TLfDI
Thüringer Landesbeauftragter
für den Datenschutz und die Informationsfreiheit

Leitfaden

für die Videoüberwachung

durch öffentliche Stellen in Thüringen

Stand Juli 2021

Inhalt

Die Videoüberwachung im öffentlichen Raum ist ein seit Jahren aktuelles Thema und nimmt immer mehr an Bedeutung zu. Daher gilt es, die Interessen der öffentlichen Stellen (einschließlich des steigenden Sicherheitsbedürfnisses der Bevölkerung) und die Rechte der betroffenen Personen ins Gleichgewicht zu bringen.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) freut sich, Ihnen den nachfolgenden Leitfaden zur Videoüberwachung durch öffentliche Stellen zur Verfügung zu stellen. Damit soll zur Beantwortung immer wiederkehrender Fragen und Probleme sowie zur besseren Verständlichkeit der aktuellen Rechtslage beigetragen werden.

Zu den jeweiligen Punkten finden Sie Beispiele, die häufig in der Beratungstätigkeit des TLfDI thematisiert wurden.

Haben Sie Nachfragen oder Anregungen, dann nehmen Sie gern Kontakt mit dem TLfDI auf. Seine Kontaktdaten finden Sie am Ende dieses Leitfadens.

I. Wer ist öffentliche Stelle im Sinne dieses Leitfadens?

Dieser Leitfaden richtet sich im Freistaat Thüringen an die Behörden, Gerichte - soweit sie in Verwaltungsangelegenheiten tätig werden - und sonstigen öffentlichen Stellen, die Gemeinden und Gemeindeverbände, die sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts sowie deren Vereinigungen.

Für diese öffentlichen Stellen gilt das Thüringer Datenschutzgesetz (ThürDSG), siehe § 2 Abs. 1 ThürDSG.

Als öffentliche Stellen gelten auch juristische Personen und sonstige Vereinigungen des privaten Rechts, die Aufgaben der öffentlichen Verwaltung wahrnehmen und an denen eine oder mehrere juristische Personen des öffentlichen Rechts beteiligt sind (§ 2 Abs. 2 ThürDSG)

Nehmen nichtöffentliche Stellen hoheitliche Aufgaben der öffentlichen Verwaltung wahr, gelten sie insoweit als öffentliche Stellen.

Umgekehrt gelten für öffentliche Stellen, die am Wettbewerb teilnehmen, gemäß § 26 ThürDSG die Bestimmungen des Teils 2 des Bundesdatenschutzgesetzes (BDSG) sowie die §§ 3-12 ThürDSG. Maßgeblich ist dabei, dass die öffentliche Stelle Leistungen erbringt, die auch von Privaten erbracht werden (können) und sie dabei keine Monopolstellung innehat. Handelt die öffentliche Stelle hoheitlich, liegt kein Wettbewerb vor.

Beispiel: *Betreibt eine Stadt ein Freizeitbad als GmbH, nimmt sie am Wettbewerb mit anderen konkurrierenden Bädern teil. Es gelten dann die Vorschriften des Teils 2 BDSG.*

Eine spezielle Vorschrift zur Videoüberwachung durch öffentliche Stellen, die am Wettbewerb teilnehmen, hat der Gesetzgeber nicht geschaffen. Sie richtet sich nach Art. 6 Abs. 1 Satz 1 Buchst. f) Datenschutz-Grundverordnung (DS-GVO). § 4 BDSG ist nicht anwendbar, denn er gehört nicht zum 2. Teil des BDSG, auf welchen § 26 ThürDSG verweist, und ist zudem europarechtswidrig (BVerwG vom 27.03.2019, Az. 6 C 2/18).

Dieser Leitfaden richtet sich auch an die jeweiligen Datenschutzbeauftragten der öffentlichen Stellen.

Für die Thüringer Polizei gelten Sondervorschriften, wie z.B. § 33 Thüringer Polizeiaufgabengesetz, §§ 12a, 19a Versammlungsgesetz (VersammlG), auf welche hier nicht eingegangen werden soll.

II. Allgemeine Begriffsbestimmungen nach Art. 4 DS-GVO

Art. 4 DS-GVO gibt eine Vielzahl von Definitionen für Begriffe vor, die in der DS-GVO verwendet werden.

Nachfolgend sollen die für die Videoüberwachung wichtigsten Begriffe sowie ihre Definitionen wiedergegeben und mit Anmerkungen versehen werden. Sie werden im weiteren Text dieses Leitfadens entsprechend dieser Begriffsbestimmungen verwendet.

Alle weiteren Begriffsbestimmungen entnehmen Sie bitte den übrigen Ziffern des Art. 4 DS-GVO.

1. personenbezogene Daten (Art. 4 Ziff. 1 DS-GVO)

„Personenbezogene Daten“ sind *„alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als **identifizierbar** wird eine natürliche Person angesehen, die direkt oder **indirekt**, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.“*

***Beispiel:** Auch ein gefilmtes Kennzeichen stellt ein personenbeziehbares Datum dar, denn es lässt letztendlich eine eindeutige Zuordnung zur Person des Fahrzeughalters zu.*

***Beispiel:** Eine Webcam mit fest eingestelltem nicht schwenkbarem Objektiv zur Anzeige des Wetters vor Ort, die ausschließlich den Himmel abbildet, ist keine Videoüberwachung, weil keine personenbezogenen oder -beziehbaren Daten erhoben werden.*

***Beispiel:** Eine Verkehrszählungskamera mit fest eingestelltem nicht schwenkbarem und nicht zoombarem Objektiv, die aufgrund einer dauerhaft sehr niedrig eingestellten Auflösung Gesichter von Personen, auffällige Kleidungsstücke und amtliche Kennzeichen von Fahrzeugen nicht erkennen lässt, fällt nicht unter die Videoüberwachung.*

Beispiel: *Aufnahmen aus großer Höhe, die keine Daten mit einer bestimmten Person in Verbindung bringen lassen, stellen keine Videoüberwachung dar.*

2. Verarbeitung (Art. 4 Ziff. 2 DS-GVO)

„Verarbeitung" bezeichnet „*jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.*"

Als „erhoben" gelten die im Rahmen der Videoüberwachung gewonnenen Daten, aber auch die zufällige Informationswahrnehmung oder die unaufgeforderte Informationszuleitung. (Begründung zum Thür. Datenschutz-Anpassungs-und-Umsetzungsgesetz EU zu § 30 Abs. 3).

Beispiel: *Die Aufnahme durch die Kamera(Erhebung), die Speicherung auf einem Medium, die Auswertung der Aufnahmen bezüglich Straftaten, die Übermittlung an die Polizei, die Löschung der Aufnahmen und der Abgleich der Aufnahmen zur Täterermittlung sowie die Verknüpfung mit anderen personenbezogenen Daten – all dies sind Beispiele der Verarbeitung personenbezogener Daten.*

3. Verantwortlicher (Art. 4 Ziff. 7 DS-GVO)

„Verantwortlicher" ist „*die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so können der Verantwortliche beziehungsweise die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.*"

Da hier die Videoüberwachung öffentlicher Stellen näher betrachtet werden soll, ist Verantwortlicher die jeweilige öffentliche Stelle gem. § 2 Abs. 1 ThürDSG (siehe oben I.), welche die Daten im Rahmen der Videoüberwachung selbst erhebt oder

erheben lässt. Verantwortlich ist die öffentliche Stelle als solche. Sie wird vertreten durch ihre Leitung, die dann im Rahmen der rechtlichen Vertretung die tatsächliche Verantwortung trägt.

4. Auftragsverarbeiter (Art. 4 Ziff. 8 DS-GVO)

„Auftragsverarbeiter“ ist „*eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.“*

Die maßgeblichen Entscheidungen (Zweck und Mittel) trifft jedoch nach wie vor der Verantwortliche. Der Auftragsverarbeiter verarbeitet weisungsgebunden die vom Verantwortlichen überlassenen personenbezogenen Daten.

Beispiel: *Hierunter fällt z. B. ein privater Sicherheitsdienst, der das Monitoring für die Videoüberwachung im Auftrag der Gemeinde übernimmt und/oder die Firma, welche die Wartung der Kameras im Auftrag eines Landratsamtes durchführt.*

Unter Umständen kann eine öffentliche Stelle Auftragsverarbeiter für eine andere öffentliche Stelle sein.

An den Auftragsverarbeiter findet zwar eine Datenübermittlung statt (vgl. Kühling/Buchner DS-GVO, BDSG, 2. Aufl., Art. 3 Rn. 38), jedoch ist eine gesonderte Rechtsgrundlage für die „Datenübermittlung“ nicht erforderlich (so auch Kühling/Buchner, DS-GVO, BDSG, 2. Aufl. Art. 28 Rn. 15 m. w. N.). Es bedarf dafür aber eines Auftragsverarbeitungsvertrages.

Zwischen Verantwortlichem und Auftragsverarbeiter ist jedoch ein Auftragsverarbeitungsvertrag gemäß Art. 28 Abs. 3 DS-GVO abzuschließen.

Eine Formulierungshilfe dafür finden Sie auf der Homepage des TLfDI unter:

https://www.tlfdi.de/mam/tlfdi/themen/tlfdi_formulierungshilfe_fur_auftragsverarbeitungsvertraege.pdf

III. Definition „Videoüberwachung“

Den Begriff „Videoüberwachung“ definiert § 30 ThürDSG als Videobeobachtung und Videoaufnahme mit Hilfe optisch-elektronischer Einrichtungen.

1. optisch-elektronische Einrichtungen

Optisch-elektronische Einrichtungen sind sämtliche Geräte, die Bilder übertragen und/oder aufzeichnen.

Beispiel: *Webcams, Dome-Kameras*

„Der Begriff Einrichtung erfordert eine Installation, die zumindest vorübergehend ortsgebunden ist.“ (Begründung zum Entwurf des Thür. Datenschutz-Anpassungs- und-Umsetzungsgesetz EU zu § 30 Abs. 1, TLT Drs. 6/4943, S. 31)

Bespiel: *Nicht erfasst von § 30 ThürDSG sind daher Flugdrohnen, die eine erhebliche Gefahr für Datenschutzgrundrechte darstellen -* ***sofern sie personenbezogene Daten erheben*** *- und ggf. gegen Luftsicherheitsgesetze verstoßen können. Flugdrohnen,* ***die personenbezogene Daten erheben****, benötigen für ihre Anwendung im öffentlichen Bereich in Thüringen daher eine allgemeine oder bereichsspezifische Rechtsgrundlage. In Betracht kommt Art. 6 Abs. 1 S. 1 Buchst. e), 3 DS-GVO i. V. m. § 16 ThürDSG. Die Anwendbarkeit dieser Regelungen ist immer im Einzelfall zu prüfen. Es bedarf einer verfassungskonformen Auslegung. Der Verhältnismäßigkeitsgrundsatz ist zu prüfen.*

Zu berücksichtigen ist insoweit der Grundsatz der Datenminimierung (Art. 5 Abs. 1 Buchst. c) DS-GVO). Die personenbezogenen Daten müssen für die Zwecke, zu

denen sie verarbeitet werden, angemessen und erheblich sowie auf das für die Zwecke ihrer Verarbeitung notwendige Maß beschränkt sein (vgl. Erwägungsgrund 39 DS-GVO).

Gleiches gilt auch für die Ordnungsbehörden, die nach entsprechender Prüfung (siehe VII. 3.) bei Vorliegen der Voraussetzungen ggf. nach § 26 Abs. 2 Ordnungsbehördengesetz (OBG) videoüberwachen dürfen.

Details zur Zulässigkeit von Drohnen können Sie der Orientierungshilfe des TLfDI zu „Flugdrohnen im öffentlichen Bereich“ entnehmen.

2. Videobeobachtung

Mit der Videobeobachtung erfolgt die Datenerhebung. Es werden Bilder aufgenommen und auf einen Monitor weitergeleitet.

Hierunter ist zum einen die reine Fernbeobachtung zu verstehen. Dabei werden die Aufnahmen einer Beobachtungskamera 1:1 auf einen Bildschirm übertragen. Die Kamera übernimmt dabei lediglich die Aufgabe, die eine Person vor Ort haben würde, z.B. eine Wache, („verlängertes Auge“). Bildaufzeichnungen werden nicht gefertigt, d.h. es wird nicht gespeichert (ausschließlich Monitoring).

Beispiel: *Ein Wachhabender erhält auf seinen Bildschirm von verschiedenen Standorten des zu überwachenden Geländes Live-Aufnahmen, die nicht gespeichert werden.*

Unter Videobeobachtung fällt zum anderen auch eine Fernbeobachtung mit zusätzlicher Zoomfunktion. Auch hier werden die Bilder einer Beobachtungskamera in Echtzeit auf einen Bildschirm weitergeleitet. Die Kamera ist jedoch mit einer Zoom-Funktion ausgestattet, um Details, z.B. Gesichter, besser erkennen zu können. Bild**aufzeichnungen** werden nicht gefertigt.

Beispiel: *Sieht die Wache aus dem vorherigen Beispiel eine ihr verdächtig vorkommende Person, kann sie das Bild näher heranzoomen, um mehr Details erkennen zu können, ohne dass das Bild gespeichert wird.*

3. Videoaufzeichnung

Die während einer Fernbeobachtung oder Fernbeobachtung mit Zoomfunktion gefertigten Aufnahmen werden aufgezeichnet, d.h. gespeichert.

Hierunter fallen auch die Varianten, in denen die Kamera nur im Alarm- oder Bedarfsfall aufzeichnet. Es ist unerheblich, ob die Aufnahmen vom Betreiber angesehen, ausgewertet oder ungesehen gelöscht werden.

Beispiel: *Eine Kamera fertigt erst Aufnahmen, wenn eine Bewegung im zu überwachenden Bereich wahrgenommen wird und speichert diese auf einer internen Festplatte. Dabei werden die Aufnahmen nach einer festgelegten Zeit von 72 Stunden wieder überschrieben, ohne dass die Aufnahmen angesehen werden: Es liegt von Anfang an eine Videoüberwachung vor.*

Beispiel: *Auch das sogenannte „Blackbox-Verfahren“, bei welchem die Aufzeichnungen automatisch nach festgelegter Zeitspanne gelöscht/überschrieben und nur dann gesichtet werden, wenn entsprechende Vorkommnisse vorliegen, fällt unter die Videoüberwachung.*

4. Ist jede Aufnahme eine Verarbeitung personenbezogener Daten im Sinne des ThürDSG und der DS-GVO?

a) Fehlender Personenbezug und fehlende Personenbeziehbarkeit

Eine Verarbeitung personenbezogener Daten und damit eine Videoüberwachung im datenschutzrechtlichen Sinne liegt nicht vor, wenn die Aufnahme keinen direkten oder indirekten Bezug zu einer bestimmten Person herstellen kann. Voraussetzung ist jedoch, dass einzelne Personen oder zuordnungsfähige andere personenbezogene bzw. personenbeziehbare Merkmale nicht erkennbar abgebildet sind. Die Videoübertragung oder -aufnahme muss so eingestellt sein, dass das Verhalten einzelner Personen weder zeitlich noch räumlich auch bei einem längeren Beobachtungszeitraum nachvollzogen werden kann.

Dies kann z. B. aufgrund der Verpixelung oder der Kameraposition, der fehlenden Zoommöglichkeit und entsprechend großer Entfernung oder mit niedriger Auflösung erreicht werden. Zu beachten ist jedoch, dass diese Funktionen dann dauerhaft eingeschaltet (Verpixelung) bzw. ausgeschaltet sein müssen und die Wiederein- bzw. -ausschaltung durch berechtigte Personen mittels technisch-organisatorischer Maßnahmen, z.B. Dienstanweisungen, verhindert wird.

***Beispiele für nicht personenbezogene oder-beziehbare Daten** finden Sie unter II.1.*

b) Kameraattrappen / unzutreffende Hinweise auf Videoüberwachung

Kameraattrappen verarbeiten keine personenbezogenen Daten. Jedoch können sowohl sie als auch unzutreffende Hinweise auf eine Videoüberwachung (Hinweisschilder, obwohl keine Kamera vorhanden ist) einen Überwachungsdruck erzeugen, der aufgrund der Verdachtssituation geeignet ist, Persönlichkeitsrechte zu verletzen. Es ist von außen nicht erkennbar, dass die Funktionsfähigkeit der Kamera fehlt oder gar keine Kamera installiert ist.
Daher können ggf. zivilrechtliche Abwehransprüche ausgelöst werden.
Der TLfDI ist bei der Verwendung von Kameraattrappen und auch für das Anbringen von Hinweisschildern ohne Installation einer Kamera nicht zuständig, weil keine personenbezogenen Daten verarbeitet werden.

c) Tonaufzeichnungen

Tonaufzeichnungen stellt § 201 StGB („Verletzung der Vertraulichkeit des Wortes“) unter Strafe. Danach ist es verboten, das nichtöffentliche Wort eines anderen auf einem Tonträger aufzunehmen oder eine so hergestellte Aufnahme zu gebrauchen oder Dritten zugänglich zu machen sowie abzuhören oder das so aufgenommene oder abgehörte nichtöffentliche Wort eines anderen öffentlich mitzuteilen.
Sofern eine Videoüberwachungskamera über eine Audiofunktion verfügt, ist diese daher irreversibel zu deaktivieren.

IV. Warum ist die Videoüberwachung so kritisch zu betrachten? – Verletzte Rechte der aufgenommenen Person

Um die Tragweite einer Entscheidung zur Einrichtung einer Videoüberwachung verdeutlichen zu können, ist es notwendig, zu betrachten, ob und ggf. welche Rechte der betroffenen Personen hierdurch beeinträchtigt sind:

Sowohl bei einer reinen Fernbeobachtung als auch bei der Fernbeobachtung mit Zoom-Funktion beginnt die Beeinträchtigung der Rechte der betroffenen Person bereits mit Betreten des überwachten Bereichs. Bei der Fernbeobachtung mit Zoom

ist bereits die Möglichkeit des Zoomens ausreichend, um die Rechte Betroffener zu beeinträchtigen. Die Beobachtung endet zwar sofort bei Verlassen dieses Bereichs. Die Beeinträchtigungen der Rechte der betroffenen Person bleiben jedoch bestehen, denn die Person kann nicht mehr kontrollieren, was mit ihren Daten geschieht. Dabei ist unerheblich, ob die Person vom Beobachter am Bildschirm gesehen wurde oder nicht.

Bei der Videoaufzeichnung können die Aufnahmen der beobachteten Person beliebig wiederholt abgespielt, an Dritte weitergegeben oder anderweitig verarbeitet werden. Hier hat die betroffene Person erst recht keine Kontrolle darüber, was mit ihren Daten geschieht. Auch hierbei ist es unerheblich, ob die aufgezeichneten Daten angesehen, ausgewertet oder ungesehen gelöscht werden.

Wie wirkt sich der Verlust der Kontrolle über die eigenen Daten auf die Rechte der betroffenen Personen aus? Nachfolgend werden diese Rechte und ihre Grundlagen skizziert.

1. Art. 8 der Charta der Grundrechte der Europäischen Union (EU-Grundrechte-Charta)

Bereits aus der Aufnahme des Art. 8 in die EU-Grundrechte-Charta wird deutlich, welchen hohen Stellenwert der Datenschutz im Bereich der Europäischen Union innehat:

„(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.“

Jede Verarbeitung personenbezogener Daten - und damit auch die Videoüberwachung - greift in dieses geschützte Grundrecht ein. Es sind daher klare Grundsätze zu den Voraussetzungen der Datenverarbeitung, zu Auskunfts-, Berichtigungs- und Kontrollrechten aufgestellt. Datenverarbeitung – und damit auch Videoüberwachung – haben ausschließlich, wie es Art. 8 Abs. 2 Grundrechte-Charta bestimmt

a) nach Treu und Glauben

und

b) für festgelegte Zwecke

und

c) mit Einwilligung der betroffenen Person

oder

d) auf gesetzlicher Grundlage

zu erfolgen.

Zu den Grundsätzen des Datenschutzes finden Sie weitere Ausführungen unten unter VI.

2. Recht auf informationelle Selbstbestimmung (BVerfG)

Das Recht auf informationelle Selbstbestimmung ist im Grundgesetz nicht explizit geregelt. Es wurde vom Bundesverfassungsgericht (BVerfG) in seinem sogenannten Volkszählungs-Urteil vom 15.12.1983 (1 BvR 209/83; 1 BvR 269/83; 1 BvR 362/83;1 BvR 420/83; 1 BvR 440/83; 1 BvR 484/83) als Ausprägung des allgemeinen Persönlichkeitsrechts nach Art. 2 Abs. 1, Art. 1 Abs. 1 GG anerkannt und weit gefasst.

Das Recht auf informationelle Selbstbestimmung ist das Recht des Einzelnen, grundsätzlich über die Preisgabe und Verwendung seiner personenbezogenen Daten selbst zu bestimmen.

„Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.

Dieses Recht auf "informationelle Selbstbestimmung" ist nicht schrankenlos gewährleistet. Der Einzelne hat nicht ein Recht im Sinne einer absoluten, uneinschränkbaren Herrschaft über "seine" Daten; er ist vielmehr eine sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit. Information, auch soweit sie personenbezogen ist, stellt ein Abbild sozialer Realität dar, das nicht ausschließlich dem Betroffenen allein zugeordnet werden kann. Das Grundgesetz hat, wie in der Rechtsprechung des Bundesverfassungsgerichts mehrfach hervorgehoben ist, die Spannung Individuum - Gemeinschaft im Sinne der Gemeinschaftsbezogenheit und Gemeinschaftsgebundenheit der Person entschieden (BVerfGE 4, 7 [15]; 8, 274 [329]; 27, 1 [7]; 27, 344 [351 f.]; 33, 303 [334]; 50, 290 [353]; 56, 37 [49]). Grundsätzlich muss daher der Einzelne Einschränkungen seines Rechts auf informationelle Selbstbestimmung im überwiegenden Allgemeininteresse

hinnehmen.“ (BVerfG vom 15. Dezember 1983, „Volkszählungsurteil“, 1 BvR 209/83, Rdn. 147, 148)
Die freie Selbstbestimmung ist gefährdet durch die Bedingungen der modernen Datenverarbeitung und damit auch durch die Videoüberwachung. Zwar sind Einschränkungen dieses Rechts möglich. Sie müssen jedoch auf einer gesetzlichen Grundlage erfolgen, die zwischen dem Geheimhaltungsinteresse des Betroffenen und dem öffentlichen Informationsinteresse genauestens abwägt.

3. Art. 6 Abs. 2 und 3 Thüringer Verfassung

Auch nach der Verfassung des Freistaats Thüringen unterliegt der Schutz personenbezogener Daten einem hohen Schutz.

Artikel 6 der Thüringer Verfassung regelt:

(1) Jeder hat das Recht auf Achtung und Schutz seiner Persönlichkeit und seines privaten Lebensbereiches.

(2) Jeder hat Anspruch auf Schutz seiner personenbezogenen Daten. Er ist berechtigt, über die Preisgabe und Verwendung solcher Daten selbst zu bestimmen.

(3) Diese Rechte dürfen nur auf Grund eines Gesetzes eingeschränkt werden. Den Belangen historischer Forschung und geschichtlicher Aufarbeitung ist angemessen Rechnung zu tragen.

(4) Jeder hat nach Maßgabe der Gesetze ein Recht auf Auskunft darüber, welche Informationen über ihn in Akten und Dateien gespeichert sind und auf Einsicht in ihn betreffende Akten und Dateien.

Artikel 6 Abs. 2 Satz 2 der Thüringer Verfassung erteilt die Berechtigung, über Preisgabe und Verwendung personenbezogener Daten selbst zu bestimmen und macht damit die Einwilligung in den Grundrechtseingriff möglich. Im öffentlichen

Bereich kommt die Einwilligung jedoch nur ausnahmsweise zum Tragen, siehe unten VII. 1.1.
Zudem – und das ist wesentlich - kann im Sinne der oben erwähnten Volkszählungs-Entscheidung des Bundesverfassungsgerichts auch gem. Art. 6 Abs. 3 Satz 1 der Thüringer Verfassung dieses Grundrecht vom Gesetzgeber eingeschränkt bzw. konkretisiert werden.

4. Recht am eigenen Bild (§§ 22 ff. KunstUrhG)

Das Recht am eigenen Bild ist eine weitere Ausprägung des allgemeinen Persönlichkeitsrechts. § 22 Kunsturhebergesetz (KunstUrhG) stellt dabei sicher, dass jeder selbst darüber entscheiden darf, ob Bilder von seiner Person öffentlich verwendet werden.

§ 22 Satz 1 KunstUrhG bestimmt:

„Bildnisse dürfen nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden.“

Nach dem Tode bedarf es bis zum Ablauf von 10 Jahren der Einwilligung der Angehörigen.

Gem. § 24 KunstUrhG dürfen von Behörden für Zwecke der Rechtspflege und der öffentlichen Sicherheit Bildnisse ohne Einwilligung des Berechtigten sowie des Abgebildeten oder seiner Angehörigen *vervielfältigt, verbreitet und öffentlich zur Schau gestellt werden*. Hier hat jedoch eine Verhältnismäßigkeitsprüfung und daher eine genaue Abwägung stattzufinden.

5. Höchstpersönlicher Lebensbereich (§ 201a StGB)

§ 201a Strafgesetzbuch (StGB) schützt den höchstpersönlichen Lebensbereich vor der Verletzung durch Bildaufnahmen.

Geschützt sind hiernach Personen vor Herstellung und Übertragung unbefugter Bildaufnahmen und die dadurch entstehende Verletzung ihres höchstpersönlichen Lebensbereichs in bestimmten Situationen und örtlichen Bereichen.

Hierunter fällt ggf. die Videoüberwachung in besonders sensiblen Bereichen, *wie z.B.*

Beispiel: *Zu den besonders sensiblen Bereichen gehören Umkleideräume und Toiletten*.

6. Mitbestimmung der Personalvertretung (§§ 68 Abs. 1 Nr. 9, Abs. 2, 73 ThürPersVG)

Im Rahmen der Videoüberwachung bestimmter Bereiche sind neben den Besuchern häufig auch die Mitarbeiterinnen und Mitarbeiter der öffentlichen Stelle betroffen. Das Thüringer Personalvertretungsgesetz (ThürPersVG) sieht in diesem Fall die Mitwirkung der Personalvertretung vor, die auf die Wahrung des

Datenschutzes für alle Beschäftigten hinzuwirken hat, § 68 Abs.1 Nr. 9 ThürPersVG.

Der Personalrat ist frühzeitig zu unterrichten und in die Entscheidung einzubeziehen. Näheres siehe unten VIII.6.

V. Datenschutzregime: DS-GVO oder JI-Richtlinie?

Für öffentliche Stellen gelten der 1. und 2. Abschnitt des ThürDSG in Verbindung mit der DS-GVO.

Ausnahmen gelten nur für ein bestimmtes Tätigwerden der Ordnungsbehörde. Auch bei ihr fallen jegliche Datenverarbeitungen unter den 1. und 2. Abschnitt des ThürDSG und die DS-GVO, solange und soweit wie das von ihr geführte Verfahren nicht in ein konkretes Ordnungswidrigkeitenverfahren übergeht (Mitteilung des BMI vom 04. Januar 2019). Ob sich das Verfahren im Stadium des Verwaltungsverfahrens befindet oder bereits ein konkretes Ordnungswidrigkeitenverfahren vorliegt, ist maßgebend

dafür, ob die Behörde ihr Handeln auf das Thüringer Verwaltungsverfahrensgesetz (ThürVwVfG) oder das Gesetz über Ordnungswidrigkeiten (OWiG) zu stützen hat.
Die Ermittlung, Verfolgung, Ahndung und Vollstreckung von Ordnungswidrigkeiten fallen unter den Anwendungsbereich der Richtlinie (EU) 2016/680 (JI-Richtlinie). Die JI-Richtlinie ist in Thüringen in Abschnitt 3 (§§ 31ff. des ThürDSG) umgesetzt.

Unter Umständen ist also im laufenden Verfahren ein Wechsel des Datenschutzregimes zu beachten.

VI. Grundprinzipien des Datenschutzrechts gelten auch für Videoüberwachung

Um in die Rechte der aufgenommenen Personen so wenig wie möglich einzugreifen, sind die nachfolgenden Grundprinzipien des Datenschutzrechts von den öffentlichen Stellen auch im Rahmen der Videoüberwachung einzuhalten. Sie sind bereits in Art. 8

der EU-Grundrechte-Charta aufgeführt (siehe oben IV.1.) und in der DS-GVO detailliert geregelt.

Art. 5 DS-GVO gibt die Grundsätze der Datenverarbeitung wieder, die nachfolgend insbesondere im Zusammenhang mit der Videoüberwachung betrachtet werden sollen. Der Verantwortliche hat für ihre Einhaltung zu sorgen und muss ihre Einhaltung nachweisen können. Er ist also rechenschaftspflichtig.

1. Rechtmäßigkeit, Verarbeitung nach Treu und Glauben (Art. 5 Abs. 1 Buchst. a) DS-GVO)

Nach Artikel 5 Abs. 1 Buchst. a) DS-GVO müssen personenbezogene Daten auf rechtmäßige Weise und nach Treu und Glauben verarbeitet werden. Rechtmäßig ist die Verarbeitung nur, wenn eine der in Art. 6 Abs. 1 DS-GVO genannten Rechtsgrundlagen (siehe unten VII.1 ff) vorliegt.

Eine Verarbeitung nach Treu und Glauben meint einen fairen Umgang des Verantwortlichen mit den Daten, auch im Rahmen der Videoüberwachung.

2. Transparenz (Art. 5 Abs. 1 Buchst. a), 12 DS-GVO)

Die Verarbeitung hat in einer für die betroffene Person nachvollziehbaren Art und Weise zu erfolgen. Hieraus resultieren die Informationspflichten gem. Art. 13/14 DS-GVO. Die betroffene Person ist daher z.B. zu informieren über den Zweck und den Umfang der Datenverarbeitung sowie, an wen die Daten übermittelt werden. Daher ist in einem videoüberwachten Gebiet ausdrücklich auf die Videoüberwachung hinzuweisen. Auf dem Hinweisschild sind die Informationen gemäß Art. 13/14 DS-GVO zu erteilen. Siehe dazu auch VII. 2.2.

Transparenz heißt auch in leicht zugänglicher Art und Weise, präzise und verständlich sowie in klarer und einfacher Sprache. Entsprechend sind die Hinweisschilder zu gestalten. Die Verwendung von Piktogrammen unterstützt die Verständlichkeit.

3. Zweckbindung (Art. 5 Abs. 1 Buchst. b) DS-GVO)

Es besteht eine enge Zweckbindung für die Datenverarbeitung. Personenbezogene Daten dürfen somit nur für festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden.

Änderungen des Zweckes der Verarbeitung sind nur unter sehr engen Voraussetzungen erlaubt, wenn sie mit dem ursprünglichen Erhebungszweck vereinbar sind, Art. 5 Abs. 1 Buchst. b) i. V. m. Art. 6 Abs. 4 DS-GVO und § 17 ThürDSG.

Der Zweck der Videoüberwachung ist zwingend vor der Installation festzulegen und zu dokumentieren. Abweichungen von diesem Zweck sind im Rahmen der Videoüberwachung nach der spezialrechtlichen Regelung des Art. 30 Abs. 4 ThürDSG möglich. Siehe dazu unter VII 2.4.

4. Datenminimierung (Art. 5 Abs. 1 Buchst. c) DS-GVO)

Die personenbezogenen Daten müssen für den Zweck angemessen sowie auf das für diesen Zweck notwendige Maß beschränkt werden.

Dies gilt auch und ganz besonders für die Videoüberwachung. Eine flächendeckende Videoüberwachung ist unzulässig.

Beispiel: *Bereiche, die nach dem festgelegten Zweck nicht relevant sind, müssen von vornherein aus der Videoüberwachung ausgespart werden. Hierbei sind auch die technischen Möglichkeiten zu nutzen, z.B. Bildausschnitte zu schwärzen.*

5. Datenrichtigkeit (Art. 5 Abs. 1 Buchst. d) DS-GVO)

Es sind alle erforderlichen Maßnahmen zu ergreifen, damit die personenbezogenen Daten sachlich richtig und erforderlichenfalls auf dem neuesten Stand sind. Unrichtige Daten sind unverzüglich zu löschen oder zu berichtigen.

6. Speicherbegrenzung (Art. 5 Abs. 1 Buchst. e) DS-GVO)

Die personenbezogenen Daten dürfen nur in der Form gespeichert werden, die eine Identifizierung der Person nur so lange ermöglicht, wie es für den festgelegten Zweck erforderlich ist.

Bei der Videoüberwachung ist daher zu prüfen und festzulegen, wie lange die Speicherung der Aufnahmen erfolgt. Sie ist zeitlich so kurz wie möglich zu halten.

Beispiel: *Ein in einer städtischen Behörde tätiger Wachdienst ist täglich vor Ort und berechtigt, Videoaufzeichnungen zu sichten. In diesem Fall ist eine Speicherung von längstens 72 Stunden ausreichend, um entsprechende Maßnahmen zu ergreifen, wenn Straftaten aufgezeichnet wurden.*

7. Datensicherheit (Art. 5 Ab. 1 Buchst. f); Art. 32 DS-GVO)

Die personenbezogenen Daten sind vor unbefugter oder unrechtmäßiger Verarbeitung oder vor Verlust zu schützen. Hierzu haben der Verantwortliche oder auch Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen zu ergreifen.

Dies bedeutet, dass bei der Videoüberwachung vor allem die Speichermedien vor dem Zugriff unbefugter Personen oder Zerstörung zu schützen sind. Es gilt zum einen physische Schutzmaßnahmen, z.B. durch abschließbare Räume oder Schränke, zum anderen auch organisatorische Maßnahmen zu ergreifen. Hierfür sind beispielsweise die für den Zugriff befugten Personen vorab schriftlich festzulegen (siehe auch unten XI.4., 5., 8.)

Der Sicherheitsstand muss im Verhältnis zum Risiko stehen. Ggf. sind die personenbezogenen Daten zu verschlüsseln.

VII. Umsetzung der Grundprinzipien des Datenschutzrechts für die Videoüberwachung – die speziellen Voraussetzungen

Die Videoüberwachung ist eine Form der Datenverarbeitung.

Grundsätzlich gilt das Prinzip, dass jede Verarbeitung personenbezogener Daten erst einmal verboten ist (Verbotsprinzip).
Jede Videoüberwachung bedarf daher zunächst einer Rechtsgrundlage.

Vorweggeschickt sei: Die Aufklärung von Straftaten und Ordnungswidrigkeiten ist nur ein Nebeneffekt der Videoüberwachung, nie Hauptzweck.
Die Verfolgung von Straftaten obliegt Polizei, Staatsanwaltschaft und Gerichten, nicht den öffentlichen Stellen i. S. d. § 2 ThürDSG. Auch existiert keine Rechtsgrundlage dafür, mit einer Videoüberwachung Ordnungswidrigkeiten zu verfolgen. Dies kann für „normale“ Behörden ohne Sonderbefugnisse nie ausschließlicher Zweck der Videoüberwachung sein.

1. Rechtsgrundlagen nach DS-GVO

Die Verarbeitung personenbezogener Daten ist nur dann rechtmäßig, wenn eine der in Art. 6 Abs. 1 DS-GVO genannten Bedingungen erfüllt ist.

1.1. Einwilligung

Für die Videoüberwachung durch öffentliche Stellen kommt eine Einwilligung **nicht in Betracht**. Sie setzt ein aktives Verhalten und eine unmissverständliche

Willensbekundung voraus und muss freiwillig erfolgen. Allein der Aufenthalt in einem videoüberwachten Bereich stellt keine Einwilligung dar.

Zudem ist zu beachten, dass zwischen Bürger und öffentlicher Stelle zumeist ein Ungleichgewicht oder ein Unter-/Überordnungsverhältnis besteht, welches die Freiwilligkeit einer Einwilligungserklärung in Frage stellt. Die Behörden treten als Hoheitsträger auf. Sie vertreten den Staat gegenüber dem Bürger. Inwieweit in diesem Verhältnis eine Einwilligung freiwillig erfolgen würde, ist sehr zweifelhaft.

1.2. Erfüllung eines Vertrages

Videoüberwachung in Erfüllung eines Vertrages kommt **nicht in Betracht**, da die öffentliche Stelle dann in der Regel nicht als Verantwortlicher, sondern als Auftragsverarbeiter tätig wird (siehe Definitionen unter II.).

1.3. Erfüllung einer rechtlichen Verpflichtung

Gemeint ist seitens des EU-Gesetzgebers ausschließlich die rechtliche **Verpflichtung durch Rechtsvorschriften**, nicht durch Rechtsgeschäfte, die nach deutschem Recht ebenfalls rechtliche Verpflichtungen nach sich ziehen.

Gemäß Art. 6 Abs. 3 DS-GVO wird die Rechtsgrundlage für die Verarbeitung personenbezogener Daten nach Art. 6 Abs. 1 Satz 1 Buchst. c) DS-GVO durch das Recht der Europäischen Union oder der Mitgliedsstaaten festgelegt. Für öffentliche Stellen in Thüringen ist eine rechtliche Verpflichtung in Form einer Rechtsvorschrift im Zusammenhang mit der Videoüberwachung landesrechtlich jedoch nicht normiert. § 30 ThürDSG spricht gerade keine Verpflichtung aus.

In Betracht kämen als Rechtsgrundlage auch kommunale Satzungen. Allerdings müssten diese dann präzise die Verarbeitungsvoraussetzungen regeln, wie in Art. 6 Abs. 3 Buchst. b) DS-GVO gefordert. Bislang ist dem TLfDI eine kommunale Satzung im Zusammenhang mit Videoüberwachung, die diese Voraussetzungen erfüllt, nicht bekannt.

1.4. Erforderlichkeit zum Schutz lebenswichtiger Interessen betroffener oder anderer natürlicher Personen

Nach dem Erwägungsgrund (EG) 46 zur DS-GVO sollten personenbezogene Daten nur dann aufgrund eines lebenswichtigen Interesses einer anderen natürlichen Person verarbeitet werden, wenn die Verarbeitung nicht auf eine andere Rechtsgrundlage gestützt werden kann. Als Beispiel wird genannt, dass die Verarbeitung aus humanitären Zwecken einschließlich Überwachung von Epidemien und deren Ausbreitung sowie in humanitären Notfällen erforderlich sein soll. Die Videoüberwachung stellt für derartige Zwecke jedoch grundsätzlich kein geeignetes Mittel dar, so dass Art. 6 Abs. 1 Satz 1 Buchst. d) DS-GVO als Rechtsgrundlage nicht in Betracht kommt.

1.5. Erforderlichkeit zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde

Im Rahmen der Videoüberwachung durch öffentliche Stellen ist der Hauptanwendungsbereich Art. 6 Abs. 1 Satz 1 Buchst. e) DS-GVO. Hiernach muss die Verarbeitung für die Wahrnehmung einer **Aufgabe**, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde, erforderlich sein.

Gem. Artikel 6 Abs. 3 DS-GVO wird die Rechtsgrundlage hierfür durch das Recht der Europäischen Union oder der Mitgliedsstaaten (sogenannte Öffnungsklausel) festgelegt.

Die Videoüberwachung durch öffentliche Stellen ist für den Freistaat Thüringen in § 30 ThürDSG geregelt. Er bildet in Verbindung mit Art. 6 Abs. 1 Satz 1 Buchst. e) und Abs. 3 Satz 1 Buchstabe b) DS-GVO eine mögliche Rechtsgrundlage der Videoüberwachung.

Eine weitere mögliche Rechtsgrundlage kann § 26 Abs. 2 ThürOBG sein.

1.6. Wahrung berechtigter Interessen

Für Behörden in Erfüllung ihrer Aufgaben gilt Art. 6 Abs. 1 Satz 1 Buchst. f) DS-GVO **nicht** (siehe Art 6 Abs. 1 S. 2 DS-GVO).

2. § 30 ThürDSG i. V. m. Art. 6 Abs. 1 Satz 1 Buchst. e und Abs. 2 DS-GVO

In § 30 ThürDSG i. V. m. Art. 6 Abs. 1 Satz 1 Buchst. e), Abs. 2 DS-GVO ist speziell geregelt, unter welchen Voraussetzungen in Thüringen die Videoüberwachung durch öffentliche Stellen zulässig und wie diese auszugestalten ist.

2.1. Zulässigkeitsvoraussetzungen (§ 30 Abs. 1 ThürDSG)

Gem. § 30 Abs. 1 ThürDSG ist die Videoüberwachung nur zulässig, *„wenn dies zur Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe oder in Ausübung öffentlicher Gewalt*

(1)
zum Schutz von Personen, die der überwachenden Stelle angehören oder sie aufsuchen, oder

(2)
zum Schutz von Sachen, die der zu überwachenden Stelle oder den Personen nach Nummer 1 gehören, erforderlich ist. Es dürfen keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der betroffenen Person überwiegen.“

Hinsichtlich der Verfolgung von Straftaten und Ordnungswidrigkeiten ist nochmals darauf hinzuweisen, dass diese nicht Zweck einer Videoüberwachung nach § 30 ThürDSG sind. Vielmehr sind die Zwecke des § 30 Abs. 1 ThürDSG genauestens zu prüfen. Erst wenn diese vorliegen, kann **im Rahmen einer Zweckänderung eine Übermittlung** an die zur Verfolgung von Straftaten und Ordnungswidrigkeiten von erheblicher Bedeutung zuständigen Behörden geprüft und vorgenommen werden, vgl. § 30 Abs. 4 ThürDSG.

Die einzelnen Voraussetzungen des § 30 Abs. 1 ThürDSG:

a) „zur Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe oder in Ausübung öffentlicher Gewalt“
Ausschließlich zur Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe oder in Ausübung öffentlicher Gewalt ist eine Videoüberwachung durch öffentliche Stellen gerechtfertigt.

Im öffentlichen Interesse liegende Aufgaben sind alle Aufgaben, die der öffentlichen Stelle gesetzlich übertragen wurden. Gemeint ist ferner die Wahrnehmung von Aufgaben zumindest auch im Interesse des Gemeinwohls oder in Ausübung hoheitlicher Befugnisse.
Für private Zwecke dürfen öffentliche Stellen keine Videoüberwachung einrichten oder nutzen.

b) „zum Schutz von Personen, die der überwachenden Stelle angehören oder sie aufsuchen“

Zweck der Videoüberwachung kann der Schutz von Personen sein, die sich dort aufhalten, entweder, weil sie der überwachenden Stelle angehören oder weil sie sie aufsuchen. Es soll ein störungsfreier Benutzerverkehr von öffentlichen Stellen und in ihren Gebäuden sichergestellt werden.

Der TLfDI interpretiert den Gesetzestext dahingehend, dass auch die Personen, die der zu überwachenden Stelle angehören oder diese aufsuchen, vom Schutz umfasst sind. Überwachende und zu überwachende Stelle können außerdem zusammenfallen.

c) „Schutz von Sachen, die der zu überwachenden Stelle oder den Personen nach Nummer 1 gehören“

Weiterer Zweck der Videoüberwachung kann der Schutz von Sachen sein. Es sind sowohl Eigentum als auch Besitz der zu überwachenden Stelle, der überwachenden Stelle oder der Personen, die diesen angehören oder sie aufsuchen, geschützt.

Hierunter fallen auch die Gebäude der öffentlichen Stelle. Eine ungestörte Nutzung soll sichergestellt werden. Hierbei ist es unerheblich, ob die überwachende Stelle und die zu überwachende Stelle identisch sind. Jedenfalls schließt die seitens des Gesetzgebers gewählte Formulierung auch hier nicht aus, dass die überwachte und die überwachende Stelle identisch sind.

d) „erforderlich“

Die Videoüberwachung muss erforderlich sein, um den festgelegten Zweck (Schutz von Personen oder Sachen) zu erreichen.

- **Gefährdung und Prognose**

Der Begriff „erforderlich“ setzt eine Notwendigkeit der Videoüberwachung in Form einer Gefährdung voraus, auch wenn dies nicht ausdrücklich dem Gesetzestext zu entnehmen ist. Gefährdung ist hier nicht im Sinne einer polizeirechtlich oder gefahrenabwehrrechtlich geregelten Gefahr zu verstehen. Der Gesetzgeber verlangt zum Schutz der Rechtsgüter nach § 30 Abs. 1 ThürDSG eine Erforderlichkeit. Diese beinhaltet eine konkrete Gefährdung, andernfalls ist ein Schutz und damit eine Videoüberwachung nicht erforderlich (so auch BayLfD

„Videoüberwachung durch bayerische öffentliche Stellen“ Rdn. 46 und der LfDI Baden-Württemberg „Videoüberwachung durch öffentliche Stellen“ S. 10/11 mit ähnlichen Formulierungen einer „Erforderlichkeit in den jeweiligen Landesdatenschutzgesetzen). Eine flächendeckende Videoüberwachung ist unzulässig. Daher genügt die rein theoretische Möglichkeit einer Gefährdung nicht. Vielmehr ist im Einzelnen zu prüfen, ob in der Vergangenheit konkrete sicherheitsrelevante Vorkommnisse im Überwachungsbereich gegeben waren, und es ist eine **Prognose** zu erstellen. Es muss also eine Gefährdungslage gegeben sein und die Verletzung von Rechtsgütern wahrscheinlich eintreten.

Die Vorkommnisse der Vergangenheit müssen nach Ansicht des TLfDI so spezifiziert wie möglich und nachweisbar sein. Dies bedeutet, diese Ereignisse sind mit Ort, Datum, Uhrzeit, Art des Vorfalls und Schadenshöhe sorgfältig zu dokumentieren. Sollten Strafanzeigen erstattet worden, Hinweise oder Beschwerden oder Schadensmeldungen an Versicherungen eingereicht worden sein, wären auch diese zu dokumentieren. Es empfiehlt sich, eine zeitlich und räumlich geordnete Aufstellung zu fertigen.

Je genauer die Dokumentation vorgenommen wird, umso genauer kann die Prognose erstellt werden. Dies führt dazu, dass die Videoüberwachung dann ebenfalls genauer zeitlich und räumlich eingegrenzt werden kann.

Beispiel: *07.08.2019, ca. 22 Uhr, Rückseite Gebäude… (Adresse), Sachbeschädigung durch Graffiti über die gesamte Gebäudefront im Erdgeschoss, Schadenshöhe…, Strafanzeige erstattet, Az. Staatsanwaltschaft Erfurt…, Schaden der Versicherung … am … gemeldet*

-> erfolgen derartige Sachbeschädigungen immer nur in den Nachtstunden und im Erdgeschoss, ist die Videoüberwachung räumlich auf das Erdgeschoss und zeitlich auf diese Nachtstunden zu begrenzen.

Zu beachten sind zudem die Gewichtung des gefährdeten Rechtsgutes und die Höhe des voraussichtlich eintretenden Schadens. Daher sind die Anforderungen an die Prognose bei einer Gefährdung von Menschen (Leben, Gesundheit, Freiheit)

geringer als bei einer Gefährdung von Sachen und hier wiederum evtl. abgestuft nach dem Wert der Sache oder dem (finanziellen) Aufwand der Beseitigung von Beeinträchtigungen.

Beispiel: *Soll die Videoüberwachung zum Zweck der Verhinderung weiterer Brandstiftungen in einem Gebäude erfolgen, in welchem sich regelmäßig Menschen aufhalten, sind an die Wahrscheinlichkeit des Eintritts eines Schadens geringere Anforderungen zu stellen, als wenn Sachbeschädigungen an einer Gebäudefassade verhindert werden sollen.*
Hier wiederum sind die Anforderungen an die Prognose geringer, wenn eine nur sehr aufwändig zu reinigende unter Denkmalschutz stehende Fassade betroffen ist, als wenn es sich um eine einfache verputzte Wand handelt.

Auf keinen Fall ausreichend sind ein unspezifisches Unsicherheitsgefühl oder Vermutungen.

❖ **Verhältnismäßigkeitsgrundsatz**

Bejaht die öffentliche Stelle das Vorliegen der bisher dargestellten Voraussetzungen des § 30 Abs. 1 ThürDSG, hat sie des Weiteren nach pflichtgemäßem Ermessen (§ 40 Thüringer Verwaltungsverfahrensgesetz - ThürVwVG) zu entscheiden, ob und wie sie die Videoüberwachung durchführt.

Die gesetzlichen Grenzen des Ermessens im Sinne von § 40 ThürVwVfG sind die oben unter IV. dargelegten (Grund-) Rechte der Betroffenen. Diese sind abzuwägen mit dem Interesse der öffentlichen Stelle an der Durchführung der Videoüberwachung. Die Abwägung erfolgt entsprechend des Verhältnismäßigkeitsgrundsatzes wie folgt:

- **Geeignetheit der Videoüberwachung**
  Ist die Videoüberwachung, so wie sie konkret geplant ist, ein **geeignetes Mittel**, um den gewünschten Schutz überhaupt herzustellen? Dies ist nur dann der Fall, wenn eine Verminderung der Gefährdung eintreten würde. Prävention ist ein anerkanntes Schutzziel. Es kann jedoch nur erreicht werden, wenn die Videoüberwachung das Verhalten eventueller Störer auch steuern würde.

Beispiel: *Zweck ist der Schutz von Personen, die die überwachende Stelle aufsuchen. Eine reine Videoaufzeichnung im Black-Box-Verfahren ist zur Verhinderung von Gefährdungen von Personen nicht geeignet, weil mangels Kenntnis der Aufnahme keine direkte Eingriffsmöglichkeit besteht. Diese ist nur gegeben, wenn ein Monitoring erfolgt und beispielweise das Sicherheitspersonal zeitnah eingreifen kann. Die Täterermittlung im Nachhinein ist kein Schutzzweck des*
§ 30 Abs. 1 ThürDSG und kann daher im hier interessierenden Zusammenhang nie Zweck einer Videoüberwachung sein.

Werden an einem Objekt mehrere Kameras eingesetzt, ist die Geeignetheit für den Standort jeder einzelnen Kamera zu prüfen.

- **Erforderlichkeit**
  - **mildestes Mittel?**

    Ferner muss die Videoüberwachung erforderlich sein. Hierbei ist zu prüfen, ob sie das mildeste Mittel ist, um den festgelegten Zweck zu erreichen. Dies ist nur dann der Fall, wenn der zuvor festgelegte Zweck nicht mit anderen zumutbaren Mitteln erreicht werden kann, die weniger in die Rechte der Betroffenen eingreifen würden.

    Deshalb muss vor Installation einer Videoüberwachungsanlage genauestens geprüft werden, ob bauliche, organisatorische oder technische Alternativen bestehen, die ebenfalls den gewünschten Zweck erfüllen.

    Beispiel: *Das Gelände eines kommunalen Entsorgungshofes könnte mit einer Umzäunung statt einer Videoüberwachung geschützt werden.*

    Weitere Beispiele *für mögliche Alternativen zur Videoüberwachung:*

    - *längere Öffnungszeiten,*
    - *Installation einer Alarmanlage,*
    - *Einbau von Sicherheitsschlössern*
    - *Einbau einbruchsicherer Fenster und Türen,*

- *spezielle Oberflächenbeschichtungen gegen Verschmutzungen wie Graffiti*
- *bessere Ausleuchtung des Geländes*
- *Rückschnitt von Sträuchern und ähnlichem Bewuchs, damit Gelände besser einsehbar wird von außen*
- *Wachpersonal, das regelmäßige Kontrollgänge durchführt,*
- *Einsatz eines Pförtners,*
- *Regelmäßige Bestreifung durch Ordnungsamt/Polizei*

Ein höherer finanzieller Aufwand einer Alternativmethode gegenüber der Videoüberwachung rechtfertigt nicht von vornherein die Ablehnung von Alternativmaßnahmen. Hier kommt es im Einzelfall auf die Höhe der Kosten und des Aufwandes an.

- **Zeitlich und räumlich erforderlich**

  Der Begriff „erforderlich“ enthält auch eine Pflicht zu prüfen, **ob** und **wie** die Videoüberwachung **zeitlich** und **räumlich** notwendig ist. Hier sind insbesondere die Datenschutzgrundsätze der Datenminimierung und Speicherbegrenzung zu beachten, siehe oben unter VI.4. und 6.

  Vorab ist daher zu überprüfen, an welchen Orten tatsächlich Kameras zur Zweckerreichung notwendig sind. Es sind nur die Orte zu erfassen, an denen sich eine Gefährdung verwirklichen könnte. Sichere Bereiche sind auszunehmen entweder durch technische Maßnahmen oder durch die konkrete Platzierung der Kameras.

  Zu prüfen ist, ob wirklich der gesamte Aufnahmebereich der Kamera überwacht werden muss oder Teilbereiche ausgeblendet (geschwärzt) oder unkenntlich (verpixelt, unscharf) gemacht werden können und müssen. Hierfür existieren spezielle technische Möglichkeiten.

  Beispiel: *Im Aufnahmebereich halten sich regelmäßig Mitarbeiter an bestimmten Stellen auf. Die Gesichter können an diesen Orten „verschleiert“ oder verpixelt werden.*

Beispiel: *Im Aufnahmebereich befinden sich Fenster, in denen Personen erkennbar sind. Diese müssen in den Aufnahmen geschwärzt werden.*

Beispiel: *Der Aufnahmebereich umfasst die angrenzende Fahrbahn oder den Fußweg. Er ist so einzustellen, dass diese Bereiche entweder nicht erfasst oder geschwärzt/verpixelt werden. Es gilt bei Aufnahmen von Außenfassaden einen Abstand von 1m ab Fassade einzuhalten; der öffentliche Verkehrsraum darf insoweit erfasst werden (Rechtsprechung).*

- **Wie?**

  Ist eine Live-Übertragung im Rahmen eines Monitorings ausreichend? Ist wirklich eine Speicherung notwendig zur Zweckerreichung? In diesem Zusammenhang sind Monitoring inklusive Aufzeichnungen, das Black-Box-Verfahren, ein Auslösen der Aufnahme durch manuelle Betätigung/durch Bewegung oder reines Monitoring genauestens gegeneinander abzuwägen.

- **Zu welchen Zeiten?**

  Ferner ist zu prüfen, zu welchen Zeiten die Videoüberwachung erforderlich erscheint. Genügt beispielsweise die Überwachung nachts oder am Wochenende oder außerhalb von Öffnungszeiten? Ggf. könnte ein Probebetrieb der Videoüberwachung mit anschließender Auswertung hilfreich sein. Dieser ersetzt jedoch nicht die im Vorfeld zu erstellende Gefährdungsprognose nebst Dokumentation!

- **Welche technische Ausstattung?**

  Auch die technische Ausstattung der Kameras ist zu prüfen. Sind Zoom-, Schwenk-, Fernsteuerungs-, Nachverfolgungs- und/oder Nachtsichtfunktionen tatsächlich notwendig zur Erreichung des Schutzzweckes? Dies ist nur dann der Fall, wenn in dem gesamten damit abdeckbaren Bereich die Gefährdung, die prognostiziert wurde, eintreten könnte.

Sind einzelne Funktionen nicht zur Zweckerreichung notwendig, sind sie dauerhaft auszuschalten.

e) *„keine Anhaltspunkte, dass schutzwürdige Interessen der betroffenen Person überwiegen“ - Angemessenheit*

Hier ist eine **Interessenabwägung** vorzunehmen. Abzuwägen ist zwischen den Interessen der überwachenden öffentlichen Stelle und den Interessen der von der Überwachung betroffenen Person. Auf der einen Seite stehen ihre Rechte (wie oben dargelegt), insbesondere auf informationelle Selbstbestimmung und unbeobachteten Aufenthalt in den betroffenen Bereichen. Auf der anderen Seite steht das Eigentums- oder Besitzrecht der öffentlichen Stelle oder das Recht ihrer Mitarbeiter auf Schutz der körperlichen Unversehrtheit.

Es sind die Gesamtumstände zu betrachten und eine Einzelfallbetrachtung vorzunehmen, in die einfließen muss, wie sehr die jeweilige Maßnahme in die Rechte des Betroffenen eingreift. Zu betrachten ist:

- der Informationsgehalt / die Art der Information
- die Informationsdichte / der Umfang der Informationen
- das zeitliche und räumliche Maß der Beeinträchtigung
- der betroffene Personenkreis /Anzahl der betroffenen Personen
- die Ausweichmöglichkeiten
- Art und Umfang der Datenverarbeitung

Auf beiden Seiten sind so die Interessen gegenüber zu stellen. Die hierdurch gewonnenen Erkenntnisse sind dann zu gewichten. Die öffentliche Stelle muss begründen, warum sie welchem Interesse den Vorzug gibt und erneut prüfen, ob die Videoüberwachung räumlich und zeitlich angemessen ist.

Beispiel: *Eine dauerhafte „24/7-Überwachung“ einer Eingangstür zum Schutz des Gebäudes beeinträchtigt Besucher eines öffentlichen Gebäudes mehr als eine Überwachung außerhalb der Öffnungszeiten.*

Beispiel: *Kann eine Person dem Aufnahmebereich nicht ausweichen, wie beispielweise ein(e) Mitarbeiter(in), der/die dort arbeitet, ist dies schwerwiegender, als wenn ein Besucher die Aufnahmebereiche der Kamera meiden kann.*

Beispiel: *Gleiches gilt für die Bewohner eines Wohnheims oder Internats (sofern diese von einer öffentlichen Stelle betrieben werden, z.B. Internat Schmalkalden-Meiningen, siehe 12. TB S. 99 „Videogaga 1“), die auf den Zugang angewiesen sind. In ihren äußerst persönlichen Wohnbereich würde mit einer Videoüberwachung auf den Fluren massiv eingegriffen. Dies wiegt schwerer als der Schutz vor Sachbeschädigung am Gebäude. Anders kann sich die Situation darstellen, wenn Leib und Leben gefährdet wären.*

Beispiel: *Aufnahmen, die die Intimsphäre verletzten, z.B. vom Eingangsbereich zu Toiletten, sind stets unzulässig, weil hier die Interessen der Betroffenen eindeutig überwiegen.*

Es gilt: Je mehr persönliche Informationen erhoben werden, umso größer ist der Eingriff in die Rechte der Betroffenen, umso sorgfältiger hat die Interessenabwägung stattzufinden.

2.2. Informationspflichten (§ 30 Abs.2 ThürDSG)

„Der Umstand der Videoüberwachung und die Informationen nach Artikel 13 Abs. 1 Buchst. a bis c der Verordnung (EU) 2016/679 sowie die Möglichkeit, beim Verantwortlichen die weiteren Informationen nach Artikel 13 der Verordnung (EU) 2016/679 zu erhalten, sind durch geeignete Maßnahmen erkennbar zu machen.“

Absatz 2 des § 30 ThürDSG spezifiziert für die Videoüberwachung das Transparenzgebot (siehe VI.2.) Die öffentliche Stelle als Verantwortlicher hat gesteigerte Informationspflichten. Entsprechend des Transparenzgebots gem. Art. 12 DS-GVO sind alle Informationen zur Verarbeitungstätigkeit leicht zugänglich und verständlich, in klarer, einfacher Sprache abgefasst, zu positionieren.

Nach dem Willen des Thüringer Gesetzgebers müssen nicht alle Informationen unmittelbar vorliegen. Es ist mit einem Hinweisschild in unmittelbarer Nähe der

Kamera darauf aufmerksam zu machen, dass eine Videoüberwachung erfolgt. Die verantwortliche öffentliche Stelle hat ferner Informationen zu sich als verantwortliche Stelle und ihrem Vertreter sowie dazu, wo weitergehende Informationen zu erhalten sind, anzugeben, nämlich:

- Kontaktdaten des Datenschutzbeauftragten
- Zwecke der Datenverarbeitung
- Rechtsgrundlage für die Verarbeitung
- Kontaktdaten der Stelle, wo der Betroffene weitere Informationen zur Verarbeitung seiner personenbezogenen Daten erhält, wie z.B. Speicherdauer, Weiterleitung, Empfänger, Rechte der Betroffenen

Das Hinweisschild ist ungefähr auf Augenhöhe gut sichtbar anzubringen.
Ein Piktogramm erleichtert die Erkennbarkeit.

Die betroffene Person muss vor Betreten des Aufnahmebereichs über die Videoüberwachung informiert werden. Entsprechend ist das Hinweisschild zu positionieren.

Ein vom TLfDI erstelltes Muster finden Sie hier:

https://www.tlfdi.de/mam/tlfdi/datenschutz/video/informationsblatt_videoueberwachung_oeffentliche_stellen.pdf

Die weitergehenden Informationen können an einem zentral zugänglichen Platz ausgehängt oder ausgelegt werden, z.B. im Rathaus.

2.3. Zweckbindung (§ 30 Abs. 3 ThürDSG)

„Eine Verarbeitung“ (siehe oben II.2) *„der im Rahmen der Videoüberwachung erhobenen Daten ist zulässig, wenn dies zu dem“* (vorab festgelegten!) *„verfolgten Zweck erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der betroffenen Person überwiegen."*

Die Regelung des § 30 Abs. 3 ThürDSG entspricht § 25a Abs. 3 ThürDSG alte Fassung und legt eine Zweckbindung entsprechend
Art. 5 Abs. 1 Buchst. b) DS-GVO fest. Die erhobenen Daten dürfen nur zum Erreichen des verfolgten Zwecks, der vorab festgelegt wurde, verarbeitet werden. Für die Videoüberwachung und die Verwendung der erhobenen Daten sollen die gleichen Maßstäbe gelten. Als erhoben gelten Daten bei der Videoaufzeichnung aber auch bei der zufälligen Informationswahrnehmung und unaufgeforderten Informationszuleitung (Begründung zum Thüringer Datenschutz-Anpassungs-und –Umsetzungsgesetz EU).

Es hat auch im Rahmen der Verarbeitung eine Interessenabwägung stattzufinden (siehe oben VII.2.e).

Einzige Ausnahme von der Zweckbindung bildet §30 Abs. 4 ThürDSG (siehe unten VII.2.4).

2.4. Ausnahme von der Zweckbindung (§ 30 Abs. 4 ThürDSG)

„Für einen anderen als den von vornherein festgelegten Zweck dürfen die erhobenen Daten nur verarbeitet werden, soweit dies zur Abwehr von Gefahren für die öffentliche Sicherheit, zur Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung oder zur Verfolgung von Straftaten erforderlich ist.“

Nur im **äußerst eingeschränkten Maße** ist also eine Abweichung von der Zweckbindung im Rahmen der Videoüberwachung möglich.
Hintergrund ist vor allem die Übermittlung von Daten an die für die Verfolgung von **Straftaten und Ordnungswidrigkeiten von erheblicher Bedeutung** zuständigen Behörden.

Absatz 4 des § 30 ThürDSG setzt zunächst immer voraus, dass die Kriterien des Absatzes 1 erfüllt sind. Erst, wenn die Datenerhebung zu den dort beschriebenen Schutzzwecken, die Interessenabwägung und die Verhältnismäßigkeit vorgenommen wurde bzw. gegeben sind, kann eine Zweckänderung nach Absatz 4 erfolgen.

Die Voraussetzungen sind im Einzelnen zu prüfen. Ob eine Ordnungswidrigkeit von erheblicher Bedeutung vorliegt, richtet sich nach Art des beeinträchtigten Rechtsguts, der Höhe des entstandenen Schadens sowie Art und Höhe der Sanktion und ist im Einzelfall zu prüfen.

Die Vorschrift entspricht § 25a Abs. 3 Satz 2 ThürDSG a.F.

2.5. Löschung (§ 30 Abs. 5 ThürDSG)

„Videoaufzeichnungen und aus der Videoüberwachung erhobene Daten sind unverzüglich zu löschen. Sie sind nur dann abweichend von Artikel 17 Abs. 1 der Verordnung (EU) 2016/679 nicht unverzüglich zu löschen, soweit sie zur Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung, zur Verfolgung von Straftaten oder zur Geltendmachung von Rechtsansprüchen benötigt werden.“

Entsprechend des in Art. 17 DS-GVO normierten Rechts auf Löschung und Vergessenwerden sind Videoaufzeichnungen und aus der Videoüberwachung erhobene Daten unverzüglich zu löschen. Nur soweit sie zur Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung, zur Verfolgung von Straftaten oder zur Geltendmachung von Rechtsansprüchen benötigt werden, sind sie nicht unverzüglich zu löschen.

Die Löschung hat zu erfolgen, sobald die Daten ihren ursprünglichen Erhebungs- und Verarbeitungszweck erfüllt haben und eine weitere Speicherung den schutzwürdigen Interessen Betroffener entgegensteht. Dienen die Aufzeichnungen der Beweissicherung, dürfte innerhalb von 1-2 Tagen aufzuklären sein, ob sie zur Verfolgung von Straftaten oder Ordnungswidrigkeiten von erheblicher Bedeutung oder zur Geltendmachung von Rechtsansprüchen gesichert werden müssen.

Die Grundsätze der Datenminimierung und Speicherbegrenzung nach Art. 5 Abs. 1 Buchst. c) und d) DS-GVO sind einzuhalten. Somit müsste nach spätestens 48 Stunden die Löschung erfolgen. Eine längere Speicherfrist kann angenommen werden in Einzelfällen, wenn am Wochenende oder an Feiertagen die öffentliche Stelle nicht durch zugriffsberechtigte Personen besetzt ist. Maximal 72 Stunden Speicherfrist sind dann zulässig.

Automatische Löschungen in festgelegten Zeitabständen, z.B. das automatische Überschreiben alle 72 Stunden, sind die sicherste Variante.

3. Gefahrenabwehr durch die Ordnungsbehörden (§ 26 ThürOBG)

Für die Thüringer Ordnungsbehörden gilt hinsichtlich des Datenschutzes und der Videoüberwachung zur Abwehr von konkreten Gefahren für die öffentliche Sicherheit und Ordnung § 26 Thüringer Ordnungsbehördengesetz (OBG):

„(1) Sofern Ordnungsbehörden Daten im Rahmen der Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung verarbeiten, finden der Erste, Dritte und Vierte Abschnitt des Thüringer Datenschutzgesetzes (ThürDSG) Anwendung; im Übrigen gilt die 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 (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72; L 127 vom 23.05.2018, S. 2) in Verbindung mit dem Ersten, Zweiten, Vierten und Sechsten Abschnitt des Thüringer Datenschutzgesetzes, mit der Maßgabe der Absätze 2 bis 5.

(2) Die Ordnungsbehörden können personenbezogene Daten, auch durch Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufnahmen oder -aufzeichnungen, bei oder im Zusammenhang mit öffentlichen Veranstaltungen und Ansammlungen, die nicht dem Versammlungsgesetz unterliegen, oder zur Erfüllung ihrer sonstigen Aufgaben nur erheben, soweit tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass Gefahren für die öffentliche Sicherheit oder Ordnung entstehen. Die Unterlagen sind spätestens zwei Monate nach Ablauf des auslösenden Ereignisses zu vernichten, soweit sie nicht zur Verfolgung von Straftaten oder Ordnungswidrigkeiten benötigt werden.

(3) Für Datenerhebungen bei oder im Zusammenhang mit öffentlichen Versammlungen und Aufzügen gelten die §§ 12a und 19a des Versammlungsgesetzes.

(4) Stellen die Ordnungsbehörden fest, dass bei der Verarbeitung von Daten im Rahmen der Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung unrichtige oder unzulässig gespeicherte personenbezogene Daten übermittelt worden sind und ist der Empfänger bekannt, gelten die §§ 35 und 43 ThürDSG.

(5) In Ausführung von § 35 Abs. 5 ThürDSG findet § 40 Abs. 4 und 5 PAG entsprechend Anwendung."

3.1. Allgemeines

§ 26 OBG regelt die Befugnisse der Ordnungsbehörden in Ausübung der Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung. Grundsätzlich ist verschärftes Augenmerk darauf zu legen, dass die Ordnungsbehörden nicht die Aufgaben der Strafverfolgung übernehmen dürfen. Diese sind ausschließlich der Polizei und Staatsanwaltschaft vorbehalten. Hier ist eine klare Abgrenzung vorzunehmen.

Die Videoüberwachung dient auch im Bereich des § 26 OBG nur als Nebeneffekt der Aufklärung von Ordnungswidrigkeiten. Der Zweck ist in erster Linie die Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung. Erst wenn dieser erfüllt wird, ist eine Verwendung der erhobenen Daten zur Übermittlung an die Polizei bzw. zur Verfolgung von Ordnungswidrigkeiten durch die Ordnungsbehörde zu prüfen und ggf. vorzunehmen.

Im Zusammenhang mit öffentlichen Versammlungen und Aufzügen gelten §§ 12a und 19a Versammlungsgesetz. Hiernach hat ausschließlich die Polizei die Befugnis, Bild- und Tonaufnahmen zu fertigen. Befugnisse für die Ordnungsbehörde sind nicht gegeben.
Nachfolgend wird kurz der Begriff der „Ordnungsbehörden" definiert, und ihre Aufgaben nach dem OBG werden genannt:

*„**Ordnungsbehörden** im Sinne dieses Gesetzes sind die Gemeinden, die Verwaltungsgemeinschaften, die erfüllenden Gemeinden und die Landkreise im übertragenen Wirkungskreis sowie das Landesverwaltungsamt und das für die öffentliche Sicherheit und Ordnung zuständige Ministerium. Die Abwehr von*

Zuwiderhandlungen gegen Satzungen in Selbstverwaltungsangelegenheiten ist Aufgabe des eigenen Wirkungskreises der Landkreise und Gemeinden." (§ 1 OBG).

„Die Ordnungsbehörden haben die Aufgabe, ***die öffentliche Sicherheit oder Ordnung*** *durch Abwehr von Gefahren und durch Unterbindung und Beseitigung von Störungen aufrechtzuerhalten." (§2 Abs. 1OBG).*

„Die Ordnungsbehörden können die ***notwendigen Maßnahmen*** *treffen, um eine im einzelnen Falle bestehende Gefahr für die öffentliche Sicherheit oder Ordnung abzuwehren, soweit nicht dieses Gesetz oder andere Rechtsvorschriften die Befugnisse der Ordnungsbehörden besonders regeln. (§ 5 Abs. 1 OBG)*

Die Definitionen der öffentlichen Sicherheit und Ordnung sowie der verschiedenen Gefahreneinstufungen finden sich in § 54 OBG.

3.2. Gefahrenabwehr mittels Videoüberwachung

Für die Gefahrenabwehr durch Videoüberwachung gelten
§ 26 Abs. 2 und 3 OBG. Damit ist die Anfertigung von Bild- und Tonaufnahmen oder -aufzeichnungen bei öffentlichen Veranstaltungen und Ansammlungen oder zur Erfüllung der sonstigen Aufgaben der Ordnungsbehörden nur dann zulässig, wenn **tatsächliche Anhaltspunkte** für das Entstehen von Gefahren für die öffentliche Sicherheit oder Ordnung bestehen.

Die „Erfüllung der sonstigen Aufgaben" bedarf einer gesetzlichen Grundlage. Nur wenn die Aufgabe tatsächlich gesetzlich der Kommune zugewiesen ist, darf die Ordnungsbehörde tätig werden.

Ferner sind Voraussetzung für die Datenerhebung jeweils konkrete tatsächliche Anhaltspunkte, die die Annahme rechtfertigen, dass Gefahren für die öffentliche Sicherheit und Ordnung entstehen. Der TLfDI sieht im einzelnen Fall das Erfordernis einer konkreten Gefahr, die bestehen (§§ 5 Abs. 1, 54 Abs. 3 Buchst. a) OBG) oder im Entstehen (§ 26 Abs. 2 OBG) sein muss.

Das Vorliegen tatsächlicher Anhaltspunkte ist jeweils im Einzelfall zu prüfen und zu dokumentieren, siehe dazu oben VII.2.1. d). Die Prognose erfordert konkrete Kenntnisse der Ordnungsbehörde, z.B. Indizien für Straftaten, Aufruf zu Gewaltakten. Lediglich Verdachtsmomente, Vermutungen, vage Andeutungen Dritter oder allgemeine Erfahrungssätze genügen nicht.

Bis zur Einleitung eines konkreten Ordnungswidrigkeitenverfahrens gelten auch für die Videoüberwachung die Grundsätze des ThürDSG i. V. m. der DS-GVO (siehe oben V.). Daher gelten auch hier zunächst die unter VI. dargestellten Grundsätze, wie z.B. das Transparenzgebot (Hinweisschilder). Erst wenn das Ordnungswidrigkeitenverfahren gegen eine bestimmte Person eingeleitet wird, sind die Vorschriften ab Abschnitt 3 des ThürDSG anzuwenden.

Im Übrigen ist umstritten, ob § 26 Abs. 2 OBG eine Ermächtigungsgrundlage für die kommunale Videoüberwachung in Thüringen darstellt. Es bedürfe besonderer Befugnisse, die der gesteigerten Eingriffsintensität durch die Videoüberwachung durch Begrenzung des Anwendungsbereichs und verfassungsrechtliche Ausgestaltung im Einzelnen Rechnung tragen (so Schwan, Ordnungsbehördengesetz, 2. Auflage, § 26 Rdn. 303).

Eine verfassungskonforme Anwendung ist jedenfalls zu gewährleisten. Hierfür ist zu beachten, dass auch im Rahmen des § 26 Abs. 2 OBG der Verhältnismäßigkeitsgrundsatz nach § 40 ThürVwVfG gilt. Dieser ist bereits unter VII.2.1. d) ausführlich dargestellt, so dass hier nur noch auf die speziell die Gefahrenabwehr betreffenden Voraussetzungen eingegangen werden soll.

Es sind zu prüfen:

a) **Geeignetheit** der Videoüberwachung in ihrer konkreten Ausgestaltung **zur Erreichung des Zwecks** der Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung,

b) **Erforderlichkeit** der Videoüberwachung in ihrer konkreten Ausgestaltung zur Erreichung des Zwecks der Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung.

   Existieren mildere Mittel, die den Zweck gleich effektiv erreichen, aber weniger intensiv in die Rechte der betroffenen Personen eingreifen?

c) **Angemessenheit** der Videoüberwachung in ihrer konkreten Ausgestaltung zur Erreichung des Zwecks der Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung.

   Es ist festzustellen, welche widerstreitenden Interessen bestehen und wie diese rechtlich zu beurteilen und zu gewichten sind, und es ist eine Abwägung der Interessen vorzunehmen. Das sogenannte Übermaßverbot ist zu beachten. Daher ist es notwendig, dass eine Maßnahme durch einen im Verhältnis zum Grundrechtseingriff hinreichend gewichtigen Rechtsgüterschutz gerechtfertigt ist. Angesichts des Eingriffsgewichts einer Videoüberwachung (Eingriff in Grundrechte) muss sie daher dem Schutz von Rechtsgütern von zumindest erheblichem Gewicht oder einem vergleichbar gewichtigen öffentlichen Interesse dienen. (vgl. BVerfG, Entscheidung vom 18. Dezember 2019, 1 BvR 142/15, Rdn. 95; siehe auch juris BVerfG, 1 BvR 142/15, Rdn. 95). Die Abwehr jeder (noch so kleinen) Gefahr für die Rechtsordnung und damit der ganz allgemeine Schutz der öffentlichen Sicherheit und Ordnung rechtfertigt eine Videoüberwachung nicht.

3.3. Löschung der Daten

Die Daten sind spätestens zwei Monate nach Ablauf des auslösenden Ereignisses zu vernichten, sofern sie nicht zur Verfolgung von Straftaten oder

Ordnungswidrigkeiten benötigt werden. Diese Frist stellt eine **Höchstfrist** dar, innerhalb derer die Löschung der Videoaufzeichnungen vorgenommen werden muss, so dass diese nicht wiederherstellbar sind.

Der Verantwortliche, d.h. hier die Ordnungsbehörde, hat die personenbezogenen Daten unverzüglich zu löschen, wenn die Verarbeitung unzulässig ist, sie zur Erfüllung einer rechtlichen Verpflichtung gelöscht werden müssen oder ihre Kenntnis für seine Aufgabenerfüllung nicht mehr erforderlich ist, § 35 Abs. 2 ThürDSG.

Im Zusammenhang mit öffentlichen Versammlungen und Aufzügen gelten die §§ 12a und 19a Versammlungsgesetz. Hiernach hat ausschließlich die Polizei die Befugnis, Bild- und Tonaufnahmen zu fertigen. Befugnisse für die Ordnungsbehörde sind nicht gegeben.

VIII. Vorbereitung der Videoüberwachung - Checkliste

Folgende Schritte sind vor der Installation einer Videoüberwachung zu prüfen und/oder zu erfüllen:

1. Dokumentation sicherheitsrelevanter Vorkommnisse

Die sicherheitsrelevanten Vorkommnisse im geplanten Videoüberwachungsbereich (§ 30 ThürDSG) bzw. die tatsächlichen Anhaltspunkte für das Be- oder Entstehen einer konkreten Gefahr (§§ 26 Abs. 2, 54 Nr. 3a OBG) sind

Ergibt die Dokumentation der Vorkommnisse, dass die Gefährdung bzw. Gefahrenlage sich fortsetzt oder verschärft, können die nachfolgenden Schritte eingeleitet werden.

2. Erstellung eines Sicherheitskonzepts

Das Sicherheitskonzept enthält die Planung, welche Maßnahmen ergriffen werden können, um die gegenwärtige Gefahrensituation zu beseitigen. Hierbei ist abzustufen nach den zunächst weniger in die Rechte der Betroffenen

eingreifenden Maßnahmen. Näheres siehe oben unter VII.2.d) zu milderen Mitteln.

3. Durchführung der milderen Mittel und Prüfung des Erfolgs einschließlich Dokumentation

Die nach Sicherheitskonzept möglichen milderen Mittel sind für einen festgelegten Zeitraum, der Erfolg verspricht, anzuwenden. Die Dokumentation der sicherheitsrelevanten Vorkommnisse ist in dieser Zeit fortzusetzen. Bringen die ergriffenen Maßnahmen nicht den gewünschten Erfolg, ist das Ergebnis zu dokumentieren. Sind alle milderen Mittel ausgeschöpft, kann die Umsetzung der Videoüberwachung in Betracht gezogen werden.

4. Prüfung der Voraussetzungen des § 30 Abs. 1 ThürDSG bzw. § 26 Abs. 2 OBG

Siehe oben VII.2. und 3.

Führt die Prüfung der Voraussetzungen dazu, dass die Zulässigkeit der Videoüberwachung bejaht wird, nimmt der Verantwortliche die Verhältnismäßigkeitsprüfung und die Interessenabwägung
(§ 30 ThürDSG) bzw. die Rechtsgütergewichtung (§ 26 OBG) vor. Diese sollten dokumentiert werden.

5. Nicht vergessen: Datenschutzbeauftragten einbeziehen

Nach Art. 28 Abs. 1 DS-GVO ist der (von der öffentlichen Stelle benannte) Datenschutzbeauftragte **frühzeitig!** und ordnungsgemäß einzubinden.

Verantwortlicher und Auftragsverarbeiter unterstützen den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben durch erforderliche Ressourcen, Zugang zu personenbezogenen Daten, Zugang zu Verarbeitungsvorgängen, Ressourcen zur Erhaltung seines Fachwissens, Sicherstellung, dass er weder Anweisungen erhält noch abberufen oder benachteiligt wird **(Art. 38 Abs. 2, 3 DS-GVO).**

Sehen Sie den Datenschutzbeauftragten als Ihren „Verbündeten“ an. Er kann Ihnen wichtige Hinweise zur Einhaltung der datenschutzrechtlichen Vorschriften erteilen und beratend, entsprechend seiner Aufgaben (Art.39 DS-GVO) zur Seite stehen.

Die Stellungnahme des Datenschutzbeauftragten sollte ebenfalls dokumentiert werden.

6. Personalrat einbeziehen

Wird der videoüberwachte Bereich auch von den Mitarbeiterinnen und Mitarbeitern betreten, ist bereits frühzeitig (möglichst bereits während der Planung) die Personalvertretung umfassend und mit einschlägigen Unterlagen zu unterrichten (§ 68 Abs. 2 Thüringer Personalvertretungsgesetz-ThürPersVG).

Bei Einführung, Anwendung, wesentlicher Änderung oder Erweiterung automatisierter Verarbeitung personenbezogener Daten der Beschäftigten hat der Personalrat nach § 73 Abs. 3 ThürPersVG mitzubestimmen.

Die Videoüberwachung erzeugt bei Beschäftigten einen erheblichen Anpassungs- und Leistungsdruck. Daher ist der Abschluss einer Dienstvereinbarung nach § 75 ThürPersVG zu prüfen. Diese sollte vor allem eine Regelung zur Leistungs- und Verhaltenskontrolle (in der Regel Ausschluss; nur im Ausnahmefall bei welchem konkreten Verdacht möglich?) enthalten und den Zweck der Videoüberwachung konkret beschreiben.

7. Technische Vorbereitung

Es sind technisch-organisatorische Maßnahmen zu ergreifen, um sicherzustellen und den Nachweis zu erbringen, dass die Videoüberwachung entsprechend der Vorschriften der DS-GVO erfolgt (**Art. 24 Abs. 1 DS-GVO**). Hieraus ergibt sich eine **umfassende Dokumentationspflicht.**

Hinsichtlich der technischen Umsetzung ist zu beachten, dass die eingesetzten **technischen Mittel** zur Erreichung des festgelegten Zweckes **geeignet** sein müssen. Dies beginnt bereits bei der Auswahl der jeweiligen Kamera. Kameras mit umfassenden Funktionen – wie z.B. Dome-Kameras – greifen intensiver in Rechte der Betroffenen ein als andere Kameras. Es ist bereits hier zu prüfen, welche Funktionen tatsächlich benötigt werden.

Vor allem auf Art. **25 DS-GVO** wird hingewiesen. Im Sinne der Erfüllung der allgemeinen Datenschutzgrundsätze ist auf Voreinstellungen zu achten, die Pseudonymisierung, Datenminimierung und die Erforderlichkeit der Aufnahmen für den festgelegten Zweck sicherstellen. Bereits bei der Anschaffung ist daher darauf zu achten, dass die entsprechenden technischen Möglichkeiten vorhanden sind.

Beispiel: *Die Kamera würde trotz Einstellung eines entsprechenden Winkels Mitarbeiterbereiche aufzeichnen. Hier besteht die Verpflichtung, eine Schwärzung der Aufnahmen in Teilbereichen voreinzustellen. Die Kamera muss über diese technische Möglichkeit verfügen.*

Im Rahmen der vorbereitenden organisatorischen Maßnahmen ist auch festzulegen, welche Art der Videoüberwachung durchgeführt werden soll (Monitoring, Aufzeichnung, Kombination aus beidem, siehe oben VII.2.1. d))

8. Entscheidung über Videoüberwachung und Beschaffung

Liegen alle Vorbereitungen vor, ist zu entscheiden, ob die Videoüberwachung tatsächlich in Betrieb genommen werden soll.

Danach kann die Beschaffung von Hard- und Software sowie entsprechender Dienstleistungen eingeleitet werden.

IX. Umsetzung der Videoüberwachung

1. Auftragsverarbeitungsvertrag

Sind im Rahmen der Videoüberwachung Dritte im Auftrag der öffentlichen Stelle tätig, ist zwingend ein schriftlicher Auftragsverarbeitungsvertrag zu schließen und bei der Auswahl des Auftragsverarbeiters und bezüglich des Inhalts des Vertrages **Art. 28 DS-GVO** zu beachten.

2. Installation

Im Rahmen der Installation sind die während der Vorbereitung festgelegten technischen Einstellungen der Kameras, des räumlichen und zeitlichen Aufnahmebereichs, der Art der Videoüberwachung (Monitoring usw.) und die sonstigen Kriterien zur Zweckerreichung umzusetzen.

3. Anbringen von Hinweisschildern

Die dargelegten Informationspflichten nach § 30 Abs. Abs. 2 ThürDSG i. V. m. Art. 13 DS-GVO sind zu erfüllen. Entsprechende Hinweisschilder sind anzubringen, siehe oben unter VII.2.2.

4. IT-Sicherheitskonzept

Die Videoüberwachung ist in das IT-Sicherheitskonzept der öffentlichen Stelle einzubinden. Es sollte eine systematische Dokumentation vorliegen.

Für das IT-Sicherheitskonzept und die zu ergreifenden technisch organisatorischen Maßnahmen gelten Art. 25 und 32 DS-GVO.

Art. 25 DS-GVO bestimmt u.a.:

„(1) Unter Berücksichtigung des Stands der Technik, der … trifft der Verantwortliche … geeignete technische und organisatorische Maßnahmen, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

(2) *Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellungen nur personenbezogene Daten, deren Verarbeitung für den jeweiligen Zweck erforderlich ist, verarbeitet werden…“*

Art. 32 DS-GVO gibt umfänglich Maßnahmen zur Sicherheit der Verarbeitung vor. Es ist der jeweilige Stand der Technik zu berücksichtigen, ebenso wie die Art der verarbeiteten personenbezogenen Daten. Das Verfahren der Videoüberwachung ist an die gesetzlichen Vorgaben anzupassen und mit konkreten Maßnahmen zu belegen.

Für die Erstellung eines IT-Sicherheitskonzepts gibt das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zum jeweils aktuellen Standard.

Diese finden Sie hier:

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/bsi-standards_node.html

Ferner kann auch auf die Methodik des Standard-Datenschutzmodells (SDM) zurückgegriffen werden. Die 95. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder verabschiedete am 26. April 2018 die Version 1.1 des SDM. Sie bietet Hilfsmittel für die Erstellung eines IT-Sicherheitskonzepts.

Näheres erfahren Sie hier:

https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/

Hinweise des TLfDI zu den Datenschutzanforderungen im Kontext zur IT-Sicherheit für öffentliche Stellen finden Sie hier:

https://www.tlfdi.de/mam/tlfdi/datenschutz/ds-anforderungen-it-sicherheit_offtl_stellen_stand_februar_2021.pdf

5. Spezielle technisch-organisatorische Maßnahmen im Rahmen der Videoüberwachung

Im Rahmen der technisch-organisatorischen Maßnahmen nach Art. 24, 25 und 32 DS-GVO sind Schutzvorkehrungen für die Videoüberwachung zu treffen, die den Datenschutz gewährleisten. Sie müssen in einem angemessenen Verhältnis zu den Risiken für die Rechte und Freiheiten natürlicher Personen stehen, die sich aus der zufälligen oder unrechtmäßigen Zerstörung, dem Verlust, der Veränderung, der unbefugten Weitergabe oder dem unbefugten Zugang zu Videoüberwachungsdaten ergeben (Europ. Datenschutzausschuss, Guidelines 3/2019, Version 2.0, Rdn. 123).

Alle Komponenten des Videoüberwachungssystems und die Daten sind in jeder Phase angemessen zu schützen. Daher sind die technischen und die organisatorischen Maßnahmen miteinander zu kombinieren (Europ. Datenschutzausschuss, Guidelines 3/2019, Version 2.0, Rdn. 128).

Hieraus ergeben sich insbesondere folgende beispielhafte Maßnahmen:

Kameras, Monitore, andere Anzeigegeräte, Aufzeichnungen, Datenübertragungen, Speichermedien (auch für Backups) und die Übermittlung von Daten an Dritte (z.B. Strafverfolgungsbehörden) müssen vor dem Zugriff unbefugter Dritter geschützt sein.

Kameras sind so anzubringen, dass sie vor Demontage, Verstellen des Aufnahmebereichs und Zugriff durch unbefugte Dritte geschützt sind.

Die gesamte Videoüberwachungsanlage ist physisch gegen wetterbedingte Einflüsse, z.B. extreme Temperaturen, und menschlich verursachte Schäden, z.B. verschüttete Getränke, zu schützen.

Die Übertragung von Daten der Kamera auf Monitore oder Speichermedien muss passwortgeschützt (kabellose Übertragung) bzw. ausreichend physisch gesichert vor unbefugtem Zugriff (Übertragung per Netzwerkkabel) erfolgen.

Die Monitore sind vor Blicken Unbefugter zu schützen.

Die Hardware der Videoüberwachungsanlage (PCs) ist vor unbefugtem Zugriff zu schützen, z.B. durch abschließbare Räume, Passwörter, Zugriffsrechte, Protokollierung.

Die Software ist mit Sicherheits-Updates stets aktuell zu halten und vor Zugriff von außen mittels Firewall und Virenscanner zu schützen.

Erkennung und Meldung des Systems bei Ausfall von Komponenten, Software oder Verbindungen ist angebracht.

6. Dokumentation der einzelnen Kameras

Für die Videoüberwachungsanlage sind **für jede einzelne Kamera** umfassende Dokumentationen vorzunehmen zu folgenden Punkten:

- Kamerabezeichnung
- Kamerastandort
- Datum der Inbetriebnahme
- Technische Daten
    - Kamera (Typ, Modell)
    - Auflösung des Kamerabildes (höchstmögliche angeben)
    - Verstell- /Schwenkbereich (vorhanden/nicht vorhanden/verwendet/nicht verwendet/Einstellungen)
    - WLAN-Funktion und Internetfähigkeit (wenn ja: Art der Datenübermittlung, Protokolltyp, Verschlüsselung, Einstellungen)
    - Fernsteuerungsmöglichkeit /Remotezugang zur Kamerasteuerung (wenn ja: Art der Authentifizierung, Protokolltyp, Verschlüsselung, Einstellungen)
    - Änderung des Standart-Zugangspassworts
- Zweck der Kamera
- Betroffener Personenkreis
- Festlegung der Zugriffsberechtigung verarbeitungsberechtigter Personen / Dokumentation (Wo und wie festgelegt? z.B. 4-Augen-Prinzip für angezeigte oder gespeicherte Daten, festgelegt in Dienstanweisung Nr. … vom …)
- Bezug zum IT-Sicherheitskonzept (Verweis Dokument vom…)
- Einbeziehung Datenschutzbeauftragter (Dokumentation)
- Durchführung Datenschutz-Folgeabschätzung (Wenn ja: mit welchem Ergebnis? Wenn nein: Begründung)
- Sichtwinkel der Kamera (in Skizze, Lageplan oder Zeichnung eintragen)
- Angaben zur Datenverarbeitung
    - Beobachtung („verlängertes Auge“ ja/nein)
    - Aufzeichnung (ja/nein)
    - Speicherfristen (Regelfristen, Begründung für die Dauer, ggf. Ausnahmefristen, Begründung unter welchen Voraussetzungen)

- Art der Datenlöschung (automatisch, Überschreiben nach…. Stunden)

- Skizze /Lageplan/Zeichnung (für **alle** Videokameras, Kennzeichnung der beschriebenen Kamera
- Screenshot der beschriebenen Kamera (ggf. mehrere Ansichten, wenn zoom- oder schwenkbar bzw. in seitlichem Winkel veränderlich einstellbar)

7. Verzeichnis von Verarbeitungstätigkeiten

Hier gibt **Art. 30 DS-GVO** die einzelnen Angaben, die dieses enthalten muss, vor. Hervorzuheben ist immer wieder die Festlegung des Zweckes der Videoüberwachung. Erforderlich ist eine systematische Dokumentation der Videoüberwachungsanlage(n).

Die Ausnahme, dass Einrichtungen mit weniger als 250 Mitarbeitern ein Verzeichnis von Verarbeitungstätigkeiten nicht zu führen haben, gilt für die Videoüberwachung nicht, denn die Videoüberwachung stellt eine Verarbeitung von personenbezogenen Daten dar, die ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt und nicht nur gelegentlich erfolgt (siehe Art. 30 Abs. 5 DS-GVO).

Ein Beispiel eines Verzeichnisses finden Sie hier:

https://www.tlfdi.de/mam/tlfdi/datenschutz/muster_verarbeitungsv.pdf

Ausführliche Hinweise können Sie hier nachlesen:

https://tlfdi.de/mam/tlfdi/themen/hinweise_zum_verzeichnis_von_verarbeitungstatigkeiten.pdf

8. Dienstanweisung

Alle in die Videoüberwachung einbezogenen und konkret benannten Mitarbeiter sind einzuarbeiten und zu schulen. Sie müssen im Rahmen einer schriftlichen Dienstanweisung eine Arbeitsanleitung/-anweisung erhalten. Diese hat auch

entsprechende Belehrungen über den Zugriff auf personenbezogene Daten zu enthalten.

9. Datenschutz-Folgenabschätzung

Es ist zu prüfen, ob eine **Datenschutz-Folgenabschätzung** gem. **Art.35 DS-GVO** unter Einbeziehung des Datenschutzbeauftragten der öffentlichen Stelle vorzunehmen ist. Vor allem eine systematische umfangreiche (Video-)Überwachung öffentlich zugänglicher Bereiche erfordert eine Datenschutz-Folgenabschätzung.

Ergibt die Datenschutz-Folgenabschätzung, dass die Verarbeitung der personenbezogenen Daten ein hohes Risiko zur Folge hätte, konsultiert der Verantwortliche den TLfDI als Aufsichtsbehörde vor der Verarbeitung, sofern er keine Maßnahmen zur Eindämmung des Risikos trifft (vgl. Art. 36 Abs. 1 DS-GVO). Er stellt der Aufsichtsbehörde bei einer Konsultation die in Art. 36 Abs. 3 DS_GVO genannten Informationen zur Verfügung.

Videoüberwachungsanlagen, die bereits vor Inkrafttreten der DS-GVO in Betrieb waren und nicht in Art, Umfang und Zweck der Verarbeitung
oder durch Verwendung neuer Technologien verändert wurden, bedürfen nach Ansicht des TLfDI einer Datenschutz-Folgenabschätzung nicht.

Eine vorläufige Liste der Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung vorzunehmen ist, finden Sie hier:

https://www.tlfdi.de/mam/tlfdi/datenschutz/dsfa_muss-liste_04_07_18.pdf

Bitte beachten Sie, dass diese Liste nicht dem Umkehrschluss unterliegt, d.h. wenn Verarbeitungsvorgänge nicht in dieser Liste enthalten sind, bedeutet dies nicht, dass eine Datenschutz-Folgenabschätzung nicht notwendig wäre. Dies ist immer im Einzelfall zu prüfen. Bitte beachten Sie daher dringend die dortigen Hinweise!

X. Regelmäßige Überprüfung

1. Technische Überprüfung

Die technische Funktionsfähigkeit der Videoüberwachungsanlage ist in regelmäßigen festgelegten Abständen zu prüfen.

2. Rechtliche Überprüfung

Die rechtlichen Voraussetzungen der Videoüberwachung sind in regelmäßigen Abständen vom Betreiber einer Videoüberwachungsanlage zu überprüfen. Der TLfDI empfiehlt mindestens 1x jährlich eine Überprüfung, ggf. häufiger – je nach Zweck und Erfolg der Maßnahme.

Die Überprüfungszeiträume sind konkret festzulegen im Rahmen des Verzeichnisses der Verarbeitungstätigkeiten und einzuhalten. Das Ergebnis der Überprüfung ist schriftlich festzuhalten.
Vor allem die Fragen der **Geeignetheit und Erforderlichkeit** der Videoüberwachung zur Erreichung des festgelegten Zwecks **sind regelmäßig** zu prüfen.

Beispiel: *War die Kamera ein Jahr lang in Betrieb und lassen sich dann keine Tatsachen (mehr) feststellen, welche die Annahme rechtfertigen, dass das überwachte Objekt gefährdet ist, ist die Videoüberwachung einzustellen.*
Gleiches gilt, wenn der festgelegte Zweck gar nicht erreicht wurde.

Auch in räumlichen und örtlichen Teilbereichen der Videoüberwachung ist dies genau zu prüfen und ggf. auch in diesen Teilbereichen die Videoüberwachung einzustellen.

Beispiel: *Werden sicherheitsrelevante Vorkommnisse nur noch in bestimmten Zeiten, z.B. von 2-5 Uhr nachts, festgestellt, ist die Videoüberwachung auf diese Zeitspanne zu begrenzen.*
Beispiel: *Sind 5 verschiedene Kameras zur Sicherung eines Gebäudes installiert und ergibt die jährliche Prüfung, dass nur in 3 Aufnahmebereichen*

sicherheitsrelevante Vorkommnisse festzustellen sind, sind die Kameras der anderen beiden Aufnahmebereiche zu deaktivieren bzw. zu deinstallieren.

Schlussendlich ist auch zu überprüfen, ob die äußeren Gegebenheiten sich verändert haben und eine Videoüberwachung hinfällig ist, z.B. weil das von der öffentlichen Stelle gemietete Objekt nun vom Eigentümer eingezäunt wurde.

Das Ergebnis der Überprüfung ist schriftlich zu dokumentieren.

XI. Zusammenfassung

Die Videoüberwachung stellt ein komplexes Feld der Datenverarbeitung dar.
Die öffentliche Stelle ist Verantwortlicher und hat sich dieser umfassenden Verantwortung stets bewusst zu sein.

Aufgrund der massiven Beeinträchtigung der (Grund-)Rechte der betroffenen Personen hat eine strikte Prüfung hinsichtlich der Geeignetheit, Erforderlichkeit und Verhältnismäßigkeit dieser Maßnahme stattzufinden. Der Zweck der Videoüberwachung ist vorab festzulegen und einzuhalten. Abweichungen sind nur unter engen Voraussetzungen möglich. Nur wenn die Videoüberwachung das mildeste und letzte Mittel zur Erreichung des Zwecks darstellt, darf sie eingerichtet werden.
Es bestehen umfassende Dokumentationspflichten. Die Dokumente sind dem TLfDI als Aufsichtsbehörde auf Verlangen vorzulegen.

Gegenüber der betroffenen Person bestehen seitens der öffentlichen Stelle umfangreiche Auskunfts- und Informationspflichten (Art. 13, 14 DS-GVO).

Sollten Sie Fragen rund um die Videoüberwachung haben, steht der TLfDI gern beratend zur Verfügung. In diesem Fall wenden Sie sich bitte an

Thüringer Landesbeauftragter

für den Datenschutz und die Informationsfreiheit
Häßlerstraße 8
99096 Erfurt
poststelle@datenschutz.thueringen.de

HINWEIS: Aus Sicherheitsgründen ist es nicht mehr möglich, E-Mails mit dem Dateiformat *.doc zu senden.

Tel.: +49 (361) 57-3112900
Fax: +49 (361) 57-3112904