Handreichung zur Videoüberwachung

durch öffentliche Stellen
in Ausübung des Hausrechts nach § 30 Abs.7 HmbDSG

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

Hamburg

Vorbemerkung

Am 15.09.2010 hat die Hamburgische Bürgerschaft mit dem Fünften Gesetz zur Änderung des Hamburgischen Datenschutzgesetzes (Drucksache 19/6086,vgl. http://www.buergerschaft-hh.de/parldok/) den § 30 (Videoüberwachung) neu beschlossen.

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 nach § 30 Absatz 7 HmbDSG zu fertigenden Dokumentation und zur Unterstützung der vor der Einführung vorzunehmenden Abwägungsprozesse hat der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit zur Orientierung ein Musterformular erstellt (http://www.hamburg.de/datenschutzrecht/)und bietet mit dieser Handreichung weitergehende Hinweise und Ausfüllhilfen an.

Diese Handreichung soll insbesondere auch als Hilfestellung für die erforderlichen Abwägungen gemäß § 30 Absatz 7 Nummer 6 HmbDSG 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 § 30 HmbDSG.

Die Erläuterungen zum Musterformular folgen dem Aufbau des Musterformulars und der dortigen Nummerierung. Die hier behandelten Stichworte sind darin bis auf diejenigen des Titels entsprechend der Nummerierung in § 30 HmbDSG und im Formular 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 be-

liebigen 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, die 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 § 30 HmbDSG

§ 30 HmbDSG regelt als Querschnittsgesetz die Videoüberwachung öffentlicher Stellen ausschließlich zu Zwecken des öffentlichen Hausrechts. Der Gesetzgeber hat damit eine Regelung getroffen, die geeignet ist, einen angemessenen Ausgleich zwischen dem Recht der Betroffenen, sich unbeobachtet im öffentlichen Raum zu bewegen, und dem öffentlichen Interesse an einem geordneten, störungsfreien Dienstbetrieb zu schaffen.

1.2.1. Verhältnis zu anderen Spezialregelungen, Behandlung von Altfällen

Festzuhalten bleibt aber, dass der Hamburgische Gesetzgeber anders als z.B. der Bundesgesetzgeber eine restriktive Regelung treffen wollte. Eine allgemeine Ermächtigung zur Videoüberwachung zu Zwecken der Aufgabenerfüllung erfolgte nicht.
Soweit spezialgesetzliche Regelungen zur Videoüberwachung bestehen, ist zunächst zu prüfen, ob sie hinsichtlich des Hausrechts eine abschließende Regelung beinhalten.
Zu den zur Zeit bestehenden Regelungen gilt folgendes: § 31 SchulG, § 119 StrVollzG, 115 JStrVollzG und § 102 UHaftG sind abschließende Regelungen, so dass § 30 HmbDSG in diesen Bereichen keine Anwendung findet. Lediglich § 8 PolDVG enthält verschiedene spezialgesetzliche Ermächtigungen zur Videoüberwachung als spezifisches Arbeitsinstrument zur polizeilichen Gefahrenabwehr, nicht aber zur Videoüberwachung zu Hausrechtszwecken. Sollen Polizeidienststellen aus Gründen des Hausrechts überwacht werden, findet somit § 30 HmbDSG Anwendung.
Da die Videoüberwachung als spezielle Form der personenbezogenen Datenverarbeitung unter dem Vorbehalt des Gesetzes steht und die früher praktizierte analoge Anwendung des § 6 b des Bundesdatenschutzgesetzes (BDSG) verfassungswidrig war, sind jetzt auch die noch bestehenden Altanlagen anhand der neuen Vorschrift zu überprüfen.
Einschränkungen gelten insbesondere für Videoüberwachungen, die der Erfüllung der funktional übertragenen Aufgaben dienten (§ 6 b Abs. 1Satz 1 Nummer 1 BDSG). Diese soll nach dem Willen des Hamburgischen Gesetzgebers jetzt spezialgesetzlichen Regelungen vorbehalten bleiben. Nicht zulässig ist danach z.B. die Überwachung von Baufortschritten auf Baustellen oder zur Sicherung des Verkehrs auf Klappbrücken oder Schleusen.
Zu beachten ist auch, dass die Definitionen und Voraussetzungen von Videoüberwachung, -beobachtung und –aufzeichnung von § 6 b BDSG abweichen (siehe dazu näher unter 2.3).

1.2.2 Rechtliche Anforderungen

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

Grundvoraussetzung für die Anwendung des § 30 HmbDSG ist, dass die anwendende Stelle Hausrecht besitzt (zum Begriff siehe unter 2, zur Überschrift, Hausrecht).

Videoüberwachung umfasst die Videobeobachtung und die Videoaufzeichnung (zu den Begrifflichkeiten siehe unter Erläuterungen, zu 3).

Sie muss im Einzelfall geeignet sein, das Hausrecht zu den in Absatz 1 genannten Zwecken wahrzunehmen, und ist auf das erforderliche Maß zu beschränken. Es gilt der Grundsatz des geringstmöglichen Eingriffs.
Das Bundesverfassungsgericht hat die Videobeobachtung als weniger eingriffsintensiv gegenüber der Videoaufzeichnung beschrieben. 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.

Der Hamburgische Gesetzgeber hat dementsprechend an Videobeobachtung und an Videoaufzeichnung unterschiedliche Anforderungen formuliert:
Videobeobachtung kann im Wesentlichen unterstützend und präventiv eingesetzt werden, um unmittelbar auf Störer einzuwirken und Hausverbote zu überwachen.
Videoaufzeichnung kann der Vorbereitung und Überwachung von Hausverboten dienen. Dies setzt jedoch voraus, dass Tatsachen die Annahme rechtfertigen, dass es zu weiteren Rechts-

verstößen kommt, was in der Regel nur aufgrund vorangegangener Vorkommnisse angenommen werden kann.

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 und zur Abwehr von Gefahren für Leib, Leben oder Freiheit einer Person 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 über die Datenverarbeitung zusätzlich 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.

1.2.3 Technische Anforderungen

Die verantwortliche Stelle hat auch zu gewährleisten, dass die für die jeweils angestrebte Videoüberwachung erforderlichen und angemessenen technisch-organisatorischen Maßnahmen getroffen werden (vgl. näher unter Erläuterungen, zu 7). 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?

Dazu sind die allgemeinen Sicherungsziele der Vertraulichkeit, der Integrität, der Verfügbarkeit, der Authentizität und der Revisionsfähigkeit, wie sie in §§ 8 Abs. 3 und 30 Abs. 6 HmbDSG beschrieben sind, zu überprüfen. Dies setzt eine Feststellung des Gefährdungspotentials ebenso voraus wie die Einschätzung der geplanten technischen und organisatorischen Maßnahmen (näheres siehe unter 2.7).
Die Anforderungen an die Dokumentation regelt Absatz § 30 Absatz 7 HmbDSG. Dabei ist sicherzustellen, dass auch die Abwägungsgründe gemäß Absatz 7 Ziffer 6 jeweils nachvollziehbar dokumentiert werden.

2. Erläuterungen zum Musterformular

Zur Überschrift:

Videoüberwachungsmaßnahmen:
Sie umfassen die Videobeobachtung und / oder die Videoaufzeichnung (zu den Begrifflichkeiten siehe unter 2.3). Die Befugnis beschränkt sich auf die optische Überwachung. Eine akustische Überwachung ist nach § 30 HmbDSG 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.
§ 30 HmbDSG befugt zu einer Videoüberwachung ausschließlich in Ausübung des Hausrechts der öffentlichen Stelle. Soll eine Videoüberwachung zu Zwecken der Aufgabenerfüllung erfolgen, bedarf dies gesonderter spezialgesetzlicher Ermächtigungen. Sind diese nicht vorhanden, ist die Videoüberwachung unzulässig.
Diese Einschränkung ist insbesondere bei der Überprüfung der Altverfahren zu beachten, vgl. näher unter 1.2.1.

Die Videobeobachtung wird vom Bundesverfassungsgericht (1 BvR 2368/06, Rz 38, 52, 56) als weniger belastend angesehen als die Videoaufzeichnung. Es ist daher je nach Ausgestaltung des Verfahrens zu prüfen und zu dokumentieren, ob die spezifischen Tatbestandsvoraussetzungen für die Beobachtung oder die Aufzeichnung gegeben sind (siehe näher unter 2.3).

Öffentliche Stellen:
Öffentliche Stellen sind alle Stellen, die nach § 2 HmbDSG unter die Anwendung des HmbDSG fallen, also insbesondere die Kernbehörden, sonstige Körperschaften des öffentlichen Rechts und Beliehene. Auch soweit Behörden am Wettbewerb teilnehmen, unterliegen sie trotz § 2 Absatz 2 Satz 1 HmbDSG hinsichtlich des anzuwendenden Hausrechts doch ausschließlich dem HmbDSG, da die abweichende Anwendbarkeit des Bundesdatenschutzgesetzes nur für die jeweiligen Aufgabenstellungen besteht, die dem Wettbewerb tatsächlich unterliegen (vgl. Erläuterungen zu § 2 HmbDSG,
http://www.hamburg.de/contentblob/254544/data/hamburgisches-datenschutzgesetz-1990-07-05-erlaeuterungen.pdf). Hierzu zählt das Hausrecht naturgemäß nicht.

Hausrecht:
Grundsätzlich ist das Hausrecht an die Verfügungsbefugnis des Berechtigten geknüpft und umfasst das Recht zu bestimmen, wer eine Örtlichkeit betreten darf und wer nicht.

§ 30 HmbDSG regelt ausschließlich das Hausrecht öffentlicher Stellen, also das öffentlich-rechtliche Hausrecht. Es leitet sich aus den der öffentlichen Stelle übertragenen Aufgaben ab und dient der Wahrung und Erhaltung des Hausfriedens als Voraussetzung eines geordneten Dienstbetriebs. Es hat insoweit präventiven Charakter. Es soll den widmungsgemäßen Gebrauch vor Störungen schützen und dient somit in erster Linie der Gefahrenabwehr. Das Hausrecht kann nur in engem örtlichem und sachlichem Zusammenhang auch Flächen außerhalb der einzelnen Dienstgebäude umfassen. Eine Überwachung des angrenzenden Straßenraums ist nach § 30 HmbDSG grundsätzlich nicht zulässig. Sie kann nur toleriert werden, soweit dies unvermeidbar ist.
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.

Zu Nummer 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. Sie ist damit auch die verantwortliche Daten verarbeitende Stelle nach § 4 HmbDSG.
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, sind folgende Grenzen zu beachten: Der Auftragnehmer darf nach § 3 HmbDSG nur technische Unterstützungsleistungen oder ähnliche Hilfsdienste erbringen. Dies sind nicht die Beobachtung selbst und Auswertung der Bilder sowie insbesondere die Entscheidung über Folgemaßnahmen, da hiermit Ermessensentscheidungen verbunden sind. Diese Aufgaben können nur im Wege der Funktionsübertragung (Beleihung) vergeben werden.
Auch die Befugnisse der öffentlichen Stelle werden durch die Beauftragung einer privaten Stelle nicht erweitert, also: keine aufgabenbezogene Videoüberwachung durch Vergabe an private Dritte. 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. Die Videoüberwachung nach § 30 HmbDSG ist ausschließlich entsprechend dem Hausrecht im und in engem räumlichen Bezug zum Dienstgebäude zulässig.

Betroffener Gebäudeteil/Außenfläche:
§ 30 HmbDSG ermächtigt bei Vorliegen der weiteren Voraussetzungen zur Überwachung folgender Bereiche: 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 allgemei-

nen 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 (vgl. Gesetzesbegründung, S. 3 f)sind Bereiche mit gesondertem, erhöhtem Schutzbedürfnis, wie dies z.B. bei Serverräumen oder der besonderen Geheimhaltung unterliegenden Datenbeständen (Zeugenschutzprogramme, Inkognito-Adoptionsverfahren u.ä.) 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.

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

Zu Nummer 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 § 30 HmbDSG neben der Ausübung des Hausrechts 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 Nummer 3: Rechtsgrundlage

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 Beschwer 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.

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 bloße Videobeobachtung.
Sie darf daher erst dann vorgenommen werden, wenn Tatsachen die Annahme rechtfertigen, dass mit einer erheblichen Verletzung der Rechtsgüter nach § 30 Abs.1 HmbDSG künftig 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.
In der Vergangenheit wurde das Verfahren als besonders datenschutzfreundlich in weiten Bereichen eingesetzt. Da es sich hierbei um ein Verfahren handelt, das Daten zunächst ohne konkreten Anlass speichert, kommt eine Nutzung künftig nur als Aufzeichnungsverfahren nach § 30 Absatz 2 in Betracht, wenn nämlich Tatsachen die Annahme rechtfertigen, dass künftig mit einer Verletzung der Rechtsgüter nach § 30 Abs. 1 HmbDSG zu rechnen ist. Bei vorhandenen Anlagen ist das Vorliegen dieser Voraussetzungen sorgfältig zu prüfen.

Videokamera-Attrappe (siehe auch Pkt. 6.5):
Videokamera-Attrappen sind Vorkehrungen, die den Anschein einer Videoüberwachung erwecken sollen, tatsächlich aber keine Bilddaten verarbeiten. Sie sind damit an sich nicht geeignet, die Schutzziele des § 30 HmbDSG zu erreichen. Sie sind in der Vergangenheit verschiedentlich eingesetzt worden, um verhaltenslenkend auf die Betroffenen einzuwirken. Durch Attrappen ist weniger das informationelle Selbstbestimmungsrecht und damit das Datenschutzrecht als vielmehr das allgemeine Persönlichkeitsrecht betroffen. Ohne diese Regelung könnten sie deshalb unkontrolliert eingesetzt werden.
Um die grundrechtseinschränkende Wirkung zu begrenzen, fordert § 30 Abs. 9 HmbDSG deshalb eine Abwägung der Erforderlichkeit entsprechend § 30 Abs. 1 HmbDSG, also insbesondere die Prüfung, ob mildere Mittel zur Verfügung stehen, die Abwägung mit den Interessen der Betroffenen sowie die Kennzeichnung und die Überprüfung der weiteren Erforderlichkeit nach Ablauf von spätestens zwei Jahren.
Die Kennzeichnung erfolgt am besten entsprechend 1.2.2 als Piktogramm und sollte sich beschränken auf die Angabe der verantwortlichen Stelle.

Zu Nummer 4: 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.
Werden auch Mitarbeiter erfasst, so darf dies nicht zu einer Leistungsüberwachung führen. Im Übrigen bleibt die Videoüberwachung von Mitarbeitern sonstigen spezifischen gesetzlichen Regelungen wie § 28 HmbDSG und der Regelung von Dienstvereinbarungen vorbehalten.
Besonders betroffen können Personenkreise sein, deren Überwachung eine hohe Persönlichkeitsrelevanz aufweisen kann. Dies gilt für alle Informationen nach § 5 Abs. 1 Satz 2 HmbDSG, insbesondere bei Informationen mit Gesundheitsbezug, Sozialdatenbezug, aber auch bei Hinweisen auf Kontakte zum Personalrat oder zum behördlichen Datenschutzbeauftragten. Dies ist bei der Abwägung unter 2.6 besonders zu berücksichtigen.

Sonstige Betroffene:
Hier sind alle weiteren Personen aufzulisten, die von der Videoüberwachung erfasst sein können, um das Gefährdungspotential zutreffend einschätzen zu können.

Zu Nummer 5: Personenkreis mit Zugang zu den erhobenen Bilddaten

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

Zu Nummer 6: 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 allein Anhaltspunkte nicht ausgeschlossen werden können, nach denen die Interessen der Betroffenen die öffentlichen Interessen überwiegen können, ist die jeweilige Form der Videoüberwachung 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 6.1: 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.
Beachtlich ist immer das Interesse, sich unbeobachtet im öffentlichen Raum bewegen zu können.
Weitere schutzwürdige Interessen sind insbesondere in Bereichen, gegeben, die Rückschlüsse auf bestimmte besonders geschützte Informationen zulassen wie Gesundheits- oder Sozialbelange, Bezug zu Personalrat oder behördlichem Datenschutzbeauftragten.
Werden auch Mitarbeiter erfasst, so darf dies nicht zu einer Leistungsüberwachung führen. Im Übrigen bleibt die Videoüberwachung von Mitarbeitern sonstigen spezifischen gesetzlichen Regelungen und der Regelung von Dienstvereinbarungen vorbehalten.
Überwiegende schutzwürdige Interessen können sich auch aus allgemeinen Rechtsgrundsätzen ergeben wie der Gerichtsöffentlichkeit, der öffentlichen Stimmauszählung nach Wahlen oder der Teilnahme an öffentlichen Sitzungen der Bezirksausschüsse. In allen diesen Fällen dient die Teilnahme an Sitzungen und Stimmauszählungen der Transparenz und der demokratischen Kontrolle. In diesen Fällen genießt auch schon der unbeobachtete Weg zum Gerichtssaal, zum Wahllokal u.ä. besonderen Schutz.

Höchstpersönlicher Bereich privater Lebensführung / Intimbereich:
Betroffen im Zusammenhang mit öffentlichem Hausrecht können z.B. Umkleidekabinen, Toiletten oder Ruheräume sein. Hier ist die Videoüberwachung zu Hausrechtszwecken ausgeschlossen, da grundsätzlich das schutzwürdige Interesse der Betroffenen überwiegt.

Zu 6.2: 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 6.3: Videoaufzeichnung

Welche Rechtsgüter sollen geschützt werden?
Hier bitte die Rechtsgüter nach § 30 Abs. 1 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, die 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 6.1. 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:
§ 30 Abs. 5 HmbDSG definiert die längst mögliche Speicherdauer mit einer Woche. Grundsätzlich besteht die Pflicht, mögliche kürzere 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.

Schutzwürdige Interessen, die einer Regel-Speicherung entgegenstehen können:
Es gelten auch hier die zur Beobachtung 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 6.4: 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 § 30 Absatz 1 HmbDSG.
- ➔ die weitere Verarbeitung zu anderen Zwecken. Sie ist abschließend im Gesetz aufgezählt:
  zur Verfolgung von Straftaten sowie zur Abwehr von Gefahren für Leib, Leben und Gesundheit.

Eine Übermittlung kann erfolgen aufgrund einer selbst erstatteten Strafanzeige oder auf Ersuchen der Staatsanwaltschaft bzw. der Polizei nach den Vorschriften der StPO. In beiden Fällen rechtfertigt § 30 HmbDSG nur die Nutzung zur Verfolgung herausgehobener und bedeutsamer Werte sowie Schaden von besonderem Ausmaß. Dies hat die Daten verarbeitende Stelle vor Übermittlung zu prüfen. Eine Übermittlung zum Zwecke der Verfolgung von Ordnungswidrigkeiten scheidet mangels ausdrücklicher Regelung aus.

Zweck, für den sie erhoben wurden:
Gemeint sind die eigenen Zwecke des Hausrechtsbesitzers nach § 30 Absatz 1 HmbDSG, also insbesondere die Dokumentation von Vorfällen, um darauf ein Hausverbot oder sonstige hauseigene Maßnahmen stützen zu können.

Verfolgung von Straftaten:
Die Verfolgung von Straftaten kann mangels Regelungsbefugnis des Hamburgischen Gesetzgebers nicht der maßgebliche Grund für eine Speicherung sein. Allein ohnehin vorhandene Aufzeichnungen können von Polizei und Staatsanwaltschaft nach StPO und PolDVG ausgewertet werden. Eine Auswertung allein zur Verfolgung von Ordnungswidrigkeiten ist unzulässig.

Abwehr von Gefahren für Leib, Leben oder Freiheit einer Person, Gefahr für bedeutende Sach- und Vermögenswerte:
Zur Gefahrenabwehr können Aufzeichnungen immer nur parallel zur direkten Beobachtung eingesetzt werden, denn Bildaufnahmen können keine Gefahren abwehren, sondern sie nur dokumentieren; es bedarf vielmehr des unmittelbaren Eingreifens zuständiger Stellen.

Zu 6.5:Videokamera-Attrappen
Zu Videokamera-Attrappen vgl. Pkt. 4.

Zu 6.6: Gründe für die weitere Erforderlichkeit der Videoüberwachung:
Nach § 30 Abs. 8 HmbDSG ist die Videoüberwachung mindestens alle zwei Jahre auf ihre Erforderlichkeit zu überprüfen. Schwerpunktmäßig ist zu prüfen, ob die angenommenen Gefährdungslagen fortbestehen. Als Anhaltspunkt für die Geeignetheit bei Vorkommnissen ist zu prüfen, wie deren weitere Entwicklung unter der Videoüberwachung verlief.
Die Gründe sollten nachvollziehbar dokumentiert werden.

Zu Nummer 7: Technische und organisatorische Maßnahmen nach Absatz 6

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. Entsprechend den allgemeinen Verwaltungsgrundsätzen ist dies auch revisionssicher zu dokumentieren. Dies betrifft bei der Videoüberwachung, egal ob in digitaler oder analoger Form, die Ziele der Vertraulichkeit, der Integrität, der Verfügbarkeit, der Authentizität und der Revisionsfähigkeit gemäß §§ 8 Abs. 2, 30 Abs. 6 HmbDSG. Die Schutzziele müssen für alle Kameras 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 privatmasking (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 Verzicht auf bzw. die besondere Reglementierung von Fernsteuerungsfunktionen, Vandalismusschutz für die Kamera, Zugangs- und Zugriffsbeschränkungen zur Anlage.

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.

Die nachfolgende Darstellung orientiert sich an dem Aufbau der Handreichung zur Risikoanalyse nach § 8 Abs. 2 HmbDSG (vgl. checkliste auf http://www.hamburg.de/datenschutzrecht/) und geht dabei den spezifischen Anforderungen an Videoüberwachungsanlagen nach.
Sie kann als Grundlage für die Einzelbeurteilung kopiert und, z.B. bei mehreren Kameras, um die jeweils erforderlichen Aspekte ergänzt werden.

Vertraulichkeit
Das Schutzziel der Vertraulichkeit bedeutet, dass technische und organisatorische Maßnahmen zu treffen sind, die geeignet sind zu 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 der Zuordnungsfähigkeit 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 (s. oben, 6) 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 Alternative 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 im § 8 Abs. 2 HmbDSG festgeschriebenen Ziele herangezogen werden: Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität und Revisionssicherheit.

Eine große Transparenz kann erzielt werden, wenn man den Schutzbedarf differenziert betrachtet und tabellarisch darstellt (Tab 1). Die Beteiligten können so das Ergebnis leichter nachvollziehen.

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 Schutzbedarfsfeststellung (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	Vertaulichkeit
	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, Mo-

nitore, 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?

Für die einzelnen bedrohten Objekte wird der Schaden jeweils durch den höchsten Wert einer Zeile aus Tab. 1 bestimmt. Es gilt das Maximumprinzip. Die größten negativen Auswirkungen bestimmen damit 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?
2. Kamera mit gespeicherten Daten	Diebstahl	Vertraulichkeit, Verfügbarkeit, Integrität, Authentizität	3	nein
3. ...				

Tab. 3: 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 ge-

geben sein. Auch organisatorische Abhängigkeiten wie z.B. die Widerspruchsfreiheit zu bestehenden Regeln und Betriebsvereinbarungen 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 Schutzmaßnahmen erforderlich.
Da die Analyse neben technischen Details der Schutzmaßnahmen auch Restrisiken beschreibt, sollte sie vertraulich behandelt werden und nicht unmittelbar Bestandteil der Dokumentation werden,.

Zu Nummer 8: Art der Geräte:

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 Nummer 9: Art der Überwachung:

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 als ganzen den datenschutzrechtlichen Anforderungen entspricht.

Zu Nummer 10: 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 Nummer 11: nächster Prüfungstermin:

Gemäß § 30 Abs. 8 HmbDSG hat eine Überprüfung der Videoüberwachung auf ihre Erforderlichkeit mindestens alle zwei Jahre zu erfolgen.

Aus spezifischen Gründen kann diese Frist verkürzt sein.
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, bei Gerichtsverhandlungen und Strafanstalten: Leibesvisitation; bei Gerichtsverhandlungen: Überwachung nur bei einzelnen gefährdeten Verfahren, keine generelle Eingangsüberwachung (Gerichtsöffentlichkeit)

innerhalb von Dienstgebäuden:
Einlasskontrollen, Begleitung der Besucher
allgemeine sozialen 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