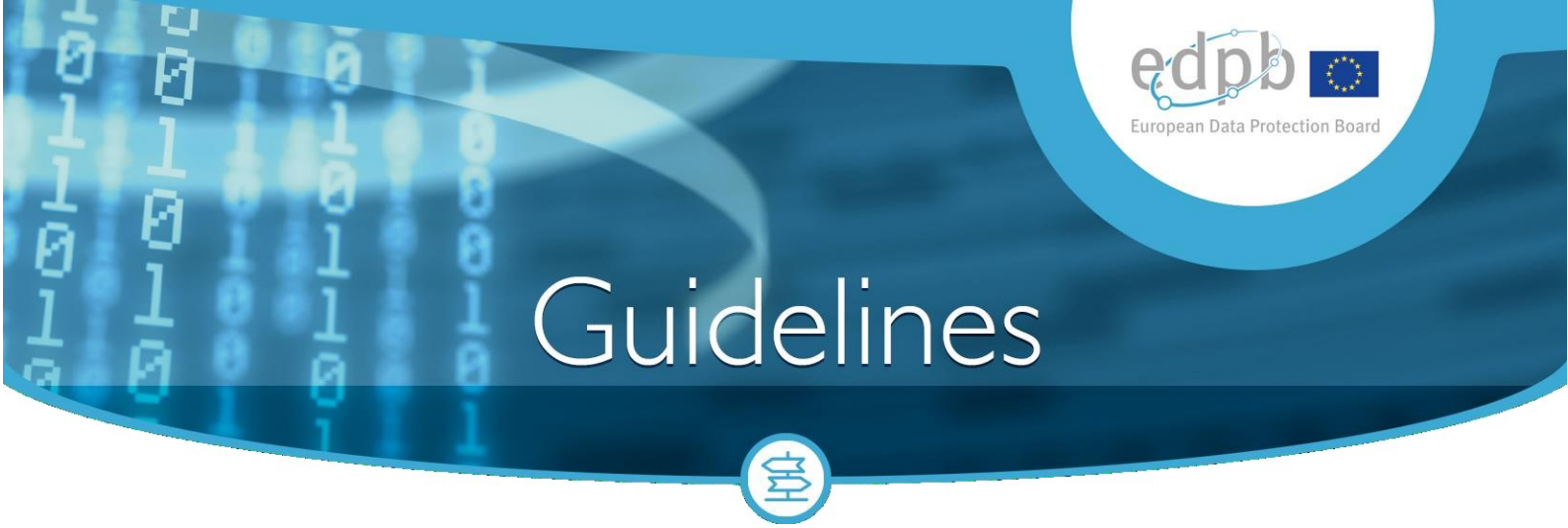


Richtlinien 3/2019 zur Verarbeitung persönlicher Daten durch Videogeräte

Version 2.0

Angenommen am 29. Januar 2020

Dieses Dokument ersetzt die Version vom Juli 2019
Von Nicholas Vollmer mittels www.deepl.com übersetzt.

Versionsgeschichte

Version 2.0	29. Januar 2020	Verabschiedung der Richtlinien nach öffentlicher Konsultation
Version 1.0	10. Juli 2019	Verabschiedung der Richtlinien für die öffentliche Konsultation

Der Europäische Datenschutzrat

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

gestützt auf das EWR-Abkommen, insbesondere auf Anhang XI und Protokoll 37, in der durch den Beschluss des Gemeinsamen EWR-Ausschusses Nr. 154/2018 vom 6. Juli 20181 geänderten Fassung,

gestützt auf Artikel 12 und Artikel 22 seiner Geschäftsordnung,

HAT DIE FOLGENDEN RICHTLINIEN VERABSCHIEDET

1 EINLEITUNG

1. Die intensive Nutzung von Videogeräten hat Auswirkungen auf das Verhalten der Bürger. Eine bedeutende Implementierung solcher Instrumente in vielen Lebensbereichen des Einzelnen wird einen zusätzlichen Druck auf den Einzelnen ausüben, um die Entdeckung von möglicherweise als Anomalien empfundenen Anomalien zu verhindern. De facto können diese Technologien die Möglichkeiten der anonymen Bewegung und der anonymen Nutzung von Diensten einschränken und generell die Möglichkeit, unbemerkt zu bleiben, einschränken. Die Auswirkungen auf den Datenschutz sind massiv.

2. Auch wenn sich der Einzelne mit einer Videoüberwachung, die z.B. für einen bestimmten Sicherheitszweck eingerichtet wurde, wohlfühlen mag, müssen Garantien gegeben werden, um jeglichen Missbrauch für völlig andere und - für die betroffene Person - unerwartete Zwecke zu vermeiden (z.B. für Marketingzwecke, Überwachung der Mitarbeiterleistung usw.). Darüber hinaus werden jetzt viele Werkzeuge implementiert, um die erfassten Bilder zu nutzen und herkömmliche Kameras in intelligente Kameras zu verwandeln. Die durch das Video generierte Datenmenge, kombiniert mit diesen Werkzeugen und Techniken, erhöht die Risiken einer sekundären Nutzung (unabhängig davon, ob sie mit dem ursprünglich dem System zugewiesenen Zweck zusammenhängt oder nicht) oder sogar die Risiken eines Missbrauchs. Die allgemeinen Grundsätze des GDPR (Artikel 5) sollten bei der Videoüberwachung stets sorgfältig berücksichtigt werden.

3. Videoüberwachungssysteme verändern in vielerlei Hinsicht die Art und Weise, wie Fachleute aus dem privaten und öffentlichen Sektor an privaten oder öffentlichen Orten interagieren, um die Sicherheit zu erhöhen, Publikumsanalysen zu erhalten, personalisierte Werbung zu liefern usw. Die Videoüberwachung ist durch die zunehmende Einführung intelligenter Videoanalysen sehr leistungsfähig geworden. Diese Techniken können aufdringlicher (z.B. komplexe biometrische Technologien) oder weniger aufdringlich (z.B. einfache Zählalgorithmen) sein. Anonym zu bleiben und seine Privatsphäre zu wahren, wird im Allgemeinen immer schwieriger. Die Datenschutzfragen, die in jeder Situation aufgeworfen werden, können unterschiedlich sein, ebenso wie die rechtliche Analyse bei der Verwendung der einen oder anderen dieser Technologien.

4. Neben Fragen der Privatsphäre gibt es auch Risiken im Zusammenhang mit möglichen Fehlfunktionen dieser Geräte und den durch sie verursachten Verzerrungen. Forscher berichten, dass Software, die für die Gesichtsidentifizierung, -erkennung oder -analyse verwendet wird, je nach Alter, Geschlecht und ethnischer Zugehörigkeit der zu identifizierenden Person unterschiedliche Leistungen erbringt.

---

[1] Die in dieser Stellungnahme gemachten Verweise auf "Mitgliedstaaten" sind als Verweise auf "EWR-Mitgliedstaaten" zu verstehen. Die Algorithmen würden auf der Grundlage unterschiedlicher demographischer Daten funktionieren, daher droht die Verzerrung bei der Gesichtserkennung die Vorurteile der Gesellschaft zu verstärken. Deshalb müssen die für die Datenverarbeitung Verantwortlichen auch dafür sorgen, dass die Verarbeitung biometrischer Daten aus der Videoüberwachung regelmäßig auf ihre Relevanz und die Angemessenheit der gebotenen Garantien hin überprüft wird.

5. Die Videoüberwachung ist nicht zwangsläufig eine Notwendigkeit, wenn es andere Mittel gibt, um den zugrunde

liegenden Zweck zu erreichen. Andernfalls riskieren wir eine Änderung der kulturellen Normen, die dazu führt, dass der Mangel an Privatsphäre als allgemeiner Ausgangspunkt akzeptiert wird.

6. Diese Richtlinien sollen eine Anleitung zur Anwendung der GDPR in Bezug auf die Verarbeitung personenbezogener Daten durch Videogeräte geben. Die Beispiele sind nicht erschöpfend, die allgemeine Argumentation lässt sich auf alle möglichen Anwendungsbereiche anwenden.

2 ANWENDUNGSBEREICH2

2.1 Persönliche Daten

7. Die systematische automatische Überwachung eines bestimmten Raums mit optischen oder audiovisuellen Mitteln, meist zum Schutz von Eigentum oder zum Schutz von Leben und Gesundheit des Einzelnen, ist zu einem bedeutenden Phänomen unserer Tage geworden. Diese Aktivität bewirkt die Sammlung und Speicherung von bildlichen oder audiovisuellen Informationen über alle Personen, die den überwachten Raum betreten, die anhand ihres Aussehens oder anderer spezifischer Elemente identifiziert werden können. Die Identität dieser Personen kann auf der Grundlage dieser Angaben festgestellt werden. Sie ermöglicht auch die Weiterverarbeitung von persönlichen Daten über die Anwesenheit und das Verhalten der Personen im gegebenen Raum. Das potenzielle Risiko eines Missbrauchs dieser Daten wächst in Abhängigkeit von der Dimension des überwachten Raums sowie von der Anzahl der Personen, die den Raum frequentieren. Diese Tatsache spiegelt sich in der Allgemeinen Datenschutzverordnung in Artikel 35 Absatz 3 Buchstabe c wider, der im Falle einer systematischen Überwachung eines öffentlich zugänglichen Bereichs in großem Maßstab die Durchführung einer Datenschutzfolgenabschätzung vorschreibt, sowie in Artikel 37 Absatz 1 Buchstabe b, der die Auftragsverarbeiter verpflichtet, einen Datenschutzbeauftragten zu benennen, wenn die Verarbeitung ihrer Natur nach eine regelmäßige und systematische Überwachung der betroffenen Personen erfordert.

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: Das GDPR gilt nicht für gefälschte Kameras (d.h. jede Kamera, die nicht als Kamera funktioniert und somit keine personenbezogenen Daten verarbeitet). *In einigen Mitgliedstaaten könnte sie jedoch anderen Rechtsvorschriften unterliegen.*
>
> Beispiel: Aufzeichnungen aus großer Höhe fallen nur dann in den Anwendungsbereich des GDPR, wenn die verarbeiteten Daten unter den gegebenen Umständen einer bestimmten Person zugeordnet werden können.
>
> Beispiel: Eine Videokamera ist in ein Auto integriert, um Einparkhilfe zu leisten. Wenn die Kamera so konstruiert oder eingestellt ist, dass sie keine Informationen über eine natürliche Person erfasst (z.B. Kennzeichen oder Informationen, die Passanten identifizieren könnten),

9. gilt die GDPR nicht.

2.2 Anwendung der Strafverfolgungsrichtlinie, LED (EU2016/680)

10. Insbesondere die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Feststellung oder Verfolgung von Straftaten oder der Vollstreckung strafrechtlicher Sanktionen, einschließlich des Schutzes und der Abwehr von Gefahren für die öffentliche Sicherheit, fällt unter die Richtlinie EU2016/680.

2.3 Haushaltsbefreiung

11. Gemäß Artikel 2 Absatz 2 Buchstabe c) fällt die Verarbeitung personenbezogener Daten durch eine natürliche Person im Rahmen einer rein persönlichen oder häuslichen Tätigkeit, die auch eine Online-Aktivität umfassen kann, nicht in den Anwendungsbereich des GDPR. [3]

12. Diese Bestimmung - die so genannte Haushaltsbefreiung - ist im Zusammenhang mit der Videoüberwachung eng auszulegen. Daher ist, wie der Europäische Gerichtshof festgestellt hat, der so genannte "Haushalt

---

[2] Das EDPB stellt fest, dass in den Fällen, in denen das GDPR dies zulässt, spezifische Anforderungen in der nationalen Gesetzgebung gelten könnten.

[3] Siehe auch Erwägungsgrund 18.

Die "Befreiung" muss "*so ausgelegt werden, dass sie sich nur auf Tätigkeiten bezieht, die im Rahmen des Privat- oder Familienlebens von Personen ausgeübt werden, was eindeutig nicht der Fall ist, wenn die Verarbeitung personenbezogener Daten in der Veröffentlichung im Internet besteht, so dass diese Daten einer unbestimmten Anzahl von Personen zugänglich gemacht werden*". [4] Wenn ein Videoüberwachungssystem, soweit es die ständige Aufzeichnung und Speicherung personenbezogener Daten beinhaltet und "*auch nur teilweise einen öffentlichen Raum* abdeckt *und daher aus dem privaten Umfeld der Person, die die Daten auf diese Weise verarbeitet, nach außen gerichtet ist, kann es nicht als eine Tätigkeit angesehen werden, die eine rein "persönliche oder häusliche" Tätigkeit im Sinne von Artikel 3 Absatz 2 zweiter Gedankenstrich der Richtlinie 95/46 ist*"[5].

13. Was Videogeräte betrifft, die innerhalb der Räumlichkeiten einer Privatperson betrieben werden, kann es unter die Haushaltsbefreiung fallen. Sie wird von mehreren Faktoren abhängen, die alle berücksichtigt werden müssen, um zu einer Schlussfolgerung zu gelangen. Abgesehen von den oben genannten Elementen, die in den Urteilen des EuGH festgestellt wurden, muss der Nutzer von Videoüberwachung zu Hause prüfen, ob er eine Art persönliche Beziehung zur betroffenen Person hat, ob der Umfang oder die Häufigkeit der Überwachung auf eine Art berufliche Tätigkeit seinerseits schließen lässt und welche negativen Auswirkungen die Überwachung auf die betroffenen Personen haben könnte. Das Vorhandensein eines einzigen der oben genannten Elemente lässt nicht unbedingt darauf schließen, dass die Verarbeitung außerhalb des Geltungsbereichs der Haushaltsbefreiung liegt, für diese Feststellung ist eine Gesamtbewertung erforderlich.

Beispiel: Ein Tourist nimmt sowohl über sein Mobiltelefon als auch über einen Camcorder Videos auf, um seinen Urlaub zu dokumentieren. Er zeigt das Filmmaterial Freunden und Familie, macht es aber nicht für eine unbestimmte Anzahl von Personen zugänglich. Dies würde unter die Haushaltsbefreiung fallen.

Beispiel: Eine Downhill-Mountainbikerin will ihre Abfahrt mit einer Actioncam aufnehmen. Sie reitet in einem abgelegenen Gebiet und plant, die Aufnahmen nur zu ihrer persönlichen Unterhaltung zu Hause zu verwenden. Dies würde unter die Haushaltsbefreiung fallen, auch wenn in gewissem Umfang personenbezogene Daten verarbeitet werden.

14. Beispiel: Jemand überwacht und zeichnet seinen eigenen Garten auf. Das Grundstück ist eingezäunt und nur der Kontrolleur selbst und seine Familie betreten den Garten regelmäßig. Dies würde unter die Ausnahmeregelung für Haushalte fallen, sofern die Videoüberwachung nicht auch nur teilweise auf einen öffentlichen Raum oder ein Nachbargrundstück ausgedehnt

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

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

3 RECHTMÄßIGKEIT DER VERARBEITUNG

15. Vor der Verwendung müssen die Zwecke der Verarbeitung im Einzelnen festgelegt werden (Artikel 5 (1) (b)). Die Videoüberwachung kann vielen Zwecken dienen, z.B. dem Schutz von Eigentum und anderen Vermögenswerten, dem Schutz des Lebens und der körperlichen Unversehrtheit von Personen, der Sammlung von Beweisen für zivilrechtliche Ansprüche. [6] Diese Überwachungszwecke sollten schriftlich dokumentiert werden (Artikel 5 (2)) und müssen für jede verwendete Überwachungskamera spezifiziert werden. Kameras, die von einem einzigen Controller für den gleichen Zweck verwendet werden, können gemeinsam dokumentiert werden. Darüber hinaus müssen die betroffenen Personen gemäß Artikel 13 über den Zweck bzw. die Zwecke der Verarbeitung informiert werden (*siehe Abschnitt 7, Transparenz- und Informationspflichten*). Eine Videoüberwachung, die auf dem bloßen Zweck der "Sicherheit" oder "zu Ihrer Sicherheit" beruht, ist nicht spezifisch genug (Artikel 5 (1) (b)). Sie widerspricht ferner dem Grundsatz, dass personenbezogene Daten rechtmäßig, nach Treu und Glauben und in Bezug auf die betroffene Person transparent verarbeitet werden müssen (siehe Artikel 5 Absatz 1 Buchstabe a).

16. Im Prinzip kann jeder Rechtsgrund nach Artikel 6 Absatz 1 eine Rechtsgrundlage für die Verarbeitung von Videoüberwachungsdaten bieten. So gilt beispielsweise Artikel 6 Absatz 1 Buchstabe c), wenn das nationale Recht eine Verpflichtung zur Durchführung von Videoüberwachung vorsieht. [7] In der Praxis werden jedoch am ehesten die folgenden Bestimmungen verwendet

- Artikel 6 (1) (f) (berechtigtes Interesse),
- Artikel 6 (1) (e) (Notwendigkeit der Erfüllung einer Aufgabe, die im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt ausgeführt wird).

In eher außergewöhnlichen Fällen kann Artikel 6 Absatz 1 Buchstabe a (Zustimmung) vom für die Verarbeitung Verantwortlichen als Rechtsgrundlage herangezogen werden.

3.1 Berechtigtes Interesse, Artikel 6 (1) (f)

17. Die rechtliche Bewertung von Artikel 6 (1) (f) sollte in Übereinstimmung mit Erwägungsgrund 47 auf den folgenden Kriterien beruhen.

3.1.1 Vorhandensein legitimer Interessen

18. Die Videoüberwachung ist rechtmäßig, wenn sie erforderlich ist, um den Zweck eines berechtigten Interesses zu erfüllen, das von einem für die Verarbeitung Verantwortlichen oder einem Dritten verfolgt wird, es sei denn, diese Interessen werden durch die Interessen der betroffenen Person oder die Grundrechte und -freiheiten überlagert (Artikel 6 Absatz 1 Buchstabe f)). Legitime Interessen, die von einem für die Verarbeitung Verantwortlichen oder einem Dritten verfolgt werden, können rechtliche8, wirtschaftliche oder nichtmaterielle Interessen sein. [9] Der für die Verarbeitung Verantwortliche sollte jedoch berücksichtigen, dass der für die Verarbeitung Verantwortliche, wenn die betroffene Person gemäß Artikel 21 Einwände gegen die Überwachung erhebt, nur dann mit der Videoüberwachung dieser Person fortfahren kann, wenn es sich um ein *zwingendes* berechtigtes Interesse handelt, das die Interessen, Rechte und Freiheiten der betroffenen Person oder für die Feststellung, Ausübung oder Verteidigung von Rechtsansprüchen überwiegt.

19. In einer realen und gefährlichen Situation kann der Zweck, Eigentum vor Einbruch, Diebstahl oder Vandalismus zu schützen, ein legitimes Interesse an der Videoüberwachung darstellen.

---

[6] Die Regeln für die Sammlung von Beweisen für zivilrechtliche Ansprüche sind in den Mitgliedstaaten unterschiedlich.

[7] Diese Leitlinien analysieren nicht die nationalen Gesetze, die sich von Mitgliedstaat zu Mitgliedstaat unterscheiden können, und gehen auch nicht auf Einzelheiten ein.

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

[9] siehe WP217, Arbeitsgruppe "Artikel 29".

20. Das legitime Interesse muss real existieren und muss ein aktuelles Thema sein (d.h. es darf nicht fiktiv oder spekulativ sein)[10]. Bevor mit der Überwachung begonnen wird, muss eine reale Notsituation vorliegen - wie z.B. Schäden oder schwerwiegende Zwischenfälle in der Vergangenheit. Angesichts des Prinzips der Rechenschaftspflicht wären die Kontrolleure gut beraten, relevante Vorfälle (Datum, Art und Weise, finanzieller Verlust) und die damit verbundenen Strafanzeigen zu dokumentieren. Diese dokumentierten Vorfälle können ein starker Beweis für die Existenz eines legitimen Interesses sein. Das Vorliegen eines berechtigten Interesses sowie die Notwendigkeit der Überwachung sollte in periodischen Abständen (z. B. einmal jährlich, je nach den Umständen) neu beurteilt werden.

Beispiel: Ein Ladenbesitzer möchte ein neues Geschäft eröffnen und möchte ein Videoüberwachungssystem installieren, um Vandalismus zu verhindern. Er kann durch die Vorlage von Statistiken zeigen, dass die Erwartung von Vandalismus in der nahen Nachbarschaft hoch ist. Auch Erfahrungen aus benachbarten Geschäften sind nützlich. Es ist nicht notwendig, dass ein Schaden bei dem betreffenden für die Verarbeitung Verantwortlichen entstanden sein muss. Solange Schäden in der Nachbarschaft auf eine Gefahr oder Ähnliches hindeuten und somit ein Hinweis auf ein berechtigtes Interesse sein können. Es reicht jedoch nicht aus, nationale oder allgemeine Kriminalitätsstatistiken zu

21.

22. Drohende Gefahrensituationen können ein berechtigtes Interesse darstellen, wie z. B. Banken oder Geschäfte, die wertvolle Waren verkaufen (z. B. Juweliere), oder Bereiche, die als typische Tatorte für Eigentumsdelikte bekannt sind (z. B. Tankstellen).

23. Das GDPR besagt auch klar, dass sich die öffentlichen Behörden nicht auf ihre Verarbeitung aufgrund eines berechtigten Interesses berufen können, solange sie ihre Aufgaben erfüllen, Artikel 6 (1) Satz 2.

3.1.2 Notwendigkeit der Verarbeitung

24. Personenbezogene Daten sollten angemessen und sachdienlich sein und auf das für die Zwecke, für die sie verarbeitet werden, erforderliche Maß beschränkt werden ("Datenminimierung"), siehe Artikel 5 Absatz 1 Buchstabe c). Vor der Installation eines Videoüberwachungssystems sollte der Controller immer kritisch prüfen, ob diese Maßnahme erstens geeignet ist, das gewünschte Ziel zu erreichen, und zweitens für ihre Zwecke angemessen und notwendig ist. Videoüberwachungsmaßnahmen sollten nur dann gewählt werden, wenn der Zweck der Verarbeitung vernünftigerweise nicht durch andere Mittel erfüllt werden könnte, die die Grundrechte und -freiheiten der betroffenen Person weniger stark beeinträchtigen.

25. Angesichts der Situation, dass ein Kontrolleur Eigentumsdelikte verhindern will, könnte er anstelle der Installation eines Videoüberwachungssystems auch alternative Sicherheitsmaßnahmen ergreifen, wie z.B. die Umzäunung des Geländes, die Einrichtung regelmäßiger Patrouillen des Sicherheitspersonals, den Einsatz von Pförtnerinnen und Pförtnern, die Bereitstellung besserer Beleuchtung, die Installation von Sicherheitsschlössern, manipulationssicheren Fenstern und Türen oder das Aufbringen von Anti-Graffiti-Beschichtungen oder Folien an den Wänden. Diese Maßnahmen können ebenso wirksam sein wie Videoüberwachungssysteme gegen Einbruch, Diebstahl und Vandalismus. Der Kontrolleur muss von Fall zu Fall beurteilen, ob solche Maßnahmen eine vernünftige Lösung sein können.

26. Vor dem Betrieb eines Kamerasystems ist der Controller verpflichtet, zu prüfen, wo und wann Videoüberwachungsmaßnahmen unbedingt erforderlich sind. Normalerweise wird ein Überwachungssystem, das sowohl nachts als auch außerhalb der regulären Arbeitszeiten arbeitet, den Bedürfnissen des Kontrolleurs gerecht, um Gefahren für sein Eigentum zu verhindern.

[10] siehe WP217, Arbeitsgruppe "Artikel 29", S. 24 ff. Siehe auch EuGH, Rechtssache C-708/18, S.44

27. Im Allgemeinen endet die Notwendigkeit, die Räumlichkeiten der Kontrolleure durch Videoüberwachung zu schützen, an den Grundstücksgrenzen. [11] Es gibt jedoch Fälle, in denen die Überwachung des Eigentums für einen wirksamen Schutz nicht ausreicht. In einigen Einzelfällen kann es notwendig sein, die Videoüberwachung auf die unmittelbare Umgebung des Geländes auszudehnen. In diesem Zusammenhang sollte der Controller physikalische und technische Mittel in Betracht ziehen, z.B. das Ausblenden oder Verpixeln nicht relevanter Bereiche.

Beispiel: Eine Buchhandlung will ihre Räumlichkeiten vor Vandalismus schützen. Im Allgemeinen sollten die Kameras nur die Räumlichkeiten selbst filmen, da es nicht notwendig ist, zu diesem Zweck benachbarte Räumlichkeiten oder öffentliche Bereiche in der Umgebung des Buchladens zu beobachten.

28.

29. Fragen zur Notwendigkeit der Verarbeitung stellen sich auch hinsichtlich der Art und Weise der Beweissicherung. In einigen Fällen kann es notwendig sein, Black Box-Lösungen zu verwenden, bei denen das Filmmaterial nach einer bestimmten Speicherzeit automatisch gelöscht und nur im Falle eines Zwischenfalls abgerufen wird. In anderen Situationen ist es vielleicht gar nicht notwendig, das Videomaterial aufzuzeichnen, sondern es ist besser, stattdessen eine Echtzeitüberwachung zu verwenden. Die Entscheidung zwischen Black-Box-Lösungen und Echtzeit-Überwachung sollte sich auch nach dem verfolgten Zweck richten. Wenn beispielsweise der Zweck der Videoüberwachung die Beweissicherung ist, sind Echtzeit-Methoden in der Regel nicht geeignet. Manchmal kann die Echtzeit-Überwachung auch aufdringlicher sein als das Speichern und automatische Löschen von Material nach einer begrenzten Zeitspanne (z. B. wenn jemand ständig den Monitor beobachtet, kann es aufdringlicher sein, als wenn überhaupt kein Monitor vorhanden ist und das Material direkt in einer Blackbox gespeichert wird). Der Grundsatz der Datenminimierung muss in diesem Zusammenhang betrachtet werden (Artikel 5 Absatz 1 Buchstabe c). Es sollte auch bedacht werden, dass es möglich ist, dass der Kontrolleur anstelle der Videoüberwachung Sicherheitspersonal einsetzt, das in der Lage ist, sofort zu reagieren und einzugreifen.

3.1.3 Interessenausgleich

30. Unter der Annahme, dass die Videoüberwachung zum Schutz der berechtigten Interessen eines für die Verarbeitung Verantwortlichen notwendig ist, darf ein Videoüberwachungssystem nur dann in Betrieb genommen werden, wenn die berechtigten Interessen des Verantwortlichen oder Dritter (z.B. Schutz des Eigentums oder der körperlichen Unversehrtheit) nicht durch die Interessen oder die Grundrechte und -freiheiten der betroffenen Person überlagert werden. Der für die Verarbeitung Verantwortliche muss 1) prüfen, inwieweit die Überwachung die Interessen, Grundrechte und -freiheiten von Personen beeinträchtigt und 2) ob dies zu Verletzungen oder negativen Folgen in Bezug auf die Rechte der betroffenen Person führt. In der Tat,
Der Interessenausgleich ist obligatorisch. Die Grundrechte und -freiheiten einerseits und die legitimen Interessen des Kontrolleurs andererseits müssen sorgfältig bewertet und gegeneinander abgewogen werden.

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

Beispiel: Ein privates Parkunternehmen hat wiederkehrende Probleme mit Diebstählen in den geparkten Autos dokumentiert. Der Parkplatz ist ein offener Platz, der für jedermann leicht zugänglich ist, aber mit Schildern und Straßensperren um den Platz herum deutlich gekennzeichnet ist. Die Parkplatzfirma hat ein berechtigtes Interesse (Diebstähle in den Autos der Kunden zu verhindern), den Bereich während der Tageszeit, in der sie Probleme hat, zu überwachen. Die betroffenen Personen werden in einem begrenzten Zeitrahmen überwacht, sie befinden sich nicht zu Erholungszwecken in der Gegend und es liegt auch in ihrem eigenen Interesse, dass Diebstähle verhindert werden. Das Interesse der betroffenen Personen, nicht überwacht zu werden, wird in diesem Fall durch das berechtigte Interesse des für die Verarbeitung Verantwortlichen überlagert.

Beispiel: Ein Restaurant beschließt, in den Toiletten Videokameras zu installieren, um die
31. Sauberkeit der sanitären Einrichtungen zu kontrollieren. In diesem Fall haben die Rechte der

3.1.3.1 Entscheidungen von Fall zu Fall treffen

32. Da die Interessenabwägung nach der Verordnung obligatorisch ist, muss die Entscheidung im Einzelfall getroffen werden (siehe Artikel 6 (1) (f)). Die Bezugnahme auf abstrakte Situationen oder der Vergleich ähnlicher Fälle untereinander ist unzureichend. Der für die Verarbeitung Verantwortliche hat die Risiken des Eingriffs in die Rechte der betroffenen Person zu bewerten; dabei ist das entscheidende Kriterium die Intensität des Eingriffs für die Rechte und Freiheiten des Einzelnen.

33. Die Intensität kann u.a. durch die Art der gesammelten Informationen (Informationsgehalt), den Umfang (Informationsdichte, räumliche und geographische Ausdehnung), die Anzahl der betroffenen Personen, entweder als bestimmte Anzahl oder als Anteil an der relevanten Bevölkerung, die jeweilige Situation, die tatsächlichen Interessen der Gruppe der betroffenen Personen, alternative Mittel sowie durch Art und Umfang der Datenbewertung definiert werden.

34. Wichtige ausgleichende Faktoren können die Größe des überwachten Gebiets und die Menge der überwachten Personen sein. Der Einsatz von Videoüberwachung in einem abgelegenen Gebiet (z. B. zur Beobachtung von Wildtieren oder zum Schutz kritischer Infrastruktur wie einer privaten Radioantenne) muss anders bewertet werden als die Videoüberwachung in einer Fußgängerzone oder einem Einkaufszentrum.

Beispiel: Wenn eine Strichkamera installiert ist (z. B. zum Zweck der Beweissicherung bei einem Unfall), muss sichergestellt werden, dass diese Kamera nicht ständig den Verkehr sowie Personen, die sich in der Nähe einer Straße aufhalten, aufzeichnet. Andernfalls kann das Interesse an Videoaufzeichnungen als Beweismittel im eher theoretischen Fall eines Verkehrsunfalls diesen schwerwiegenden Eingriff in die Rechte der betroffenen Personen
35. nicht rechtfertigen. [11]

3.1.3.2 Vernünftige Erwartungen der Betroffenen

36. Gemäß Erwägungsgrund 47 muss das Vorhandensein eines legitimen Interesses sorgfältig geprüft werden. Dabei sind die angemessenen Erwartungen der betroffenen Person zum Zeitpunkt und im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten einzubeziehen. Was die systematische Überwachung betrifft, so kann die Beziehung zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen erheblich variieren und sich darauf auswirken, welche angemessenen Erwartungen die betroffene Person haben könnte. Die Interpretation des Begriffs der vernünftigen Erwartungen sollte nicht nur auf den betreffenden subjektiven Erwartungen beruhen. Das entscheidende Kriterium muss vielmehr sein, ob ein objektiver Dritter vernünftigerweise erwarten und schlussfolgern kann, dass er in dieser spezifischen Situation einer Überwachung unterliegt.

37. So erwartet ein Arbeitnehmer an seinem Arbeitsplatz in den meisten Fällen wahrscheinlich nicht, dass er von seinem Arbeitgeber überwacht wird. [12] Darüber hinaus ist eine Überwachung im privaten Garten, in Wohnbereichen oder in Untersuchungs- und Behandlungsräumen nicht zu erwarten. Ebenso wenig ist eine Überwachung in Sanitär- oder Saunaanlagen zu erwarten - die Überwachung solcher Bereiche stellt einen intensiven Eingriff in die Rechte der betroffenen Person dar. Die berechtigten Erwartungen der betroffenen Personen sind, dass in diesen Gebieten keine Videoüberwachung stattfindet. Andererseits könnte der Kunde einer Bank erwarten, dass er innerhalb der Bank oder am Geldautomaten überwacht wird.

38. Die betroffenen Personen können auch erwarten, dass sie in öffentlich zugänglichen Bereichen nicht überwacht werden, insbesondere wenn diese Bereiche typischerweise für Erholung, Regeneration und Freizeitaktivitäten sowie an Orten genutzt werden, an denen sich Personen aufhalten und/oder kommunizieren, wie z.B. Sitzecken, Tische in Restaurants, Parks, Kinos und Fitnesseinrichtungen. Hier werden die Interessen oder die Rechte und Freiheiten der betroffenen Person häufig die legitimen Interessen des für die Verarbeitung Verantwortlichen überwiegen.

39. Beispiel: In Toiletten erwarten die Betroffenen, dass sie nicht überwacht werden. Videoüberwachung zum Beispiel zur Verhinderung von Unfällen ist nicht proportional.

40. Zeichen, die die betroffene Person über die Videoüberwachung informieren, sind für die Bestimmung dessen, was eine betroffene Person objektiv erwarten kann, nicht relevant. Das bedeutet, dass sich z.B. ein Ladenbesitzer nicht darauf verlassen kann, dass die Kunden *objektiv* vernünftige Erwartungen haben, dass sie überwacht werden, nur weil ein Schild die Person am Eingang über die Überwachung informiert.

3.2 Notwendigkeit der Erfüllung einer Aufgabe, die im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt ausgeführt wird, die dem für die Verarbeitung Verantwortlichen übertragen wurde, Artikel 6 (1) (e)

41. Personenbezogene Daten könnten durch Videoüberwachung nach Artikel 6 Absatz 1 Buchstabe e) verarbeitet werden, wenn dies zur Erfüllung einer Aufgabe erforderlich ist, die im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt ausgeführt wird. [13] Es kann sein, dass die Ausübung öffentlicher Gewalt eine solche Verarbeitung nicht zulässt, aber andere gesetzliche Grundlagen wie "Gesundheit und Sicherheit" zum Schutz von Besuchern und Angestellten können einen begrenzten Spielraum für die Verarbeitung bieten, wobei die GDPR-Pflichten und die Rechte der betroffenen Personen weiterhin berücksichtigt werden.

42. Die Mitgliedstaaten können spezifische nationale Rechtsvorschriften für die Videoüberwachung beibehalten oder einführen, um die Anwendung der Regeln des GDPR durch die Festlegung genauerer spezifischer Anforderungen an die Verarbeitung anzupassen, solange diese mit den im GDPR festgelegten Grundsätzen (z.B. Lagerungsbeschränkung, Verhältnismäßigkeit) in Einklang stehen.

---

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

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

3.3 Zustimmung, Artikel 6 (1) (a)

43. Die Zustimmung muss frei, spezifisch, informiert und eindeutig sein, wie in den Richtlinien zur Zustimmung beschrieben. [14]

44. Was die systematische Überwachung betrifft, so 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 auf einmal überwacht. Der für die Verarbeitung 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 zieht ihre Einwilligung zurück, wird es für den für die Verarbeitung Verantwortlichen schwierig sein, nachzuweisen, dass personenbezogene Daten nicht mehr verarbeitet werden (Artikel 7 Absatz 3).

Beispiel: Die Athleten können eine Überwachung während einzelner Übungen beantragen, um ihre Techniken und Leistungen zu analysieren. Wenn andererseits ein Sportverein die Initiative ergreift, eine ganze Mannschaft für den gleichen Zweck zu überwachen, ist die Zustimmung oft nicht gültig, da sich die einzelnen Athleten unter Druck gesetzt fühlen können, ihre Zustimmung zu erteilen, damit sich ihre Verweigerung der Zustimmung nicht nachteilig auf die Teamkollegen auswirkt.

45.

46. Wenn der für die Verarbeitung Verantwortliche sich auf die Zustimmung verlassen möchte, ist es seine Pflicht, sicherzustellen, dass jede betroffene Person, die den Bereich, der unter Videoüberwachung steht, betritt, ihre Zustimmung gegeben hat. Diese Zustimmung muss die Bedingungen von Artikel 7 erfüllen. Das Betreten eines markierten überwachten Bereichs (z.B. werden die Personen aufgefordert, durch einen bestimmten Gang oder ein bestimmtes Tor zu gehen, um einen überwachten Bereich zu betreten) stellt keine Erklärung oder eindeutige positive Maßnahme dar, die für die Zustimmung erforderlich ist, es sei denn, sie erfüllt die Kriterien von Artikel 4 und 7, wie in den Richtlinien zur Zustimmung beschrieben. [15]

47. Angesichts des Machtungleichgewichts zwischen Arbeitgebern und Arbeitnehmern sollten sich die Arbeitgeber in den meisten Fällen bei der Verarbeitung personenbezogener Daten nicht auf eine Zustimmung verlassen, da es unwahrscheinlich ist, dass sie frei gegeben wird. Die Richtlinien zur Zustimmung sollten in diesem Zusammenhang berücksichtigt werden.

48. Die Gesetze oder Tarifverträge der Mitgliedstaaten, einschließlich der "Betriebsvereinbarungen", können besondere Vorschriften für die Verarbeitung personenbezogener Daten der Arbeitnehmer im Rahmen der Beschäftigung vorsehen (siehe Artikel 88).

[14] Artikel-29-Arbeitsgruppe (Art. 29 WP) "Leitlinien für die Zustimmung gemäß Verordnung 2016/679" (WP 259 rev. 01). - vom EDPB gebilligt

[15] Arbeitsgruppe "Artikel 29" (Art. 29 WP) "Leitlinien für die Zustimmung nach der Verordnung 2016/679" (WP 259) - vom EDPB gebilligt - die berücksichtigt werden sollten.

4 WEITERGABE VON VIDEOMATERIAL AN DRITTE

49. Grundsätzlich gelten für die Weitergabe von Videoaufzeichnungen an Dritte die allgemeinen Bestimmungen des GDPR.

4.1 Offenlegung von Videomaterial an Dritte im Allgemeinen

50. Offenlegung wird in Artikel 4 (2) definiert als Übermittlung (z.B. individuelle Kommunikation), Verbreitung (z.B. Online-Veröffentlichung) oder anderweitige Verfügbarmachung. Dritte sind in Artikel 4 (10) definiert. Bei der Weitergabe an Drittstaaten oder internationale Organisationen gelten zusätzlich die besonderen Bestimmungen der Artikel 44 ff.

51. Jede Offenlegung von personenbezogenen Daten ist eine separate Art der Verarbeitung personenbezogener Daten, für die der für die Verarbeitung Verantwortliche eine Rechtsgrundlage in Artikel 6 haben muss.

52. Beispiel: Ein für die Verarbeitung Verantwortlicher, der eine Aufzeichnung in das Internet hochladen möchte, muss sich auf eine rechtliche Grundlage für diese Verarbeitung stützen, beispielsweise durch Einholung der Zustimmung der betroffenen Person gemäß Artikel 6 Absatz 1 Buchstabe a).

53. Die Übertragung von Videomaterial an Dritte zu einem anderen Zweck als dem, für den die Daten gesammelt wurden, ist nach den Bestimmungen von Artikel 6 Absatz 4 möglich.

54. Beispiel: Die Videoüberwachung einer Schranke (auf einem Parkplatz) wird zum Zweck der Schadensbeseitigung installiert. Ein Schaden entsteht und die Aufzeichnung wird einem Anwalt übergeben, um einen Fall zu verfolgen. In diesem Fall ist der Zweck der Aufzeichnung derselbe wie der der Übertragung.

Beispiel: Die Videoüberwachung einer Schranke (auf einem Parkplatz) wird zum Zweck der Schadensbeseitigung installiert. Die Aufnahme wird aus reinem Vergnügungsgründen online veröffentlicht. In diesem Fall hat sich der Zweck geändert und ist mit dem ursprünglichen Zweck nicht vereinbar. Außerdem wäre es problematisch, eine rechtliche Grundlage für diese

55. Ein Dritter, der das Material erhält, muss seine eigene rechtliche Analyse durchführen und insbesondere die Rechtsgrundlage gemäß Artikel 6 für seine Verarbeitung (z.B. Erhalt des Materials) ermitteln.

4.2 Weitergabe von Videomaterial an Strafverfolgungsbehörden

56. Die Weitergabe von Videoaufzeichnungen an die Strafverfolgungsbehörden ist ebenfalls ein unabhängiger Prozess, der eine gesonderte Rechtfertigung für den Kontrolleur erfordert.

57. Gemäß Artikel 6 Absatz 1 Buchstabe c) ist die Verarbeitung rechtmäßig, wenn sie zur Erfüllung einer rechtlichen Verpflichtung, der der für die Verarbeitung Verantwortliche unterliegt, erforderlich ist. Obwohl das geltende Polizeigesetz eine Angelegenheit ist, die unter der alleinigen Kontrolle der Mitgliedstaaten steht, gibt es höchstwahrscheinlich allgemeine Regeln, die die Übermittlung von Beweismitteln an die Strafverfolgungsbehörden in jedem Mitgliedstaat regeln. Die Verarbeitung des für die Datenübergabe verantwortlichen Mitarbeiters wird durch das GDPR geregelt. Wenn die nationale Gesetzgebung den für die Verarbeitung Verantwortlichen zur Zusammenarbeit mit den Strafverfolgungsbehörden verpflichtet (z. B. bei Ermittlungen), ist die Rechtsgrundlage für die Übergabe der Daten die rechtliche Verpflichtung nach Artikel 6 Absatz 1 Buchstabe c).

58. Die Zweckbindung in Artikel 6 Absatz 4 ist dann oft unproblematisch, da die Offenlegung ausdrücklich auf das Recht der Mitgliedstaaten zurückgeht. Eine Berücksichtigung der besonderen Voraussetzungen für eine Zweckänderung im Sinne von lit. a - e ist daher nicht erforderlich.

Beispiel: Ein Ladenbesitzer zeichnet an seinem Eingang Aufnahmen auf. Das Filmmaterial zeigt eine Person, die einer anderen Person die Brieftasche stiehlt. Die Polizei bittet den Kontrolleur, das Material zu übergeben, um bei den Ermittlungen zu helfen. In diesem Fall würde der Geschäftsinhaber die Rechtsgrundlage nach Artikel 6 Absatz 1 Buchstabe c (rechtliche Verpflichtung) in Verbindung mit dem entsprechenden nationalen Recht für die Verarbeitung der Übertragung verwenden.

59.

Beispiel: In einem Geschäft wird aus Sicherheitsgründen eine Kamera installiert. Der Ladenbesitzer glaubt, dass er etwas Verdächtiges in seinem Filmmaterial aufgenommen hat und beschließt, das Material an die Polizei zu schicken (ohne jeglichen Hinweis darauf, dass es eine laufende Untersuchung irgendeiner Art gibt). In diesem Fall muss der Ladenbesitzer beurteilen, ob die Bedingungen in den meisten Fällen nach Artikel 6 (1) (f) erfüllt sind. Dies ist in der Regel der Fall, wenn der Ladenbesitzer den begründeten Verdacht hat, dass ein Verbrechen begangen wurde.

60.

61. Die Verarbeitung der personenbezogenen Daten durch die Strafverfolgungsbehörden selbst erfolgt nicht nach der GDPR (siehe Artikel 2 Absatz 2 Buchstabe d), sondern nach der Strafverfolgungsrichtlinie (EU2016/680).

5 VERARBEITUNG BESONDERER DATENKATEGORIEN

62. Videoüberwachungssysteme sammeln in der Regel große Mengen an personenbezogenen Daten, die Daten höchstpersönlicher Art und sogar besondere Datenkategorien offenbaren können. Tatsächlich können scheinbar nicht signifikante Daten, die ursprünglich per Video gesammelt wurden, dazu verwendet werden, auf andere Informationen zu schließen, um einen anderen Zweck zu erreichen (z.B. um die Gewohnheiten einer Person abzubilden). Die Videoüberwachung wird jedoch nicht immer als Verarbeitung besonderer Kategorien personenbezogener Daten betrachtet.

> Beispiel: Videomaterial, das eine betroffene Person mit einer Brille oder einem Rollstuhl zeigt, gilt nicht per se als besondere Kategorie personenbezogener Daten.

63.

64. Wenn das Videomaterial jedoch verarbeitet wird, um spezielle Datenkategorien abzuleiten, findet Artikel 9 Anwendung.

> Beispiel: Politische Meinungen könnten z.B. aus Bildern abgeleitet werden, die identifizierbare Personen zeigen, die an einer Veranstaltung teilnehmen, an einem Streik teilnehmen usw. Dies würde unter Artikel 9 fallen.
>
> Beispiel: Ein Krankenhaus, das eine Videokamera installiert, um den Gesundheitszustand eines Patienten zu überwachen, würde als Verarbeitung besonderer Kategorien personenbezogener

65.

66. Generell sollte bei der Installation eines Videoüberwachungssystems grundsätzlich das Prinzip der Datenminimierung sorgfältig berücksichtigt werden. Daher sollte der für die Datenverarbeitung Verantwortliche auch in Fällen, in denen Artikel 9 Absatz 1 nicht anwendbar ist, immer versuchen, das Risiko der Erfassung von Filmmaterial, das andere sensible Daten (über Artikel 9 hinaus) offenbart, unabhängig vom Ziel, zu minimieren.

> Beispiel: Die Videoüberwachung, die eine Kirche erfasst, fällt nicht per se unter Artikel 9. Allerdings muss der für die Verarbeitung Verantwortliche bei der Beurteilung der Interessen der betroffenen Person eine besonders sorgfältige Bewertung gemäß Artikel 6 Absatz 1 Buchstabe f) vornehmen und dabei die Art der Daten sowie das Risiko der Erfassung anderer sensibler Daten (über Artikel 9 hinaus) berücksichtigen.

67.

68. Wenn ein Videoüberwachungssystem zur Verarbeitung besonderer Datenkategorien verwendet wird, muss der für die Verarbeitung Verantwortliche sowohl eine Ausnahme für die Verarbeitung besonderer Datenkategorien gemäß Artikel 9 (d.h. eine Ausnahme von der allgemeinen Regel, dass man keine besonderen Datenkategorien verarbeiten darf) als auch eine Rechtsgrundlage gemäß Artikel 6 festlegen.

69. So könnte beispielsweise Artikel 9 Absatz 2 Buchstabe c ("[...] *Verarbeitung ist notwendig, um die lebenswichtigen Interessen der betroffenen Person oder einer anderen natürlichen Person* [...]") - theoretisch und ausnahmsweise - angewandt werden, doch müsste der für die Verarbeitung Verantwortliche dies als absolute Notwendigkeit zur Wahrung der lebenswichtigen Interessen einer Person begründen und nachweisen, dass diese "[...] betroffene Person *physisch oder rechtlich nicht in der Lage ist, ihre Einwilligung zu geben*". Darüber hinaus darf der für die Datenverarbeitung Verantwortliche das System aus keinem anderen Grund nutzen.

70. Dabei ist es wichtig zu beachten, dass nicht jede der in Artikel 9 aufgeführten Ausnahmen geeignet ist, die Verarbeitung besonderer Datenkategorien durch Videoüberwachung zu rechtfertigen. Genauer gesagt können sich die für die Verarbeitung dieser Daten im Rahmen der Videoüberwachung Verantwortlichen nicht auf Artikel 9 Absatz 2 Buchstabe e berufen, der eine Verarbeitung erlaubt, die sich auf personenbezogene Daten bezieht, die von der betroffenen Person offenkundig öffentlich gemacht wurden. Die bloße Tatsache, dass die betroffene Person in den Erfassungsbereich der Kamera gelangt, bedeutet nicht, dass sie beabsichtigt, besondere Kategorien von sie betreffenden Daten zu veröffentlichen.

71. Darüber hinaus erfordert die Verarbeitung spezieller Datenkategorien eine erhöhte und ständige Wachsamkeit in Bezug auf bestimmte Verpflichtungen, z.B. ein hohes Maß an Sicherheit und Datenschutzfolgenabschätzung, wo dies erforderlich ist.

> Beispiel: Ein Arbeitgeber darf keine Videoüberwachungsaufnahmen, die eine Demonstration zeigen, verwenden, um Streikende zu identifizieren.

72.

5.1 Allgemeine Überlegungen bei der Verarbeitung biometrischer Daten

73. Die Verwendung biometrischer Daten und insbesondere der Gesichtserkennung bringt erhöhte Risiken für die Rechte der Betroffenen mit sich. Es ist von entscheidender Bedeutung, dass der Einsatz solcher Technologien unter gebührender Beachtung der Grundsätze der Rechtmäßigkeit, Notwendigkeit, Verhältnismäßigkeit und Datenminimierung gemäß GDPR erfolgt. Während der Einsatz dieser Technologien als besonders wirksam angesehen werden kann, sollten die für die Verarbeitung Verantwortlichen zunächst die Auswirkungen auf die Grundrechte und -freiheiten bewerten und weniger eingreifende Mittel in Betracht ziehen, um den legitimen Zweck der Verarbeitung zu erreichen.

74. Um als biometrische Daten im Sinne des GDPR zu gelten, muss die Verarbeitung von Rohdaten, wie z.B. physische, physiologische oder Verhaltensmerkmale einer natürlichen Person, eine Messung dieser Merkmale implizieren. Da biometrische Daten das Ergebnis solcher Messungen sind, stellt das GDPR in seinem Artikel fest 4.14 daß es "[...] *das Ergebnis einer spezifischen technischen Verarbeitung ist, die sich auf die physischen, physiologischen oder Verhaltensmerkmale einer natürlichen Person bezieht und die eine eindeutige Identifizierung dieser natürlichen Person ermöglicht oder bestätigt [...]".* Das Videomaterial einer Person kann jedoch für sich genommen nicht als biometrische Daten im Sinne von Artikel 9 betrachtet werden, wenn es nicht speziell technisch verarbeitet wurde, um zur Identifizierung einer Person beizutragen. [16]

75. Damit sie als Verarbeitung besonderer Kategorien personenbezogener Daten (Artikel 9) betrachtet werden kann, muss die Verarbeitung biometrischer Daten "zum Zweck der eindeutigen Identifizierung einer natürlichen Person" erfolgen.

76. Zusammenfassend müssen im Lichte von Artikel 4.14 und 9 drei Kriterien berücksichtigt werden:

- **Art der Daten :** Daten, die sich auf physische, physiologische oder Verhaltensmerkmale einer natürlichen Person beziehen,
- **Mittel und Art der Verarbeitung** : Daten, die "aus einer bestimmten technischen Verarbeitung resultieren",
- **Zweck der Verarbeitung:** Die Daten müssen zum Zweck der eindeutigen Identifizierung einer natürlichen Person verwendet werden.

77. Die Nutzung von Videoüberwachung einschließlich biometrischer Erkennungsfunktionen, die von privaten Einrichtungen für ihre eigenen Zwecke (z.B. Marketing, Statistik oder sogar Sicherheit) installiert werden, wird in den meisten Fällen die ausdrückliche Zustimmung aller betroffenen Personen erfordern (Artikel 9 Absatz 2 Buchstabe a)), doch könnte auch eine andere geeignete Ausnahme in Artikel 9 anwendbar sein.

---

[16] Erwägungsgrund 51 GDPR unterstützt diese Analyse und stellt fest, dass "[...] *Die Verarbeitung von Lichtbildern sollte nicht systematisch als Verarbeitung besonderer Kategorien personenbezogener Daten betrachtet werden, da sie nur dann unter die Definition der biometrischen Daten fällt, wenn sie mit Hilfe eines spezifischen technischen Mittels verarbeitet wird, das die eindeutige Identifizierung oder Authentifizierung einer natürlichen Person ermöglicht. […]*".

Beispiel: Um seinen Service zu verbessern, ersetzt ein privates Unternehmen die Kontrollpunkte zur Identifizierung von Passagieren innerhalb eines Flughafens (Gepäckabgabe, Einsteigen) durch Videoüberwachungssysteme, die Gesichtserkennungstechniken zur Überprüfung der Identität der Passagiere, die sich für ein solches Verfahren entschieden haben, verwenden. Da die Verarbeitung unter Artikel 9 fällt, müssen sich die Passagiere, die zuvor ihre ausdrückliche und informierte Zustimmung gegeben haben, beispielsweise an einem automatischen Terminal anmelden, um ihre Gesichtsvorlage in Verbindung mit ihrer Bordkarte und ihrer Identität zu erstellen und zu registrieren. Die Kontrollpunkte mit Gesichtserkennung müssen klar getrennt sein, z. B. muss das System innerhalb eines Portals installiert werden, damit die biometrischen Vorlagen von nicht einwilligenden Personen nicht erfasst werden. Nur die Passagiere, die zuvor ihre Zustimmung gegeben haben und mit der Anmeldung fortfahren, werden die mit dem biometrischen System ausgestattete Schilderbrücke benutzen.

Beispiel: Ein Kontrolleur verwaltet den Zugang zu seinem Gebäude mit Hilfe einer Gesichtserkennungsmethode. Personen können diesen Weg des Zugangs nur dann nutzen, wenn sie zuvor ihre explizit erteilte Zustimmung (gemäß Artikel 9 (2) (a)) gegeben haben. Um jedoch sicherzustellen, dass niemand, der nicht zuvor seine Zustimmung gegeben hat, erfasst wird, sollte die Gesichtserkennungsmethode von der betroffenen Person selbst ausgelöst

78. werden, z.B. durch Drücken eines Knopfes. Um die Rechtmäßigkeit der Verarbeitung zu

79. In dieser Art von Fällen, in denen biometrische Templates generiert werden, müssen die für die Verarbeitung Verantwortlichen sicherstellen, dass nach dem Erhalt eines Übereinstimmungs- oder Nichtübereinstimmungsergebnisses alle Zwischenvorlagen, die (mit der ausdrücklichen und informierten Zustimmung der betroffenen Person) on the fly" erstellt wurden, um mit den von den betroffenen Personen zum Zeitpunkt der Anwerbung erstellten Vorlagen verglichen zu werden, sofort und sicher gelöscht werden. Die für die Einberufung erstellten Vorlagen sollten nur für die Realisierung des Verarbeitungszwecks aufbewahrt und nicht gespeichert oder archiviert werden.

80. Wenn jedoch der Zweck der Verarbeitung beispielsweise darin besteht, eine Kategorie von Personen von einer anderen zu unterscheiden, aber nicht darin, jemanden eindeutig zu identifizieren, fällt die Verarbeitung nicht unter Artikel 9.

Beispiel: Ein Ladenbesitzer möchte seine Werbung auf der Grundlage von Geschlechts- und Altersmerkmalen des Kunden, die von einem Videoüberwachungssystem erfasst wurden, individuell gestalten. Wenn dieses System keine biometrischen Vorlagen erzeugt, um Personen eindeutig zu identifizieren, sondern nur diese physischen Merkmale erkennt, um die Person zu klassifizieren, dann würde die Verarbeitung nicht unter Artikel 9 fallen (solange

81. keine anderen Arten von speziellen Datenkategorien verarbeitet werden).

82. Artikel 9 findet jedoch Anwendung, wenn der für die Verarbeitung Verantwortliche biometrische Daten speichert (meistens durch Vorlagen, die durch die Extraktion von Schlüsselmerkmalen aus der Rohform der biometrischen Daten (z.B. Gesichtsmessungen aus einem Bild) erstellt werden), um eine Person eindeutig zu identifizieren. Wenn ein für die Verarbeitung Verantwortlicher eine betroffene Person beim Wiedereintritt in den Bereich oder beim Betreten eines anderen Bereichs entdecken möchte (z.B. um weiterhin kundenspezifische Werbung zu projizieren), dann würde der Zweck darin bestehen, eine natürliche Person eindeutig zu identifizieren, was bedeutet, dass der Vorgang von Anfang an unter Artikel 9 fällt. Dies könnte der Fall sein, wenn ein Controller generierte Vorlagen speichert, um weitere maßgeschneiderte Werbung auf mehreren Plakatwänden an verschiedenen Stellen innerhalb des Geschäfts bereitzustellen. Da das System physische Merkmale verwendet, um bestimmte Personen, die in den Bereich der Kamera zurückkommen (wie die Besucher eines Einkaufszentrums), zu erkennen und zu verfolgen, würde es eine biometrische Identifizierungsmethode darstellen, da es auf eine Erkennung durch den Einsatz spezifischer technischer Verfahren abzielt.

Beispiel: Ein Ladenbesitzer hat in seinem Geschäft ein Gesichtserkennungssystem installiert, um die Werbung auf Einzelpersonen zuzuschneiden. Der für die Datenverarbeitung Verantwortliche muss die ausdrückliche und informierte Zustimmung aller betroffenen Personen einholen, bevor er dieses biometrische System verwendet und maßgeschneiderte Werbung liefert. Das System wäre unrechtmäßig, wenn es Besucher oder Passanten erfasst, die der Erstellung ihrer biometrischen Vorlage nicht zugestimmt haben, selbst wenn ihre Vorlage innerhalb kürzester Zeit gelöscht wird. Tatsächlich stellen diese temporären Vorlagen biometrische Daten dar, die verarbeitet werden, um eine Person, die möglicherweise keine gezielte Werbung erhalten möchte, eindeutig zu identifizieren.

83.

84. Der EDPB stellt fest, dass einige biometrische Systeme in unkontrollierten Umgebungen17 installiert sind, was bedeutet, dass das System die fliegende Erfassung der Gesichter aller Personen beinhaltet, die sich im Bereich der Kamera bewegen, einschließlich der Personen, die dem biometrischen Gerät nicht zugestimmt haben, und somit biometrische Vorlagen erstellt werden. Diese Vorlagen werden mit den Vorlagen verglichen, die von den betroffenen Personen erstellt wurden, die ihre vorherige Einwilligung während eines Anwerbungsverfahrens gegeben haben (d.h. ein Benutzer eines biometrischen Geräts), damit der für die Datenverarbeitung Verantwortliche erkennen kann, ob die Person ein Benutzer eines biometrischen Geräts ist oder nicht. In diesem Fall ist das System oft so konzipiert, dass es die Personen, die es aus einer Datenbank erkennen will, von denjenigen unterscheidet, die nicht eingetragen sind. Da der Zweck darin besteht, natürliche Personen eindeutig zu identifizieren, ist eine Ausnahme nach Artikel 9 (2) GDPR nach wie vor erforderlich für jeden, der von der Kamera erfasst wird.

Beispiel: Ein Hotel nutzt die Videoüberwachung, um den Hotelmanager automatisch zu benachrichtigen, dass ein VIP eingetroffen ist, wenn das Gesicht des Gastes erkannt wird. Diese VIPs haben ihre ausdrückliche Zustimmung zur Verwendung der Gesichtserkennung gegeben, bevor sie in einer zu diesem Zweck eingerichteten Datenbank erfasst werden. Diese Systeme zur Verarbeitung biometrischer Daten wären unrechtmäßig, wenn nicht alle anderen überwachten Gäste (zur Identifizierung der VIPs) der Verarbeitung gemäß Artikel 9 Absatz 2 Buchstabe a) GDPR zugestimmt haben.

Beispiel: Ein Controller installiert ein Videoüberwachungssystem mit Gesichtserkennung am Eingang des von ihm verwalteten Konzertsaals. Der Kontrolleur muss klar getrennte Eingänge einrichten; einen mit und einen ohne biometrisches System (wo man stattdessen z.B. ein Ticket einscannt). Die mit biometrischen Geräten ausgestatteten Eingänge müssen so installiert und zugänglich gemacht werden, dass das System keine biometrischen Vorlagen

85.

86. Wenn die Zustimmung nach Artikel 9 GDPR erforderlich ist, darf der für die Datenverarbeitung Verantwortliche den Zugang zu seinen Diensten nicht von der Annahme der biometrischen Verarbeitung abhängig machen. Mit anderen Worten, insbesondere wenn die biometrische Verarbeitung zum Zweck der Authentifizierung verwendet wird, muss der für die Verarbeitung Verantwortliche eine Alternativlösung anbieten, die keine biometrische Verarbeitung beinhaltet - ohne Einschränkungen oder zusätzliche Kosten für die betroffene Person. Diese Alternativlösung ist auch für Personen erforderlich, die die Einschränkungen des biometrischen Geräts nicht erfüllen (Erfassung oder Auslesen der biometrischen Daten nicht möglich, Situation einer Behinderung, die die Nutzung erschwert, usw.), und im Vorgriff auf die Nichtverfügbarkeit des biometrischen Geräts (wie z.B. eine Fehlfunktion des Geräts) muss eine "Backup-Lösung" implementiert werden, um die Kontinuität des vorgeschlagenen Dienstes zu gewährleisten, die jedoch auf eine außergewöhnliche Nutzung beschränkt ist. In Ausnahmefällen kann es eine Situation geben, in der die Verarbeitung biometrischer Daten die Kerntätigkeit einer vertraglich vereinbarten Dienstleistung ist, z.B.

[17] Es bedeutet, dass sich das biometrische Gerät in einem öffentlich zugänglichen Raum befindet und in der Lage ist, auf jeden zu wirken, der vorbeikommt, im Gegensatz zu den biometrischen Systemen in kontrollierten Umgebungen, die nur von folgenden Personen benutzt werden können
die Zustimmung zur Teilnahme einer Person.

Museum, das eine Ausstellung zur Demonstration des Einsatzes eines Gesichtserkennungsgerätes einrichtet. In diesem Fall kann die betroffene Person die Verarbeitung biometrischer Daten nicht ablehnen, wenn sie an der Ausstellung teilnehmen möchte. In diesem Fall ist die nach Artikel 9 erforderliche Zustimmung noch immer gültig, wenn die Anforderungen in Artikel 7 erfüllt sind.

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

87. In Übereinstimmung mit dem Prinzip der Datenminimierung müssen die für die Datenverarbeitung Verantwortlichen sicherstellen, dass die aus einem digitalen Bild extrahierten Daten zur Erstellung einer Vorlage nicht übermäßig groß sind und nur die für den angegebenen Zweck erforderlichen Informationen enthalten, wodurch jede mögliche Weiterverarbeitung vermieden wird. Es sollten Maßnahmen ergriffen werden, um zu gewährleisten, dass die Vorlagen nicht über biometrische Systeme hinweg übertragen werden können.

88. Identifizierung und Authentifizierung/Verifizierung erfordern wahrscheinlich die Speicherung der Vorlage zur Verwendung bei einem späteren Vergleich. Der für die Datenverarbeitung Verantwortliche muss den am besten geeigneten Speicherort für die Daten in Betracht ziehen. In einer kontrollierten Umgebung (abgegrenzte Flure oder Kontrollpunkte) werden die Vorlagen auf einem individuellen Gerät gespeichert, das vom Benutzer unter seiner alleinigen Kontrolle gehalten wird (in einem Smartphone oder der ID-Karte) oder - wenn für bestimmte Zwecke und bei Vorliegen objektiver Bedürfnisse erforderlich - in einer zentralen Datenbank in verschlüsselter Form mit einem Schlüssel/Geheimnis ausschließlich in den Händen der Person gespeichert, um den unbefugten Zugang zu der Vorlage oder dem Speicherort zu verhindern. Wenn der für die Datenverarbeitung Verantwortliche den Zugriff auf die Vorlagen nicht vermeiden kann, muss er geeignete Maßnahmen ergreifen, um die Sicherheit der gespeicherten Daten zu gewährleisten. Dazu kann die Verschlüsselung der Vorlage mit einem kryptographischen Algorithmus gehören.

89. In jedem Fall hat der für die Verarbeitung Verantwortliche alle erforderlichen Vorkehrungen zu treffen, um die Verfügbarkeit, Integrität und Vertraulichkeit der verarbeiteten Daten zu wahren. Zu diesem Zweck ergreift der für die Verarbeitung Verantwortliche insbesondere folgende Maßnahmen: Abschottung der Daten während der Übertragung und Speicherung, Speicherung biometrischer Vorlagen und Rohdaten oder Identitätsdaten in verschiedenen Datenbanken, Verschlüsselung biometrischer Daten, insbesondere biometrischer Vorlagen, und Festlegung einer Richtlinie für die Verschlüsselung und die Schlüsselverwaltung, Integration einer organisatorischen und technischen Maßnahme zur Betrugserkennung, Zuordnung eines Integritätscodes zu den Daten (z.B. Unterschrift oder Hash) und Verbot jeglichen externen Zugriffs auf die biometrischen Daten. Solche Maßnahmen müssen sich mit dem Fortschritt der Technologien weiterentwickeln.

90. Außerdem sollten die für die Datenverarbeitung Verantwortlichen die Rohdaten (Gesichtsbilder, Sprachsignale, den Gang usw.) löschen und die Wirksamkeit dieser Löschung sicherstellen. Wenn es keine gesetzliche Grundlage mehr für die Verarbeitung gibt, müssen die Rohdaten gelöscht werden. Soweit biometrische Vorlagen von solchen Daten abgeleitet werden, kann man in der Tat davon ausgehen, dass der Aufbau von Datenbanken eine gleichwertige, wenn nicht sogar größere Bedrohung darstellen könnte (da es nicht immer einfach ist, eine biometrische Vorlage ohne das Wissen um ihre Programmierung zu lesen, während Rohdaten die Bausteine jeder Vorlage sind). Für den Fall, dass der für die Datenverarbeitung Verantwortliche solche Daten aufbewahren müsste, müssen geräuschadditive Methoden (wie z.B. Wasserzeichen) erforscht werden, die die Erstellung der Vorlage unwirksam machen würden. Der für die Verarbeitung Verantwortliche muss auch biometrische Daten und Vorlagen im Falle eines unbefugten Zugriffs auf das Lese-Vergleichsterminal oder den Speicherserver löschen und alle Daten, die am Ende der Lebensdauer des biometrischen Geräts nicht für die weitere Verarbeitung nützlich sind, löschen.

6 RECHTE DER BETROFFENEN PERSON

91. Aufgrund des Charakters der Datenverarbeitung bei der Verwendung von Videoüberwachung dienen einige Rechte der betroffenen Person nach GDPR der weiteren Klärung. Dieses Kapitel ist jedoch nicht erschöpfend, alle Rechte nach dem GDPR gelten für die Verarbeitung personenbezogener Daten durch Videoüberwachung.

6.1 Recht auf Zugang

92. Eine betroffene Person hat das Recht, vom für die Verarbeitung Verantwortlichen eine Bestätigung darüber zu erhalten, ob ihre persönlichen Daten verarbeitet werden oder nicht. Für die Videoüberwachung bedeutet dies, dass der für die Verarbeitung Verantwortliche, wenn keine Daten gespeichert oder in irgendeiner Weise übertragen werden, nach Ablauf des Echtzeit-Überwachungsmoments nur noch die Information geben könnte, dass keine personenbezogenen Daten mehr verarbeitet werden (neben den allgemeinen Informationspflichten nach Artikel 13, siehe *Abschnitt 7 - Transparenz- und Informationspflichten*). Werden die Daten jedoch zum Zeitpunkt des Antrags noch verarbeitet (d.h. werden die Daten gespeichert oder kontinuierlich auf andere Weise verarbeitet), sollte die betroffene Person Zugang und Informationen gemäß Artikel 15 erhalten.

93. Es gibt jedoch eine Reihe von Einschränkungen, die in einigen Fällen in Bezug auf das Recht auf Zugang gelten können.

- Artikel 15 (4) GDPR, beeinträchtigt die Rechte anderer

94. Da in derselben Sequenz der Videoüberwachung eine beliebige Anzahl von betroffenen Personen aufgezeichnet werden kann, würde eine Überprüfung dann eine zusätzliche Verarbeitung von personenbezogenen Daten anderer betroffener Personen verursachen. Wenn die betroffene Person eine Kopie des Materials erhalten möchte (Artikel 15 Absatz 3), könnte dies die Rechte und Freiheiten anderer betroffener Personen in dem Material beeinträchtigen. Um diesen Effekt zu verhindern, sollte der für die Verarbeitung Verantwortliche daher berücksichtigen, dass er aufgrund der aufdringlichen Natur des Videomaterials in einigen Fällen kein Videomaterial aushändigen sollte, bei dem andere betroffene Personen identifiziert werden können. Der Schutz der Rechte Dritter sollte jedoch nicht als Entschuldigung dafür benutzt werden, berechtigte Ansprüche auf Zugang durch Einzelpersonen zu verhindern; der für die Verarbeitung Verantwortliche sollte in diesen Fällen technische Maßnahmen zur Erfüllung des Zugangsantrags durchführen (z.B. Bildbearbeitung wie Maskierung oder Verschlüsselung). Die für die Verarbeitung Verantwortlichen sind jedoch nicht verpflichtet, solche technischen Maßnahmen durchzuführen, wenn sie anderweitig sicherstellen können, dass sie in der Lage sind, auf einen Antrag nach Artikel 15 innerhalb des in Artikel 12 Absatz 3 festgelegten Zeitrahmens zu reagieren.

- Artikel 11 (2) GDPR, der für die Verarbeitung Verantwortliche ist nicht in der Lage, die betroffene Person zu identifizieren

95. Wenn das Videomaterial nicht nach personenbezogenen Daten durchsuchbar ist (d.h. der für die Verarbeitung Verantwortliche müsste wahrscheinlich eine große Menge an gespeichertem Material durchsuchen, um die betreffende Person zu finden), kann der für die Verarbeitung Verantwortliche die betroffene Person möglicherweise nicht identifizieren.

96. Aus diesen Gründen sollte die betroffene Person (neben der Identifizierung, auch mit einem Ausweis oder persönlich) in ihrem Antrag an den für die Verarbeitung Verantwortlichen angeben, wann sie - innerhalb eines angemessenen Zeitrahmens im Verhältnis zur Menge der erfassten Personen - den überwachten Bereich betreten hat. Der für die Verarbeitung Verantwortliche sollte die betroffene Person vorher darüber informieren, welche Informationen benötigt werden, damit der für die Verarbeitung Verantwortliche dem Antrag nachkommen kann. Wenn der für die Verarbeitung Verantwortliche nachweisen kann, dass er nicht in der Lage ist, die betroffene Person zu identifizieren, muss er die betroffene Person, wenn möglich, entsprechend informieren. In einer solchen Situation sollte der für die Verarbeitung Verantwortliche in seiner Antwort an die betroffene Person über den genauen Bereich für die Überwachung, die Überprüfung der verwendeten Kameras usw. informieren, damit die betroffene Person in vollem Umfang versteht, welche personenbezogenen Daten von ihr möglicherweise verarbeitet wurden.

Beispiel: Wenn eine betroffene Person eine Kopie ihrer personenbezogenen Daten anfordert, die durch Videoüberwachung am Eingang eines Einkaufszentrums mit 30 000 Besuchern pro Tag verarbeitet werden, sollte die betroffene Person angeben, wann sie den überwachten Bereich innerhalb eines Zeitraums von etwa einer Stunde passiert hat. Wenn der Controller das Material noch verarbeitet, sollte eine Kopie des Videomaterials zur Verfügung gestellt werden. Wenn andere betroffene Personen in demselben Material identifiziert werden können, sollte dieser Teil des Materials anonymisiert werden (z.B. durch Verwischung der Kopie oder von Teilen davon), bevor die Kopie der betroffenen Person, die den Antrag gestellt hat, ausgehändigt wird.

Beispiel: Wenn der für die Verarbeitung Verantwortliche das gesamte Filmmaterial
97. automatisch löscht, z.B. innerhalb von 2 Tagen, kann der für die Verarbeitung Verantwortliche

- Artikel 12 GDPR, übermäßige Anträge

98. Im Falle übermäßiger oder offensichtlich unbegründeter Anträge einer betroffenen Person kann der für die Verarbeitung Verantwortliche entweder eine angemessene Gebühr gemäß Artikel 12 Absatz 5 Buchstabe a) GDPR erheben oder die Bearbeitung des Antrags ablehnen (Artikel 12 Absatz 5 Buchstabe b) GDPR). Der für die Verarbeitung Verantwortliche muss in der Lage sein, den offenkundig unbegründeten oder übertriebenen Charakter des Antrags nachzuweisen.

6.2 Recht auf Löschung und Recht auf Widerspruch

6.2.1 Recht auf Löschung (Recht, vergessen zu werden)

99. Wenn der für die Verarbeitung Verantwortliche weiterhin personenbezogene Daten über die Echtzeitüberwachung hinaus verarbeitet (z.B. Speicherung), kann die betroffene Person die Löschung der personenbezogenen Daten gemäß Artikel 17 GDPR beantragen.

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

- *für die Zustimmung*, wenn die Zustimmung zurückgezogen wird (und es keine andere rechtliche Grundlage für die Verarbeitung gibt)
- für ein *berechtigtes Interesse*:
    - wenn die betroffene Person das Widerspruchsrecht ausübt (siehe *Abschnitt 6.2.2*) und keine zwingenden legitimen Gründe für die Verarbeitung vorliegen, oder
    - im Falle von Direktmarketing (einschließlich Profiling), wenn die betroffene Person der Verarbeitung widerspricht.

101. Wenn der für die Verarbeitung Verantwortliche das Videomaterial öffentlich gemacht hat (z.B. durch Ausstrahlung oder Online-Streaming), müssen angemessene Schritte unternommen werden, um andere für die Verarbeitung Verantwortliche (die jetzt die betreffenden personenbezogenen Daten verarbeiten) gemäß Artikel 17 Absatz 2 GDPR über den Antrag zu informieren. Die angemessenen Schritte sollten technische Maßnahmen umfassen, wobei die verfügbare Technologie und die Kosten der Umsetzung zu berücksichtigen sind. Soweit möglich, sollte der für die Verarbeitung Verantwortliche gemäß Artikel 19 GDPR - nach der Löschung der persönlichen Daten - jeden benachrichtigen, dem die persönlichen Daten zuvor mitgeteilt wurden.

102. Neben der Verpflichtung des für die Verarbeitung Verantwortlichen, personenbezogene Daten auf Antrag der betroffenen Person zu löschen, ist der für die Verarbeitung Verantwortliche nach den allgemeinen Grundsätzen des GDPR verpflichtet, die gespeicherten personenbezogenen Daten zu begrenzen (siehe *Abschnitt 8)*.

103. Bei der Videoüberwachung ist zu beachten, dass z.B. durch Unschärfen des Bildes ohne rückwirkende Möglichkeit der Wiederherstellung der persönlichen Daten, die das Bild zuvor enthielt, die persönlichen Daten gemäß GDPR als gelöscht gelten.

> Beispiel: Ein Lebensmittelladen hat Probleme mit Vandalismus, insbesondere im Außenbereich, und setzt daher Videoüberwachung vor dem Eingang in direkter Verbindung mit den Wänden ein. Ein Passant bittet darum, dass seine persönlichen Daten von diesem Moment an gelöscht werden. Der für die Verarbeitung Verantwortliche ist verpflichtet, auf das Ersuchen unverzüglich, spätestens jedoch innerhalb eines Monats zu antworten. Da das fragliche Filmmaterial nicht mehr dem Zweck entspricht, für den es ursprünglich gespeichert wurde (in der Zeit, in der die betroffene Person vorbeikam, ist kein Vandalismus aufgetreten), besteht zum Zeitpunkt der Anfrage kein berechtigtes Interesse an der Speicherung der Daten, das die Interessen der betroffenen Personen überwiegen würde. Der für die Verarbeitung

104.

6.2.2 Recht auf Einspruch

105. Bei der Videoüberwachung aufgrund eines *berechtigten Interesses* (Artikel 6 Absatz 1 Buchstabe f) GDPR) oder aufgrund der Notwendigkeit bei der Wahrnehmung einer Aufgabe im *öffentlichen Interesse* (Artikel 6 Absatz 1 Buchstabe e) GDPR) hat die betroffene Person jederzeit das Recht, aus Gründen, die mit ihrer besonderen Situation zusammenhängen, der Verarbeitung gemäß Artikel 21 GDPR zu widersprechen. Sofern der für die Verarbeitung Verantwortliche keine zwingenden legitimen Gründe nachweist, die die Rechte und Interessen der betroffenen Person überlagern, muss die Verarbeitung der Daten der Person, die Widerspruch eingelegt hat, dann eingestellt werden. Der für die Verarbeitung Verantwortliche sollte verpflichtet sein, auf Anfragen der betroffenen Person ohne unangemessene Verzögerung und spätestens innerhalb eines Monats zu antworten.

106. Im Zusammenhang mit der Videoüberwachung könnte dieser Einwand entweder beim Betreten, während der Zeit im überwachten Bereich oder nach dem Verlassen des überwachten Bereichs erhoben werden. In der Praxis bedeutet dies, dass die Überwachung eines Bereichs, in dem natürliche Personen identifiziert werden könnten, nur dann rechtmäßig ist, wenn entweder

(1) der Kontrolleur in der Lage ist, die Verarbeitung personenbezogener Daten durch die Kamera sofort zu unterbinden, wenn er dazu aufgefordert wird, oder

(2) der überwachte Bereich so detailliert eingeschränkt ist, dass der für die Verarbeitung Verantwortliche die Zustimmung der betroffenen Person vor dem Betreten des Bereichs sicherstellen kann und es sich nicht um einen Bereich handelt, zu dem die betroffene Person als Bürger berechtigt ist.

107. Diese Richtlinien zielen nicht darauf ab, zu bestimmen, was als *zwingendes* legitimes Interesse (Artikel 21 GDPR) angesehen wird.

108. Bei der Nutzung der Videoüberwachung für Direktmarketingzwecke hat die betroffene Person das Recht, der Verarbeitung nach eigenem Ermessen zu widersprechen, da das Widerspruchsrecht in diesem Zusammenhang absolut ist (Artikel 21
(2) und (3) GDPR).

Beispiel: Ein Unternehmen hat Schwierigkeiten mit Sicherheitsverletzungen an seinem öffentlichen Eingang und setzt die Videoüberwachung aus berechtigtem Interesse ein, um diejenigen zu erwischen, die unrechtmäßig eindringen. Ein Besucher widerspricht der Verarbeitung seiner Daten durch das Videoüberwachungssystem aus Gründen, die sich auf seine besondere Situation beziehen. Das Unternehmen lehnt die Anfrage jedoch in diesem Fall mit der Erklärung ab, dass das gespeicherte Filmmaterial aufgrund einer laufenden internen Untersuchung benötigt wird und somit zwingende legitime Gründe für die weitere Verarbeitung der persönlichen Daten vorliegen.

109.

7 TRANSPARENZ- UND INFORMATIONSPFLICHTEN[18]

110. Es ist seit langem im europäischen Datenschutzrecht verankert, dass sich die Betroffenen der Tatsache bewusst sein sollten, dass eine Videoüberwachung in Betrieb ist. Sie sollten detailliert über die überwachten Orte informiert werden. [19] Nach der GDPR sind die allgemeinen Transparenz- und Informationspflichten in Artikel 12 GDPR und folgende festgelegt. Weitere Einzelheiten sind in den "Leitlinien der Artikel-29-Arbeitsgruppe zur Transparenz gemäß Verordnung 2016/679 (WP260)" enthalten, die am 25. Mai 2018 vom EDPB gebilligt wurden. In Übereinstimmung mit WP260 par. 26 ist es Artikel 13 GDPR, der anwendbar ist, wenn personenbezogene Daten "[...] von einer betroffenen Person durch Beobachtung (z.B. unter Verwendung von automatischen Datenerfassungsgeräten oder Datenerfassungssoftware wie Kameras [...]" erhoben werden.

111. In Anbetracht des Umfangs der Informationen, die der betroffenen Person zur Verfügung gestellt werden müssen, können die für die Verarbeitung Verantwortlichen einen mehrschichtigen Ansatz verfolgen, wenn sie sich für eine Kombination von Methoden entscheiden, um die Transparenz zu gewährleisten (WP260, Abs. 35; WP89, Abs. 22). Bei der Videoüberwachung sollten die wichtigsten Informationen auf dem Warnschild selbst angezeigt werden (erste Ebene), während die weiteren obligatorischen Angaben auf andere Weise gemacht werden können (zweite Ebene).

7.1 Informationen der ersten Schicht (Warnzeichen)

112. Die erste Schicht betrifft die primäre Art und Weise, in der der für die Verarbeitung Verantwortliche zum ersten Mal mit der betroffenen Person in Kontakt tritt. In dieser Phase können die Kontrolleure ein Warnschild mit den entsprechenden Informationen verwenden. Die angezeigten Informationen können in Kombination mit einem Symbol bereitgestellt werden, um auf leicht sichtbare, verständliche und klar lesbare Weise einen aussagekräftigen Überblick über die beabsichtigte Verarbeitung zu geben (Artikel 12
(7) BIPR). Das Format der Informationen sollte an den jeweiligen Standort angepasst werden (WP89 Abs. 22).

7.1.1 Positionierung des Warnzeichens

113. Die Informationen sollten so positioniert werden, dass die betroffene Person die Umstände der Überwachung leicht erkennen kann, bevor sie den überwachten Bereich betritt (etwa auf Augenhöhe). Es ist nicht notwendig, die Position der Kamera zu verraten, solange kein Zweifel darüber besteht, welche Bereiche überwacht werden und der Kontext der Überwachung eindeutig geklärt ist (WP 89, Abs. 22). Die betroffene Person muss in der Lage sein, abzuschätzen, welcher Bereich von einer Kamera erfasst wird, so dass sie sich der Überwachung entziehen oder ihr Verhalten gegebenenfalls anpassen kann.

7.1.2 Inhalt der ersten Schicht

114. Die Informationen der ersten Schicht (Warnzeichen) sollten im Allgemeinen die wichtigsten Informationen vermitteln, z.B. die Einzelheiten über die Zwecke der Verarbeitung, die Identität des für die Verarbeitung Verantwortlichen und das Bestehen der Rechte der betroffenen Person, zusammen mit Informationen über die größten Auswirkungen der Verarbeitung. [20] Dazu können beispielsweise die vom für die Verarbeitung Verantwortlichen (oder von einem Dritten) verfolgten legitimen Interessen und die Kontaktdaten des Datenschutzbeauftragten (falls zutreffend) gehören. Sie muss sich auch auf die detailliertere zweite Informationsebene beziehen und darauf, wo und wie sie zu finden ist.

115. Darüber hinaus sollte das Zeichen auch alle Informationen enthalten, die die betroffene Person überraschen könnten (WP260, Abs. 38). Das können zum Beispiel Übertragungen an Dritte sein, insbesondere wenn sie sich

---

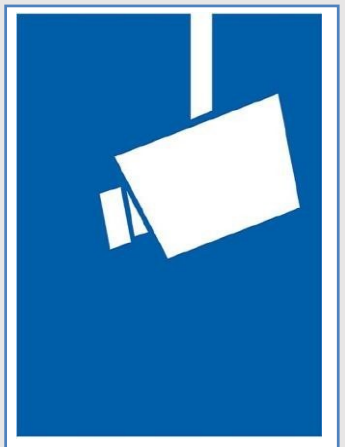
[18] Es könnten besondere Anforderungen in der nationalen Gesetzgebung gelten.

[19] Siehe WP859, Stellungnahme 4/2004 zur Verarbeitung personenbezogener Daten durch Videoüberwachung durch die Artikel-29-Datenschutzgruppe).

[20] Siehe WP260, par. 38.

außerhalb der EU, und die Aufbewahrungszeit. Wenn diese Informationen nicht angegeben werden, sollte die betroffene Person darauf vertrauen können, dass es sich ausschließlich um eine Live-Überwachung (ohne jegliche Datenaufzeichnung oder Übertragung an Dritte) handelt.

Beispiel (unverbindlicher Vorschlag):



Videoüberwachung

Weitere Informationen sind verfügbar:
- über Mitteilung
- an unserer Rezeption/ Kundeninformation/ Register
- über das Internet (URL)...

Identität des Controllers und ggf. des Vertreters des Controllers: Kontaktdaten, einschließlich der des Datenschutzbeauftragten (falls zutreffend):

Informationen über die Verarbeitung, die sich am stärksten auf die betroffene Person auswirkt (z.B. Aufbewahrungsfrist oder Live-Überwachung, Veröffentlichung oder Übertragung von Videomaterial an Dritte):

Zweck(e) der Videoüberwachung:

Rechte der betroffenen Personen: Als betroffene Person haben Sie mehrere Rechte, insbesondere das Recht, von dem für die Verarbeitung Verantwortlichen Zugang zu Ihren persönlichen Daten oder deren Löschung zu verlangen.

Einzelheiten zu dieser Videoüberwachung einschließlich Ihrer Rechte finden Sie in den vollständigen Informationen, die der Controller über die links dargestellten Optionen zur

116.

7.2 Informationen der zweiten Schicht

117. Die Informationen der zweiten Ebene müssen ebenfalls an einem für die betroffene Person leicht zugänglichen Ort zur Verfügung gestellt werden, z.B. als vollständiges Informationsblatt, das an einem zentralen Ort (z.B. Informationsschalter, Rezeption oder Kasse) erhältlich ist oder auf einem leicht zugänglichen Plakat angebracht wird. Wie oben erwähnt, muss das Warnzeichen der ersten Schicht eindeutig auf die Informationen der zweiten Schicht verweisen. Darüber hinaus ist es am besten, wenn die Informationen der ersten Schicht auf eine digitale Quelle (z.B. QR-Code oder eine Website-Adresse) der zweiten Schicht verweisen. Die Informationen sollten jedoch auch leicht nicht-digital verfügbar sein. Es sollte möglich sein, auf die Informationen der zweiten Ebene zuzugreifen, ohne den erfassten Bereich zu betreten, insbesondere wenn die Informationen digital zur Verfügung gestellt werden (dies kann z.B. durch einen Link erreicht werden). Ein anderes geeignetes Mittel könnte eine Telefonnummer sein, die angerufen werden kann. Wie auch immer die Informationen bereitgestellt werden, sie müssen alles enthalten, was nach Artikel 13 GDPR obligatorisch ist.

118. Zusätzlich zu diesen Möglichkeiten und auch um sie effektiver zu machen, fördert das EDPB den Einsatz technologischer Mittel zur Information der betroffenen Personen. Dies kann zum Beispiel die Geolokalisierung von Kameras und die Aufnahme von Informationen in Kartierungsanwendungen oder Websites umfassen, so dass der Einzelne einerseits die Videoquellen im Zusammenhang mit der Ausübung seiner Rechte leicht identifizieren und spezifizieren und andererseits detailliertere Informationen über den Verarbeitungsvorgang erhalten kann.

Beispiel: Ein Ladenbesitzer überwacht seinen Laden. Um Artikel 13 zu erfüllen, reicht es aus, an einer gut sichtbaren Stelle am Eingang seines Geschäfts ein Warnschild anzubringen, das die Informationen der ersten Schicht enthält. Darüber hinaus muss er an der Kasse oder an
119. einer anderen zentralen und leicht zugänglichen Stelle in seinem Geschäft ein Informationsblatt mit den Informationen der zweiten Ebene vorlegen.

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 (1) (c) und (e) GDPR). In einigen Mitgliedstaaten gibt es möglicherweise besondere Bestimmungen für die Aufbewahrungszeiträume in Bezug auf die Videoüberwachung gemäß Artikel 6 (2) GDPR.

121. Ob die persönlichen Daten zur Speicherung notwendig sind oder nicht, sollte innerhalb eines engen Zeitrahmens kontrolliert werden. Im Allgemeinen sind legitime Zwecke der Videoüberwachung häufig der Schutz von Eigentum oder die Beweissicherung. In der Regel können aufgetretene Schäden innerhalb von ein oder zwei Tagen erkannt werden. Um den Nachweis der Einhaltung des Datenschutzrahmens zu erleichtern, liegt es im Interesse des für die Verarbeitung Verantwortlichen, im Vorfeld organisatorische Vorkehrungen zu treffen (z. B. gegebenenfalls einen Vertreter für die Vorführung und Sicherung von Videomaterial zu benennen). unter Berücksichtigung der Grundsätze des Artikels 5 Absatz 1 Buchstabe c) und
(e) GDPR, d.h. Datenminimierung und Speicherbegrenzung, sollten die personenbezogenen Daten in den meisten Fällen (z.B. zum Zwecke der Aufdeckung von Vandalismus) nach einigen Tagen, idealerweise automatisch, gelöscht werden. Je länger die festgelegte Aufbewahrungsfrist (insbesondere wenn sie über 72 Stunden hinausgeht), desto mehr muss für die Legitimität des Zwecks und die Notwendigkeit der Aufbewahrung argumentiert werden. Wenn der für die Verarbeitung Verantwortliche die Videoüberwachung nicht nur zur Überwachung seiner Räumlichkeiten nutzt, sondern auch beabsichtigt, die Daten zu speichern, muss er sicherstellen, dass die Speicherung tatsächlich notwendig ist, um den Zweck zu erreichen. Wenn dies der Fall ist, muss die Aufbewahrungsdauer klar definiert und für jeden einzelnen Zweck individuell festgelegt werden. Es liegt in der Verantwortung des für die Verarbeitung Verantwortlichen, die Aufbewahrungsfrist in Übereinstimmung mit den Grundsätzen der Notwendigkeit und Verhältnismäßigkeit festzulegen und die Einhaltung der Bestimmungen der GDPR nachzuweisen.

122. Beispiel: Ein Besitzer eines kleinen Geschäfts würde normalerweise jeden Vandalismus noch am selben Tag zur Kenntnis nehmen. Folglich ist eine regelmäßige Lagerzeit von 24 Stunden ausreichend. Geschlossene Wochenenden oder längere Feiertage können jedoch Gründe für eine längere Lagerdauer sein. Wenn ein Schaden festgestellt wird, muss er das Videomaterial unter Umständen auch länger aufbewahren, um rechtliche Schritte gegen den Täter einleiten zu können.

9 TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

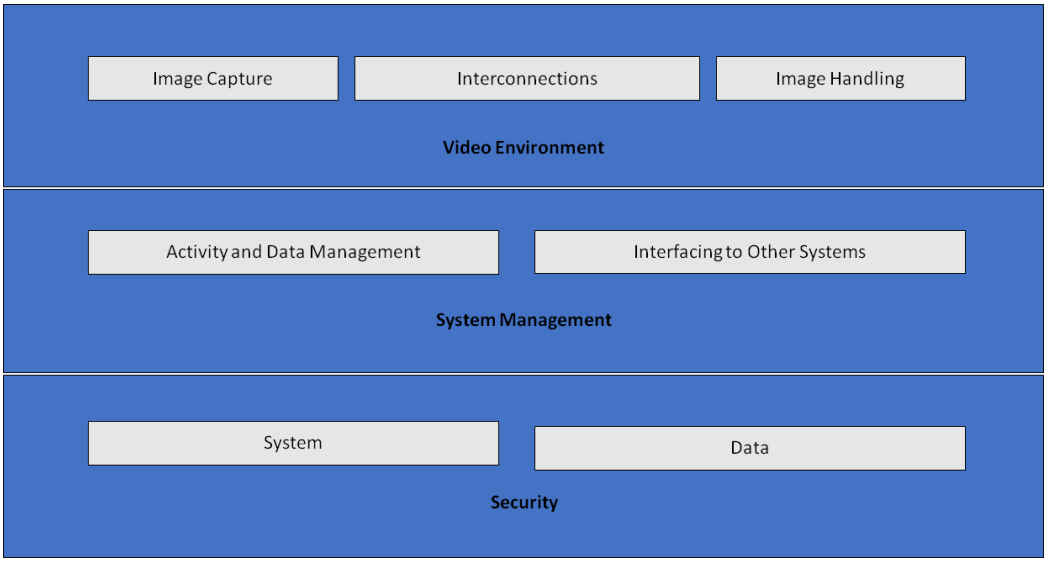
123. Wie in Artikel 32 (1) GDPR festgelegt, muss die Verarbeitung personenbezogener Daten bei der Videoüberwachung nicht nur rechtlich zulässig sein, sondern die für die Verarbeitung Verantwortlichen und Verarbeiter müssen sie auch angemessen sichern. Die ergriffenen **organisatorischen und technischen Maßnahmen** müssen **in einem angemessenen Verhältnis zu den Risiken stehen, die sich** aus der zufälligen oder unrechtmäßigen Zerstörung, dem Verlust, der Änderung, der unbefugten Weitergabe oder dem unberechtigten Zugriff auf Videoüberwachungsdaten für die **Rechte und Freiheiten natürlicher Personen** ergeben. Gemäß Artikel 24 und 25 GDPR müssen die für die Verarbeitung Verantwortlichen technische und organisatorische Maßnahmen ergreifen, um auch alle Datenschutzgrundsätze während der Verarbeitung zu gewährleisten und Mittel zur Ausübung der Rechte der betroffenen Personen gemäß Artikel 15-22 GDPR zu schaffen. Die für die Datenverarbeitung Verantwortlichen sollten einen internen Rahmen und Richtlinien verabschieden, die diese Umsetzung sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der Verarbeitung selbst gewährleisten, einschließlich der Durchführung von Datenschutzfolgenabschätzungen, wenn dies erforderlich ist.

9.1 Übersicht über das Videoüberwachungssystem

124. Ein Videoüberwachungssystem (VSS)[21] besteht aus analogen und digitalen Geräten sowie aus Software, um Bilder einer Szene zu erfassen, zu bearbeiten und einem Bediener anzuzeigen. Seine Komponenten sind in die folgenden Kategorien eingeteilt:

- Videoumgebung: Bilderfassung, Verbindungen und Bildhandhabung:
    - Der Zweck der Bilderfassung ist die Erzeugung eines Bildes der realen Welt in einem solchen Format, dass es vom Rest des Systems verwendet werden kann,
    - Verbindungen beschreiben die gesamte Übertragung von Daten innerhalb der Videoumgebung, d.h. Verbindungen und Kommunikationen. Beispiele für Verbindungen sind Kabel, digitale Netzwerke und drahtlose Übertragungen. Kommunikation beschreibt alle Video- und Steuerdatensignale, die digital oder analog sein können,
    - Die Bildbearbeitung umfasst die Analyse, Speicherung und Präsentation eines Bildes oder einer Bildsequenz.
- Aus Sicht der Systemverwaltung hat ein VSS folgende logische Funktionen:
    - Datenmanagement und Aktivitätsmanagement, das die Handhabung von Bedienerbefehlen und vom System generierten Aktivitäten (Alarmprozeduren, Alarmierung der Bediener) umfasst,
    - Die Schnittstellen zu anderen Systemen können die Verbindung zu anderen Sicherheitssystemen (Zugangskontrolle, Feueralarm) und Nicht-Sicherheitssystemen (Gebäudeverwaltungssysteme, automatische Kennzeichenerkennung) umfassen.
- Die Sicherheit von VSS besteht aus der Vertraulichkeit, Integrität und Verfügbarkeit von Systemen und Daten:
    - Die Systemsicherheit umfasst die physische Sicherheit aller Systemkomponenten und die Kontrolle des Zugriffs auf den VSS,
    - Datensicherheit umfasst die Verhinderung von Datenverlust oder -manipulation.

[21] GDPR gibt keine Definition dafür, eine technische Beschreibung findet sich z.B. in EN 62676-1- 1:2014 Videoüberwachungssysteme für den Einsatz in Sicherheitsanwendungen - Teil 1-1: Anforderungen an Videosysteme.



125.

Abbildung 1: Videoüberwachungssystem

9.2 Datenschutz durch Design und Standard

126. Wie in Artikel 25 GDPR festgelegt, müssen die für die Verarbeitung Verantwortlichen geeignete technische und organisatorische Datenschutzmaßnahmen durchführen, sobald sie eine Videoüberwachung planen - bevor sie mit der Sammlung und Verarbeitung von Videomaterial beginnen. Diese Prinzipien betonen die Notwendigkeit eingebauter Technologien zur Verbesserung der Privatsphäre, Standardeinstellungen, die die Datenverarbeitung minimieren, und die Bereitstellung der notwendigen Werkzeuge, die den höchstmöglichen Schutz persönlicher Daten ermöglichen22.

127. Die für die Verarbeitung Verantwortlichen sollten den Datenschutz und den Schutz der Privatsphäre nicht nur in die Designspezifikationen der Technologie, sondern auch in die organisatorischen Praktiken einbauen. Wenn es um organisatorische Praktiken geht, sollte der Kontrolleur einen geeigneten Verwaltungsrahmen annehmen, Richtlinien und Verfahren im Zusammenhang mit der Videoüberwachung festlegen und durchsetzen. Aus technischer Sicht sollten die Systemspezifikation und das Systemdesign Anforderungen an die Verarbeitung personenbezogener Daten in Übereinstimmung mit den in Artikel 5 GDPR genannten Grundsätzen (Rechtmäßigkeit der Verarbeitung, Zweck und Datenbeschränkung, Datenminimierung im Sinne von Artikel 25 (2) GDPR, Integrität und Vertraulichkeit, Verantwortlichkeit usw.) enthalten. Falls ein Controller plant, ein kommerzielles Videoüberwachungssystem zu erwerben, muss er diese Anforderungen in die Kaufspezifikation aufnehmen. Der für die Verarbeitung Verantwortliche muss die Einhaltung dieser Anforderungen sicherstellen, indem er sie auf alle Komponenten des Systems und auf alle von ihm verarbeiteten Daten während ihres gesamten Lebenszyklus anwendet.

9.3 Konkrete Beispiele für relevante Maßnahmen

128. Die meisten Maßnahmen, die zur Sicherung der Videoüberwachung eingesetzt werden können, insbesondere wenn digitale Geräte und Software verwendet werden, werden sich nicht von denen unterscheiden, die in anderen IT-Systemen verwendet werden. Unabhängig von der gewählten Lösung muss der Controller jedoch alle Komponenten eines Videoüberwachungssystems und die Daten in allen Phasen angemessen schützen, d.h. während der Speicherung (Daten in Ruhe), der Übertragung (Daten im Transit) und

[22] WP 168, Stellungnahme zur "Zukunft des Datenschutzes", gemeinsamer Beitrag der Datenschutzgruppe "Artikel 29" und der Gruppe "Polizei und Justiz" zur Konsultation der Europäischen Kommission über den Rechtsrahmen für das Grundrecht auf den Schutz personenbezogener Daten (angenommen am 01. Dezember 2009).

Verarbeitung (verwendete Daten). Dazu ist es notwendig, dass für die Verarbeitung Verantwortliche und Verarbeiter organisatorische und technische Maßnahmen kombinieren.

129. Bei der Auswahl technischer Lösungen sollte der für die Verarbeitung Verantwortliche datenschutzfreundliche Technologien auch deshalb in Betracht ziehen, weil sie die Sicherheit erhöhen. Beispiele für solche Technologien sind Systeme, die bei der Bereitstellung von Videomaterial an die betroffenen Personen das Ausblenden oder Verschlüsseln von Bereichen ermöglichen, die für die Überwachung nicht relevant sind, oder das Herausschneiden von Bildern Dritter. [23] Andererseits sollten die gewählten Lösungen keine Funktionen bieten, die nicht notwendig sind (z.B. unbegrenzte Bewegung der Kameras, Zoom-Fähigkeit, Funkübertragung, Analyse und Audio-Aufnahmen). Die vorgesehenen, aber nicht notwendigen Funktionen müssen deaktiviert werden.

130. Zu diesem Thema gibt es eine Menge Literatur, darunter internationale Normen und technische Spezifikationen zur physischen Sicherheit von Multimediasystemen24 und zur Sicherheit allgemeiner IT-Systeme25. Daher bietet dieser Abschnitt nur einen hochrangigen Überblick über dieses Thema.

9.3.1 Organisatorische Maßnahmen

131. Abgesehen von einer möglicherweise erforderlichen DPIA (siehe *Abschnitt 10*) sollten die Kontrolleure bei der Erstellung ihrer eigenen Videoüberwachungsrichtlinien und -verfahren die folgenden Themen berücksichtigen:

- Wer für die Verwaltung und den Betrieb des Videoüberwachungssystems verantwortlich ist.
- Zweck und Umfang des Videoüberwachungsprojekts.
- Angemessene und verbotene Nutzung (wo und wann Videoüberwachung erlaubt ist und wo und wann nicht; z.B. Verwendung von versteckten Kameras und Audio zusätzlich zur Videoaufzeichnung) [26].
- Transparenzmaßnahmen gemäß *Abschnitt 7 (Transparenz- und Informationspflichten).*
- Wie und für welche Dauer Video aufgezeichnet wird, einschließlich der Archivierung von Videoaufzeichnungen im Zusammenhang mit Sicherheitsvorfällen.
- Wer und wann muss eine entsprechende Ausbildung absolvieren.
- Wer hat Zugang zu Videoaufzeichnungen und für welche Zwecke.
- Betriebsverfahren (z.B. von wem und von wo aus die Videoüberwachung überwacht wird, was im Falle einer Datenverletzung zu tun ist).
- Welche Verfahren externe Parteien befolgen müssen, um Videoaufzeichnungen zu beantragen, und welche Verfahren zur Ablehnung oder Bewilligung solcher Anträge es gibt.
- Verfahren für die Beschaffung, Installation und Wartung von VSS.
- Vorfallmanagement und Wiederherstellungsverfahren.

9.3.2 Technische Maßnahmen

132. **Unter Systemsicherheit** versteht man die **physische Sicherheit** aller Systemkomponenten und die Systemintegrität, d.h. den **Schutz vor und die Widerstandsfähigkeit gegen absichtliche und unbeabsichtigte Eingriffe in den normalen Betrieb** und die **Zugangskontrolle**. Datensicherheit bedeutet **Vertraulichkeit** (die Daten sind nur denjenigen zugänglich, denen der Zugang gewährt wird), **Integrität** (Schutz vor Datenverlust oder Manipulation) und **Verfügbarkeit** (auf die Daten kann zugegriffen werden, wenn sie benötigt werden).

---

[23] Der Einsatz solcher Technologien kann in einigen Fällen sogar zwingend vorgeschrieben sein, um Artikel 5 (1) (c) zu erfüllen. In jedem Fall können sie als Best-Practice-Beispiele dienen.

[24] IEC TS 62045 - Multimediale Sicherheit - Richtlinie für den Schutz der Privatsphäre von Geräten und Systemen im und außerhalb des Gebrauchs.

[25] ISO/IEC 27000 - Reihe Informationssicherheits-Managementsysteme.

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

133. **Die physische Sicherheit** ist ein wichtiger Teil des Datenschutzes und die erste Verteidigungslinie, denn sie schützt die VSS-Ausrüstung vor Diebstahl, Vandalismus, Naturkatastrophen, von Menschen verursachten Katastrophen und versehentlichen Schäden (z.B. durch elektrische Überspannungen, extreme Temperaturen und verschütteten Kaffee). Im Falle eines analog basierten Systems spielt die physische Sicherheit die Hauptrolle bei ihrem Schutz.

134. **Die System- und Datensicherheit, d.h.** der Schutz vor absichtlichen und unabsichtlichen Eingriffen in den normalen Betrieb, kann eingeschlossen sein:

- Schutz der gesamten VSS-Infrastruktur (einschließlich der entfernten Kameras, der Verkabelung und der Stromversorgung) vor physischer Manipulation und Diebstahl.
- Schutz der Filmmaterialübertragung mit abhörsicheren Kommunikationskanälen
- Datenverschlüsselung.
- Einsatz von Hardware- und Software-basierten Lösungen wie Firewalls, Virenschutz oder Intrusion Detection Systeme gegen Cyber-Angriffe.
- Erkennung von Fehlern von Komponenten, Software und Verbindungen.
- Mittel zur Wiederherstellung der Verfügbarkeit und des Zugriffs auf das System im Falle eines physischen oder technischen Zwischenfalls.

135. **Die Zugriffskontrolle** stellt sicher, dass nur autorisierte Personen auf das System und die Daten zugreifen können, während andere daran gehindert werden. Zu den Maßnahmen, die die physische und logische Zugangskontrolle unterstützen, gehören

- Sicherstellen, dass alle Räumlichkeiten, in denen eine Überwachung durch Videoüberwachung erfolgt und in denen Videomaterial aufbewahrt wird, gegen den unbeaufsichtigten Zugriff Dritter gesichert sind.
- Monitore so zu positionieren (insbesondere wenn sie sich in offenen Bereichen wie einem Empfang befinden), dass nur autorisierte Bediener sie sehen können.
- Es werden Verfahren für die Gewährung, Änderung und den Widerruf des physischen und logischen Zugangs definiert und durchgesetzt.
- Methoden und Mittel zur Benutzerauthentifizierung und -autorisierung, einschließlich z.B. der Länge der Passwörter und der Änderungshäufigkeit, sind implementiert.
- Vom Benutzer ausgeführte Aktionen (sowohl am System als auch an den Daten) werden aufgezeichnet und regelmäßig überprüft.
- Die Überwachung und Erkennung von Zugangsfehlern erfolgt kontinuierlich und identifizierte Schwachstellen werden so schnell wie möglich behoben.

10 DATENSCHUTZFOLGENABSCHÄTZUNG

136. Gemäß Artikel 35 Absatz 1 sind die für die Verarbeitung Verantwortlichen des GDPR verpflichtet, Datenschutzfolgenabschätzungen (DPIA) durchzuführen, wenn eine Art der Datenverarbeitung wahrscheinlich zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen führen wird. Artikel 35 (3) (c) GDPR legt fest, dass die für die Verarbeitung Verantwortlichen verpflichtet sind, Datenschutzfolgenabschätzungen durchzuführen, wenn die Verarbeitung eine systematische Überwachung eines öffentlich zugänglichen Bereichs in großem Maßstab darstellt. Darüber hinaus ist nach Artikel 35 Absatz 3 Buchstabe b) GDPR auch eine Datenschutzfolgenabschätzung erforderlich, wenn der für die Verarbeitung Verantwortliche beabsichtigt, besondere Datenkategorien in großem Umfang zu verarbeiten.

137. Die Leitlinien zur Datenschutzfolgenabschätzung27 enthalten weitere Ratschläge und ausführlichere Beispiele, die für die Videoüberwachung relevant sind (z.B. bezüglich der "Verwendung eines Kamerasystems zur Überwachung des Fahrverhaltens auf Autobahnen"). Artikel 35 (4) GDPR verlangt, dass jede Aufsichtsbehörde eine Liste der Art von Verarbeitungen veröffentlicht, die in ihrem Land der DPIA-Pflicht unterliegen. Diese Listen sind in der Regel auf den Websites der Behörden zu finden. Angesichts der typischen Zwecke der Videoüberwachung (Schutz von Personen und Eigentum, Erkennung, Verhütung und Kontrolle von Straftaten, Sammlung von Beweisen und biometrische Identifizierung von Verdächtigen) kann man davon ausgehen, dass in vielen Fällen der Videoüberwachung eine DPIA erforderlich sein wird. Daher sollten die für die Datenverarbeitung Verantwortlichen diese Dokumente sorgfältig konsultieren, um festzustellen, ob eine solche Bewertung erforderlich ist, und sie gegebenenfalls durchführen. Das Ergebnis der durchgeführten DPIA sollte die Wahl des für die Verarbeitung Verantwortlichen für die implementierten Datenschutzmaßnahmen bestimmen.

138. Wenn die Ergebnisse der DPIA darauf hindeuten, dass die Verarbeitung trotz der vom für die Verarbeitung Verantwortlichen geplanten Sicherheitsmaßnahmen zu einem hohen Risiko führen würde, muss vor der Verarbeitung die zuständige Aufsichtsbehörde konsultiert werden. Einzelheiten über vorherige Konsultationen finden sich in Artikel 36.

Für den Europäischen Datenschutzrat Der

Vorsitzende

(Andrea Jelinek)

[27] WP248 rev.01, Leitlinien zur Datenschutzfolgenabschätzung (DPIA) und zur Bestimmung, ob die Verarbeitung "wahrscheinlich zu einem hohen Risiko führt", für die Zwecke der Verordnung 2016/679. - vom EDPB gebilligt