Handreichung zur Videoüberwachung
nach § 14 Niedersächsisches Datenschutzgesetz (NDSG)

Vorbemerkung

Dieses Dokument ist im Wesentlichen der Handreichung zur Videoüberwachung durch öffentliche Stellen in Ausübung des Hausrechts nach § 30 Abs.7 Hamburger Datenschutzgesetz-alt (HmbDSG-alt) entnommen. Es wurde versucht, sie dem niedersächsischen Datenschutzgesetz (NDSG), hier speziell § 14, unter Einbeziehung des Kommentars zu diesem Paragrafen vom Landesbeauftragten für den Datenschutz Niedersachsen anzupassen..

Jede Daten verarbeitende Stelle ist für die Rechtmäßigkeit der von ihr vorgenommenen Videoüberwachung verantwortlich. Dabei handelt es sich um eine komplexe Entscheidung, bei der die öffentlichen Interessen mehrfach mit den Interessen der Betroffenen abgewogen werden müssen.

Zur Erleichterung der vorgeschriebenen Vorabkontrolle und der anzufertigenden und auf dem aktuellen Stand zu haltenden Verfahrensbeschreibung wurde ein Musterformular erstellt, für das mit dieser Handreichung weitergehende Hinweise und Ausfüllhilfen angeboten werden.

Diese Handreichung soll insbesondere auch als Hilfestellung für die erforderlichen Abwägungen vor der Entscheidung über die Einführung und Ausgestaltung der Videoüberwachung dienen und gleichzeitig die verschiedenen Begrifflichkeiten erläutern. Sie gliedert sich in eine allgemeine Einführung und in die Erläuterungen zum Musterformular.

Die allgemeine Einführung beleuchtet die Grundrechtsproblematik der Videoüberwachung und die allgemeinen Anforderungen einer Videoüberwachung nach § 14 NDSG.
Die Erläuterungen zum Musterformular folgen dessen Aufbau und der dortigen Nummerierung. Die hier behandelten Stichworte sind in diesem Musterformular jeweils mit einem * gekennzeichnet.

1. Allgemeine Einführung

1.1 Allgemeine Anforderungen an eine Videoüberwachung

Videoüberwachung ist eine besondere Form der Verarbeitung personenbezogener Daten. Auch Videoüberwachung steht damit unter dem Vorbehalt des Gesetzes und hat wie jede andere Form personenbezogener Datenverarbeitung insbesondere den Grundsätzen der Erforderlichkeit, der Datensparsamkeit und der Zweckbindung zu entsprechen.

Videoüberwachung unterscheidet sich aber grundsätzlich von der sonstigen automatisierten Datenverarbeitung öffentlicher Stellen. Hierbei ist die Verarbeitung nicht auf einzelne, zur Aufgabenerfüllung erforderliche Informationen (vordefinierte Datenfelder) eines bestimmbaren Betroffenenkreises beschränkt.
Im Rahmen herkömmlicher Videoüberwachungsmaßnahmen werden vielmehr sämtliche visuell wahrnehmbaren Daten wie Aufenthaltsort und -zeit, Gesicht und Mimik, Frisur/ Kopfbedeckung, Art und Zustand der Kleidung, Gepäck, optisch erkennbarer Allgemeinzustand, Kontakt- und Begleitpersonen, Verhalten allein und in der Gruppe, etc. erhoben und ggf. für eine weitere Nutzung gespeichert. Damit werden Detail-Informationen vollständiger Lebenssituationen von beliebigen Personen verarbeitet, die in der Regel nichts weiter verbindet, als dass sie den überwachten öffentlichen Raum zum ganz überwiegenden Teil gesetzeskonform nutzen.

Videoüberwachungsanlagen sind in der Vergangenheit immer komplexer und immer leistungsfähiger geworden. Sie können über Webanbindungen ferngesteuert und ferngewartet werden.
Daneben bestehen Einzelanlagen mit mehreren hundert Kameras. Die Tendenz geht auch im öffentlichen Bereich hin zu Einzelanlagen mit einer Vielzahl von Kameras.

Es bestehen Angebote der Privatwirtschaft, schon ab geringsten monatlichen Beträgen sowohl die Projektierung als auch die Betreuung von Videoüberwachungsanlagen zu übernehmen. Oft entsprechen diese Angebote nicht öffentlich-rechtlichen Anforderungen.

Eine derart umfassende Erhebung und weitere Verarbeitung von personenbezogenen Daten kennt das Datenschutzrecht in anderen Bereichen nicht. Es schützt vielmehr jedes einzelne personenbezogene Datum nach dem Grundsatz der Erforderlichkeit.

Das Bundesverfassungsgericht hat deshalb festgestellt, dass jede Form der Videoüberwachung im öffentlichen Raum einen erheblichen Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen darstellt. Dies umso mehr, je weniger der einzelne Betroffene durch sein Verhalten selbst Anlass für die Überwachung gibt. Das Gewicht des Eingriffs wird noch verstärkt, wenn die Lebenssachverhalte nicht nur beobachtet, sondern auch aufgezeichnet werden.
Deshalb bedarf die Videoüberwachung jeweils einer normenklaren und verhältnismäßigen gesetzlichen Regelung, welche die spezifischen Voraussetzungen der Datenverarbeitung regelt, mithin hinreichende Vorgaben für Anlass und Grenzen der Videoüberwachung enthält.
Jede Videoüberwachungsmaßnahme muss danach geeignet, erforderlich und verhältnismäßig sein.

Die wesentlichen Fragestellungen dazu lauten allgemein:

- Welche Ziele sollen mit der konkreten Überwachungsmaßnahme erreicht werden?
- Welche konkreten Umstände rechtfertigen eine Videobeobachtung, welche eine Videoaufzeichnung?
- Ist die Videobeobachtung geeignet und erforderlich, oder gibt es mildere Mittel, um die Ziele zu erreichen?
- Ist die Videoaufzeichnung geeignet und erforderlich, oder gibt es mildere Mittel, um die Ziele zu erreichen?
- Gibt es Anhaltspunkte dafür, dass die Interessen der Betroffenen überwiegen?
- Beschränken sich die Verarbeitungsmöglichkeiten auf die gesetzlichen Befugnisse?
- Reichen die technisch-organisatorischen Maßnahmen aus, um die Datensicherheit mit dem geringstmöglichen Eingriff in das informationelle Selbstbestimmungsrecht zu gewährleisten?
- Ist die Überwachung für die Betroffenen erkennbar?
- Ist eine Fortführung der Videoüberwachung erforderlich?

1.2. Rechtliche Anforderungen

In einem ersten Schritt ist die rechtliche Zulässigkeit der geplanten Videoüberwachung zu prüfen:

Grundvoraussetzung ist, dass die anwendende Stelle **Hausrecht** besitzt.
Grundsätzlich ist das Hausrecht an die Verfügungsbefugnis des Berechtigten geknüpft und umfasst das Recht zu bestimmen, wer eine Örtlichkeit betreten darf und wer nicht. Werden private Flächen angemietet, geht grundsätzlich auch das Hausrecht auf den Nutzer über. Die Befugnisse öffentlicher Stellen werden dadurch aber nicht erweitert, sondern sind auch in diesem Fall auf das öffentlich-rechtliche Hausrecht beschränkt.

Videoüberwachung umfasst die Videobeobachtung und / oder die Videoaufzeichnung Die Befugnis beschränkt sich auf die optische Überwachung. Eine akustische Überwachung ist nicht zulässig. Es sollten daher bevorzugt Systeme eingesetzt werden, die von vornherein keine Audiofunktionen anbieten. Werden Kameras eingesetzt, die auch eine akustische Überwachung ermöglichen, so ist diese vorab dauerhaft auszuschließen, in der Regel durch ihre Zerstörung.

Die Videobeobachtung wird vom Bundesverfassungsgericht (1 BvR 2368/06, Rz 38, 52, 56) als weniger belastend angesehen als die Videoaufzeichnung. Da auch sie in der überwiegenden Zahl Betroffene erfasst, die durch ihr Verhalten selbst keinen Anlass für eine Beobachtung oder Aufzeichnung geben, stellt auch die bloße Beobachtung immer einen erheblichen Eingriff in die Rechte der Betroffenen dar und auch ihre Erforderlichkeit ist deshalb kritisch zu hinterfragen.

Es ist daher je nach Ausgestaltung der Videoüberwachung zu prüfen und zu dokumentieren, ob die spezifischen Tatbestandsvoraussetzungen für die Beobachtung oder die Aufzeichnung gegeben sind.

Sie muss im Einzelfall geeignet sein, das Hausrecht zu den in § 14 NDSG genannten Zwecken wahrzunehmen, und ist auf das erforderliche Maß zu beschränken. Es gilt der Grundsatz des geringstmöglichen Eingriffs.

Bei der Entscheidung über die Einführung ist ein strenger Maßstab anzulegen. Immer ist hierfür auch die Kombination mit verschiedenen anderen Maßnahmen wie Schließanlagen, anlassbezogene Beobachtung u.ä zu prüfen. Beide Verarbeitungsformen sind nur dann zulässig, wenn sichergestellt ist, dass keine Anhaltspunkte für ein Überwiegen der Interessen der Betroffenen vorliegen. Die Interessenabwägung hat für jede Variante getrennt zu erfolgen.

Auch die weitere Verarbeitung der Aufzeichnungen durch die verantwortliche Daten verarbeitende Stelle ist grundsätzlich auf die Wahrnehmung des Hausrechts beschränkt. Eine darüber hinaus gehende weitere Verarbeitung zu anderen Zwecken kommt erst im Anschluss daran und nur in Betracht zur Verfolgung von Straftaten oder zur Abwehr von Gefahren für die öffentliche Sicherheit oder für bedeutende Sach- oder Vermögenswerte.
Eine originäre Aufzeichnung zum Zwecke der Strafverfolgung ist mangels Gesetzgebungskompetenz nicht zulässig. Polizei und Staatsanwaltschaft können aber innerhalb der festgelegten Speicherfrist nach den Vorschriften der Strafprozessordnung relevante Kopien anfordern.

Um die Betroffenenrechte wahrnehmen zu können, ist die Videoüberwachung unter Angabe der verantwortlichen Stelle deutlich sichtbar zu kennzeichnen. Der Hinweis soll ausweislich der Gesetzesbegründung auch erkennen lassen, ob beobachtet oder auch aufgezeichnet wird. Die konkrete Ausgestaltung des Hinweises steht im Ermessen der verantwortlichen Stelle.
Es wird empfohlen, in unmittelbarer Nähe des überwachten Bereichs etwa in Sichthöhe mit Hinweisschildern zu arbeiten, die mit einem Piktogramm versehen sind, den Umstand der Überwachung und die jeweilige verantwortliche Stelle benennen. Die Angabe einer Telefonnummer ist nicht erforderlich, da die Überwachung in der Regel in den Räumen der verantwortlichen Stelle oder in deren unmittelbarer Nähe stattfindet.
Im Internet können verschiedene Beispiele für Piktogramme und Beschriftungen gefunden werden.

Sind die Betroffenen der verantwortlichen Stelle bekannt, sind sie nach § 14 NDSG über die Datenverarbeitung zu benachrichtigen.

Die verantwortliche Stelle hat die Rechtmäßigkeit und Angemessenheit der Videoüberwachung vor der Einführung zu prüfen, nachprüfbar zu dokumentieren und das Fortbestehen der Rechtmäßigkeit und Angemessenheit in regelmäßigen Abständen zu überprüfen.
Über jede Videoüberwachung ist eine Verfahrensbeschreibung anzufertigen und stetig zu aktualisieren.

Bei dem Einsatz von dauerhaft defekten Kameras oder nicht genutzten Kameras und Attrappen, so genannter „Dummies“, findet keine Bildübertragung statt. Somit werden keine Daten verarbeitet und das NDSG ist daher nicht einschlägig.
Diese Kameravarianten greifen zwar nicht in das Recht auf informationelle Selbstbestimmung ein, wohl aber in das Recht auf freie Entfaltung der Persönlichkeit der Betroffenen (Art. 2 Abs. 1 GG), da sie zu einer Verhaltensbeeinflussung führen. Bei dem Bürger wird der Anschein einer Datenverarbeitung erweckt, so dass die Auswirkungen für den Betroffenen die gleichen wie bei einer „echten“ Datenverarbeitung sind. Dies wird gegebenenfalls noch durch entsprechende Hinweisschilder bestärkt. Eine Rechtsgrundlage für diesen Eingriff ist nicht ersichtlich.

Problematisch wird es für die verantwortliche Stelle spätestens, wenn sich Betroffene an die vermeintlich videoüberwachende Stelle wenden, um z. B. auf das Fehlen "geeigneter Maßnahmen" gemäß § 14 NDSG hinzuweisen, um Auskunft nach § Art. 15 DSGVO zu verlangen. Die Behörde müsste zugeben, rechtswidrig gehandelt zu haben, indem sie etwas behauptet hat („Hier wird videoüberwacht“), von dem sie weiß, dass es nicht zutrifft. Sofern es trotzdem zu einem schädigenden Ergebnis kommen würde, müsste die verantwortliche Stelle die o.a. Umstände einräumen und sich gegebenenfalls mit entsprechenden Ansprüchen auseinandersetzen.

1.3 Technische Anforderungen

Die verantwortliche Stelle hat auch zu gewährleisten, dass die für die jeweils angestrebte Videoüberwachung erforderlichen und angemessenen technisch-organisatorischen Maßnahmen getroffen werden. Das mit der Videoüberwachung einhergehende Gefährdungspotential muss wirksam beherrscht werden.

Der Prüfung der rechtlichen Zulässigkeit an sich muss sich deshalb eine weitere Prüfung anschließen, in welcher grundsätzlich vor der Entscheidung über die Einführung - anhand der konkreten Konzeption der Anlage - geprüft wird, ob auch die gewählten technischen und organisatorischen Maßnahmen geeignet und erforderlich sind, um die Rechtmäßigkeit der Videoüberwachung in ihrer konkreten Ausgestaltung sicherzustellen.

- Kann der Zweck der Videoüberwachung mit der vorgesehenen Ausgestaltung der Anlage erreicht werden?
- Sind die Ziele auch mit Maßnahmen geringerer Eingriffstiefe erreichbar?
- In welchem Umfang sind mit der Nutzung des Verfahrens Gefahren für die Rechte von Betroffenen verbunden und wie können diese beherrscht werden?
- Können und werden die technischen und organisatorischen Maßnahmen getroffen, die erforderlich sind, um die Ausführung datenschutzrechtlichen Bestimmungen und datenschutzrechtlichen Grundsätze zu gewährleisten?

Nach § 14 NDSG ist durch die behördliche Datenschutzbeauftragte oder den behördlichen Datenschutzbeauftragten stets eine Datenschutz-Folgenabschätzung gem. Art. 35 DSGVO durchzuführen.

2. Erläuterungen zum Musterformular

Zu Musterformularnummer 1: Beschreibung der Maßnahme

Verantwortliche Stelle / Daten verarbeitende Stelle:
Verantwortliche Stelle ist diejenige Stelle, die Inhaberin des öffentlich-rechtlichen Hausrechts ist und bei der deshalb die Zuständigkeit für die Anordnung der Videoüberwachung liegt.
Betreibt eine öffentliche Stelle allein für eigene Zwecke Videoüberwachung und erfasst dabei auch Bereiche einer anderen öffentlichen Stelle, deren Besuch Rückschlüsse auf besonders geschützte Daten zulässt (z.B. Besuch einer Gesundheitsdienststelle), so hat auch sie die sich daraus ergebenden engeren Grenzen der Verarbeitungsbefugnis zu beachten, da es nicht nur darauf ankommt, wo die Kamera hängt und wer sie betreibt, sondern wen und was sie aufnimmt.

Werden dritte Stellen im Wege der Auftragsdatenverarbeitung mit der Videoüberwachung beauftragt, ist Art. 28 DSGVO zu beachten.
Die Befugnisse der öffentlichen Stelle werden durch die Beauftragung einer privaten Stelle nicht erweitert. Es empfiehlt sich eine kritische Prüfung der angebotenen Standardverträge.

Dienstgebäude:
Dienstgebäude meint die von den Trägern öffentlicher Gewalt zur Aufgabenerfüllung genutzten Räumlichkeiten, in

denen sie Hausrecht haben.

Betroffener Gebäudeteil/Außenfläche:
Im Kommentar zum § 25 a NDSG-alt sind unter Punkt 4. und unter Punkt 5. der zulässige Überwachungsbereich beschrieben. Bei Vorliegen aller Voraussetzungen ist die Überwachung erlaubt für öffentlich zugängliche Bereiche in Dienstgebäuden und besonders gefährdete Bereiche innerhalb und außerhalb von Dienstgebäuden.
Die Befugnis zur Überwachung außerhalb von Dienstgebäuden besteht ausschließlich in engem räumlichen Zusammenhang zu dem Dienstgebäude, an dem das öffentlich-rechtliche Hausrecht besteht, beispielsweise an dem im Innenhof eines Gebäudes liegende Parkplatz. Eine Überwachung angrenzender öffentlicher Wege ist danach nicht zulässig, sondern nur in dem Umfang hinnehmbar, der für die Aufgabenwahrnehmung unvermeidbar ist.

Öffentlich zugängliche Bereiche:
Öffentlich zugängliche Bereiche können sowohl innerhalb als auch außerhalb von Gebäuden liegen. Sie sind ihrem Zweck nach bestimmt, durch eine unbestimmte Zahl oder nach allgemeinen Merkmalen bestimmbaren Personen betreten oder genutzt zu werden. Als öffentlich zugängliche Bereiche innerhalb von Dienstgebäuden kommen alle Bereiche in Betracht, die zumindest regelhaft dem Publikumsverkehr dienen oder z.B. den Mitgliedern von öffentlich-rechtlichen Körperschaften allgemein zur Verfügung stehen. Im Gegensatz dazu stehen Räumlichkeiten und Bereiche, die nur durch Mitarbeiter genutzt oder betreten werden dürfen.
Daneben können Bereiche innerhalb und außerhalb von Dienstgebäuden betroffen sein, die wegen ihrer besonderen Schutzwürdigkeit nur beschränkt zugänglich sind.

Besonders gefährdete Bereiche:
Besonders gefährdete Bereiche sind Bereiche mit gesondertem, erhöhtem Schutzbedürfnis, wie dies z.B. bei Serverräumen oder der besonderen Geheimhaltung unterliegenden Datenbeständen der Fall sein kann. Eine besondere Gefährdung außerhalb von Dienstgebäuden bedarf eines hinreichenden räumlichen Bezugs zum Hausrecht am Dienstgebäude und kann bei einem Parkplatz am oder im Gebäude angenommen werden, wenn dieser von Personen genutzt wird, die dem Personenschutz unterliegen. Die Vorschrift ermächtigt nicht zur zielgerichteten Überwachung des öffentlichen Straßenraums.

Art der Videoüberwachung:
a)Videobeobachtung:
Videobeobachtung meint als einheitlichen Lebenssachverhalt die Ermöglichung der visuellen Wahrnehmung von Räumen mit Hilfe einer optischen Einrichtung (Kamera) durch Übertragung der erfassten Bilddaten auf einen ortsfernen oder -unabhängigen Monitor in Echtzeit, um unabhängig von der Örtlichkeit zeitgleich durch einen Mitarbeiter beobachtet zu werden (sog. verlängertes Auge oder Kamera-Monitoring). Über technisch erforderliche, temporäre Speicherungen von Daten für die Realisierung und beschränkt auf die Dauer des Datenübertragungsprozesses hinaus werden keine Daten gespeichert.
Gleichwohl ist auch hiermit eine deutliche Gefährdung des Rechts auf informationelle Selbstbestimmung der beobachteten Personen verbunden:
Schon bei der bloßen Videobeobachtung ohne Speicherung können Betroffene identifizierbar wahrgenommen, ihre ganze Erscheinung und ihre Verhaltensweisen detailliert nachvollzogen und individuell zugeordnet werden. Videobeobachtung ist auch darauf gerichtet, das Verhalten der Betroffenen zu lenken.

b)Videoaufzeichnung:
Videoaufzeichnung beinhaltet zusätzlich eine anhaltende Speicherung von Bilddaten, die eine zeitversetzte oder wiederholte Beobachtung und weitere Auswertung ermöglicht. Gespeicherte Daten könnten auch mit anderen verbunden und an Dritte übermittelt werden. Die dadurch eröffneten Verarbeitungsmöglichkeiten können die Interessen der Betroffenen in wesentlich höherem Maße beeinträchtigen als die reine Videobeobachtung.

Sie darf daher erst dann vorgenommen werden, wenn Tatsachen die Annahme rechtfertigen, dass mit einer erheblichen Verletzung der Rechtsgüter zu rechnen ist. In der Regel wird dies erst nach entsprechenden Vorkommnissen in der

Vergangenheit angenommen werden können. Entsprechend dem Erforderlichkeitsgrundsatz ist jeweils zu prüfen, ob z.B. eine anlassbezogene Einzelfallaufzeichnung, eine zeitlich begrenzte oder eine fortlaufende Aufzeichnung ausreicht. Handelt es sich um eine Zugangsregelung, so erscheint eine anlassbezogene Aufzeichnung oft ausreichend, wie z.B. das Auslösen der Videoüberwachung durch Klingeln an einer Schranke vor einem Parkplatz.

Zur Videoaufzeichnung gehört auch das sog. Black-Box-Verfahren. Bei diesem Verfahren werden die über optische Einrichtungen (Kameras) erfassten Bilddaten fortlaufend oder ereignisgesteuert über einen bestimmten Zeitraum für eine künftige Nutzung aufgezeichnet bzw. gespeichert, ohne dass eine dauerhafte Zugriffsmöglichkeit besteht oder eine Beobachtung in Echtzeit erfolgt. Eine Auswertung erfolgt nur nach dem Eintreten bestimmter, vor der Aufnahme definierter Vorfälle und unter Einhaltung vorgegebener Auswertungsabläufe. Dazu gehört in der Regel die Einsichtnahme nach dem Vier-Augen-Prinzip, die Protokollierung der Einsichtnahme und ggf. der Weitergabe des Bildmaterials.

Kurzbeschreibung:
Die Kurzbeschreibung soll dazu dienen, einen groben Überblick über Art und Ausmaß der Anlage zu erhalten.

Zu Musterformularnummer 2: Zweck

Schutz von Personen und Sachen:
Entsprechend dem erheblichen Eingriffscharakter der anlasslosen Videoüberwachung zu Zwecken des Hausrechts rechtfertigt nach dem Willen des Gesetzgebers nur der Schutz wichtiger Rechtsgüter (Personen und Sachen) die Überwachung.
Es ist zu beachten, dass nach § 14 NDSG weder die fachliche Aufgabenwahrnehmung noch die Verfolgung von Ordnungswidrigkeiten und Straftaten eine Beobachtung oder Aufzeichnung rechtfertigen.

Überwachung von Zugangsberechtigungen:
Öffentlich zugängliche Räume unterliegen im Allgemeinen keinen Zugangsbeschränkungen und bedürfen insoweit keiner Überwachung von Zugangsberechtigungen. Es müssen daher besondere Gründe für ein videogesteuertes Zugangskontrollsystem vorliegen.
Auch nicht öffentlich zugängliche Räume wie solche ohne Publikumsverkehr bedürfen üblicherweise keiner Videoüberwachung. Erst wenn ein Bereich besonders gefährdet ist wie Serverräume oder Datensammlungen von besonderer Geheimhaltungsbedürftigkeit oder besonders gefährdete Personen, kann eine Videoüberwachung in Betracht kommen, soweit nicht weniger belastende Maßnahmen wie Zugangsschlüssel oder -karten eine hinreichende Sicherung gewährleisten.

Zu Musterformularnummer 3: Kreis der Betroffenen

Kreis der Betroffenen:
Betroffene sind alle Personen, die sich in den Aufnahmebereich einer Kamera begeben. Es kommt darauf an, den Aufnahmewinkel und die sonstigen Einstellungen so zu definieren, dass z.B. die Aufnahme von Passanten im Außenbereich auf das unvermeidbare Maß beschränkt bleibt. Unzulässig ist daher die Überwachung einer Behörde von der gegenüber liegenden Straßenseite aus, wenn dadurch auch unbeteiligte Passanten, Lieferanten u.ä. erfasst werden.
Sind auch Mitarbeiter betroffen, so darf dies nicht zu einer Leistungsüberwachung führen. Im Übrigen bleibt die Videoüberwachung von Mitarbeitern sonstigen spezifischen gesetzlichen Regelungen wie der Regelung über Dienstvereinbarungen vorbehalten.

Sonstige Betroffene:
Hier sind alle weiteren Personen aufzulisten, die von der Videoüberwachung erfasst werden können, um das

Gefährdungspotential zutreffend einschätzen zu können.

Zu Musterformularnummer 4: Personenkreis mit Zugang zu den erhobenen Bilddaten Sonstige Zugangsberechtigte:

Hier sind alle weiteren Personen aufzulisten, die Zugang zu den Daten haben.

Zu Musterformularnummer 5: Abwägung von Zielen und Gefahren

Abwägung der Interessenlagen:
Hier sind die allgemeinen Abwägungen für die Erforderlichkeit und Rechtmäßigkeit der Videobeobachtung, der Videoaufzeichnung, der angemessenen technisch-organisatorischen Ausgestaltung und der Fortführung der Videoüberwachung darzustellen.
Die öffentlichen Interessen der Dienststelle sind unter diesen Aspekten mehrfach mit den Interessen der Betroffenen abzuwägen. Schon wenn ein Anhaltspunkt nicht ausgeschlossen werden kann, nach denen die Interessen der Betroffenen die öffentlichen Interessen überwiegen können, ist die jeweilige Form der Videoüberwachung unzulässig. Für Bereiche, die dem höchstpersönlichen oder Intimbereich der beobachteten Personen zuzuordnen sind, überwiegt in der Regel das Interesse der betroffenen Personen. So ist z.B. die Videoüberwachung von Toiletten, Duschen oder Umkleideräumen unzulässig.

Videobeobachtung tangiert immer das Recht, sich unbeobachtet im öffentlichen Raum bewegen zu dürfen. Videoaufzeichnungen verstärken immer die Gefahren der weiteren Auswertung, der Verknüpfung mit anderen Datenbeständen, der Profilbildung und der Übermittlung an Dritte. Je nach Standort und Kameraeinstellung können die Interessen der Betroffenen in unterschiedlichem Maße betroffen sein. Dementsprechend ist festzuhalten, warum die Videoüberwachung gleichwohl für erforderlich und ausreichend erachtet wird.

Dazu sind verschiedene Tatbestandsmerkmale zu prüfen:

Zu 5.1: Alternativen zur Videoüberwachung:

Sowohl bei der Videobeobachtung als auch bei der Videoaufzeichnung ist im Einzelfall zunächst abstrakt zu prüfen, ob es weniger belastende Maßnahmen gibt und welches Maßnahmenpaket die geringste Eingriffstiefe aufweist. Die Prüfung ist nicht nur abstrakt vorzunehmen, sondern hat alle maßgeblichen Umstände des Einzelfalls zu berücksichtigen. In diesem Zusammenhang sind insbesondere solche Maßnahmen zu prüfen, die eine Verarbeitung personenbezogener Daten gar nicht oder in geringerem Umfang erfordern (Grundsatz der Datensparsamkeit).
Grundsätzlich können dabei folgende Fragestellungen verfolgt werden:

- Können die Ziele oder einzelne Teilziele ohne die Verarbeitung personenbezogener Daten erreicht werden?
- Gibt es alternative bzw. flankierende Maßnahmen?
- Kann der Umfang der personenbezogenen Daten reduziert werden, z.B. durch Reduzierung des Blickwinkels, der Bildauflösung und der Betriebszeiten, Verzicht/Einschränkung von Videoaufzeichnungen, Reduzierung der Speicherdauer, ereignisgesteuerte Aufnahmen o.ä.?
- Kann eine Anonymisierung erfolgen? Wenn ja, zu welchem Zeitpunkt?
- Kann eine Pseudonymisierung erfolgen? Wenn ja, zu welchem Zeitpunkt?

Eine Auflistung möglicher Maßnahmen im Zusammenhang mit der Videoüberwachung ist ohne Anspruch auf Vollständigkeit als Anlage beigefügt.

Überwiegende schutzwürdige Interessen der Betroffenen:
Sowohl bei der Videobeobachtung als auch je gesondert bei der Videoaufzeichnung und der Speicherdauer ist zu prüfen, ob Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.
Dafür sind zunächst die möglichen Interessen der Betroffenen zu ermitteln. Zu beachten ist immer das Interesse, sich unbeobachtet im öffentlichen Raum bewegen zu können.
Weitere schutzwürdige Interessen sind insbesondere n Bereichen, gegeben, die Rückschlüsse auf bestimmte besonders geschützte Informationen zulassen wie Gesundheits- oder Sozialbelange, Bezug zu Personalrat oder behördlichem Datenschutzbeauftragten.

Zu 5.2: Videobeobachtung

Gründe für den Einsatz einer Videobeobachtung:
Bitte die Gründe auflisten, die nach Abwägung die abschließende Beurteilung rechtfertigen.

Anhaltspunkte für ein überwiegendes Interesse:
Bitte die möglichen Anhaltspunkte benennen.

Wie werden die Interessen der Betroffenen berücksichtigt und geschützt?
Bitte alle Maßnahmen darstellen. In Betracht kommen z.B. die Maßnahmen bzw. Alternativen aus der Anlage.

Zu 5.3: Videoaufzeichnung

Welche Rechtsgüter sollen geschützt werden?
Hier bitte die Rechtsgüter nach § 25a Abs. 1 NDSG benennen.

Warum kann der Zweck nicht durch Beobachtung erreicht werden?
Die Aufzeichnung ist erst dann ins Auge zu fassen, wenn sonstige Maßnahmen und die Beobachtung den Zweck nicht erreichen können. Bitte die Gründe auflisten, die nach Abwägung die abschließende Beurteilung rechtfertigen.

Vorkommnisse der Vergangenheit:
Es können nur Tatsachen aus der Vergangenheit die Annahme rechtfertigen, dass weitere Vorkommnisse zu erwarten sind. Sie sind nachvollziehbar zu benennen, z.B. mit Aktenzeichen des Hausverbots, Aktenzeichen der Strafanzeige. Es empfiehlt sich daher, zu diesem Zweck einen Sammelvorgang anzulegen.

Tatsachen, welche die Annahme künftiger Rechtsverletzungen rechtfertigen:
Bitte Tatsachen benennen und belegen. Vermutungen und subjektive Empfindungen wie ein erhöhtes Sicherheitsgefühl reichen nicht aus. Die Tatsachen müssen die Annahme künftiger Rechtsverletzungen rechtfertigen. Es müssen erhebliche Rechtsgüter im Sinne des Abs. 1 betroffen sein.
Es gelten die Hinweise unter 5.1. Für die Videoaufzeichnung sind die Interessen der Betroffenen erneut abzuwägen: mit der allgemeinen Speicherung erhöhen sich die Gefahren der weiteren Auswertung, der Verknüpfung mit anderen Datenbeständen, der Profilbildung und der Übermittlung an Dritte.

Anhaltspunkte für ein Überwiegen der Interessen der Betroffenen:
Bitte die möglichen Anhaltspunkte benennen.

Speicherdauer:
Nach dem Kommentar (Nr.13) zu § 25a NDSG-alt ist eine Speicherung maximal bis zum nächsten Arbeitstag zulässig. Ein Schaden kann zwar nicht immer sofort festgestellt werden (z.B. Urlaub des Verantwortlichen), dennoch besteht die

Pflicht, mögliche kurze Speicherfristen nach dem Erforderlichkeitsprinzip zu ermitteln und festzulegen.
Die Daten sind darüber hinaus unverzüglich vorzeitig zu löschen, sobald feststeht, dass die schutzwürdigen Interessen des Betroffenen einer weiteren Speicherung entgegenstehen. Dies kann sich zum Beispiel aus dem persönlichen Vortrag des Betroffenen ergeben.
Eine Ausdehnung der Aufzeichnung auf 72 Stunden ist in begründeten Fällen tolerabel.

Schutzwürdige Interessen, die einer Regel-Speicherung entgegenstehen können:
Es gelten auch hier die bei der Videobeobachtung behandelten Fallgruppen. Allerdings beinhaltet die Aufzeichnung einen erheblich tieferen Eingriff in das informationelle Selbstbestimmungsrecht, so dass die Gewichtung sich zugunsten des Betroffenen verschieben kann.

Verfahren zur vorzeitigen Löschung im Einzelfall:
Soweit schutzwürdige Interessen überwiegen, sind die Aufzeichnungen vorzeitig, d.h. vor Ablauf der festgesetzten Speicherfrist, zu löschen. Das Verfahren muss sichergestellt sein und ist hier zu beschreiben.

Regelung des Zugriffs auf Aufzeichnungen:
Das Verfahren zum Zugriff auf Aufnahmen sollte besonders dokumentiert werden. Es muss revisionssicher nachvollziehbar sein, wer wann aus welchem Grund auf welche Daten zugegriffen hat. Zusätzliche Anforderungen sind insbesondere beim Black-Box-Verfahren zu stellen.(Vieraugenprinzip, Verschlüsselung, Protokollierung u.ä).
Grundsätzlich ist festzulegen, zu welchen Zwecken einzelne Kameras dienen und zu welchem Zweck durch wen auf die Aufzeichnungen zugegriffen werden kann. Der Zugriff kann z.B. auch schon durch zeitgleiche Beobachtung erfolgen oder erst im Wege des näher zu regulierenden Ablaufs bei der Auswertung von Blackbox-Verfahren.

Zu 5.4: Verfahren zur weiteren Bearbeitung, betroffene Rechtsgüter

Verfahren zur weiteren Verarbeitung:
Das Gesetz unterscheidet zwei grundsätzliche Varianten:

- Die weitere Verarbeitung zu den Zwecken, zu denen die Daten erhoben wurden.
  Dies sind die näher zu bezeichnenden Zwecke nach § 14 NDSG.
- Die weitere Verarbeitung zu anderen Zwecken. Diese sind abschließend im Gesetz aufgezählt:
  Zur Abwehr von Gefahren für die öffentliche Sicherheit oder zur Verfolgung von Straftaten. Dazu muss die Verarbeitung erforderlich sein oder die Betroffenen müssen ausdrücklich eingewilligt haben.

Zu 5.5: Gründe für die weitere Erforderlichkeit der Videoüberwachung:

Der Daten verarbeitenden Stelle obliegt die fortwährende Verpflichtung zur Prüfung, ob die Voraussetzungen für die Videoüberwachung und die weitere Verarbeitung der Bilddaten noch gegeben sind. Ist dies nicht mehr der Fall, ist die Überwachung einzustellen und die Videoanlage abzubauen, gespeicherte Bilddaten sind zu löschen.

Zu Musterformularnummer 6: Technische und organisatorische Maßnahmen

Ist die rechtliche Erforderlichkeit einer Videoüberwachungsmaßnahme grundsätzlich festgestellt worden, bedeutet dies noch nicht, dass jedes handelsübliche Gerät ohne weiteres zur Überwachung genutzt werden kann. In der Regel wird vielmehr eine Vielzahl flankierender, technischer und organisatorischer Maßnahmen notwendig sein, um den allgemeinen datenschutzrechtlichen Grundsätzen und datenschutzrechtlichen Bestimmungen zu genügen.

Schutzziele
Die verantwortliche Stelle hat nach Feststellung der rechtlichen Zulässigkeit die technisch-organisatorischen

Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes sicherzustellen.
Die Schutzziele müssen für alle Kameras durch eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO gesondert geprüft und festgestellt werden. Sind weitere Komponenten und Schnittstellen vorhanden, sind auch diese in die Bewertung und Dokumentation einzubeziehen.

So muss durch geeignete technische und organisatorische Maßnahmen gewährleistet werden, dass der Aufnahmebereich tatsächlich auf das rechtlich zulässige Maß beschränkt wird .Dies kann feste Kameraeinstellungen in Verbindung mit der Nutzung von Funktionen wie dem privat-masking (Definition von Privatbereichen) erfordern. Es muss sichergestellt werden, dass ein rechtlich zulässiger Aufnahmebereich nicht durch unbefugte Änderung der Einstellungen und der Ausrichtung der Kameras in unzulässiger Weise verändert wird. Dies beinhaltet ggf. den Vandalismusschutz für die Kamera, Zugangs- und Zugriffsbeschränkungen zur Anlage, den Verzicht auf bzw. die besondere Reglementierung von Fernsteuerungsfunktionen,

Auch bei der technischen Ausgestaltung des Verfahrens und im Betrieb ist der Grundsatz der Erforderlichkeit zu beachten. Nicht sämtliche verfügbaren Funktionalitäten (Hochauflösung, Fernsteuerung, Zoom, Benachrichtigungsfunktionen, Audio, etc.) sind erforderlich oder rechtlich zulässig. Durch Reduzierung des Blickwinkels der Kamera, Verzicht auf Aufzeichnung bzw. Beschränkung der Aufnahmezeiten, verkürzte Speicherzeiten sowie den Einsatz existierender technischer Möglichkeiten wie die Verschleierung (verpixeln) von Video-Klardaten in Echtzeit können Daten zudem erheblich reduziert werden.

Generell sollten nur Systeme mit den für die Aufgabenerfüllung unabdingbar erforderlichen Leistungsmerkmalen eingesetzt werden. Zusätzlich Funktionalitäten beinhalten weitere Gefahren für die Rechte von Betroffenen und sind ggf. auch rechtlich nochmals gesondert zu betrachten.

Vertraulichkeit
Das Schutzziel der Vertraulichkeit bedeutet, dass technische und organisatorische Maßnahmen zu treffen sind, die gewährleisten, dass nur dazu Befugte die erhobenen und ggf. gespeicherten Bilddaten zur Kenntnis nehmen können.
Die Vertraulichkeit muss für den gesamten Verarbeitungsprozess gewährleistet werden, die Sicherheitsmaßnahmen daher sämtliche Systemkomponenten (Kamera, Verbindungswege, Monitore, Rekorder, Server, Datenträger etc.) und organisatorische Maßnahmen zur Sicherung vor unbefugter Einsichtnahme auf den Monitor erfassen.
Es bedarf eines Zugangs- und Zugriffskonzeptes, in welchem die jeweiligen Verarbeitungsbefugnisse und Verantwortlichkeiten festgeschrieben werden.
Hinreichende Sicherungsvorkehrungen sind insbesondere auch bei drahtloser Verbindung einzelner Komponenten zu treffen.

Integrität:
Integrität bedeutet, dass die Daten während des gesamten Bearbeitungszeitraums unverfälscht, vollständig und widerspruchsfrei bleiben.
Sowohl Videobeobachtung als auch Videoaufzeichnung können ohne Integrität der Daten nicht auskommen. Es ist zwingend erforderlich, dass sich Beobachter und Gericht darauf verlassen können, dass ein gezeigtes Bild das Geschehen an einem bestimmten Ort zu einer bestimmten Zeit zutreffend wiedergibt.

Verfügbarkeit
Verfügbarkeit verlangt, dass die personenbezogenen Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können. Dazu bedarf es u.a. eines ordnungsgemäßen Zugangs zum System (Passwortschutz, Rollenkonzept), angemessener Belichtung, ausreichender Speicherkapazität, eines hinreichenden Löschungsschutzes und einer hinreichend belastbaren Hardware. Erforderlich sind ggf. eine redundante Ausstattung, Backups sowie Schutz vor Witterungseinflüssen und Vandalismus.

Authentizität:
Authentizität bedeutet, dass Daten ihrem Ursprung zugeordnet werden können.

Staatliche Stellen sind hierauf für die Beweiskraft angewiesen. Die Auswertung setzt auf derZuordnungsfähigkeit der Bilder auf. Je nach Nutzung können hieraus gravierende Folgen für die Betroffenen entstehen. Nur durch eine hinreichende Dokumentation der Abläufe, der eingesetzten Geräte und der Systemkonfiguration (welche Kameras mit welchem Blickwinkel werden wann wo eingesetzt, wer hat aus welchem Anlass wann Zugriff,etc.) kann belastbares Material produziert werden.

Revisionsfähigkeit:
Revisionsfähigkeit bedeutet, dass festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Art verarbeitet hat. Auch hier kommt es auf die authentische und unverfälschte aber auch den Nachweis einer rechtmäßigen Nutzung der Daten an. Werden Aufnahmen (unbefugt) bearbeitet und verändert, sind sie als Beweismittel wertlos, ebenso, wenn nicht hinreichend sicher nachgewiesen werden kann, dass eine Veränderung nicht stattgefunden hat.
Tauchen Bilddaten aus den Überwachungskameras in anderen Zusammenhängen auf, muss nachvollziehbar sein, wer wann Zugriff auf die entsprechenden Daten hatte.
Dabei sind pro Komponente sowohl die spezifische Gefährdung der einzelnen Schutzziele als auch die dagegen getroffenen Maßnahmen zu beschreiben und einer abschließenden Gesamtbewertung zu unterziehen.
Die Sicherung der technischen und organisatorischen Belange ist immer eine kontextabhängige, oft iterative und mit zunehmender Komplexität der Verfahren auch anspruchsvollere Angelegenheit. Hier ist neben dem Grundsatz der Datensparsamkeit vor allem der Schutzbedarf zu beachten, der sich einerseits aus dem Zweck der Verarbeitung, der Art und dem Umfang der zu verarbeitenden Daten ergibt und andererseits abhängt von der Ausgestaltung des technischen Verfahrens.

Schutzbedarfsfeststellung
Für die näher in Betracht zu ziehende Videoüberwachungsalternative wird der Schutzbedarf festgestellt. Hierbei werden die Fragestellungen beantwortet:

- Welche Verfahren und welche zu verarbeitenden Informationen werden betrachtet?
- Wie hoch sind Schäden aufgrund von Bedrohungen zu bewerten?

Die Schadenshöhe kann mit einer 3-stufigen Skala (1=normal, 2= hoch, 3= sehr hoch) bewertet werden, deren Skalierung ggf. auf die spezifischen Bedingungen angepasst werden muss.
Als Schutzziele sollten die hier genannten Ziele herangezogen werden: Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität und Revisionssicherheit.

Bedrohtes Objekt	Wert der Vertraulichkeit	Wert der Integrität	Wert der Verfügbarkeit	Wert der Authentizität	Wert der Revisionsfähigkeit
1.)Kamera mit internem Speicher	3	2	2	2	2
2.) Netzverbindungen					

Tab.1: Ergebnis der Schutzbedarffeststellung (Beispiel)

Bedrohungsanalyse
Für die Bedrohungsanalyse werden die Fragestellungen beantwortet:

- Welche Objekte werden bedroht?
- Welchen Bedrohungen sind die Objekte ausgesetzt?

Bei der Bedrohungsanalyse werden die bereits vorhandenen Schutzmaßnahmen berücksichtigt. Das Ergebnis der Bedrohungsanalyse ist eine vollständige Aufzählung aller möglichen Bedrohungen, die einen Einfluss auf das zu erstellende Sicherheitskonzept haben. An dieser Stelle sollte die Vollständigkeit der Auflistung im Vordergrund stehen.

Welche Bedeutung die einzelnen Bedrohungen für das Verfahren haben, ist Gegenstand der folgenden Stufe und ergibt sich z.T. auch erst aus der Gesamtschau der möglichen Bedrohungen. Die Bedrohungen können in unterschiedlichem Detaillierungsgrad dargestellt werden. Der zuvor festgestellte Schutzbedarf liefert dafür wichtige Hinweise. Bei einem hohen Schutzbedarf sollten die Bedrohungen differenziert dargestellt werden. Insbesondere neuartige Bedrohungen sollten ausführlich erläutert werden. Zum einen kann auf diese Weise eine gemeinsame Beurteilung durch alle Beteiligten leichter erzielt werden, da ein gleiches Verständnis der Sachlage geschaffen wird. Zum anderen können sich daraus später wichtige Hinweise für technische und organisatorische Schutzmaßnahmen ergeben.

Bedrohtes Objekt	Darstellung der Bedrohung	Bedrohtes Schutzziel
1. Kamera ohne internen Speicher	Diebstahl	Verfügbarkeit
	Vandalismus	Verfügbarkeit
	Wasser, Feuer, Sturm	Verfügbarkeit
	Unberechtigter Zugriff	Vertraulichkeit
	Manipulation	Vertraulichkeit, Verfügbarkeit, Authentizität
2. Netzverbindungen	…	

Tab. 2: Ausschnitt aus einer Bedrohungsanalyse (Beispiel)

Die Bedrohungsanalyse muss um die spezifischen Gefahren der betrachteten Anlage und für sämtliche Systemkomponenten/Objekte (Netzverbindungen Kabel/Funk, Aufnahmegeräte, Monitore, Datenträger etc,) ergänzt werden.

Risikobewertung

In der Risikobewertung werden der Schutzbedarf und die ermittelten Bedrohungen zusammengeführt und die Eintrittswahrscheinlichkeit möglicher Schäden bestimmt.
Es wird die Frage beantwortet:

- Wie hoch ist der mögliche Schaden, der bei den einzelnen Objekten auftreten kann?

Die größten negativen Auswirkungen bestimmen maßgeblich die Risikobewertung.

Ergänzend kann noch betrachtet werden, ob einzelne Objekte deutlich häufiger Bedrohungen ausgesetzt sind. Die höhere Eintrittswahrscheinlichkeit eines Schadens sollte dann dazu führen, für dieses Objekt stärkere Schutzmaßnahmen abzuleiten.
Folgende Faktoren beeinflussen die Eintrittswahrscheinlichkeiten:

- der Nutzen, den Angreifer aus dem Angriff ziehen können; es sind materielle als auch immaterielle Werte in Betracht zu ziehen
- der Aufwand (zeitlich, finanziell, Ressourcen), der betrieben werden muss, um einen Angriff zu ermöglichen
- die notwendigen Kenntnisse, die für einen Angriff erforderlich sind
- die Gefahr für den Angreifer erkannt zu werden,
- die Schwere der Sanktionen für einen Angreifer,
- die Häufigkeit der Angriffsmöglichkeiten, z.B. die Häufigkeit der Datenübertragungen
- die Zugänglichkeit der einzelnen Komponenten des Verfahrens
- die Anzahl der Personen, die Zugang zum Verfahren haben oder sich Zugang verschaffen können.

Die Ergebnisse der Risikobewertung werden in einer Tabelle zusammengestellt:

Bedrohtes Objekt	**Darstellung der Bedrohung**	**Bedrohtes Schutzziel**	**Schadenshöhe**	**Risiko tragbar?**

1. Kamera mit gespeicherten Daten	Diebstahl	Vertraulichkeit, Verfügbarkeit, Integrität, Authentizität	**3**	**Nein**
3. ...				

Tab. 2: Ergebnis einer Risikobewertung (Beispiel)

Ableitung von Schutzmaßnahmen
Für alle untragbaren Risiken müssen geeignete technische und organisatorische Maßnahmen konzipiert werden, die die Eintrittswahrscheinlichkeit und/oder die Schadenshöhe so weit reduzieren, dass die Schwelle der tolerierten Risiken unterschritten wird. Die zusätzlich durchzuführenden Schutzmaßnahmen dürfen dabei nicht isoliert betrachtet werden. Es sind sowohl gegenseitige Abhängigkeiten als auch die Einbettung in den bestehenden technischen und organisatorischen Rahmen zu berücksichtigen. Die Kompatibilität der Einzelmaßnahmen muss gegeben sein. Auch organisatorische Abhängigkeiten wie z.B. die Widerspruchsfreiheit zu bestehenden Regeln und Dienstvereinbarungen muss gewährleistet sein bzw. durch entsprechende Anpassungen hergestellt werden. Darüber hinaus sind auch personenbezogene Aspekte zu berücksichtigen; hier vor allem die Akzeptanz der Nutzer sowie ihre Qualifikation, damit die Maßnahmen in der Praxis auch greifen. Ggf. sind auch gezielte Fortbildungsmaßnahmen durchzuführen.

Offenlegung von Restrisiken
Trotz der durchgeführten Maßnahmen können Restrisiken verbleiben. Diese sollten konkret benannt und dokumentiert werden, um sicherzustellen, dass diese Risiken von den Entscheidungsträgern als tragbar bewertet werden. Andernfalls sind zusätzliche Schutzmaßnahmenerforderlich.

Zu Musterformularnummer 7: Art der Geräte zur Videoüberwachung:

Es sind alle Bestandteile der Anlage eindeutig zu benennen einschließlich ihrer besonderen Leistungsmerkmale und Einstellungen, um die Möglichkeiten und Risiken der Anlage zutreffend zu erfassen.
Je nach Einsatz sind insbesondere die Kameras einzeln zu beschreiben.

Standort der Geräte:
Die Standorte sind abschließend zu verzeichnen.

Räumlicher Überwachungsbereich:
Zur Einschätzung der Geeignetheit und Angemessenheit ist insbesondere die bildliche Darstellung des Überwachungsbereichs und die maximalen Aufnahmemöglichkeiten der Kameras zu beschreiben. Es sind geeignete Mittel zu treffen und zu dokumentieren, die die Einhaltung der rechtlich zulässigen Videoüberwachung sicherstellen.

Zu Musterformularnummer 8: Art der Überwachung:

Dieser Punkt ist nur auszufüllen, wenn die Anlage mehrere Kameras umfasst.
Pro Kamera ist für die Anlage festzulegen, um welche Art der Videoüberwachung es sich handelt. Dabei sind auch Abstufungen von Beobachtung und Aufzeichnung einschließlich sonstiger Maßnahmen zu beschreiben.
Erst durch die einzelnen Kameraeinstellungen kann abschließend beurteilt werden, ob die Maßnahme in Gänze den datenschutzrechtlichen Anforderungen entspricht.

Zu Musterformularnummer 9: Dauer der Überwachung:

Die Überwachungsdauer ist ein an den jeweiligen Gegebenheiten des Einzelfalls orientierte Maßnahme zur Sicherung des geringst möglichen Eingriffs.
Dabei sind unter „sonstige Beobachtungs-/Aufnahmezeiten“ z.B. zeitlich befristete Veranstaltungen anzugeben.

Zu Musterformularnummer 10: Nächster Prüfungstermin:

Zwar sollte die Videoüberwachung auf ihre Erforderlichkeit fortwährend überprüft wären, aus organisatorischen Gründen kann aber hier eine Frist angegeben werden. Eine umfangreiche Überprüfung sollte mindestens alle zwei Jahre erfolgen.
Es ist daher durch Dokumentation des nächsten Prüftermins sicherzustellen, dass die jeweils erforderlichen Prüffristen festgelegt und im Rahmen des weiteren Verwaltungsablaufs überwacht werden.

Anlage

Mögliche Maßnahmen und mildere Mittel bei der Abwägung über die Einführung einer Videoüberwachungsmaßnahme:

Einlasskontrolle:

Pförtner, Logbuch, Schlüssel, Chipkarte , anlassbezogene Beobachtung, ununterbrochene Beobachtung, Beobachtung mit Aufzeichnung

Innerhalb von Dienstgebäuden:

Einlasskontrollen, Begleitung der Besucher
allgemeine soziale Kontrolle in Wartebereichen
bauliche Maßnahmen

Serverräume:

Logbuch mit Gegenzeichnung
Vieraugenprinzip,
Alarmanlage mit Videoüberwachung außerhalb der Geschäftszeiten

Kassenräume:

Vieraugenprinzip
Alarmanlage
Videobeobachtung (Achtung: Arbeitnehmerdatenschutz!)
Anlassbezogene Videoaufzeichnung außerhalb der Dienstzeit

Besonders geschützte Datenbestände:

besondere Zugangsberechtigungen
Verschluss
Alarmanlage außerhalb der Dienstzeit

Fassaden:

Nach entsprechenden Vorfällen Black-Box-Verfahren

Parkplätze:

Parkschranken mit Schlüssel,
Videoüberwachung mit Besucherklingel
Reduzierte Bildzahl

Besonders gefährdete Personen / Personenschutz:

Parkschranken / Gitter
Chipkarte
Anlassbezogene Videobeobachtung
Parkschranken, Zugänge mit Videoüberwachung