Die Datenschutz-Grundverordnung

Leitlinien für die Videoüberwachung

Datum der ersten Annahme: 13.08.2018

Datum der Aktualisierung: 19/04/2024

Inhalt

Einleitung

Seit dem 25. Mai 2018[1] gilt die DSGVO. Eine der unmittelbaren Folgen der DSGVO besteht darin, dass für **die Installation eines Videoüberwachungssystems keine vorherige Genehmigung der CNPD mehr erforderlich** ist.

Obwohl die Verpflichtung zur Einholung einer vorherigen Genehmigung bei der CNPD aufgehoben wurde, sind die für die Verarbeitung Verantwortlichen, die eine Videoüberwachung installieren oder installieren lassen, verpflichtet, die Grundsätze und Verpflichtungen einzuhalten, die sich aus der DSGVO ergeben, einschließlich der Verpflichtung, ein Register der unter ihrer Verantwortung durchgeführten Verarbeitungen personenbezogener Daten zu führen.[2] Die Verarbeitung personenbezogener Daten, die aus der Videoüberwachung entstehen, muss daher in dieses Register aufgenommen werden und alle nach Artikel 30 DSGVO erforderlichen Informationen enthalten.

Im Gegensatz zum geänderten Gesetz vom 2. August 2002[3] (aufgehoben) definiert die DSGVO den Begriff "Überwachung" nicht mehr. Gleichwohl ist die Installation eines Videoüberwachungssystems, das Arbeitnehmer überwacht, stets als Verarbeitung personenbezogener Daten zu Überwachungszwecken im Rahmen von Arbeitsverhältnissen im Sinne von Art. L. 261-1 des Arbeitsgesetzbuchs anzusehen, der vom Arbeitgeber zu befolgen ist.

Ohne Anspruch auf Vollständigkeit erheben zu wollen, möchte die CNPD darüber hinaus auf **einige der geltenden Grundsätze und Verpflichtungen im Bereich der Videoüberwachung hinweisen.**

[1] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (im Folgenden: DSGVO).
[2] *vgl.* Art. 30 DSGVO.
[3] Geändertes Gesetz vom 2. August 2002 über den Schutz von Personen bei der Verarbeitung personenbezogener Daten, aufgehoben durch das Gesetz vom 1. August 2018 zur Organisation der Nationalen Kommission für den Datenschutz und der allgemeinen Datenschutzregelung.

1. Grundsatz der Rechtmäßigkeit

Jede Verarbeitung personenbezogener Daten muss auf einer der in Artikel 6.1 DSGVO abschließend aufgezählten Rechtmäßigkeitsvoraussetzungen[4] beruhen. Im Rahmen eines Videoüberwachungssystems ist die geeignetste Voraussetzung für die Rechtmäßigkeit im Allgemeinen die der Verarbeitung, die zur Wahrung der berechtigten Interessen des für die Verarbeitung Verantwortlichen erforderlich ist, es sei denn, die Interessen oder Grundrechte und Grundfreiheiten der der Videoüberwachung unterliegenden Person(en) überwiegen (Artikel 6.1 Buchstabe f DSGVO). Die CNPD weist darauf hin, dass drei kumulative Voraussetzungen erfüllt sein müssen, um von der Zulässigkeitsvoraussetzung des berechtigten Interesses Gebrauch machen zu können:

(1) das Bestehen eines berechtigten Interesses (z. B. die Absicht, sein Vermögen vor Diebstahl oder seine Beschäftigten vor körperlichen Schäden zu schützen);[5]

(2) die Notwendigkeit, die personenbezogenen Daten für die Zwecke zu verarbeiten, die mit dem geltend gemachten berechtigten Interesse verfolgt werden (d. h. gibt es angemessene und weniger in die Privatsphäre eingreifende alternative Mittel, mit denen derselbe Zweck erreicht werden kann?); und

(3) die Tatsache, dass die Grundrechte und Interessen der betroffenen Personen nicht Vorrang vor den berechtigten Interessen des für die Verarbeitung Verantwortlichen haben dürfen ("Abwägungsverfahren").

Diese dritte Voraussetzung besteht darin, zu prüfen, ob die Gefahr besteht, dass die Videoüberwachung die Grundrechte und -interessen der betroffenen Personen beeinträchtigt, und wenn ja, ob diese Grundrechte und -interessen nicht Vorrang vor dem Interesse des für die Verarbeitung Verantwortlichen[6] an der Einrichtung eines Videoüberwachungssystems haben müssen – in diesem Fall ist die Einrichtung nicht zulässig.

In den meisten Fällen haben die Grundrechte und Grundfreiheiten der betroffenen Personen Vorrang vor den berechtigten Interessen des für die Verarbeitung Verantwortlichen, wenn bei der Videoüberwachung die Gefahr einer erheblichen Beeinträchtigung der Rechte der betroffenen Personen besteht oder an Orten, in denen eine begründete Erwartung besteht, dass sie nicht überwacht werden. Beispiele für solche Zonen sind in Abschnitt 4.5.B aufgeführt. Die Abwägung muss in jedem Fall von Fall zu Fall erfolgen.

Die für die Verarbeitung Verantwortlichen müssen in der Lage sein, die getroffenen Entscheidungen in Bezug auf den Standort der Kameras, die überwachten Bereiche und die verwendeten technischen Mittel zu erläutern.

Achtung: Grundsätzlich[7] stellt die Einwilligung keine angemessene Rechtmäßigkeitsgrundlage für die Videoüberwachung dar.

[4] *vgl.* Art. 6.1 Buchst. a – f DSGVO.
[5] In einem solchen Fall wird empfohlen, die Tatsache zu dokumentieren, dass ein Diebstahl oder ein Überfall bereits stattgefunden hat (z. B. durch Aufbewahrung einer Kopie einer bei der Polizei eingereichten Anzeige), um ein tatsächliches Interesse nachzuweisen.
[6] Für weitere Informationen über das berechtigte Interesse und die durchzuführende Analyse verweist die CNPD auf die Rn. 17 bis 40 der Leitlinien 3/2019 des Europäischen Datenschutzausschusses zur Verarbeitung personenbezogener Daten durch Videogeräte, abrufbar unter: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_de.
[7] *Siehe Artikel* 6.1 Buchstabe a DSGVO.

Denn Videoüberwachungssysteme haben ihrem Wesen nach eine unbestimmte Anzahl von Personen gleichzeitig in ihrem Blickfeld.[8] Es ist dem für die Verarbeitung Verantwortlichen jedoch grundsätzlich nicht möglich, die Einwilligung jeder Person einzuholen, die in das Sichtfeld der Kamera eindringt, oder nachzuweisen, dass jede betroffene Person ihre Einwilligung gegeben hat, bevor ihre personenbezogenen[9] Daten verarbeitet wurden. Wenn die betroffene Person ihre Einwilligung widerruft, wird der für die Verarbeitung Verantwortliche außerdem Schwierigkeiten haben, nachzuweisen, dass die personenbezogenen Daten nicht mehr verarbeitet werden.[10]

Die Einholung einer gültigen Einwilligung durch den für die Verarbeitung Verantwortlichen wird noch erschwert, wenn die Videoüberwachungskameras Mitarbeiter des für die Verarbeitung Verantwortlichen in ihrem Sichtfeld haben. Denn eine der Voraussetzungen für die Gültigkeit der Einwilligung – die sich aus Art. 4 ergeben – ist erfüllt. 11) DSGVO - ist, dass diese von der betroffenen Person freiwillig erteilt wurde. Im Rahmen von Arbeitsverhältnissen sind Arbeitnehmer angesichts der Abhängigkeit und des Machtungleichgewichts, die im Verhältnis zwischen Arbeitgeber und Arbeitnehmer bestehen können, nur sehr selten in der Lage, ihre Einwilligung zu verweigern oder zu widerrufen, ohne befürchten zu müssen, nachteilige Folgen zu erleiden.

Unter diesen Umständen kann die Einwilligung sehr selten als freiwillig erteilt angesehen werden.[11]

[8] Siehe hierzu die Ziff. 43 bis 48 der Leitlinien 3/2019 des Europäischen Datenschutzausschusses zur Verarbeitung personenbezogener Daten durch Videogeräte, abrufbar unter: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_de.
[9] *vgl.* Art. 7.1 DSGVO.
[10] *cf* Art. 7.3 DSGVO.
[11] Siehe hierzu die vom Europäischen Datenschutzausschuss übernommenen Leitlinien 5/2020 des Europäischen Datenschutzausschusses zur Einwilligung im Sinne der Verordnung (EU) 2016/679, Rn. 21 ff., abrufbar unter: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_de.pdf. Siehe auch Abschnitt 6.2 der Stellungnahme 2/2017 der Artikel-29-Datenschutzgruppe zur Verarbeitung von Daten am Arbeitsplatz (WP 249), abrufbar unter: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169.

2. Grundsatz der Zweckbindung

Nach Art. 5.1 Buchst. b der DSGVO müssen personenbezogene Daten für festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.

Die Überwachung mit Kameras kann beispielsweise folgenden Zwecken dienen:

- den Zugang zum Gebäude zu sichern;
- die Sicherheit des Personals und der Kunden zu gewährleisten;
- potenziell verdächtige oder gefährliche Verhaltensweisen zu erkennen und zu identifizieren, die zu Unfällen oder Störungen führen können;
- den Ursprung eines Vorfalls genau zu ermitteln;
- Schutz von Gütern (Gebäude, Anlagen, Material, Waren, Bargeld usw.);
- Organisation und Betreuung einer raschen Evakuierung von Personen im Falle eines Zwischenfalls;
- rechtzeitige Warnung der Rettungs-, Feuerwehr- oder Strafverfolgungsbehörden und Erleichterung ihres Eingreifens.
- ...

Hingegen ist die CNPD im Allgemeinen der Auffassung, dass die folgenden Zwecke von einem für die Verarbeitung Verantwortlichen, der ein Videoüberwachungssystem einsetzt, nicht verfolgt werden können, da ein zu diesen Zwecken installiertes Videoüberwachungssystem die nachstehend in Nr. 4 festgelegten Grundsätze nicht einhalten würde:

- sicherstellen, dass die Mitarbeiter arbeiten und nicht zu viel Zeit am Telefon verbringen oder mit ihren Kollegen reden;
- Überprüfung der ordnungsgemäßen Einhaltung der Arbeitszeiten durch die Arbeitnehmer;
- zu überprüfen, ob die Arbeitnehmer die erteilten Arbeitsanweisungen befolgen;
- zu überprüfen, ob sich die Mitarbeiter angemessen gegenüber den Kunden verhalten.

Vor der Installation eines Videoüberwachungssystems muss der für die Verarbeitung Verantwortliche den Zweck bzw. die Zwecke, die er mit einem solchen System tatsächlich verfolgen möchte, genau festlegen und darf ihn anschließend nicht für andere Zwecke verwenden. So kann beispielsweise ein Arbeitgeber, der beschließt, ein Videoüberwachungssystem ausschließlich zu dem Zweck einzurichten, die Sicherheit des Personals und der Kunden zu gewährleisten, es anschließend nicht für einen anderen Zweck verwenden, für den die Daten ursprünglich nicht erhoben und verwendet wurden und der insbesondere den Arbeitnehmern nicht zur Kenntnis gebracht wurde.

Kameras, die von einem einzigen Verantwortlichen für dieselben Zwecke verwendet werden, können gemeinsam dokumentiert werden.

Das nachstehende Beispiel in Abschnitt 4.3 dieser Leitlinien veranschaulicht diesen Grundsatz der Zweckbindung.

3. Grundsatz der Transparenz

Jeder für die Verarbeitung Verantwortliche ist verpflichtet, die betroffenen Personen über die von ihm vorgenommene Verarbeitung personenbezogener Daten zu informieren. Diese Informationen müssen den Anforderungen der Artikel 12 und 13 DSGVO entsprechen.

Nach Art. 12.1 DSGVO müssen die Unterrichtung der betroffenen Personen und die an sie gerichteten Mitteilungen in „prägnanter, *transparenter, verständlicher und leicht zugänglicher* Weise *in klarer und einfacher Sprache"* erfolgen.

Das Wort „bereitstellen" ist im vorliegenden Fall von entscheidender Bedeutung und *„bedeutet, dass der für die Verarbeitung Verantwortliche konkrete Maßnahmen ergreifen muss, um der betroffenen Person die betreffenden Informationen zur Verfügung zu stellen oder die betroffene Person aktiv zum Speicherort dieser Informationen zu leiten (z. B. durch einen direkten Link, einen QR-Code usw.)".* [12]

Um das Verständnis der betroffenen Personen für die Verarbeitung von Daten bei der Verwendung eines Videoüberwachungssystems zu erleichtern,[13] wird in den Leitlinien des Europäischen Datenschutzausschusses (EDSA) zur Verarbeitung personenbezogener Daten durch Videogeräte ein zweistufiger Ansatz vorgeschlagen.

Ein solcher Ansatz besteht darin, den Betroffenen zunächst eine Reihe von Informationen zu vermitteln, z. B. über Werbetafeln (siehe Abschnitt 3.1. Erste Informationsebene) und dann – in einem zweiten Schritt – alle nach Art. 13 DSGVO erforderlichen Informationen auf anderem Wege zu übermitteln (siehe Abschnitt 3.2. Zweite Informationsebene).

Achtung: Wenn sich die Videoüberwachung an Mitarbeiter des für die Verarbeitung Verantwortlichen richtet, weist die CNPD die für die Verarbeitung Verantwortlichen auf die zusätzlichen Pflichten hin, insbesondere auf dem Gebiet der kollektiven Information, die in Art. L. 261-1 des Arbeitsgesetzbuchs vorgesehen sind (siehe unten, Nr. 5).

In diesem Zusammenhang ist noch darauf hinzuweisen, dass die Arbeitnehmer individuell informiert werden müssen und dass die bloße Unterrichtung der Personalvertretung nicht sicherstellt, dass die Arbeitnehmer individuell über die genauen Elemente aus Art. 13 Abs.[14] 1 und 2 der DSGVO informiert wurden.

3.1. Erste Informationsebene

Um die betroffenen Personen über das Vorhandensein eines Videoüberwachungssystems zu informieren, empfiehlt die CNPD, eine erste Informationsebene, z. B. über Plakatwände, zu übermitteln, die Folgendes enthält:

- die Identität und die Kontaktdaten des für die Verarbeitung Verantwortlichen;
- Zweck(e) der Verarbeitung;
- Informationen, die den größten Einfluss auf die betroffene Person haben (z. B. Speicherdauer der Bilder, Live-Überwachung, Veröffentlichung oder Übertragung von Videomaterial an Dritte);

[12] Siehe hierzu Ziffer 33 der Leitlinien der Artikel-29-Datenschutzgruppe zur Transparenz im Sinne der Verordnung (EU) 2016/679 (WP260rev. 01), übernommen vom Europäischen Datenschutzausschuss.
[13] Leitlinien 3/2019 des Europäischen Datenschutzausschusses zur Verarbeitung personenbezogener Daten durch Videogeräte, abrufbar unter: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_de.
[14] *vgl.* Beschluss 14FR/2021 vom 12. Mai 2012 der nationalen Datenschutzkommission, Rn. 47.

- das Bestehen der Rechte, über die die betroffenen Personen verfügen;
- die Angabe, dass es umfassendere Informationen gibt (zweite Informationsebene), und die Mittel, um auf diese Informationen zuzugreifen (z. B. ein Hyperlink zur Website des für die Verarbeitung Verantwortlichen, die Verwendung eines QR-Codes, eine anzurufende Telefonnummer oder die Angabe, wo diese detaillierteren Informationen verfügbar sind.

Diese Informationstafeln müssen an den Haupteingängen und -ausgängen oder in der Umgebung der Videoüberwachungsanlage ständig sichtbar (d. h. in ausreichender Größe) und in Kopfhöhe gut lesbar sein. Die betroffenen Personen müssen dies grundsätzlich vor dem Betreten des überwachten Bereichs zur Kenntnis nehmen können. Für eine schnelle und einfache Warnung der Betroffenen wird die Plakatwand idealerweise von Piktogrammen begleitet.

Beispiel einer Plakatwand[15]

<table>
<tr><td rowspan="3"> 
</td><td><u>Identität des für die Verarbeitung Verantwortlichen:</u>

<u>Kontaktdaten des für die Verarbeitung Verantwortlichen</u></td></tr>
<tr><td><u>Zweck(e) der Videoüberwachung:</u></td></tr>
<tr><td><u>Informationen, die den größten Einfluss auf die betroffene Person haben</u>
(z. B. Aufbewahrungsdauer von Bildern, Live-Überwachung, Veröffentlichung oder Übertragung von Videomaterial an Dritte)</td></tr>
<tr><td><u>Weitere Informationen zu dieser Videoüberwachung finden Sie unter:</u>
- über unsere Informationsbroschüre;
- auf unserer Website [Hyperlink zur Website des für die Verarbeitung Verantwortlichen];
- [QR-Code einfügen]
- telefonisch
- ...</td><td><u>Rechte der betroffenen Personen:</u>

Die DSGVO räumt Ihnen als betroffene Person Rechte ein, die es Ihnen ermöglichen, die Verwendung Ihrer eigenen Daten zu kontrollieren. Insbesondere haben Sie ein <u>Auskunftsrecht und</u> ein <u>Recht auf Löschung.</u>

Weitere Informationen zu Ihren Rechten finden Sie unter [Link/QR-Code/Factsheet]</td></tr>
</table>

[15] **Achtung:** Dieses Dokument ist ein (unverbindliches) Beispiel für Informationen der ersten Ebene. Die verschiedenen Abschnitte müssen entsprechend dem vom für die Verarbeitung Verantwortlichen implementierten Videoüberwachungssystem ausgefüllt und angepasst werden.

3.2. Zweite Informationsebene

Die zweite Informationsebene muss alle nach Art. 13 DSGVO erforderlichen Informationen im Einzelnen enthalten. Er muss den Standards von Artikel 12 DSGVO entsprechen und daher prägnant, transparent, verständlich und in klarer und einfacher Sprache abgefasst sein. Die zweite Informationsebene muss an einem Ort zur Verfügung gestellt werden, der für die betroffene Person leicht zugänglich ist. Es könnte gegebenenfalls auf andere Weise zur Verfügung gestellt werden, z. B. durch eine Kopie der Datenschutzerklärung, die den Arbeitnehmern per E-Mail zugesandt wird, oder durch einen Link auf der Website zu einer Informationsbroschüre in Bezug auf nicht angestellte Dritte.[16] Eine nicht-digitale Version sollte der betroffenen Person immer zur Verfügung stehen, z. B. durch ein erläuterndes Dokument, das der für die Verarbeitung Verantwortliche zur Verfügung stellt.

Für weitere Informationen zum Grundsatz der Transparenz bei der Videoüberwachung verweisen wir auf Punkt 7 der Leitlinien 3/2019 des EDSA zur Verarbeitung personenbezogener Daten durch Videogeräte.[17]

[16] *vgl.* Beschluss 14FR/2021 der nationalen Datenschutzkommission vom 12. Mai 2021, Rn. 54.
[17] Abrufbar unter: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_de

4. Grundsatz der Notwendigkeit und Verhältnismäßigkeit (Datenminimierung)

Der Grundsatz der Notwendigkeit impliziert zunächst, dass ein für die Verarbeitung Verantwortlicher nur dann auf eine Videoüberwachungsanlage zurückgreifen darf, wenn es keine alternativen Mittel gibt, die die Privatsphäre der betroffenen Personen weniger stark beeinträchtigen, um den angestrebten Zweck zu erreichen.

Der Grundsatz der Datenminimierung im Bereich der Videoüberwachung bedeutet ferner, dass ein Videoüberwachungssystem, wenn es installiert ist, nur das filmen darf, was zur Erreichung des verfolgten Zwecks bzw. der verfolgten Zwecke unbedingt erforderlich erscheint („angemessene, relevante und auf das Erforderliche beschränkte Daten"), und dass die Verarbeitungsvorgänge im Hinblick auf diesen Zweck nicht unverhältnismäßig sein dürfen.

Zur Veranschaulichung wird in Abschnitt 4.5 ein Überblick über Gebiete gegeben, in denen die CNPD der Ansicht ist, dass ein Videoüberwachungssystem problematisch sein könnte oder nicht. Die Situation sollte jedoch von Fall zu Fall analysiert werden, um die Notwendigkeit und Verhältnismäßigkeit einer Videoüberwachung zu prüfen, insbesondere im Hinblick auf Kriterien wie z. B. die Art des Ortes, der mit Videoüberwachung überwacht werden soll, seine Situation, seine Konfiguration oder seine Anwesenheit.

4.1. Eingeschränktes Sichtfeld von Kameras, die Zugänge im Innen- oder Außenbereich oder in der Umgebung eines Gebäudes oder Standorts filmen

Kameras, die dazu bestimmt sind, einen Zugangsort (Eingang und Ausgang, Schwelle, Veranda, Tür, Markise, Halle usw.) zu überwachen, müssen ein Sichtfeld haben, das sich auf die Fläche beschränkt, die unbedingt erforderlich ist, um Personen zu sehen, die sich auf den Zugang vorbereiten. Kameras, die Außenzugänge filmen, dürfen nicht die gesamte Breite eines Bürgersteigs, der gegebenenfalls entlang des Gebäudes oder der angrenzenden öffentlichen Straßen verläuft, visieren.

Ebenso müssen Außenkameras, die in der Nähe oder in der Nähe eines Gebäudes installiert sind, so konfiguriert sein, dass sie weder die öffentliche Straße noch die Umgebung, Eingänge, Zugänge und Innenräume anderer benachbarter Gebäude erfassen, die möglicherweise in ihr Sichtfeld fallen.

Je nach Standortkonfiguration ist es manchmal unmöglich, eine Kamera zu installieren, die einen Teil der öffentlichen Straße, die Umgebung, die Eingänge, den Zugang und die Innenräume anderer Gebäude nicht in ihr Sichtfeld einschließen würde.[18] In einem solchen Fall ist die CNPD der Ansicht, dass der für die Verarbeitung Verantwortliche Maskierungs- oder Unschärfetechniken einführen muss, um das Sichtfeld auf sein Eigentum zu beschränken.

4.2. Permanente und kontinuierliche Überwachung

- **Überwachung Nicht-Angestellter**

[18] Beschluss*27FR/2021* der nationalen Datenschutzkommission vom 15. Juli 2021, Rn. 47-49.

Eine ständige Überwachung von Nicht-Angestellten ist nicht immer zulässig. Die CNPD hält es beispielsweise für unverhältnismäßig, das Innere eines Speisesaals mit Esstischen zu filmen. Gleiches gilt für die Terrasse oder den Tresen eines Cafés. Auch wenn an solchen Orten ein gewisses Risiko von Diebstahl oder Vandalismus bestehen könne, würden die anwesenden Kunden dauerhaft der Videoüberwachung unterliegen, wenn sie ein Restaurant oder ein Café als Treffpunkt wählten, um eine gute Zeit bei einer Mahlzeit zu verbringen, sich zu unterhalten oder zu entspannen. Kunden, die sich für einen längeren oder kürzeren Zeitraum an einem solchen Ort aufhalten, müssen berechtigterweise erwarten können, in diesen privaten Momenten nicht gefilmt zu werden. Die Verwendung von Kameras im Speisesaal, einschließlich der Esstische, kann das Verhalten jedes Kunden, der an einem Tisch sitzt, filmen und für die Kunden, die sich während ihrer gesamten Anwesenheit im Restaurant beobachtet fühlen, zu Unbehagen oder sogar psychischem Druck führen. Eine solche ständige Überwachung ist daher als unverhältnismäßig zum angestrebten Zweck anzusehen und stellt einen Eingriff in die Privatsphäre des Kunden dar.

- **Überwachung der Arbeitnehmer**

Am Arbeitsplatz haben Arbeitnehmer grundsätzlich das Recht, nicht ständig überwacht zu werden.

Die Beachtung des Grundsatzes der Verhältnismäßigkeit bedeutet nämlich, dass der Arbeitgeber die Überwachungsmittel einsetzen muss, die die Privatsphäre des Arbeitnehmers am stärksten schützen. Die Einhaltung dieses Grundsatzes erfordert, dass beispielsweise eine automatische und kontinuierliche Überwachung der Arbeitnehmer vermieden werden muss.

So könne z. B. der Betreiber eines Restaurants seine Beschäftigten nicht unter Berufung auf den Schutz seines Eigentums in der Küche überwachen. Die Arbeitnehmer würden fast ständig einer Videoüberwachung unterzogen, und es ist offensichtlich, dass eine solche Überwachung einen nicht unerheblichen psychischen Druck auf die Arbeitnehmer ausüben kann, die sich beobachtet fühlen und wissen, dass sie beobachtet werden, zumal die Überwachungsmaßnahmen im Laufe der Zeit fortbestehen. Gleiches gilt z. B. für die Videoüberwachung des Innenraums eines Büros, eines offenen Raums oder einer Werkstatt, in der ständig ein oder mehrere Arbeitnehmer arbeiten. Eine ständige Überwachung gilt als unverhältnismäßig zum angestrebten Zweck und stellt einen übermäßigen Eingriff in die Privatsphäre des an seinem Arbeitsplatz beschäftigten Arbeitnehmers dar. In diesem Fall müssen die Grundrechte und Grundfreiheiten der Arbeitnehmer Vorrang vor den berechtigten Interessen des Arbeitgebers haben.

Um eine ständige und kontinuierliche Überwachung zu vermeiden, sollte der für die Verarbeitung Verantwortliche das Sichtfeld der Kameras auf die zur Erreichung der verfolgten Zwecke erforderliche Fläche beschränken.

So kann beispielsweise die Kameraüberwachung einer Kasse eines Geschäfts den Zweck haben, das Eigentum des für die Verarbeitung Verantwortlichen vor Diebstahl durch seine Mitarbeiter oder einen Kunden/Nutzer zu schützen und die Sicherheit seines Personals zu gewährleisten. Um jedoch die Privatsphäre der Mitarbeiter nicht zu beeinträchtigen, muss die Kamera so konfiguriert werden, dass die Mitarbeiter hinter einem Kassenschalter nicht ins Visier genommen werden, indem ihr Sichtfeld auf die Kasse selbst und die Vorderseite des Schalters, d. h. den Wartebereich der Kunden vor dem Schalter, gerichtet wird, um beispielsweise die Identifizierung der Täter zu ermöglichen.

4.3. Überwachung der Leistungen und/oder des Verhaltens der Arbeitnehmer

Die CNPD ist der Ansicht, dass die Videoüberwachung nicht dazu verwendet werden sollte, das Verhalten und die Leistung der Mitarbeiter des für die Verarbeitung Verantwortlichen außerhalb der Zwecke, für die sie eingerichtet wurde, zu beobachten.

So hat ein Arbeitgeber das Recht, Bilder eines Arbeitnehmers zu verwenden, der einen Warendiebstahl begeht und die aus einem Videoüberwachungssystem stammen, das zu einem Zweck des Eigentumsschutzes verwendet wird. Er ist jedoch nicht berechtigt, die Kamera zu benutzen, um festzustellen, dass ein Arbeitnehmer zu lange mit einem Kunden oder einem Arbeitskollegen plaudert, und anschließend die Aufzeichnungen als Beweismittel zu verwenden, um Disziplinarmaßnahmen gegen diesen Arbeitnehmer zu ergreifen. Dies stelle einen durch die DSGVO verbotenen Zweckmissbrauch dar.

4.4. Orte, die den Arbeitnehmern für den privaten Gebrauch vorbehalten sind

Die CNPD ist der Ansicht, dass Überwachungskameras keine Orte filmen sollten, die für den privaten Gebrauch der Arbeitnehmer reserviert sind oder die nicht für die Erfüllung von Arbeitsaufgaben bestimmt sind, wie z. B. Toiletten, Umkleideräume, Raucherbereiche, Ruhebereiche, der Raum, der der Personaldelegation zur Verfügung gestellt wird, Küche/Küche usw.

4.5. Beispiele für Videoüberwachungsbereiche

Die nachstehenden Beispiele für Bereiche sind zusammen mit den Abschnitten 4.1 bis 4.4 zu lesen und zu betrachten.

A. Bereiche, in denen die Installation einer Videoüberwachung grundsätzlich verhältnismäßig ist:

- alle Arten des Zugangs, wobei die Sichtfelder der Kameras auf die Fläche beschränkt werden, die unbedingt erforderlich ist, um Personen zu visualisieren, die sich auf den Zugang vorbereiten. Die Kameras dürfen nicht auf öffentliche Straßen oder nicht benötigte Bereiche gerichtet sein, auch nicht indirekt, wie z. B. eine Stechuhr).[19]
- Lagerräume für Waren / Vorräte / Lagerhallen / Lagerhallen oder Lagerhallen (es sei denn, es werden ständig Mitarbeiter eingesetzt, die im Lager arbeiten, wie z. B. Lagerarbeiter);
- Verkaufsflächen eines Geschäfts / Regale eines Geschäfts / einer Einkaufspassage / eines Ausstellungsraums / eines Verkaufs- und Beratungsraums (ausgenommen ständige Arbeitsplätze hinter einem Schalter);
- Parkplatz (innen/außen/unterirdisch);
- Liefer- oder Beladebereiche/Liefer- und Entladedocks;

[19] *vgl.* Beschluss 27FR/2021 der nationalen Datenschutzkommission vom 15. Juli 2021, Rn. 47-49.

- ein EDV-Raum/ein Serverraum;
- eine automatische Fahrzeugwaschanlage / ein Carwash;
- eine Zapfsäule;
- einen Safe / einen gesicherten Raum / die Schränke der automatischen Gepäckaufbewahrung;
- Räume für Geldtransporte / ein Geldtransporter;
- technische Anlagen oder Produktionsmaschinen (sofern keine Dauerarbeitsplätze gefilmt werden);
- den Technikraum eines Gebäudes/einen Wartungsraum/einen Zählerraum einer Eigentumswohnung;
- Archivräume;
- Geldautomaten / Bankautomaten.

B. Bereiche, in denen die Installation einer Videoüberwachung grundsätzlich unverhältnismäßig ist:

- eine öffentliche Straße / ein Bürgersteig (mit Ausnahme von Ausnahmen, die von der spezifischen Konfiguration des Ortes abhängen; das Sichtfeld darf jedoch nur einen äußerst begrenzten Teil der öffentlichen Straße umfassen);
- das Innere eines Verbraucherbereichs eines Restaurants, einer Gaststätte, eines Nachtclubs usw. (Verpflegungsraum, Essenstheke, Terrasse, Kantine/Cafeteria usw.);
- das Innere einer Restaurantküche;
- der private Eingang zu einer Wohnung in einem Mehrfamilienhaus;
- benachbartes Grundstück oder Gebäude;
- das Innere eines Büros mit einem ständigen Arbeitsplatz;
- einen Ruhe- oder Aufenthaltsraum;
- das Innere eines Wellnessbereichs (Sauna, Liegestühle usw.)
- Trainingsbereiche in einem Fitnessstudio;
- Toiletten/Sanitäranlagen/Duschen;
- ein Büro der Personalvertretung oder dessen Zugang (wenn es nur zu diesem Büro führt);
- eine Küchenzeile;
- ein Raucherbereich;
- eine Garderobe/ein Schließfachraum/eine Umkleidekabine;
- Werkstatt einer Garage/Werkstatt für die Montage und Demontage von Reifen/Werkstatt für die Produktion/Werkstatt;

- den Friseurbereich eines Friseursalons;
- der Spielbereich einer Kinderkrippe.

C. Bereiche, in denen die Verhältnismäßigkeit einer Videoüberwachung von den Umständen des Einzelfalls und den zur Gewährleistung des Schutzes der Privatsphäre ergriffenen Maßnahmen abhängt

Die Videoüberwachung der nachstehend aufgeführten Bereiche kann in bestimmten Fällen zulässig sein, in anderen nicht. Ob die Videoüberwachung solcher Bereiche verhältnismäßig ist oder nicht, hängt von den Umständen des Einzelfalls ab, z. B. von der Art, der Lage oder der Konfiguration des Ortes, der Art der Tätigkeit des für die Verarbeitung Verantwortlichen und den mit dieser Tätigkeit verbundenen Risiken usw. Sie hängt auch von den Maßnahmen ab, die der für die Verarbeitung Verantwortliche ergriffen hat, um die Videoüberwachung so zu gestalten, dass die Privatsphäre der betroffenen Personen weniger beeinträchtigt wird (z. B. Einschränkung des Sichtfelds der Kameras, Einsatz von Maskierungs-/Weichzeichen-Techniken usw.). Der für die Verarbeitung Verantwortliche muss eine Einzelfallanalyse durchführen.

- die Umgebung eines Gebäudes;
- einen Warteraum;
- Schalter;
- Empfangsschalter/Empfangsschalter;
- Kassen;
- einen Kassenzählraum / einen Geldbearbeitungsraum;
- Gemeinschaftsbereiche eines Gebäudes, das sich in Miteigentum befindet;
- der Spielplatz einer Schule (und Umgebung);
- ein Schwimmbad;
- Dach eines Gebäudes;
- ein Besprechungsraum.

4.6. Die Verarbeitung von Tönen im Zusammenhang mit den Bildern

Eine Überwachung mit Videokameras darf sich nur auf Bilder ohne Ton beziehen. Denn das Live-Hören sowie die Tonaufzeichnung in Verbindung mit den Bildern macht die Videoüberwachung noch eindringlicher und ist als unverhältnismäßig anzusehen.

5. Grundsatz der Beschränkung der Aufbewahrungsdauer

Die DSGVO sieht vor, dass personenbezogene Daten in einer Form aufbewahrt werden, die die Identifizierung der betroffenen Personen für einen Zeitraum ermöglicht, der nicht länger ist, als es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. In Bezug auf die Videoüberwachung ist die CNPD der Ansicht, dass die Bilder grundsätzlich bis zu 8 Tage aufbewahrt werden können.

Der für die Verarbeitung Verantwortliche kann die Bilder ausnahmsweise für einen Zeitraum von 30 Tagen aufbewahren. Die Gründe, die eine solche Aufbewahrungsdauer rechtfertigen, sind jedoch im Register der Verarbeitungen anzugeben.

Eine Speicherdauer von mehr als 30 Tagen wird im Allgemeinen als unverhältnismäßig angesehen.[20]

Im Falle eines Vorfalls oder einer Straftat können die Bilder im Rahmen der Übermittlung der Daten an die zuständigen Justiz- und Strafverfolgungsbehörden, die für die Feststellung oder Verfolgung von Straftaten zuständig sind, über die oben genannten Fristen hinaus gespeichert werden.

Schließlich muss der für die Verarbeitung Verantwortliche sicherstellen, dass die Bilder nach Ablauf der Speicherfrist vernichtet werden. Die CNPD empfiehlt die Einführung einer automatischen Löschung.

[20] *vgl.* Beschluss 14FR/2021 der nationalen Datenschutzkommission vom 12. Mai 2021, Rn. 38.

6. Art. L. 261-1 des Arbeitsgesetzbuchs: die spezifischen gesetzlichen Bestimmungen über die Datenverarbeitung zu Überwachungszwecken im Rahmen von Arbeitsverhältnissen

Der Arbeitgeber, der eine Videoüberwachung installieren möchte, muss **neben der Einhaltung der vorstehenden Nrn. 1-4 und 6-7 auch die Einhaltung der besonderen Vorschriften des Art. L. 261-1 des Arbeitsgesetzbuchs sicherstellen.**

Art. L. 261-1 des Arbeitsgesetzbuchs erlaubt die Verarbeitung personenbezogener Daten zum Zwecke der Überwachung der Arbeitnehmer im Rahmen eines Arbeitsverhältnisses durch den Arbeitgeber nur auf **der Grundlage einer der in Art. 6.1 Buchst. a bis f der DSGVO abschließend aufgezählten Zulässigkeitsvoraussetzungen** (vgl. Nr. 1).

Für solche Verarbeitungen personenbezogener Daten, einschließlich der Videoüberwachung am Arbeitsplatz, sieht Art. L. 261-1 des Arbeitsgesetzbuchs neben **der individuellen Unterrichtung der Arbeitnehmer gemäß den Art. 12 und 13 der DSGVO eine Pflicht zur vorherigen kollektiven Unterrichtung** der Arbeitnehmervertretung vor. Diese Informationen **müssen Folgendes enthalten:**

- eine ausführliche Beschreibung des Zwecks der beabsichtigten Verarbeitung,
- eine ausführliche Beschreibung der Durchführungsmodalitäten des Überwachungssystems;
- gegebenenfalls die Dauer oder die Kriterien für die Datenspeicherung und
- eine förmliche Verpflichtung des Arbeitgebers, die erhobenen Daten nicht für einen anderen als den in der Vorabinformation ausdrücklich vorgesehenen Zweck zu verwenden.

Art. L. 261-1 des Arbeitsgesetzbuchs sieht vor, dass die Bestimmungen der Art. L. 211-8 und L.414-9 des Arbeitsgesetzbuchs Anwendung finden, es sei denn, die Verarbeitung personenbezogener Daten zu Überwachungszwecken entspricht einer rechtlichen oder regulatorischen Verpflichtung, wenn die Verarbeitung zu folgenden Zwecken erfolgt:

1. aus Gründen der Sicherheit und des Gesundheitsschutzes der Arbeitnehmer oder

2. für die Kontrolle der Produktion oder der Leistungen des Arbeitnehmers, wenn eine solche Maßnahme das einzige Mittel ist, um den genauen Lohn zu bestimmen, oder

3. im Rahmen einer Arbeitsorganisation nach dem gleitenden Stundenplan gemäß dem Arbeitsgesetzbuch.

In allen Fällen von Datenverarbeitungsprojekten zur Überwachung der Arbeitnehmer im Rahmen der Beschäftigungsverhältnisse kann die Personalvertretung oder andernfalls die betroffenen Arbeitnehmer innerhalb von 15 Tagen nach der oben genannten vorherigen Unterrichtung bei der CNPD einen **Antrag auf vorherige Stellungnahme** zur Konformität des Verarbeitungsprojekts stellen, der innerhalb eines Monats nach der Befassung zu entscheiden ist. Der Antrag hat während dieser Frist aufschiebende Wirkung.

Schließlich weist Art. L. 261-1 des Arbeitsgesetzbuchs darauf hin, dass die betroffenen Arbeitnehmer bei **einer Verletzung ihrer Rechte stets das Recht haben, bei der CNPD Beschwerde einzulegen,** da eine solche Beschwerde weder einen schwerwiegenden noch einen legitimen Kündigungsgrund darstellt.

7. Muss in Sachen Videoüberwachung eine Datenschutz-Folgenabschätzung („DPIA“) durchgeführt werden?

Art. 35 DSGVO verlangt, dass eine „DPIA“ durchgeführt wird, *„wenn eine Art der Verarbeitung, insbesondere durch den Einsatz neuer Technologien, unter Berücksichtigung der Art, des Umfangs, des Kontexts und der Zwecke der Verarbeitung* ***voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt“.***

Art. 35 Abs. 3 DSGVO sieht zudem drei Fälle vor, in denen eine „DPIA“ besonders erforderlich ist. Einer dieser drei Fälle betrifft die „systematische *großmaßstäbliche Überwachung eines öffentlich zugänglichen Gebiets“.* In bestimmten Situationen könnte die Installation eines Videoüberwachungssystems in diesen Fall fallen.

Darüber hinaus werden in den Leitlinien für die Datenschutz-Folgenabschätzung (DPIA) der Europäischen[21] Arbeitsgruppe (G29) die neun Kriterien festgelegt, die bei der Beurteilung der Frage zu berücksichtigen sind, ob eine Datenverarbeitung ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen kann und ob daher eine DPIA durchgeführt werden muss. Je nachdem, wo und in welchem Kontext Videoüberwachungskameras eingesetzt werden, könnten mehrere dieser Kriterien erfüllt sein, wie z. B. die Verarbeitung von „Daten *schutzbedürftiger Personen“* (Arbeitnehmer, Kinder, ältere Menschen usw.), die großflächige Erhebung, die „systematische *Überwachung“* oder das Kriterium der „innovativen *Nutzung oder Anwendung technologischer oder organisatorischer Lösungen“.*

Die CNPD möchte die Verantwortlichen auch auf die Leitlinien 3/2019 über die Verarbeitung personenbezogener Daten durch Videogeräte aufmerksam machen, in denen es heißt:

> *„Angesichts der üblichen Zwecke der Videoüberwachung (Schutz von Personen und Eigentum, Aufdeckung, Verhütung und Kontrolle von Straftaten, Beweiserhebung und biometrische Identifizierung von Verdächtigen) ist davon auszugehen, dass in vielen Fällen des Einsatzes von Videoüberwachung eine Datenschutz-Folgenabschätzung erforderlich sein wird. Daher ist es Sache der für die Verarbeitung Verantwortlichen, diese Dokumente sorgfältig zu konsultieren, um festzustellen, ob eine Folgenabschätzung erforderlich ist, und diese gegebenenfalls durchzuführen.*
>
> *Das Ergebnis der durchgeführten Analyse sollte als Richtschnur für die Wahl des für die Verarbeitung Verantwortlichen in Bezug auf die getroffenen Datenschutzmaßnahmen dienen. »*[22]

[21] Leitlinien der Artikel-29-Datenschutzgruppe zur Datenschutz-Folgenabschätzung (DSFA) und zur Feststellung, ob die Verarbeitung für die Zwecke der Verordnung (EU) 2016/679 „mit hohem Risiko verbunden sein kann“ (WP 248 rev.01), abrufbar unter: https://ec.europa.eu/newsroom/article29/items/611236

[22] Ziffer 137 der Leitlinien 3/2019 des Europäischen Datenschutzausschusses zur Verarbeitung personenbezogener Daten durch Videogeräte. Abrufbar unter: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_de

8. Weitere Verpflichtungen im Rahmen der DSGVO

Zusätzlich zu den in diesen Leitlinien dargelegten Grundsätzen gelten selbstverständlich alle Bestimmungen der DSGVO auch weiterhin für die Verarbeitung personenbezogener Daten im Rahmen der Videoüberwachung.

So möchte die CNPD insbesondere daran erinnern, dass, wenn der für die Verarbeitung Verantwortliche einen Dienstleister für die Installation oder Verwaltung der Videoüberwachungsanlage (z. B. ein Bewachungsunternehmen) einsetzt, dieser Dienstleister als Auftragsverarbeiter im Sinne von Art. 4 Abs. 8 DSGVO anzusehen ist, wenn er personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet. In diesem Fall muss zwischen dem Verantwortlichen und dem **Auftragsverarbeiter ein Auftragsverarbeitervertrag** geschlossen werden, der die Kriterien des Artikels 28 DSGVO erfüllt.

Darüber hinaus möchte die CNPD die Verantwortlichen und Auftragsverarbeiter auf die Verpflichtung gemäß Artikel 32 DSGVO aufmerksam machen, angemessene **technische und organisatorische Maßnahmen** zu ergreifen, um die Sicherheit und Vertraulichkeit der verarbeiteten Daten zu gewährleisten. Dies bedeutet insbesondere, dass

- Der Zugang zu den über das Videoüberwachungssystem erhobenen Daten ist auf diejenigen Personen zu beschränken, die im Rahmen ihrer Aufgaben im Hinblick auf die verfolgten Zwecke rechtmäßig Zugang zu diesen Daten benötigen.

- Der Zugang zu den Daten muss gesichert sein (z. B. durch ein sicheres Passwort und einen Benutzernamen), und jede Person, die Zugang zu den Daten hat, muss über ein individuelles Zugangskonto verfügen. Darüber hinaus muss ein Zugriffsprotokoll zur Verfügung stehen, damit im Falle eines Missbrauchs nachvollzogen werden kann, wer auf die Daten zugegriffen hat und welche Daten von diesen Personen abgerufen wurden.

Für weitere Empfehlungen, auch zu den Rechten betroffener Personen, verweist die CNPD auf die Leitlinien 3/2019 des EDSB zur Verarbeitung personenbezogener Daten durch Videogeräte.[23]

Darüber hinaus möchte die CNPD daran erinnern, dass, wenn ein Auftragsverarbeiter (z. B. ein Bewachungsunternehmen) an der Videoüberwachung beteiligt ist, ein Unterauftragsvertrag geschlossen werden muss, der die Kriterien von Artikel 28 DSGVO erfüllt. Weitere Informationen über die Vergabe von Unteraufträgen finden Sie auf der Website der CNPD.[24]

Schließlich möchte die CNPD die für die Verarbeitung Verantwortlichen auf die Bedeutung der Frage aufmerksam machen, in welchem Land die vom Videoüberwachungssystem aufgenommenen Bilder gespeichert werden, unabhängig davon, ob diese Speicherung vom für die Verarbeitung Verantwortlichen selbst oder von seinem Auftragsverarbeiter vorgenommen wird (z. B. im Falle eines Auftragsverarbeiters, der eine Lösung mit Speicherung der Bilder in der Cloud anbietet). Wenn die Bilder in ein Land außerhalb der Europäischen Union übertragen werden, muss der für die Verarbeitung Verantwortliche die

[23] Leitlinien 3/2019 des Europäischen Datenschutzausschusses zur Verarbeitung personenbezogener Daten durch Videogeräte, abrufbar unter: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_de.
[24] https://cnpd.public.lu/de/profis/obligations/subunternehmer.html

Anforderungen der DSGVO in Bezug auf die Übermittlung von Daten in Drittländer erfüllen. Weitere Informationen finden Sie auf der Website der CNPD.[25]

[25] https://cnpd.public.lu/de/thematische Dossiers/internationale Transfers-personenbezogene Daten.html