verantwortliche bei der Verarbeitung auf die Einwilligung stützen, hat er dafür Sorge zu tragen, dass jede betroffene Person, die den überwachten Bereich betritt, ihre Einwilligung gegeben hat. Diese Einwilligung muss die Bedingungen von Artikel 7 erfüllen. Das Betreten eines gekennzeichneten überwachten Bereichs (z. B. nach Aufforderung, einen bestimmten Flur zu benutzen oder ein bestimmtes Tor zu passieren, um in einen überwachten Bereich zu gelangen) stellt keine für die Einwilligung erforderliche Willensbekundung oder eindeutige bestätigende Handlung dar, es sei denn, die Kriterien der Artikel 4 und 7 werden erfüllt, wie in den Leitlinien in Bezug auf die Einwilligung beschrieben.[15]

47. Angesichts des Machtungleichgewichts zwischen Arbeitgebern und Arbeitnehmern sollten sich Arbeitgeber bei der Verarbeitung personenbezogener Daten in den meisten Fällen nicht auf eine Einwilligung stützen, da es unwahrscheinlich ist, dass sie aus freien Stücken erfolgt. In diesem Zusammenhang sollten die Leitlinien in Bezug auf die Einwilligung berücksichtigt werden.

---

[14] Artikel-29-Datenschutzgruppe „Leitlinien in Bezug auf die Einwilligung gemäß der Verordnung 2016/679“ (WP 259 rev. 01). – vom EDSA gebilligt

[15] Artikel 29-Datenschutzgruppe, „Leitlinien in Bezug auf die Einwilligung gemäß der Verordnung 2016/679“ (WP259) – vom EDSA gebilligt –, die berücksichtigt werden sollten.

48. Im Recht der Mitgliedstaaten oder in Kollektivvereinbarungen, einschließlich „Arbeitsverträgen“, können spezifische Vorschriften für die Verarbeitung personenbezogener Daten von Arbeitnehmern im Beschäftigungskontext vorgesehen werden (siehe Artikel 88).

4 OFFENLEGUNG VON VIDEOAUFZEICHNUNGEN GEGENÜBER DRITTEN

49. Grundsätzlich gelten für die Offenlegung von Videoaufzeichnungen gegenüber Dritten die allgemeinen Vorschriften der DSGVO.

4.1 Offenlegung von Videoaufzeichnungen gegenüber Dritten im Allgemeinen

50. „Offenlegung“ ist in Artikel 4 Absatz 2 definiert als Übermittlung (z. B. individuelle Kommunikation), Verbreitung (z. B. Online-Veröffentlichung) oder andere Form der Bereitstellung. „Dritte“ sind in Artikel 4 Absatz 10 definiert. Erfolgt die Offenlegung gegenüber Drittländern oder internationalen Organisationen, so gelten ferner die besonderen Bestimmungen von Artikel 44ff.

51. Jede Offenlegung personenbezogener Daten ist für sich eine Verarbeitung personenbezogener Daten, für die der Verantwortliche eine Rechtsgrundlage gemäß Artikel 6 haben muss.

> Beispiel: Ein Verantwortlicher, der eine Aufzeichnung ins Internet hochladen möchte, muss für diese Verarbeitung über eine Rechtsgrundlage verfügen, beispielsweise durch Einholung der Einwilligung der betroffenen Person gemäß Artikel 6 Absatz 1 Buchstabe a.

52.

53. Die Übermittlung von Videoaufnahmen an Dritte zu anderen Zwecken als dem, zu dem die Daten erhoben wurden, ist nach Maßgabe von Artikel 6 Absatz 4 möglich.

> Beispiel: Auf einem Parkplatz wird eine Videoüberwachung der Schranke installiert, um Beschädigungen nachgehen zu können. Es kommt zu einer Beschädigung, und die Aufzeichnung wird einem Anwalt übermittelt, um ein Verfahren einzuleiten. In diesem Fall ist der Zweck der Aufzeichnung identisch mit dem Zweck der Übermittlung.
>
> Beispiel: Auf einem Parkplatz wird eine Videoüberwachung der Schranke installiert, um Beschädigungen nachgehen zu können. Die Aufzeichnung wird allein zur Belustigung online veröffentlicht. In diesem Fall hat sich der Zweck geändert und ist nicht mit dem ursprünglichen Zweck vereinbar. Im Übrigen wäre es schwierig, eine Rechtsgrundlage für diese Verarbeitung (Veröffentlichung) zu finden.

54.

55. Der Empfänger von personenbezogenen Daten muss eine eigene rechtliche Analyse vornehmen und vor allem eine Rechtsgrundlage gemäß Artikel 6 für seine Verarbeitung ermitteln (z. B. Empfang des Materials).

4.2 Offenlegung von Videoaufzeichnungen gegenüber Strafverfolgungsbehörden

56. Die Offenlegung von Videoaufzeichnungen gegenüber Strafverfolgungsbehörden ist ebenfalls eine eigenständige Verarbeitung, die einer gesonderten Rechtsgrundlage für die Übermittlung durch den Verantwortlichen bedarf.

57. Gemäß Artikel 6 Absatz 1 Buchstabe c) ist die Verarbeitung rechtmäßig, wenn sie zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt. Wenngleich das anzuwendende Strafverfolgungs- und Polizeirecht eine Angelegenheit ist, die allein in die Zuständigkeit der Mitgliedstaaten fällt, gibt es in jedem Mitgliedstaat höchstwahrscheinlich allgemeine Vorschriften, die die Übermittlung von Beweismitteln an Strafverfolgungsbehörden regeln. Die Verarbeitung durch den Verantwortlichen, der die Daten übergibt, unterliegt der DSGVO. Wenn nationale

Rechtsvorschriften den Verantwortlichen zur Zusammenarbeit mit den Strafverfolgungsbehörden verpflichten (z. B. bei Ermittlungen), ist die Rechtsgrundlage für die Übermittlung der Daten die rechtliche Verpflichtung nach Artikel 6 Absatz 1 Buchstabe c.

58. Die Zweckbindung gemäß Artikel 6 Absatz 4 ist dann häufig unproblematisch, da die Offenlegung ausdrücklich auf das Recht der Mitgliedstaaten zurückgeht. Eine Berücksichtigung der besonderen Anforderungen an eine Zweckänderung im Sinne der Buchstaben a) bis e) ist daher nicht erforderlich.

> Beispiel: Ein Ladeninhaber überwacht den Eingang seines Ladengeschäfts . Das Videomaterial zeigt eine Person, die einer anderen Person die Geldbörse stiehlt. Die Polizei fordert den Verantwortlichen auf, das Material zu übergeben, um sie bei ihren Ermittlungen zu unterstützen. In diesem Fall kann der Ladeninhaber die Rechtsgrundlage nach Artikel 6 Absatz 1 Buchstabe c (rechtliche Verpflichtung) in Verbindung mit dem einschlägigen nationalen Recht für die Verarbeitung in Form einer Übermittlung heranziehen.

59.

> Beispiel: Aus Sicherheitsgründen wird in einem Geschäft eine Kamera installiert. Der Ladeninhaber glaubt, dass er in seinem Filmmaterial etwas Verdächtiges aufgezeichnet hat, und beschließt, das Material an die Polizei zu senden (ohne dass Hinweise auf eine laufende Ermittlung vorliegen). In diesem Fall muss der Ladeninhaber prüfen, ob die Voraussetzungen nach (in den meisten Fällen) Artikel 6 Absatz 1 Buchstabe f erfüllt sind. Dies ist in der Regel der Fall, wenn der Ladeninhaber den begründeten Verdacht hat, dass eine Straftat begangen wurde.

60.

61. Die Verarbeitung der personenbezogenen Daten durch die Strafverfolgungsbehörden selbst unterliegt nicht der DSGVO (siehe Artikel 2 Absatz 2 Buchstabe d), sondern der Strafverfolgungsrichtlinie (EU 2016/680).

5 VERARBEITUNG BESONDERER DATENKATEGORIEN

62. Videoüberwachungsanlagen erheben in der Regel äußerst große Mengen personenbezogener Daten, die auch Daten sehr persönlicher Art und sogar besondere Datenkategorien umfassen können. Tatsächlich können scheinbar belanglose Daten, die ursprünglich per Video erhoben wurden, verwendet werden, um andere Informationen zu gewinnen und damit einen anderen Zweck zu erreichen (z. B. um ein umfassendes Bild der Gewohnheiten einer Person zu gewinnen). Videoüberwachung stellt jedoch nicht immer eine Verarbeitung besonderer Kategorien personenbezogener Daten dar.

> Beispiel: Videoaufnahmen, die eine betroffene Person zeigen, die eine Brille trägt oder im Rollstuhl sitzt, gelten nicht *per se* als besondere Kategorien personenbezogener Daten.

63.

64. Wird das Videomaterial jedoch verarbeitet, um besondere Datenkategorien abzuleiten, ist Artikel 9 anzuwenden.

Beispiel: Politische Meinungen lassen sich beispielsweise aus Bildern ableiten, auf denen identifizierbare Personen zu sehen sind, die an bestimmten Veranstaltungen teilnehmen oder sich an einem Streik beteiligen usw. Dies würde in den Anwendungsbereich des Artikel 9 fallen.

Beispiel: Ein Krankenhaus, das eine Videokamera zur Überwachung des Gesundheitszustands eines Patienten installiert, verarbeitet in diesem Zusammenhang besondere Kategorien personenbezogener Daten (Artikel 9).

65.

66. Grundsätzlich sollte bei der Installation einer Videoüberwachungsanlage dem Grundsatz der Datenminimierung sorgfältig Rechnung getragen werden. Daher sollte der Verantwortliche auch in Fällen, in denen Artikel 9 Absatz 1 keine Anwendung findet, stets versuchen, das Risiko der Erfassung von Aufnahmen, aus denen andere (über Artikel 9 hinausgehende) sensitive Daten hervorgehen, unabhängig vom Zweck der Verarbeitung möglichst gering zu halten.

Beispiel: Eine Videoüberwachung in deren Erfassungsbereich sich eine Kirche befindet, fällt nicht *per se* in den Anwendungsbereich des Artikel 9. Der Verantwortliche muss jedoch bei der Bewertung der Interessen der betroffenen Person eine besonders sorgfältige Prüfung gemäß Artikel 6 Absatz 1 Buchstabe f durchführen, bei der die Art der Daten sowie das Risiko der Erfassung anderer sensibler Daten (über Artikel 9 hinaus) berücksichtigt werden.

67.

68. Wird zur Verarbeitung besonderer Datenkategorien eine Videoüberwachungsanlage eingesetzt, so muss der Verantwortliche sowohl eine Ausnahme für die Verarbeitung besonderer Datenkategorien nach Artikel 9 als auch eine Rechtsgrundlage nach Artikel 6 angeben.

69. So könnte beispielsweise Artikel 9 Absatz 2 Buchstabe c („[...] *die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich* […]“) – theoretisch und ausnahmsweise – genutzt werden, doch müsste der Verantwortliche dies als absolute Notwendigkeit zur Wahrung lebenswichtiger Interessen einer Person begründen und nachweisen, dass diese „[...] betroffene Person [...] *aus körperlichen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben*“. Darüber hinaus darf der Verantwortliche das System aus keinem anderen Grund nutzen.

70. In diesem Zusammenhang ist darauf hinzuweisen, dass wahrscheinlich kaum eine der in Artikel 9 aufgeführten Ausnahmen dazu genutzt werden kann, die Verarbeitung besonderer Datenkategorien durch Videoüberwachung zu rechtfertigen. Insbesondere können sich Verantwortliche, die diese Daten im Rahmen der Videoüberwachung verarbeiten, nicht auf Artikel 9 Absatz 2 Buchstabe e berufen, der eine Verarbeitung personenbezogener Daten erlaubt, die von der betroffenen Person offensichtlich öffentlich gemacht wurden. Die bloße Tatsache, dass sich die betroffene Person in den Erfassungsbereich der Kamera begibt, bedeutet nicht, dass sie beabsichtigt, auf sie bezogene besondere Kategorien von Daten zu veröffentlichen.

71. Wer besondere Kategorien personenbezogener Daten verarbeitet, sollte darüber hinaus seine datenschutzrechtlichen Verpflichtungen stets besonderes sorgfältig beachten, wie z. B. die Vorschriften über die Datensicherheit und ggf. zur Datenschutz-Folgeabschätzung.

Beispiel: Ein Arbeitgeber darf zur Identifizierung von Streikenden keine Videoüberwachungsaufzeichnungen von einer Demonstration verwenden.

72.

5.1 Allgemeine Erwägungen bei der Verarbeitung biometrischer Daten

73. Die Verwendung biometrischer Daten und insbesondere die Gesichtserkennung bergen erhöhte Risiken für die Rechte betroffener Personen. Von entscheidender Bedeutung ist, dass der Einsatz solcher Technologien unter gebührender Wahrung der in der DSGVO festgelegten Grundsätze der Rechtmäßigkeit, Notwendigkeit, Verhältnismäßigkeit und Datenminimierung erfolgt. Zwar kann der Einsatz dieser Technologien als besonders wirksam empfunden werden, doch sollten Verantwortliche zunächst die Auswirkungen auf die Grundrechte und Grundfreiheiten bewerten und weniger einschneidende Mittel in Betracht ziehen, um ihren legitimen Zweck der Verarbeitung zu erreichen.

74. Damit Rohdaten, wie die physischen, physiologischen oder verhaltensbezogenen Eigenschaften einer natürlichen Person, als biometrische Daten im Sinne der DSGVO eingestuft werden können, muss ihre Verarbeitung eine Messung dieser Merkmale implizieren. Da biometrische Daten das Ergebnis solcher Messungen sind, heißt es in Artikel 4 Absatz 14 DSGVO, dass sie „*[...] sich aus einer spezifischen technischen Verarbeitung der physischen, physiologischen oder verhaltensbezogenen Eigenschaften einer natürlichen Person ergeben, die die eindeutige Identifizierung dieser natürlichen Person [...] ermöglicht oder bestätigt*“. Die Videoaufnahmen einer Person können jedoch als solche nicht als biometrische Daten im Sinne von Artikel 9 betrachtet werden, wenn sie nicht speziell technisch verarbeitet wurden, um zur Identifizierung einer Person beizutragen.[16]

75. Damit von einer Verarbeitung besonderer Kategorien personenbezogener Daten (Artikel 9) gesprochen werden kann, müssen biometrische Daten „zur eindeutigen Identifizierung einer natürlichen Person“ verarbeitet werden.

76. Zusammenfassend ist festzustellen: Nach Artikel 4 Absatz 14 und Artikel 9 sind drei Kriterien zu prüfen:

- **Art der Daten**: Daten über physische, physiologische oder verhaltensbezogene Eigenschaften einer natürlichen Person,
- **Mittel und Wege der Verarbeitung**: „mit speziellen technischen Verfahren gewonnene“ Daten,
- **Zweck der Verarbeitung**: Die Daten müssen zur eindeutigen Identifizierung einer natürlichen Person verwendet werden.

77. Die Nutzung einer Videoüberwachung einschließlich Funktionen zur Erfassung biometrischer Merkmale, die von privaten Stellen für ihre eigenen Zwecke installiert wird (z. B. Marketing, Statistik oder sogar Sicherheit), erfordert in den meisten Fällen die ausdrückliche Einwilligung aller betroffenen Personen (Artikel 9 Absatz 2 Buchstabe a), auch wenn zumindest theoretisch auch alle anderen Ausnahmen des Art. 9 anwendbar sind.

[16] Dies ergibt sich aus Erwägungsgrund 51, denn dort heißt es: „*[…] Die Verarbeitung von Lichtbildern sollte nicht grundsätzlich als Verarbeitung besonderer Kategorien personenbezogener Daten angesehen werden, da Lichtbilder nur dann von der Definition des Begriffs „biometrische Daten“ erfasst werden, wenn sie mit spezifischen technischen Mitteln verarbeitet werden, die die eindeutige Identifizierung oder Authentifizierung einer natürlichen Person ermöglichen. […]*“.

Beispiel: Zur Verbesserung des Services ersetzt ein privates Unternehmen die Kontrollstellen zur Identifizierung von Fluggästen innerhalb eines Flughafens bei der Gepäckaufgabe und beim Boarding durch Videoüberwachungsanlagen, die Gesichtserkennungstechniken verwenden. Damit soll die Identität derjenigen Fluggäste überprüft werden, die freiwillig in ein solches Verfahren eingewilligt haben. Da die Verarbeitung unter Artikel 9 fällt, müssen die Fluggäste, die den Service nutzen wollen, zuvor ausdrücklich und in Kenntnis der Sachlage ihre Einwilligung erteilt und sich entsprechend registriert haben. Dann können sie sich beispielsweise an einem automatischen Terminal anmelden, wo ein Template ihres Gesichts erstellt wird, welches mit den in ihrer Bordkarte registrierten Identitätsdaten abgeglichen wird. Die Kontrollstellen mit Gesichtserkennung müssen klar von den anderen getrennt sein; so muss z. B. das System in einem separaten Durchgang installiert sein, damit keine biometrischen Templates von Personen erfasst werden, die keine Einwilligung erteilt haben. Nur die Fluggäste, die zuvor ihre Einwilligung erteilt und ihre Registrierung vorgenommen haben, dürfen die mit dem biometrischen System ausgestattete Kontrollstelle passieren.

Beispiel: Ein Verantwortlicher regelt den Zugang zu seinem Gebäude mithilfe einer Gesichtserkennungstechnologie. Personen, die das Gebäude betreten möchten, können diese Art des Zugangs nur dann rechtmäßig nutzen, wenn sie zuvor ihre ausdrückliche Einwilligung in Kenntnis der Sachlage (gemäß Artikel 9 Absatz 2 Buchstabe a) erteilt haben. Um sicherzustellen, dass niemand erfasst wird, der zuvor nicht seine Einwilligung erteilt hat, sollte die Gesichtserkennungsmethode von der betroffenen Person selbst ausgelöst werden, z. B. durch Drücken eines Knopfes. Damit die Rechtmäßigkeit der Verarbeitung gewährleistet ist, muss der Verantwortliche stets einen alternativen Zugang zum Gebäude ohne Verarbeitung biometrischer Daten anbieten, wie Zugangskarten oder Schlüssel.

78.

79. In Fällen, in denen biometrische Templates erzeugt werden, stellen die Verantwortlichen sicher, dass alle spontan (mit ausdrücklicher Einwilligung der betroffenen Person in Kenntnis der Sachlage) erstellten Zwischen-Templates, die mit den von den betroffenen Personen zum Zeitpunkt der Registrierung erstellten Templates verglichen werden, unverzüglich und sicher gelöscht werden, sobald ein Ergebnis in Form von Übereinstimmung bzw. Nichtübereinstimmung vorliegt. Die für die Registrierung erstellten Templates sollten nur für das Erreichen des Zwecks der Verarbeitung aufbewahrt und nicht gespeichert oder archiviert werden.

80. Besteht jedoch der Zweck der Verarbeitung beispielsweise darin, eine Personenkategorie von einer anderen zu unterscheiden, nicht aber darin, jemanden eindeutig zu identifizieren, fällt die Verarbeitung nicht zwangsläufig unter Artikel 9.

Beispiel: Ein Ladeninhaber möchte seine Werbung auf das Geschlecht und die Altersmerkmale des Kunden zuschneiden, der von einem Videoüberwachungssystem erfasst wird. Wenn mit diesem System keine biometrischen Templates zur eindeutigen Identifizierung von Personen generiert werden, sondern lediglich physische Merkmale erkannt werden, um die Person zu klassifizieren, würde die Verarbeitung nicht unter Artikel 9 fallen (solange keine anderen Arten besonderer Datenkategorien verarbeitet werden).

81.

82. Artikel 9 findet jedoch Anwendung, wenn der Verantwortliche biometrische Daten speichert (meist in Form von Templates, die durch Extraktion von Schlüsselmerkmalen aus der Rohform biometrischer Daten (z. B. Gesichtsmessungen aus einem Bild) erstellt werden), um eine Person eindeutig zu identifizieren. Wenn ein Verantwortlicher eine betroffene Person wiedererkennen möchte, die einen

Bereich erneut oder einen anderen Bereich betritt (z. B. um fortlaufend maßgeschneiderte Werbung zu projizieren), wäre der Zweck der Verarbeitung, eine natürliche Person eindeutig zu identifizieren. Dies bedeutet, dass der Vorgang von Anfang an nach Artikel 9 beurteilt werden muss. Dies könnte der Fall sein, wenn ein Verantwortlicher erstellte Templates speichert, um weitere maßgeschneiderte Werbeanzeigen auf mehreren Tafeln an verschiedenen Punkten innerhalb des Geschäfts bereitzustellen. Da das System physische Merkmale verwendet, um bestimmte Personen, die in den Erfassungsbereich der Kamera zurückkehren (wie Besucher eines Einkaufszentrums), zu erkennen und zu verfolgen („tracking"), handelt es sich um eine biometrische Identifizierungsmethode, da sie auf die Erkennung durch eine spezifische technische Verarbeitung abzielt.

Beispiel: Ein Ladeninhaber hat in seinem Geschäft ein Gesichtserkennungssystem eingerichtet, um seine Werbung auf Einzelpersonen zuschneiden zu können. Der Verantwortliche muss die ausdrückliche und in Kenntnis der Sachlage erteilte Einwilligung aller betroffenen Personen einholen, bevor er dieses biometrische System einsetzt und maßgeschneiderte Werbung betreibt. Das System wäre rechtswidrig, wenn es Besucher oder Passanten erfasst, die nicht in die Erstellung ihres biometrischen Templates eingewilligt haben, selbst wenn ihr Template so schnell wie möglich gelöscht wird. Auch diese temporären Templates stellen nämlich biometrische Daten dar, die verarbeitet werden, um eine Person, die möglicherweise keine gezielte Werbung erhalten möchte, eindeutig zu identifizieren.

83.

84. Der EDSA stellt fest, dass einige biometrische Systeme in nicht kontrollierten Umgebungen installiert sind[17], was bedeutet, dass das System auch spontan biometrische Templates von allen Personen erstellt, deren Gesichter, die in den Erfassungsbereich der Kamera geraten. Dazu gehören zwangsläufig auch Personen, die in die Erfassung biometrischer Merkmale nicht eingewilligt haben. Diese Templates werden mit jenen verglichen, die im Rahmen einer Registrierung mit Einwilligung der betroffenen Person erstellt wurden, damit der Verantwortliche erkennen kann, ob es sich bei der betroffenen Person um einen registrierten Nutzer handelt oder nicht. In diesem Fall zielt das System häufig darauf ab, Personen aus einer Datenbank wiederzuerkennen und von nicht-registrierten Personen zu unterscheiden. Da der Zweck darin besteht, natürliche Personen eindeutig zu identifizieren, ist in jedem Fall eine Ausnahme nach Artikel 9 Absatz 2 DSGVO für alle von der Kamera erfassten Personen erforderlich.

[17] Das bedeutet, dass sich das biometrische Gerät in einem öffentlich zugänglichen Bereich befindet und alle vorbeilaufenden Personen erfassen kann, im Gegensatz zu biometrischen Systemen in kontrollierten Umgebungen, die nur mit Einwilligung der Person genutzt werden können.

Beispiel: Ein Hotel setzt Videoüberwachung mit Gesichtserkennungstechnologie ein, um den Hotelmanager automatisch darauf aufmerksam zu machen, dass ein VIP-Gast eingetroffen ist. Diese VIP-Gäste haben ausdrücklich in den Einsatz von Gesichtserkennung eingewilligt, bevor sie in einer zu diesem Zweck eingerichteten Datenbank erfasst werden. Diese Systeme zur Verarbeitung biometrischer Daten wären rechtswidrig, sofern nicht alle anderen Gäste, die in den Erfassungsbereich geraten, in die der Verarbeitung gemäß Artikel 9 Absatz 2 Buchstabe a DSGVO eingewilligt haben.

Beispiel: Ein Verantwortlicher installiert eine Videoüberwachungsanlage mit Gesichtserkennung am Eingang des von ihm betriebenen Konzertsaals. Der Verantwortliche muss klar voneinander getrennte Eingänge einrichten: einen mit einem biometrischen System und einen ohne (wo z. B. stattdessen ein Ticket gescannt wird). Die mit biometrischen Geräten ausgestatteten Eingänge müssen so installiert und zugänglich gemacht werden, dass das System keine biometrischen Templates von Zuschauern erfassen kann, die keine Einwilligung erteilt haben.

85.

86. In Fällen in denen die Einwilligung nach Artikel 9 DSGVO erforderlich ist, darf der Verantwortliche nicht den Zugang zu seinen Dienstleistung von der Einwilligung in die Verarbeitung biometrischer Daten abhängig machen. Mit anderen Worten und insbesondere, wenn die Verarbeitung biometrischer Daten für Authentifizierungszwecke erfolgt, muss der Verantwortliche eine Alternative anbieten, die keine Verarbeitung biometrischer Daten umfasst – ohne dass Einschränkungen oder zusätzliche Kosten für die betroffene Person entstehen. Eine solche Alternative ist auch für Personen erforderlich, denen die Nutzung des biometrischen Geräts nicht möglich ist (Unmöglichkeit der Erfassung oder Auswertung der biometrischen Daten, Behinderung, die die Nutzung erschwert usw.). Ebenfalls bedarf es für den Fall einer Nichtverfügbarkeit des biometrischen Geräts (z. B. Fehlfunktion des Geräts) einer „Back-up-Lösung“, um die Kontinuität des betroffenen Dienstes in Ausnahmesituationen zu gewährleisten. In Ausnahmefällen könnte es vorkommen, dass die Verarbeitung biometrischer Daten die Kerntätigkeit einer vertraglich erbrachten Dienstleistung ist, z. B. ein Museum, das eine Ausstellung ausrichtet, um die Verwendung eines Gesichtserkennungsgeräts zu demonstrieren; in diesem Fall kann die betroffene Person die Verarbeitung biometrischer Daten nicht ablehnen, wenn sie an der Ausstellung teilnehmen möchte. Hier ist die nach Artikel 9 erforderliche Einwilligung wirksam, wenn die Voraussetzungen von Artikel 7 erfüllt sind.

5.2 Vorgeschlagene Maßnahmen zur Minimierung der Risiken bei der Verarbeitung biometrischer Daten

87. Im Einklang mit dem Grundsatz der Datenminimierung müssen Verantwortliche sicherstellen, dass Daten, die aus einem digitalen Bild extrahiert werden, um ein Template zu erstellen, nicht übermäßig sind und nur die für den angegebenen Zweck erforderlichen Informationen enthalten, wodurch eine mögliche Weiterverarbeitung vermieden wird. Es sollten Maßnahmen ergriffen werden, um sicherzustellen, dass Templates nicht zwischen biometrischen Systemen übertragen werden können.

88. Identifizierung und Authentifizierung/Verifizierung erfordern in der Regel die Speicherung der Templates für einen späteren Abgleich. Der Verantwortliche muss prüfen, welcher Ort am besten für die Speicherung der Daten geeignet ist. In einer kontrollierten Umgebung (abgegrenzte Korridore oder Kontrollpunkte) werden Templates auf einem persönlichen Gerät des Nutzers, das allein vom Nutzer und nur von ihm kontrolliert wird (in einem Smartphone oder auf der ID-Karte), oder – wenn dies für bestimmte Zwecke erforderlich ist und objektiven Bedürfnissen entspricht – in einer zentralen Datenbank in verschlüsselter Form mit einem Schlüssel/Passwort ausschließlich im Zugriff der Person

gespeichert, deren Zuständigkeit es ist, den unbefugten Zugriff auf das Template oder den Speicherort zu verhindern. Kann der Verantwortliche eine Zugangsmöglichkeit zu den Templates nicht vermeiden, muss er geeignete Maßnahmen ergreifen, um die Sicherheit der gespeicherten Daten zu gewährleisten. Dazu kann die Verschlüsselung des Templates unter Verwendung eines kryptografischen Algorithmus gehören.

89. In jedem Fall trifft der Verantwortliche alle erforderlichen Vorkehrungen, um die Verfügbarkeit, Integrität und Vertraulichkeit der verarbeiteten Daten zu wahren. Zu diesem Zweck ergreift der Verantwortliche insbesondere folgende Maßnahmen: Unterteilung der Daten während der Übermittlung und Speicherung; Speicherung biometrischer Templates und Rohdaten oder Identitätsdaten in verschiedenen Datenbanken; Verschlüsselung biometrischer Daten, insbesondere biometrischer Templates, und Festlegung einer Verschlüsselungs- und Schlüsselmanagementstrategie, Integration einer organisatorischen und technischen Maßnahme zur Betrugsaufdeckung; Verknüpfung eines Integritätscodes mit den Daten (z. B. Signatur oder Hash) und Verbot jeglichen externen Zugangs zu den biometrischen Daten. Solche Maßnahmen müssen mit dem technologischen Fortschritt weiterentwickelt werden.

90. Darüber hinaus sollten Verantwortliche Rohdaten (Gesichtsbilder, Sprachsignale, Gangart usw.) löschen und dafür sorgen, dass sie auch tatsächlich gelöscht sind. Wenn es keine Rechtsgrundlage mehr für die Verarbeitung gibt, müssen die Rohdaten gelöscht werden. Da biometrische Templates aus solchen Daten abgeleitet werden, kann davon ausgegangen werden, dass der Aufbau von Datenbanken eine gleichgroße, wenn nicht sogar größere Gefahr darstellen könnte (da es möglicherweise nicht immer einfach ist, biometrische Templates zu lesen, ohne zu wissen, wie sie programmiert wurden, während Rohdaten die Bausteine jedes Templates sind). Für den Fall, dass der Verantwortliche solche Daten aufbewahren muss, müssen Verfälschungsmethoden (ggf. Watermarking) geprüft werden,die die Erstellung eines Templates unmöglich machen würde. Der Verantwortliche muss ferner biometrische Daten und Templates löschen, wenn ein unbefugter Zugriff auf das Lesegerät oder den Speicherserver erfolgt ist, und alle Daten löschen, die am Ende der Lebensdauer des biometrischen Geräts für eine weitere Verarbeitung nicht nützlich sind.

6 RECHTE DER BETROFFENEN PERSON

91. Obwohl alle Betroffenenrechte der DSGVO auch im Rahmen der Verarbeitung personenbezogener Daten durch Videoüberwachung gelten, bedürfen manche aufgrund der Besonderheiten der Videoüberwachung weiterer Erläuterung. Dieses Kapitel behandelt daher nicht alle Betroffenenrechte.

6.1 Recht auf Auskunft

92. Eine betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu erhalten, ob ihre personenbezogenen Daten verarbeitet werden oder nicht. Für die Videoüberwachung bedeutet dies Folgendes: Werden Daten in keiner Weise gespeichert oder übertragen, kann der Verantwortliche nach einer Echtzeit-Überwachungszeit nur mitteilen, dass keine personenbezogenen Daten mehr verarbeitet werden. (Unbeschadet dessen gelten die allgemeinen Informationspflichten nach Artikel 13, siehe *Abschnitt 7 – Transparenz und Informationspflichten.*) Werden die Daten jedoch zum Zeitpunkt des Antrags noch immer verarbeitet (d. h. wenn die Daten auf andere Weise gespeichert oder fortgesetzt verarbeitet werden), muss die betroffene Person Auskunft und Informationen gemäß Artikel 15 erhalten.

93. Es gibt jedoch eine Reihe von Ausnahmen, die in einigen Fällen für das Auskunftsrecht gelten können.

- Artikel 15 Absatz 4 DSGVO: Beeinträchtigung der Rechte anderer

94. Da eine beliebige Anzahl betroffener Personen in derselben Sequenz der Videoüberwachung aufgezeichnet werden kann, würde eine Vorführung des Videomaterials zu einer zusätzlichen Verarbeitung personenbezogener Daten anderer betroffener Personen führen. Wenn die betroffene Person eine Kopie des Materials erhalten möchte (Artikel 15 Absatz 3), könnte dies die Rechte und Freiheiten anderer gefilmter betroffener Personen beeinträchtigen. Um dies zu verhindern, hat der Verantwortliche daher zu prüfen, ob in einigen Fällen auf die Herausgabe von Videoaufnahmen verzichtet, auf denen andere betroffene Personen identifiziert werden können, wenn dies zu tief in die Privatsphäre Dritter eingreift. Der Schutz der Rechte Dritter darf jedoch nicht als Vorwand genutzt werden, um legitime Auskunftsansprüche von Einzelpersonen zu verhindern; in diesen Fällen kann der Verantwortliche technische Maßnahmen ergreifen, um dem Auskunftsersuchen nachzukommen (z. B. Bildbearbeitung wie beispielsweise Schwärzen oder „Verpixeln“). Allerdings sind Verantwortliche nicht verpflichtet, solche technischen Maßnahmen umzusetzen, wenn sie auf andere Weise sicherstellen können, dass sie auf einen Antrag nach Artikel 15 innerhalb der in Artikel 12 Absatz 3 festgelegten Frist reagieren können.

- Artikel 11 Absatz 2 DSGVO: Der Verantwortliche ist nicht in der Lage, die betroffene Person zu identifizieren

95. Wenn das Videomaterial nicht nach personenbezogenen Daten durchsucht werden kann (z. B. aufgrund der großen Menge an gespeicherten Material), ist der Verantwortliche möglicherweise nicht ohne Weiteres in der Lage, die betroffene Person zu identifizieren.

96. Aus diesen Gründen sollte die betroffene Person (nachdem sie sich mit einem Personaldokument oder auch persönlich identifiziert hat) in ihrem Antrag an den Verantwortlichen angeben, in welchem Zeitraum sieden überwachten Bereich betreten hat. (Die Länge des anzugebenden Zeitraums sollte in einem angemessenen Verhältnis zu der Anzahl der regelmäßig erfassten Personen stehen.) Der Verantwortliche sollte der betroffenen Person vorab mitteilen, welche Angaben erforderlich sind, damit er dem Antrag nachkommen kann. Kann der Verantwortliche nachweisen, dass er nicht in der Lage ist, die betroffene Person zu identifizieren, so unterrichtet

er die betroffene Person hierüber, sofern möglich. In einem solchen Fall sollte der Verantwortliche in seiner Antwort an die betroffene Person über den genauen überwachten Bereich, die Überprüfung der verwendeten Kameras usw. informieren, damit die betroffene Person umfassend nachvollziehen kann, welche personenbezogenen Daten über sie verarbeitet wurden.

> Beispiel: Beantragt eine betroffene Person eine Kopie ihrer personenbezogenen Daten, die durch Videoüberwachung am Eingang eines Einkaufszentrums mit 30 000 Besuchern pro Tag verarbeitet werden, sollte die betroffene Person angeben, in welchem Zeitraum mit +/- einer Stunde sie den überwachten Bereich passiert hat. Wenn der Verantwortliche das Material noch verarbeitet, muss eine Kopie der Videoaufnahmen zur Verfügung gestellt werden. Wenn andere betroffene Personen in demselben Material identifiziert werden können, sollte dieser Teil des Materials anonymisiert werden (z. B. durch „Verpixelung" der Kopie oder Teilen davon), bevor die Kopie der antragstellenden betroffenen Person übergeben wird.
>
> Beispiel: Löscht der Verantwortliche beispielsweise automatisch alle Aufnahmen innerhalb von zwei Tagen, ist er nicht in der Lage, der betroffenen Person nach Ablauf dieser zwei Tage Aufnahmen zu übermitteln. Erhält der Verantwortliche einen Antrag nach Ablauf dieser zwei Tage, sollte die betroffene Person entsprechend unterrichtet werden.

97.

- Artikel 12 DSGVO: Exzessive Anträge

98. Im Falle exzessiver oder offenkundig unbegründeter Anträge einer betroffenen Person kann der Verantwortliche entweder eine angemessene Gebühr gemäß Artikel 12 Absatz 5 Buchstabe a DSGVO erheben oder sich weigern, dem Antrag nachzukommen (Artikel 12 Absatz 5 Buchstabe b DSGVO). Der Verantwortliche muss in der Lage sein, den offenkundig unbegründeten oder exzessiven Charakter des Antrags nachzuweisen.

6.2 Recht auf Löschung und Widerspruchsrecht

6.2.1 Recht auf Löschung (Recht auf Vergessenwerden)

99. Wenn der Verantwortliche über ein Live-Monitoring hinaus personenbezogene Daten verarbeitet (z. B. speichert), kann die betroffene Person beantragen, dass die personenbezogenen Daten gemäß Artikel 17 DSGVO gelöscht werden.

100. Auf Antrag ist der Verantwortliche verpflichtet, die personenbezogenen Daten unverzüglich zu löschen, wenn einer der in Artikel 17 Absatz 1 DSGVO aufgeführten Umstände zutrifft (und keine der in Artikel 17 Absatz 3 DSGVO aufgeführten Ausnahmen greift). Dazu gehört auch die Verpflichtung, personenbezogene Daten zu löschen, wenn sie für den Zweck, für den sie ursprünglich gespeichert wurden, nicht mehr benötigt werden, oder wenn die Verarbeitung rechtswidrig ist (siehe auch *Abschnitt 8 – Aufbewahrungsfristen und Löschungspflicht*). Darüber hinaus sollten personenbezogene Daten je nach Rechtsgrundlage gelöscht werden:

- *bei einer Einwilligung*: Wenn die Einwilligung widerrufen wird (und es keine andere Rechtsgrundlage für die Verarbeitung gibt)
- *bei berechtigtem Interesse*:
    - Wenn die betroffene Person von ihrem Widerspruchsrecht Gebrauch macht (siehe *Abschnitt 6.2.2*) und keine zwingenden berechtigten Gründe für die Verarbeitung vorliegen, oder

- bei Direktwerbung (einschließlich Profiling): wenn die betroffene Person der Verarbeitung widerspricht.

101. Hat der Verantwortliche die Videoaufnahmen öffentlich gemacht (z. B. im Internet), müssen angemessene Maßnahmen ergriffen werden, um andere Verantwortliche (die mittlerweile die betreffenden personenbezogenen Daten verarbeiten) gemäß Artikel 17 Absatz 2 DSGVO über den Antrag zu informieren. Die angemessenen Maßnahmen sollten unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten auch Maßnahmen technischer Art umfassen. Soweit möglich sollte der Verantwortliche gemäß Artikel 19 DSGVO bei der Löschung personenbezogener Daten alle Empfängern, denen die personenbezogenen Daten zuvor offengelegt wurden, über die Löschung informieren.

102. Neben der Pflicht des Verantwortlichen, personenbezogene Daten auf Antrag der betroffenen Person zu löschen, besteht nach den allgemeinen Grundsätzen der DSGVO die Verpflichtung, die Verarbeitung einzuschränken(*siehe Abschnitt 8*).

103. Bezüglich Videoüberwachung sei darauf hingewiesen, dass beispielsweise bei einer irreversible Verpixelung des Bildes die personenbezogenen Daten als im Sinne der DSGVO gelöscht gelten, soweit keineMöglichkeit besteht, die in dem Bild enthaltenen personenbezogene Daten nachträglich wiederherzustellen wiederzuerlangen.,

> Beispiel: Ein Gemischtwarenladen hat Probleme mit Vandalismus speziell an der Fassade und nutzt daher eine Videoüberwachung, die außerhalb des Eingangs unmittelbar an der Wand angebracht ist. Ein Passant beantragt die sofortige Löschung seiner personenbezogenen Daten. Der Verantwortliche ist verpflichtet, dem Antrag unverzüglich, spätestens jedoch innerhalb eines Monats nachzukommen. Falls es zudem Zeitpunkt an dem der Passant vorbeiging, keinen Fall von Vandalismus gab, entfällt der ursprüngliche Zweck für die Speicherung. Folglich besteht zum Zeitpunkt des Antrags kein berechtigtes Interesse an der Speicherung der Daten, das die Interessen der betroffenen Personen überwiegen würde. Der Verantwortliche muss die personenbezogenen Daten löschen.

104.

6.2.2 Widerspruchsrecht

105. Erfolgt die Videoüberwachung aufgrund eines *berechtigten Interesses* (Artikel 6 Absatz 1 Buchstabe f DSGVO) oder weil sie für die Wahrnehmung einer Aufgabe im *öffentlichen Interesse* erforderlich ist(Artikel 6 Absatz 1 Buchstabe e DSGVO), hat die betroffene Person das Recht, gemäß Artikel 21 DSGVO jederzeit aus Gründen, die sich aus ihrer besonderen Situation ergeben, Widerspruch gegen die Verarbeitung einzulegen. Sofern der Verantwortliche keine zwingenden berechtigten Gründe nachweist, die die Rechte und Interessen der betroffenen Person überwiegen, muss die Verarbeitung der Daten der Person, die Widerspruch eingelegt hat, dann eingestellt werden. Der Verantwortliche ist verpflichtet, Anträgen der betroffenen Person unverzüglich, spätestens jedoch innerhalb eines Monats nachzukommen.

106. Im Zusammenhang mit Videoüberwachung kann dieser Widerspruch entweder beim Betreten des überwachten Bereichs, während des Aufenthalts dort oder nach seinem Verlassen eingelegt werden. Das hat praktisch zur Folge, dass der Verantwortliche – sofern er keine zwingenden berechtigten Gründe nachweisen kann – einen Bereich, in dem natürliche Personen identifiziert werden könnten, nur dann rechtmäßig überwachen kann, wenn

(1) der Verantwortliche in der Lage ist, bei Widersprüchen die Verarbeitung personenbezogener Daten unverzüglich zu stoppen, oder

(2) der überwachte Bereich so eingeschränkt zugänglich ist, dass die betroffene Person ihn ohne ihre vorherige Zustimmung betreten kann. Das gilt nur soweit es sich nicht um einen Bereich handelt, auf dessen Betreten die betroffene Person als Bürger Anspruch hat.

107. Mit diesen Leitlinien soll nicht festgestellt werden, was unter einem *zwingenden berechtigten Interesse* zu verstehen ist (Artikel 21 DSGVO).

108. Bei der Nutzung von Videoüberwachung für Zwecke der Direktwerbung hat die betroffene Person jederzeit das Recht, Widerspruch gegen die Verarbeitung einzulegen, da das Widerspruchsrecht in diesem Zusammenhang absolut ist (Artikel 21 Absätze 2 und 3 DSGVO).

> Beispiel: Ein Unternehmen hat Schwierigkeiten mit Sicherheitsvorfällen an seinem öffentlichen Eingang und nutzt aus Gründen des berechtigten Interesses Videoüberwachung, um Unbefugte am Betreten der Räumlichkeiten zu hindern. Ein Besucher widerspricht aus Gründen, die sich aus seiner besonderen Situation ergeben, der Verarbeitung seiner Daten durch die Videoüberwachungsanlage. Wird das gespeicherte Material aufgrund einer laufenden internen Untersuchung benötigt, liegen zwingende berechtigte Gründe für die weitere Verarbeitung der personenbezogenen Daten vorliegen, so dass der Antrag zurückgewiesen werden kann.

109.

7 TRANSPARENZ UND INFORMATIONSPFLICHTEN[18]

110. Wichtiger Bestandteil des europäischen Datenschutzrechts ist es schon seit Langem, dass eine Videoüberwachung so betrieben werden muss, dass betroffene Personen sich dessen bewusst sind. Es ist insbesondere darüber zu informieren, welche Bereiche genau überwacht werden.[19] In der DSGVO sind die allgemeinen Transparenz- und Informationspflichten in Artikel 12ff. geregelt. Die „Leitlinien für Transparenz gemäß der Verordnung 2016/679 (WP260)" der Artikel-29-Datenschutzgruppe, die am 25. Mai 2018 vom EDSA gebilligt wurden, enthalten weitere Einzelheiten. Nach Randziffer 26 der Leitlinie WP260 ist Artikel 13 DSGVO anwendbar, wenn personenbezogene Daten im Wege der Beobachtung bei der betroffenen Person erhoben werden (z. B. unter Verwendung von automatisierten Datenerfassungsgeräten oder Datenerfassungssoftware wie Kameras [...]).

111. Angesichts der Menge an Informationen, die der betroffenen Person übermittelt werden müssen, kann von den Verantwortlichen ein gestuftes Verfahren eingesetzt werden. In diesem Zusammenhang kann die Information in zwei Schritten erfolgen, um Transparenz zu gewährleisten (WP260, Absatz 35; WP89, Absatz 22). Bei Videoüberwachung sollten die wichtigsten Informationen auf einem vorgelagerten Hinweisschild angezeigt werden (erste Ebene), während die weiteren obligatorischen Angaben auf anderem Wege (zweite Ebene) gemacht werden können.

7.1 Informationen der ersten Ebene (Hinweisschild)

112. Die erste Ebene betrifft die Art und Weise, in der der Verantwortliche zuerst mit der betroffenen Person Kontakt aufnimmt. In dieser Phase können Verantwortliche einen Hinweisschild verwenden, das die relevanten Informationen anzeigt. Die betreffenden Informationen können in Kombination mit einem Bildsymbol bereitgestellt werden, um in leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form einen aussagekräftigen Überblick über die beabsichtigte Verarbeitung zu vermitteln (Artikel 12 Absatz 7 DSGVO). Das Format der Informationen sollte an den jeweiligen Standort angepasst werden (WP89 Absatz 22).

7.1.1 Anbringung des Hinweisschildes

113. Die Informationen sollten so angebracht sein, dass die betroffene Person die Umstände der Überwachung leicht erkennen kann, bevor sie den überwachten Bereich betritt (etwa in Augenhöhe). Die Position der Kamera selbst muss nicht offengelegt werden, solange kein Zweifel daran besteht, welche Bereiche erfasst werden und die Umstände der Überwachung eindeutig beschrieben werden (WP89 Absatz 22). Die betroffene Person muss in der Lage sein, einzuschätzen, welcher Bereich von einer Kamera erfasst wird, damit sie der Überwachung ausweichen oder ihr Verhalten erforderlichenfalls anpassen kann.

7.1.2 Inhalt der ersten Ebene

114. Die Informationen der ersten Ebene (Hinweisschild) sollten in der Regel die wichtigsten Informationen enthalten, z. B. Angaben zu den Zwecken der Verarbeitung, zur Identität des Verantwortlichen und zum Bestehen der Rechte der betroffenen Person sowie weitere Informationen mit hoher Bedeutung.[20] Dazu können beispielsweise die berechtigten Interessen des Verantwortlichen (oder eines Dritten) und (gegebenenfalls) die Kontaktdaten des Datenschutzbeauftragten gehören. Sie

[18] Es können besondere Anforderungen in den nationalen Rechtsvorschriften gelten.

[19] Siehe Artikel-29-Datenschutzgruppe, WP89, Stellungnahme 4/2004 zum Thema Verarbeitung personenbezogener Daten aus der Videoüberwachung.

[20] Siehe WP260, Absatz 38.

müssen ferner auf die detailliertere zweite Informationsebene verweisen sowie darauf hinweisen, wo und wie sie zu finden ist.

115. Darüber hinaus sollte der Hinweis auch alle Informationen enthalten, die für die betroffene Person überraschend sein könnten (WP260, Ziffer 38). Dabei könnte es sich beispielsweise um die Übermittlung an Dritte, vor allem außerhalb der EU, und die Speicherdauer handeln. Werden diese Angaben nicht gemacht, sollte die betroffene Person darauf vertrauen können, dass es lediglich eine Live-Überwachung gibt (ohne Datenaufzeichnung oder -übermittlung an Dritte).

Beispiel (unverbindlicher Vorschlag):

116.

7.2 Informationen der zweiten Ebene

117. Informationen der zweiten Ebene müssen ebenfalls an einem für die betroffene Person leicht zugänglichen Ort zur Verfügung gestellt werden, z. B. als vollständiges Informationsblatt an einer zentralen Stelle (z. B. Informationsschalter, Empfang oder Kasse) oder auf einem leicht zugänglichen Plakat. Wie bereits erwähnt, muss der Warnhinweis der ersten Ebene eindeutig auf die Informationen der zweiten Ebene verweisen. Darüber hinaus ist es am besten, wenn die Informationen der ersten Ebene auf eine digitale Quelle (z. B. QR-Code oder Internetadresse) der zweiten Ebene verweisen. Die Informationen müssen jedoch auch auf nicht digitalem Wege leicht verfügbar sein. Es sollte möglich sein, auf die Informationen der zweiten Ebene zuzugreifen, ohne sich in den überwachten Bereich zu begeben, insbesondere wenn die Informationen digital bereitgestellt werden (beispielsweise über einen Link). Ein anderes geeignetes Mittel könnte eine Telefonnummer sein, die angerufen werden kann. Die Informationen müssen jedoch alle Angaben enthalten, die nach Artikel 13 DSGVO obligatorisch sind.

118. Um die Wirksamkeit von Transparenzmaßnahmen zu erhöhen, fördert der EDSA den Einsatz technologischer Mittel, um betroffenen Personen Informationen zur Verfügung zu stellen. Dazu zählt beispielsweise die Ausstattung von Kameras mit geografischer Ortungsmöglichkeit und ihre Aufnahme

in kartografische Apps oder Websites, sodass Personen einerseits leicht erkennen und angeben können, welche Videoquellen existieren und für die Ausübung ihrer Rechte relevant sein könnten, und andererseits ausführlichere Informationen über die jeweiligen Verarbeitungsvorgänge erhalten können.

Beispiel: Ein Ladeninhaber überwacht sein Geschäft. Um Artikel 13 Genüge zu tun, reicht es aus, an einem gut sichtbaren Punkt am Eingang seines Geschäfts einen Hinweisschild anzubringen, das die Informationen der ersten Ebene enthält. Darüber hinaus muss er ein Informationsblatt mit den Informationen der zweiten Ebene an der Kasse oder an einem anderen zentralen und leicht zugänglichen Ort in seinem Geschäft bereithalten.

119.

8 AUFBEWAHRUNGSFRISTEN UND LÖSCHUNGSPFLICHT

120. Personenbezogene Daten dürfen nicht länger gespeichert werden, als es für die Zwecke, für die sie verarbeitet werden, erforderlich ist (Artikel 5 Absatz 1 Buchstaben c und e DSGVO). In einigen Mitgliedstaaten kann es gemäß Artikel 6 Absatz 2 DSGVO besondere Bestimmungen für Speicherfristen bei Videoüberwachung geben.

121. Ob es erforderlich ist, die personenbezogenen Daten zu speichern, sollte innerhalb eines engen Zeitrahmens kontrolliert werden. Im Allgemeinen sind legitime Zwecke der Videoüberwachung häufig der Schutz des Eigentums oder die Sicherung von Beweismitteln. In der Regel werden eingetretene Schäden innerhalb von ein oder zwei Tagen erkannt. Um die Einhaltung der datenschutzrechtlichen Vorgaben leichter nachweisen zu können, liegt es im Interesse des Verantwortlichen, im Voraus organisatorische Maßnahmen zu treffen. (Z. B. kann eine Person bestimmt werden, die für die Sichtung und Sicherung von Videomaterial verantwortlich ist). Unter Berücksichtigung der Grundsätze nach Artikel 5 Absatz 1 Buchstaben c und e DSGVO (Datenminimierung und Speicherbegrenzung) sollten die personenbezogenen Daten in den meisten Fällen im Idealfall nach einigen Tagen automatisch gelöscht werden (z. B. bei Speicherung zum Zwecke der Rechtewahrnehmung bei Vandalismus). Je länger die Speicherfrist ist, desto höher ist der Argumentionsaufwand in Bezug auf die Rechtmäßigkeit des Zwecks und der Erforderlichkeit. Das gilt insbesondere, wenn sie mehr als 72 Stunden beträgt. Setzt der Verantwortliche die Videoüberwachung nicht nur zum Live-Monitoring seiner Räumlichkeiten ein, sondern beabsichtigt er auch eine Speicherung der Daten, muss er sicherstellen, dass die Speicherung für das Erreichen des Zwecks tatsächlich erforderlich ist. Ist dies der Fall, muss die Speicherdauer klar definiert und für jeden bestimmten Zweck einzeln festgelegt werden. Es liegt in der Verantwortung des Verantwortlichen, den Aufbewahrungszeitraum im Einklang mit den Grundsätzen der Erforderlichkeit und Verhältnismäßigkeit festzulegen und die Einhaltung der Bestimmungen der DSGVO nachzuweisen.

Beispiel: Ein Inhaber eines kleinen Geschäfts bemerkt Vandalismus in der Regel noch am selben Tag. Folglich reicht eine reguläre Speicherfrist von 24 Stunden aus. Schließzeiten an Wochenenden oder ein längerer Urlaub können jedoch Gründe für eine längere Speicherfrist sein. Wird ein Schaden festgestellt, muss er möglicherweise das Videomaterial länger speichern, um rechtliche Schritte gegen den Täter einzuleiten zu können.

122.

9 TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

123. Gemäß Artikel 32 Absatz 1 DSGVO muss die Verarbeitung personenbezogener Daten während der Videoüberwachung nicht nur rechtlich zulässig sein, sondern muss sie auch von Verantwortlichen und Auftragsverarbeitern in angemessener Weise abgesichert werden. Umgesetzte **organisatorische und technische Maßnahmen** müssen **in einem angemessenen Verhältnis zu den Risiken für die Rechte und Freiheiten natürlicher Personen stehen**, die sich aus der zufälligen oder unrechtmäßigen Vernichtung, dem Verlust, der Veränderung, der unbefugten Weitergabe oder dem unberechtigten Zugang zu Videoüberwachungsdaten ergeben. Gemäß Artikel 24 sowie 25 DSGVO müssen Verantwortliche auch technische und organisatorische Maßnahmen ergreifen, um alle Datenschutzgrundsätze bei der Verarbeitung zu wahren und Möglichkeiten schaffen, damit betroffene Personen ihre Rechte gemäß den Artikeln 15 bis 22 DSGVO wahrnehmen können. Für die Verarbeitung Verantwortliche sollten interne Rahmenbedingungen und Strategien festlegen, die diese Umsetzung sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der Verarbeitung selbst gewährleisten, gegebenenfalls einschließlich der Durchführung von Datenschutz-Folgenabschätzungen nach Artikel 35 DSGVO.

9.1 Überblick über eine Videoüberwachungsanlage

124. Eine Videoüberwachungsanlage[21] besteht aus analogen und digitalen Geräten sowie Software, mit der Bilder an einem Ort erfasst, die Bilder bearbeitet und einem Bediener angezeigt werden können. Ihre Bestandteile sind in folgende Kategorien eingeteilt:

- Videoumgebung: Bilderfassung, Verbindungen und Bildhandhabung:
  - Zweck der Bilderfassung ist die Generierung eines Bildes von Geschehnissen der realen Welt in einem Format, das vom Rest der Anlage genutzt werden kann.
  - Verbindungsleitungen beschreiben die gesamte Datenübertragung innerhalb der Videoumgebung, d. h. Verbindungen und Kommunikation. Beispiele für Verbindungen sind Kabel, digitale Netze und drahtlose Übertragungen. Kommunikation beschreibt alle Video- und Steuerdatensignale, die digital oder analog sein können.
  - Bildhandhabung umfasst die Analyse, Speicherung und Darstellung eines Bildes oder einer Abfolge von Bildern.
- Aus der Sicht des Systemmanagements hat eine Videoüberwachungsanlage folgende logische Funktionen:
  - Daten- und Aktivitätsmanagement, einschließlich Befehle des Bedienungspersonals und systemgenerierte Tätigkeiten (Alarmprozedur, Alarmmeldung),
  - Schnittstellen zu anderen Systemen können die Verbindung mit anderen Sicherheitssystemen (Zugangskontrolle, Feueralarm) und Nicht-Sicherheitssystemen (Gebäudeleitsysteme, automatische Kennzeichenerkennung) umfassen.

[21] Die DSGVO enthält keine Definition hierfür; eine technische Beschreibung findet sich beispielsweise in EN 62676-1-1: 2014 Video surveillance systems for use in security applications – Part 1-1: Video system requirements [Systemanforderungen (Videoüberwachungsanlagen für Sicherheitsanwendungen – Teil 1-1:)].

- Zur Gewährleistung der Sicherheit von Videoüberwachungsanlagen ist die System- und Datenvertraulichkeit, -integrität und –verfügbarkeit sicherzustellen:
    - Die Systemsicherheit umfasst die physische Sicherheit aller Systemkomponenten und die Kontrolle des Zugangs zur Videoüberwachungsanlage;
    - zur Datensicherheit gehört die Verhinderung des Verlusts oder der Manipulation von Daten.

125.

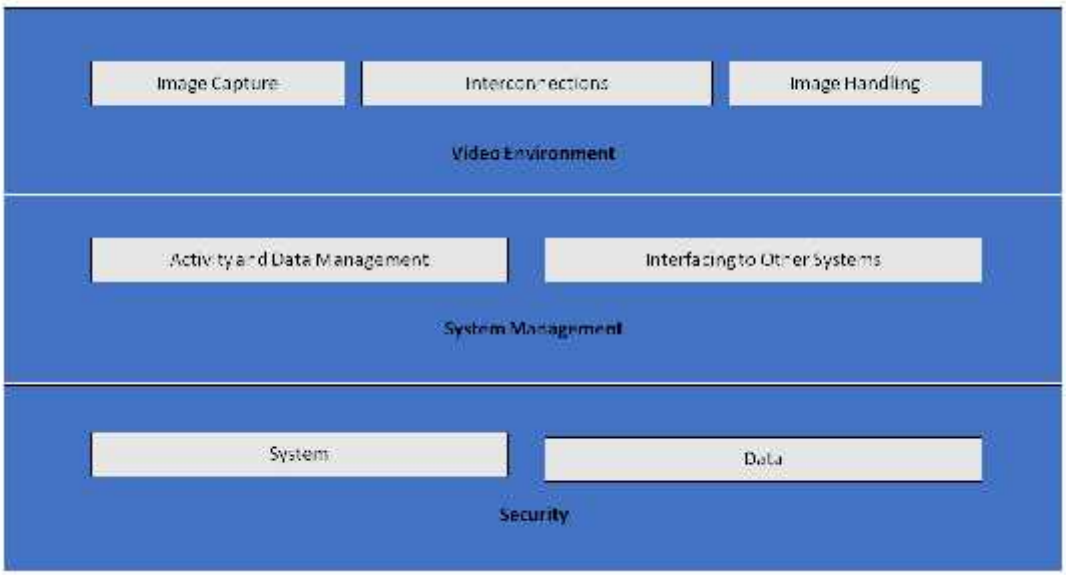

Image Capture	Bilderfassung
Interconnections	Verbindungen
Image Handling	Bildhandhabung
Video Environment	Videoumgebung
Activity and Data Management	Aktivitäts- und Datenmanagement
Interfacing to Other Systems	Schnittstelle zu anderen Systemen
System Management	Systemverwaltung
System	System
Data	Daten
Security	Sicherheit

Abbildung 1- Videoüberwachungsanlage

9.2 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

126. Gemäß Artikel 25 DSGVO müssen Verantwortliche bereits bei der Planung einer Videoüberwachung geeignete technische und organisatorische Datenschutzmaßnahmen vorsehen und diese ergreifen, bevor sie mit der Erfassung und Verarbeitung von Videoaufnahmen beginnen. Zu diesen Grundsätzen gehört auch die Auswahl von Technologien mit integrierten Datenschutzfunktionen, die Auswahl von datenschutzfreundlichen Voreinstellungen, welche die Datenverarbeitung minimieren sowie die

Bereitstellung von Werkzeugen, die den größtmöglichen Schutz personenbezogener Daten ermöglichen.[22]

127. Verantwortliche sollten Datenschutzgarantien und Garantien für den Schutz der Privatsphäre nicht nur in die Konstruktionsspezifikationen der eingesetzten Technologie, sondern auch in die Praxis ihrer Organisation aufnehmen. Bezüglich der Praxis der Organisation sollte der Verantwortliche einen geeigneten Managementrahmen vorgeben sowie Strategien und Verfahren für die Videoüberwachung festlegen und durchsetzen. Aus technischer Sicht sollten Systemspezifikation und -design Anforderungen an die Verarbeitung personenbezogener Daten im Einklang mit den Datenschutzgrundsätzen von Artikel 5 DSGVO (Rechtmäßigkeit der Verarbeitung, Zweckbindung und Datenbeschränkungen, standardmäßige Datenminimierung im Sinne von Artikel 25 Absatz 2 DSGVO, Integrität und Vertraulichkeit, Rechenschaftspflicht usw.) enthalten. Beabsichtigt ein Verantwortlicher den Erwerb einer kommerziellen Videoüberwachungsanlage, muss er diese Anforderungen in die Beschaffungsspezifikation aufnehmen. Der Verantwortliche muss sicherstellen, dass diese Anforderungen, eingehalten werden, indem er sie auf alle Systemkomponenten und alle von ihm verarbeiteten Daten während ihres gesamten Lebenszyklus anwendet.

9.3 Konkrete Beispiele für einschlägige Maßnahmen

128. Die meisten Maßnahmen, die zur Sicherung der Videoüberwachung eingesetzt werden können, insbesondere wenn digitale Geräte und Software verwendet werden, unterscheiden sich nicht wesentlich von andere IT-Systeme. Unabhängig von der gewählten Lösung muss der Verantwortliche jedoch alle Komponenten einer Videoüberwachungsanlage und die Daten in allen Phasen angemessen schützen, d. h. während der Speicherung (*data at rest*), der Übermittlung (*data in transit*) und der Verarbeitung (*data in use*). Zu diesem Zweck müssen Verantwortliche und Auftragsverarbeiter organisatorische und technische Maßnahmen miteinander kombinieren.

129. Bei der Auswahl technischer Lösungen sollte der Verantwortliche datenschutzfreundliche Technologien berücksichtigen, weil diese in der Regel auch eine erhöhte Sicherheit bieten. Beispiele für solche Technologien sind Systeme, die eine Maskierung oder Verzerrung von Bereichen ermöglichen, die für die Überwachung nicht relevant sind, oder das Weglassen von Bildern von Personen, wenn Videoaufzeichnungen betroffenen Personen zur Verfügung gestellt werden.[23] Andererseits sollten die ausgewählten Lösungen keine Funktionen bieten, die nicht notwendig sind (z. B. unbeschränkte Bewegung von Kameras, Zoomfähigkeit, Funkübertragung, Analyse und Tonaufzeichnungen). Funktionen, die bereitgestellt werden, aber nicht notwendig sind, müssen deaktiviert werden.

130. Es gibt umfangreiche Literatur zu diesem Thema, einschließlich internationaler Normen und technischer Spezifikationen zur physischen Sicherheit von Multimedia-Systemen[24] und zur Sicherheit allgemeiner IT-Systeme[25]. Daher bietet dieser Abschnitt nur einen ersten Überblick über dieses Thema.

---

[22] WP168, „Die Zukunft des Datenschutzes“, 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 personenbezogener Daten (angenommen am 1. Dezember 2009).

[23] Der Einsatz solcher Technologien kann in einigen Fällen sogar verpflichtend sein, um Artikel 5 Absatz 1 Buchstabe c zu entsprechen. In jedem Fall können sie als Beispiele für bewährte Verfahren dienen.

[24] IEC TS 62045 – Multimedia-Sicherheit – Leitfaden für den Datenschutz bei genutzten oder ungenutzten Einrichtungen und Systemen.

[25] ISO 27000 –Reihe von Standards zur Informationssicherheit.

9.3.1 Organisatorische Maßnahmen

131. Neben einer möglicherweise erforderlichen Datenschutz-Folgenabschätzung nach Artikel 35 DSGVO (*siehe Abschnitt 10*) sollten Verantwortliche bei der Erstellung ihrer eigenen Videoüberwachungsstrategien und -verfahren folgende Themen berücksichtigen:

- Wer ist für das Management und den Betrieb der Videoüberwachungsanlage zuständig?
- Gegenstand und Anwendungsbereich des Videoüberwachungsprojekts.
- Angemessener und verbotener Einsatz (wo und wann ist eine Videoüberwachung zulässig und wo und wann nicht; z. B. Einsatz verborgener Kameras und Tonaufzeichnungen zusätzlich zu Bildaufzeichnungen)[26].
- Transparenzmaßnahmen gemäß *Abschnitt 7 (Transparenz- und Informationspflichten).*
- Wie und für welche Dauer wird das Video aufgezeichnet, einschließlich der Archivierung von Videoaufzeichnungen im Zusammenhang mit Sicherheitsvorfällen?
- Wer muss wann eine entsprechende Schulung absolvieren?
- Wer hat Zugang zu Videoaufnahmen und zu welchen Zwecken?
- Operative Verfahren (z. B. von wem und wo die Videoüberwachung überwacht wird, was im Falle einer Datenschutzpanne zu tun ist).
- Welche Verfahren müssen externe Parteien befolgen, um die Bereitstellung von Videoaufzeichnungen zu beantragen, und nach welchen Verfahren werden solche Anträge abgelehnt oder genehmigt?
- Verfahren für die Beschaffung, Installation und Wartung von Videoüberwachungsanlage.
- Störfallmanagement und Verfahren zur Wiederherstellung des Betriebs.

9.3.2 Technische Maßnahmen

132. **Systemsicherheit** bedeutet **physische Sicherheit** aller Systemkomponenten und Systemintegrität, d. h. **Schutz vor und Widerstandsfähigkeit bei vorsätzlichen und unbeabsichtigten Eingriffen in den normalen Betrieb sowie die Zugangskontrolle**. Datensicherheit bedeutet **Vertraulichkeit** (Daten sind nur für diejenigen zugänglich, denen Zugang gewährt wurde), **Integrität** (Verhinderung des Verlusts oder der Manipulation von Daten) und **Verfügbarkeit** (Daten können bei Bedarf abgerufen werden).

133. Die **physische Sicherheit** ist ein wesentlicher Bestandteil des Datenschutzes und die erste äußere Schutzmaßnahme, da sie die Videoüberwachungsanlage und die damit verbundene Ausrüstung vor Diebstahl, Vandalismus, Naturkatastrophen, vom Menschen verursachten Katastrophen und unfallbedingten Schäden (z. B. vor elektrischer Überspannung, extremen Temperaturen und vergossenem Kaffee) schützt. Bei analogen Systemen spielt die physische Sicherheit die wichtigste Rolle für ihren Schutz.

134. **System- und Datensicherheit**, d. h. der Schutz vor vorsätzlichen und unbeabsichtigten Eingriffen in den normalen Betrieb, kann Folgendes umfassen:

- Schutz der gesamten Infrastruktur der Videoüberwachungsanlage (einschließlich Kameras, Verkabelung und Stromversorgung) vor physischer Manipulation und Diebstahl.
- Schutz der Übertragungswege der Videoaufzeichnungen mittels gesicherten Kommunikationskanälen gegen das Abhören durch Dritte.
- Verschlüsselung der Daten auf den Übertragungswegen sowie auf Speichersystemen.
- Einsatz von Hardware- und Softwarelösungen wie Firewalls, Antivirus- oder Angriffserkennungssystemen gegen Cyberangriffe.

[26] Dies kann von nationalen Gesetzen und sektorspezifischen Vorschriften abhängen.

- Erkennung von Ausfällen von Komponenten, Software und Verbindungen.
- Mittel zur Wiederherstellung der Verfügbarkeit und des Zugangs zum System im Falle eines physischen oder technischen Zwischenfalls.

135. Die **Zugangskontrolle** stellt sicher, dass nur befugte Personen Zugriff auf das System und die Daten haben, während andere daran gehindert werden. Zu den Maßnahmen, die die physische und logische Zugangskontrolle unterstützen, gehören:

- Gewährleistung, dass alle Räumlichkeiten, in denen die Überwachung durch Videoüberwachung erfolgt und Videoaufnahmen gespeichert werden, gegen unkontrollierten Zugang Dritter gesichert sind.
- Monitore, die so angebracht sind (insbesondere, wenn sie sich in offenen Bereichen wie dem Empfangsbereich befinden), dass sie nur von ermächtigtem Bedienungspersonal eingesehen werden können.
- Es werden Verfahren für die Gewährung, Änderung und Aufhebung des physischen und logischen Zugangs festgelegt und durchgesetzt.
- Methoden und Mittel der Nutzerauthentifizierung und Autorisierung, einschließlich z. B. Länge des Passworts und Häufigkeit der Änderung, werden umgesetzt.
- Die von Nutzern (sowohl am System als auch an den Daten) durchgeführten Maßnahmen werden aufgezeichnet und regelmäßig überprüft.
- Die Überwachung und Erkennung von fehlgeschlagenen Zugangsversuchen erfolgt kontinuierlich, und festgestellte Schwachstellen werden so bald wie möglich behoben.

10 DATENSCHUTZ-FOLGENABSCHÄTZUNG

136. Artikel 35 Absatz 1 DSGVO sieht für Verantwortliche eine obligatorische Datenschutz-Folgenabschätzung (DSFA) vor, sobald eine Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Nach Artikel 35 Absatz 3 Buchstabe c DSGVO sind Verantwortliche verpflichtet, Datenschutz-Folgenabschätzungen durchzuführen, wenn die Verarbeitung eine systematische umfangreiche Überwachung eines öffentlich zugänglichen Bereichs darstellt. Ferner ist nach Artikel 35 Absatz 3 Buchstabe b DSGVO eine Datenschutz-Folgenabschätzung erforderlich, wenn der Verantwortliche eine umfangreiche Verarbeitung besonderer Kategorien von Daten plant.

137. Die Leitlinien zur Datenschutz-Folgenabschätzung[27] bieten weitere Orientierung und detailliertere Beispiele für die Videoüberwachung (z. B. „Einsatz eines Kamerasystems zur Überwachung des Fahrverhaltens auf Schnellstraßen“). Nach Artikel 35 Absatz 4 DSGVO muss jede Aufsichtsbehörde eine Liste der Verarbeitungsvorgänge veröffentlichen, für die in ihrem Land eine Datenschutz-Folgenabschätzung durchzuführen ist. Diese Listen sind in der Regel auf den Websites der Behörden zu finden. Angesichts der typischen Zwecke der Videoüberwachung (Schutz von Personen und Eigentum, Aufdeckung, Verhütung und Bekämpfung von Straftaten, Beweiserhebung und biometrische Identifizierung von Verdächtigen) kann vernünftigerweise davon ausgegangen werden, dass viele Fälle von Videoüberwachung eine DSFA erfordern werden. Daher sollten Verantwortliche die Vorgaben in diesen Unterlagen sorgfältig berücksichtigen, um festzustellen, ob eine solche Prüfung erforderlich ist, und sie gegebenenfalls durchführen. Das Ergebnis der durchgeführten DSFA sollte über die Wahl der vom Verantwortlichen durchgeführten Datenschutzmaßnahmen entscheiden.

138. Ferner ist darauf hinzuweisen, dass vor der Verarbeitung die zuständige Aufsichtsbehörde konsultiert werden muss, wenn die Ergebnisse der DSFA darauf hindeuten, dass die Verarbeitung trotz der vom Verantwortlichen geplanten Sicherheitsmaßnahmen zu einem hohen Risiko führen würde. Einzelheiten zur vorherigen Konsultationen sind in Artikel 36 DSGVO zu entnehmen.

Für den Europäischen Datenschutzausschuss

Vorsitzende

(Andrea Jelinek)

[27] WP248 rev.01, „Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt‘“. – vom EDSA gebilligt