

Orientierungshilfe zur Vorabkontrolle einer Videoüberwachung durch öffentliche Stellen im Land Niedersachsen

Diese Orientierungshilfe für Vorabkontrollen soll möglichst viele Anwendungsfälle von Videoüberwachungsmaßnahmen durch öffentliche Stellen im Land Niedersachsen abdecken. **Für die Videoüberwachung durch Bundesbehörden, Privatpersonen und die Privatwirtschaft gilt diese Orientierungshilfe nicht.**

Die Reihenfolge spiegelt u. a. einen möglichen Aufbau einer Vorabkontrolle (früher: Technikfolgenabschätzung) wieder. Außerdem werden zu den einzelnen Prüfpunkten einer Vorabkontrolle Checklisten, Textbausteine und sonstige Hinweise angeboten.

Die Vorabkontrolle zu einer Videoüberwachung ist eine Rechtmäßigkeitsprüfung in Abwägung zwischen den Grundrechten auf informationelle Selbstbestimmung, freie Meinungsäußerung und / oder Versammlungsfreiheit und der Interessenlage der öffentlichen Stelle unter grundsätzlicher Einbindung von Personalvertretungen sowie der technischen Beherrschbarkeit.

1. Systembeschreibung

Vom Staatlichen Baumanagement Niedersachsen wurde die „technische Information Videoüberwachungstechnik in den Dienststellen des Landes Niedersachsen – TI-Video-2010“ herausgegeben, welche einen praktischen Überblick über das Thema Videoüberwachungsanlagen verschafft und dem Verfasser einer Vorabkontrolle insbesondere technisches Hintergrundwissen vermittelt.

Für den Umgang mit und dem Verständnis für Abkürzungen aus dem technischen Bereich in deutscher und englischer Sprache wird auf das erstellte Abkürzungsverzeichnis in Zusammenhang mit Videoüberwachung des Landesbeauftragten für den Datenschutz Niedersachsen verwiesen.

1.1 Ist-Zustand

Der Normalfall ist, dass der Ist-Zustand lediglich beschreiben wird, wenn es eine bereits bestehende Anlage gibt, die erneuert oder ergänzt wird. Der Ausnahmefall liegt vor, wenn eine optisch-elektronische Anlage bereits vorhanden ist, es aber in der Vergangenheit versäumt wurde, die Vorabkontrolle durchzuführen.

1.1.1 Beobachtungsmonitor(e)

- () interne Einzelplatz-Anwendung
Standort / Nutzer: _____
- () interne Mehrplatz-Anwendung
Standort / Nutzer 1: _____
Standort / Nutzer 2: _____
Standort / Nutzer 3: _____
- () externe Zugriffsmöglichkeit (z. B.: Doppelnutzung oder Verbundanlage)
Standort / Nutzer 1: _____
Standort / Nutzer 2: _____
Standort / Nutzer 3: _____

- ☐ Beobachtung und Übertragung
 - ☐ ein Monitor
 - ☐ _____ Monitore
 - ☐ ein Bild auf dem Monitor sichtbar
 - ☐ _____ Bilder auf einem Monitor sichtbar
 - ☐ automatischer Wechsel der Bilder
 - ☐ manueller Wechsel der Bilder

1.1.2 Videokamera(s)

- ☐ Domkamera _____ Stück Hersteller / Typ _____
- ☐ klassische Kamera _____ Stück Hersteller / Typ _____
- ☐ Klingelkamera _____ Stück Hersteller / Typ _____
- ☐ mobile Kamera _____ Stück Hersteller / Typ _____

Die jeweiligen Leistungsmerkmale sind aufzulisten oder auf ein Datenblatt als Anlage zu verweisen. Zu den Leistungsmerkmalen gehören mindestens die Neigungsfähigkeit, der Schwenkbereich und der Zoomfaktor.

- ☐ Standort Nr. 1 _____
- ☐ Standort Nr. 2 _____
- ☐ Standort Nr. 3 _____
- ☐ Skizze mit den Standorten siehe Anlage(n) _____
- ☐ Skizze mit den Standorten und ... siehe Anlage(n) _____
 - ☐ Blickrichtungen
 - ☐ Erfassungsbereichen
 - ☐ Kameratypen
 - ☐ Schwenkbereichen

1.1.3 Aufzeichnungsgerät(e)

- ☐ analoge Technik _____ Stück Hersteller / Typ _____
- ☐ digitale Technik _____ Stück Hersteller / Typ _____

Die Leistungsmerkmale sind ebenfalls aufzulisten oder es ist auf ein Datenblatt als Anlage zu verweisen. Bei den Leistungsmerkmalen ist mindestens die Größe des Speichermediums anzugeben.

1.1.4 Software

- ☐ Assistenzprogramme
 - ☐ konstanter Einsatz
 - ☐ temporärer Einsatz
- ☐ Mustererkennung
 - ☐ Abgleich mit biometrischen Daten
 - ☐ zur Authentisierung
 - ☐ zur Identifizierung
 - ☐ zur Klassifizierung
 - ☐ zur Selektion
 - ☐ Erkennung atypischer Verhaltensmuster
 - ☐ Personendetektion
- ☐ Vernetzung mit anderen Datenbanken
 - ☐ Mitarbeiterdatei
 - ☐ POLAS / INPOL
 - ☐ _____

1.1.5 Sonstige technische Anlage

- () Datenübertragung mittels
 () Kabelverbindung () WLAN () _____
 () Server - / Technikraum
 () vorhanden () nicht vorhanden
 () Netzwerkverbindung
 () vorhanden () nicht vorhanden

1.2 Planungszustand

Die anwendende / verantwortliche Stelle ist verpflichtet die gewünschten technischen Komponenten der geplanten Anlage an den behördlichen Datenschutzbeauftragten zu übermitteln. Der zuständige Administrator muss weitere Informationen zur technischen Infrastruktur zur Verfügung stellen.

1.2.1 Beobachtungsmonitor(e)

- () interne Einzelplatz-Anwendung
 Standort / Nutzer: _____
 () interne Mehrplatz-Anwendung
 Standort / Nutzer 1: _____
 Standort / Nutzer 2: _____
 Standort / Nutzer 3: _____
 () externe Zugriffsmöglichkeit (z. B.: Doppelnutzung oder Verbundanlage)
 Standort / Nutzer 1: _____
 Standort / Nutzer 2: _____
 Standort / Nutzer 3: _____
 () Beobachtung und Übertragung
 () ein Monitor
 () _____ Monitore
 () ein Bild auf dem Monitor sichtbar
 () _____ Bilder auf einem Monitor sichtbar
 () automatischer Wechsel der Bilder
 () manueller Wechsel der Bilder

1.2.2 Videokamera(s)

- () Domkamera _____ Stück Hersteller / Typ _____
 () klassische Kamera _____ Stück Hersteller / Typ _____
 () Klingelkamera _____ Stück Hersteller / Typ _____
 () mobile Kamera _____ Stück Hersteller / Typ _____

Die jeweiligen Leistungsmerkmale sind aufzulisten oder auf ein Datenblatt als Anlage zu verweisen. Zu den Leistungsmerkmalen gehören mindestens die Neigungsfähigkeit, der Schwenkbereich und der Zoomfaktor.

- () Standort Nr. 1 _____
 Standort Nr. 2 _____
 Standort Nr. 3 _____
 () Skizze mit den Standorten siehe Anlage(n) _____

- Seite 4

2.1 Zweckbestimmung / -bindung

Bestandteil der Rechtmäßigkeit ist die konkrete Festlegung der Zweckbestimmung. Lediglich klare und genaue Formulierungen mit nachvollziehbaren Eckpunkten gewährleisten die Möglichkeit der Einhaltung von Gesetzen, der sachgerechten Bewertung des Erfolgs sowie der Transparenz bei Mitarbeitern und in der Öffentlichkeit.

Die Videoüberwachungsmaßnahme muss ein wirksames Mittel sein, um den Zweck tatsächlich erfüllen zu können. Dies ist nicht der Fall, wenn nur eine Illusion von vermeintlicher präventiver Sicherheit vermittelt wird und die Anlage vielmehr als repressives Mittel im Rahmen der Täterermittlung bzw. bei sonstigen Hintergründen eingesetzt wird.

- () § 10 Abs. 1 NDSG
- () § 10 Abs. 4 NDSG
- () § 38 Abs. 1 NSOG
- () § 12 Abs. 4 NVersG
- () § 17 Abs. 4 NVersG
- () _____

2.2 Zulässigkeit / Erforderlichkeit

Die jeweils zutreffende Rechtsgrundlage ist anzuführen, die Gründe für eine Beobachtung und gegebenenfalls einer zusätzlichen Aufzeichnung sind separat voneinander zu begründen.

Beispiel § 25 a NDSG:

Aufgrund des intensiven Eingriffs in das Recht auf informationelle Selbstbestimmung muss es in der Vergangenheit grundsätzlich zu Vorkommnissen gekommen sein, deren Quantität und / oder Qualität eine Videoüberwachungsmaßnahme rechtfertigen könnten; der Umfang ist zu dokumentieren und in die Gesamtüberlegungen einzubeziehen. Im Einzelfall sollten entsprechende Informationen bei der zuständigen Polizeidienststelle eingeholt werden.

- () eigene Feststellungen / Anzeigen
 - () Betrug / Erschleichen von Leistungen
 - () einfacher Diebstahl / besonders schwerer Fall des Diebstahls
 - () Hausfriedensbruch
 - () Sachbeschädigung durch
 - () Schadenshöhe(n)

1. Vorkommnis _____	Euro
2. Vorkommnis _____	Euro
3. Vorkommnis _____	Euro
- () Anzeigen durch eigenes Personal
 - () Beleidigung
 - () Nötigung / Bedrohung
 - () einfache Körperverletzung / gefährliche Körperverletzung
 - () sonstige Delikte _____
- () Anzeigen durch Behördenleitung
 - () Beleidigung
 - () einfache Körperverletzung / gefährliche Körperverletzung
 - () sonstige Delikte _____

- () Anzeigen durch Dritte
 - () bei der verantwortlichen Stelle
 - () Beleidigung
 - () Nötigung / Bedrohung
 - () einfacher Diebstahl / besonders schwerer Fall des Diebstahls
 - () einfache Körperverletzung / gefährliche Körperverletzung
 - () Raub / räuberische Erpressung
 - () Sachbeschädigung durch _____
 - () sonstige Delikte _____
 - () bei der Polizei
 - () Beleidigung
 - () Nötigung / Bedrohung
 - () einfacher Diebstahl / besonders schwerer Fall des Diebstahls
 - () einfache Körperverletzung / gefährliche Körperverletzung
 - () Raub / räuberische Erpressung
 - () Sachbeschädigung durch _____
 - () sonstige Delikte _____

Bei den sonstigen gesetzlichen Grundlagen sind vergleichbare Voraussetzungen vorgegeben, die analog zu prüfen und zu begründen sind.

Im Rahmen der Erforderlichkeit sind auch zeitliche Beschränkungen für die Beobachtung und Aufzeichnung zu prüfen. In diesem Anwendungsfall ist die technische Anlage entsprechend zu programmieren.

- () Beobachtung
 - () Montag – Freitag von _____ Uhr bis _____ Uhr
 - () Samstag / Sonntag von _____ Uhr bis _____ Uhr
 - () Feiertage von _____ Uhr bis _____ Uhr
- () Aufzeichnung
 - () Montag – Freitag von _____ Uhr bis _____ Uhr
 - () Samstag / Sonntag von _____ Uhr bis _____ Uhr
 - () Feiertage von _____ Uhr bis _____ Uhr

2.2.1 Beobachtung

Eine Beobachtungsmöglichkeit mittels Monitor muss während der üblichen Betriebs- bzw. Geschäftszeiten immer gegeben sein. Sofern der Zweck der Anlage insbesondere dem Schutz von Personen – Leben, Freiheit und körperliche Unversehrtheit – dient, ist auch unabhängig von einer Aufzeichnung eine 24-stündige Beobachtung zu gewährleisten.

Die Videoüberwachung ohne Aufzeichnung soll den präventiven Zwecken nach ... dienen.

- () § 25 a Abs. 1 NDSG (öffentliche Stellen)
 - () zum Schutz von Personen
 - () eigene Mitarbeiterinnen / Mitarbeiter
 - () sonstigen Personen
 - () zum Schutz von Sachen
 - () öffentliches Eigentum
 - () privates Eigentum
 - () in sonstigen Fällen
 - () Ein- / Ausgangskontrolle
 - () Ein- / Ausfahrtskontrolle
 - () _____

- | | |
|--|--|
| ☐ § 6 b Abs. 1 BDSG | (öffentliche Wettbewerbsunternehmen) |
| ☐ zum Schutz von Personen | ☐ eigene Mitarbeiterinnen / Mitarbeiter |
| | ☐ sonstigen Personen |
| ☐ zum Schutz von Sachen | ☐ öffentliches Eigentum |
| | ☐ privates Eigentum |
| ☐ in sonstigen Fällen | ☐ Ein- / Ausgangskontrolle |
| | ☐ Ein- / Ausfahrtskontrolle |
| | ☐ _____ |
| ☐ § 32 Abs. 3 Satz 1 NSOG | (Polizei) |
| ☐ § 32 Abs. 3 Satz 1 NSOG | (Verwaltungsbehörde) |
| ☐ § 10 c Abs. 1 Satz 1 NSpielbG | (Spielbankenbetreiber) |
| ☐ § 11 Abs. 1 Nr. 8 NSpielbG | (Aufsichtsbehörde) |
| ☐ § 12 Abs. 2 Satz 1 NVersG | (Polizei) |
| ☐ § 17 Abs. 2 Satz 1 NVersG | (Polizei) |

2.2.2 Aufzeichnung

Bei der Überlegung und Begründung einer Videoüberwachung mit Aufzeichnung sind auch immer die Grundsätze der Datensparsamkeit und -vermeidung zu berücksichtigen. Daher ist grundsätzlich die Möglichkeit einer zeitlichen Beschränkungen der Aufzeichnung zu prüfen.

Die Videoüberwachung mit Aufzeichnung soll den präventiven Zwecken nach ... dienen.

- | | |
|--|---|
| ☐ § 25 a Abs. 2 NDSG | (öffentliche Stellen) |
| ☐ § 6 b Abs. 3 BDSG | (öffentliche Wettbewerbsunternehmen) |
| ☐ § 32 Abs. 1 NSOG | (Polizei) |
| ☐ § 32 Abs. 3 Satz 2 NSOG | (Polizei) |
| ☐ § 32 Abs. 4 NSOG | (Polizei) |
| ☐ § 10 c Abs. 1 Satz 2 NSpielbG | (Spielbankenbetreiber / Aufsichtsbehörde) |
| ☐ § 11 Abs. 1 Nr. 8 NSpielbG | (Aufsichtsbehörde) |
| ☐ § 190 NJVollzG | (Justizvollzug) |
| ☐ § 6 NVerfSchG | (Verfassungsschutz) |
| ☐ § 12 a VersG | (Polizei – bis 31.01.2011) |
| ☐ § 19 a VersG | (Polizei – bis 31.01.2011) |
| ☐ § 12 NVersG | (Polizei – ab 01.02.2011) |
| ☐ § 17 NVersG | (Polizei – ab 01.02.2011) |

Die optisch-elektronische Überwachung von versammlungsrechtlichen Aktionen muss immer unter dem besonderen Gesichtspunkt des Grundrechtes auf Versammlungsfreiheit nach Artikel 8 Grundgesetz betrachtet werden. Dabei ist zu berücksichtigen, dass der Grundrechtsschutz auch die An- und Abmarschwege umfasst. Erst bei Vorliegen von tatsächlichen Anhaltspunkten für erhebliche Gefahren der öffentlichen Sicherheit oder Ordnung ist eine Videoüberwachung zulässig. Diese Anhaltspunkte sind rechtzeitig vor Versammlungsbeginn im polizeilichen Einsatzbefehl und ergänzenden Lagebildern zu dokumentieren.

Die Videoüberwachung mit Aufzeichnung soll den repressiven Zwecken nach ... dienen.

- | | |
|---------------------------------------|--------------------------------|
| ☐ § 58 a StPO | (Polizei / Staatsanwaltschaft) |
| ☐ § 100 h StPO | (Polizei / Staatsanwaltschaft) |

2.2.3 Kennzeichnung

Abgesehen von wenigen Ausnahmen lassen die verschiedenen Rechtsgrundlagen zur Videoüberwachung aus Transparenzgründen nur eine offene Beobachtung zu. In den allgemeingültigen Erlaubnisnormen – § 25 a NDSG und § 6 b BDSG – ist eine Kennzeichnungspflicht verankert. In anderen Fällen (z. B. § 32 NSOG) müssen die Kameras durch den Normalbürger eindeutig erkennbar sein, ansonsten würde es sich nicht mehr um eine offene Videoüberwachung handeln. In diesen Fällen ist die Kennzeichnung zwingend erforderlich.

Die Hinweisschilder sind grundsätzlich in Augenhöhe und vor dem Erreichen des überwachten Bereiches für jedermann wahrnehmbar anzubringen.

Die Art und der Umfang der Kennzeichnung ist festzulegen und die verantwortliche Stelle auf den Schildern entsprechend auszuweisen. An Überwachungsstandorten mit internationalem Publikumsverkehr empfiehlt sich die Verwendung eines eindeutigen Piktogramms oder mehrsprachigen Texten.

- | | |
|--|--|
| ☐ § 25 Abs. 3 NDSG | ☐ Piktogramm nach DIN 33450
☐ Piktogramm sonstiger Art
☐ Beobachtung
☐ Aufzeichnung
☐ Text _____
☐ deutsch
☐ englisch
☐ _____ |
| ☐ § 6 b Abs. 2 BDSG | ☐ verantwortliche Stelle
☐ zeitliche Beschränkungen
☐ Piktogramm nach DIN 33450
☐ Piktogramm sonstiger Art
☐ Beobachtung
☐ Aufzeichnung
☐ Text _____
☐ deutsch
☐ englisch
☐ _____ |
| ☐ nicht-offene Videoüberwachung | ☐ verantwortliche Stelle
☐ zeitliche Beschränkungen
☐ durch Verwendung Domkamera
☐ durch Installation in großer Höhe
☐ durch bauliche Gegebenheiten |

Zusätzlich können gesetzliche Bestimmungen und Verordnungen die verantwortliche Stelle im Rahmen der Transparenz zum Aushang von Regelungen verpflichten, die auch eine Überwachung mit optisch-elektronischen Anlagen umfasst; z. B. Aushang der Spielordnung nach § 11 Abs. 2 NSpielbG.

2.2.4 Löschung / Löschfrist

- () manuelle Löschung => Ausnahmefall; nur noch für Altanlagen
- () automatische Löschung => Standardfall

Die Löschfrist ist genau festzulegen. Die Dauer der Aufbewahrung muss sich an der Zweckbestimmung sowie der Erforderlichkeit orientieren und darf grundsätzlich sieben Tage nicht überschreiten. In der Regel dürften wesentlich kürzere Speicherzeiten festzulegen sein.

- ☐ § 17 Abs. 2 NDSG
- ☐ § 25 a Abs. 5 NDSG
- ☐ § 39 NSOG
- ☐ § 6 b Abs. 5 BDSG
- ☐ § 10 c Abs. 1 Satz 3 NSpielbG (Speicherung mindestens zwei Wochen)
- ☐ § 11 Abs. 1 Nr. 8 NSpielbG (Vorgabe der Aufsichtsbehörde)
- ☐ § 12 Abs. 3 NVersG (spätestens nach zwei Monaten)
- ☐ § 17 Abs. 3 NVersG (spätestens nach zwei Monaten)

Ein wesentlicher Faktor für die Festlegung der Löschfrist ist die Wahrnehmung der Beobachtung mittels Monitor – unter Berücksichtigung des Schutzzweckes – durch die verantwortliche Stelle:

- ☐ im 24 Stunden-Betrieb / 7 Tage die Woche durch eigenes Personal
- ☐ im 24 Stunden-Betrieb / 7 Tage die Woche durch fremdes Personal
- ☐ während der Betriebszeiten / 5 Tage die Woche
- ☐ mit sonstiger Regelung: _____

2.2.5 Auskunftsrecht

Nach § 8 a Abs. 3 Satz 1 NDSG steht jedermann ein Einsichtsrecht in den öffentlichen Teil der landeseinheitlichen Verfahrensbeschreibung – Ziffer 1 bis 8 – zu. Hiervon ausgenommen sind gemäß § 8 a Abs. 3 Satz 2 NDSG und § 22 Abs. 5 NDSG Verfahrensbeschreibungen zu Videoüberwachungsmaßnahmen für die Strafverfolgung, nach dem Niedersächsischen Verfassungsschutzgesetz und für polizeiliche Überwachungsanlagen nach dem NSOG.

2.2.6 Benachrichtigungspflichten

Sofern Datenerhebungen ohne Kenntnis der Betroffenen stattfinden, besteht eine grundsätzliche Benachrichtigungspflicht durch die verantwortliche Stelle.

- ☐ Benachrichtigungspflicht
 - ☐ § 25 a Abs. 4 Satz 1 NDSG
 - ☐ § 6 b Abs. 4 BDSG
 - ☐ _____
- ☐ Ausnahmen von der Benachrichtigungspflicht
 - ☐ § 25 a Abs. 4 Satz 2 NDSG
 - ☐ § 19 a Abs. 2 BDSG
 - ☐ § 33 Abs. 2 BDSG
 - ☐ _____

2.3 Zweckdurchbrechung / Datenübermittlung

2.3.1 Zweckdurchbrechung

- ☐ § 10 Abs. 2 NDSG
- ☐ § 25 a Abs. 2 Satz 2 NDSG
- ☐ § 39 NSOG
- ☐ § 12 Abs. 3 Satz 1 NVersG
- ☐ § 17 Abs. 3 Satz 1 NVersG
- ☐ § 6 b Abs. 3 Satz 2 BDSG
- ☐ _____

2.3.2 Datenübermittlung

- ☐ § 11 NDSG – an Stellen innerhalb des öffentlichen Bereichs
- ☐ § 13 NDSG – an Personen oder Stellen außerhalb des öffentlichen Bereichs
- ☐ § 14 NDSG – an Personen oder Stellen außerhalb der Europäischen Union
- ☐ § 15 NDSG – an Stellen öffentlich-rechtlicher Religionsgemeinschaften
- ☐ § 40 NSOG – allgemeine Regeln
- ☐ § 41 NSOG – zwischen Verwaltungs- und Polizeibehörden
- ☐ § 43 NSOG – an
 - ☐ andere öffentliche Stellen
 - ☐ ausländische öffentliche Stellen
 - ☐ über- und zwischenstaatliche Stellen
- ☐ § 44 NSOG – an Personen und Stellen außerhalb des öffentlichen Bereiches
- ☐ § 17 NVerfSchG – an
 - ☐ inländische Behörden
 - ☐ alliierte Streitkräfte
 - ☐ ausländische öffentliche Stellen
 - ☐ Einzelpersonen oder sonstige Stellen
- ☐ § 18 Abs. 1 NVerfSchG – an Polizei
- ☐ § 19 NVerfSchG – an öffentliche Stellen
- ☐ § 161 Abs. 1 StPO
- ☐ _____

2.4 Auftragsdatenverarbeitung

- ☐ § 6 NDSG ☐ durch eine andere öffentliche Stelle; _____
☐ durch eine private Stelle; _____
- ☐ § 11 BDSG ☐ durch eine andere öffentliche Stelle; _____
☐ durch eine private Stelle; _____

Die Wahrnehmung von hoheitlichen Tätigkeiten – insbesondere § 32 NSOG – ist im Rahmen der Auftragsdatenverarbeitung nicht zulässig.

2.5 Doppelnutzung / Verbundanlage

Bei einer temporären oder dauerhaften so genannten Doppelnutzung bzw. einer Verbundanlage, bei denen entweder mehrere öffentliche Stellen oder öffentliche und nicht-öffentliche Stellen eine (Teil-)Anlage nutzen, hat jede verantwortliche Stelle eine Rechtmäßigkeitsprüfung durchzuführen.

Eine Doppelnutzung bzw. Verbundanlage in Verbindung mit Videoüberwachungsmaßnahmen kommt in der Regel nur bei polizeilich begleiteten Großveranstaltungen (Fußballspiele, Konzerte u. s. w.) vor. Dabei kann es grundsätzlich zu folgenden Konstellationen von verantwortlichen Stellen kommen:

- | | |
|---|---|
| ☐ Bundes- / Landespolizei | |
| ☐ Bahnhof | ☐ Flughafen |
| ☐ Staatsgrenze | ☐ _____ |
| ☐ Polizei / Verwaltungsbehörde | |
| ☐ kommunales Sportstadion | ☐ kommunale Veranstaltungshalle |
| ☐ _____ | ☐ _____ |
| ☐ Polizei / nicht-öffentliche Stelle | |
| ☐ vereinseigenes Sportstadion | ☐ privates Veranstaltungszentrum |
| ☐ _____ | ☐ _____ |

2.6 Informationspflichten, Beteiligungs- und Mitbestimmungsrechte

- | | |
|--|--|
| ☐ § 11 NRiG | Richterrat |
| ☐ §§ 64, 67 NPersVG | Personalrat |
| ☐ § 34 Abs. 3 NSchG | Gesamtkonferenz |
| ☐ § 96 Abs. 3 NSchG | Schulelternrat / Klassenelternschaften |

Der LfD Nds. ist bei der Entwicklung und Planung von bisher nicht eingesetzten optisch-elektronischen Überwachungsanlagen (z. B. Forschungsprojekte) rechtzeitig zu informieren, damit dem gesetzlichen Beratungsauftrag aus § 22 Abs. 1 Satz 3 NDSG nachgekommen werden kann.

- | | |
|---|---|
| ☐ § 22 Abs. 2 NDSG | Landesbeauftragter für den Datenschutz Nds. |
|---|---|

2.7 Verbote

Der Einsatz von Attrappen ist immer rechtswidrig.

Die Verwendung längerfristig defekter Kameras steht dem Einsatz von Attrappen gleich, so dass die Variante ebenfalls unzulässig ist.

Bei einer Übertragung des Bildmaterials in das Internet dürfen keine personenbezogenen (Erkennbarkeit von Einzelpersonen) oder -beziehbaren Daten (z. B. Kfz-Kennzeichen oder LKW-Aufschriften) übermittelt werden; d. h., wenn der Zoom von einer zugriffsberechtigten Stelle genutzt wird, ist die Übertragung ins world wide web automatisch zu unterbrechen.

2.8 Vorabkontrolle

Die Erstellung einer Vorabkontrolle ist in folgenden gesetzlichen Bestimmungen vorgeschrieben und durch den behördlichen Datenschutzbeauftragten (siehe § 8 a Abs. 3 Satz 3 NDSG) umzusetzen:

- ☒ Art. 20 EU-DSRL
- ☐ § 7 Abs. 3 NDSG
- ☐ § 25 a Abs. 6 NDSG
- ☐ § 4 d Abs. 5 BDSG

Bei einer Doppelnutzung bzw. Verbundanlage hat jede verantwortliche Stelle eine eigenständige Vorabkontrolle durchzuführen.

Dem behördlichen Datenschutzbeauftragten sind alle notwendigen Informationen für die Fertigung einer Vorabkontrolle zur Verfügung zu stellen. In der Regel besteht mindestens für den Administrator / Systembetreuer und die verantwortliche Stelle eine Verpflichtung entsprechende Daten und sonstige Fakten zu liefern.

Bei wesentlichen Veränderungen an der Videoüberwachungsanlage (z. B. Erhöhung der Kamerazahl, neue Kameras mit zusätzlichen / erweiterten Leistungsmerkmalen) ist die Vorabkontrolle zu aktualisieren oder gegebenenfalls neu zu fertigen.

2.9 Verfahrensbeschreibung

Die Verfahrensbeschreibung nach § 8 NDSG ist mittels landeseinheitlichen Vordruck durch die verantwortliche Stelle zu erstellen. Auch die öffentlichen Wettbewerbsunternehmen haben gemäß § 2 Abs. 3 Satz 1 NDSG das angeführte Formular zu verwenden.

In den Fällen des § 22 Abs. 5 NDSG ist die Verfahrensbeschreibung umgehend an den LfD Nds. zu übersenden.

Bei einer Doppelnutzung bzw. Verbundanlage hat jede verantwortliche Stelle eine eigenständige Verfahrensbeschreibung zu erstellen.

Bei wesentliche Veränderungen an der Videoüberwachungsanlage (z. B. Erhöhung der Kamerazahl, neue Kameras mit zusätzlichen / erweiterten Leistungsmerkmalen) ist die Verfahrensbeschreibung zu aktualisieren oder gegebenenfalls neu zu fertigen.

3. Gefahrenanalyse

Je komplexer eine Videoüberwachungsanlage ist und entsprechend umfangreiche Datenerhebungen durchgeführt werden desto intensiver muss die Gefahrenanalyse insbesondere in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit durchgeführt werden. Im Zweifelsfall können die IT-Grundschutz-Kataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI) unter www.bsi.bund.de herangezogen werden.

3.1 technische Anlage

- () Ausfall der technischen Anlage durch höhere Gewalt
 - () Blendung durch starke Lichtquellen () Blitz () Feuer
 - () Kabelbrand () Luftfeuchtigkeit () Schmutz () Staub
 - () Temperatur () Wasser () Wind
- () Ausfall der technischen Anlage durch vorsätzliches Handeln / Manipulation
 - () Beschädigung () Diebstahl () Unterbrechung
 - () Viren () Zerstörung () _____
- () Ausfall der technischen Anlage durch fahrlässiges Handeln / Unkenntnis
 - () falsche Bedienung () Einspielen von Software mit Virenbefall
 - () _____

Der Landesbeauftragte für den Datenschutz Niedersachsen

- () Ausfall der technischen Anlage durch fehlende Infrastruktur
 - () Alarmmelder () Brandabschottung () Feuerlöscher
 - () Klimaanlage () Sicherheitsfenster () Sicherheitstüren
 - () Sprinkleranlage () _____ () _____
- () Ausfall der technischen Anlage durch sonstige Umstände
 - () mangelhafte Wartung () Spannungsschwankungen
 - () sonstige technische Defekte () Überalterung der Anlage
 - () Überhitzung der Anlage () Unterbrechung der Stromversorgung
- () fehlerhafte Funktionen der Anlage
 - () defekte Datenträger () falsche Programmierung der Löschfrist
 - () fehlende Zeitsynchronisation () falsche Lagerung mobiler Datenträger
- () verbotene Datenerhebungen im Kernbereich privater Lebensgestaltung
 - () Dusche () Sauna () Toilette () Umkleide
 - ⇒ Diese Bereiche sind durch § 201 a Strafgesetzbuch besonders geschützt!
- () verbotene Datenerhebungen für Verhaltens- und Leistungskontrollen
 - () Arbeitsplatz () Bewegungsbilder () Lehrerzimmer
 - () Pausenraum () Raucherecke () Unterrichtsraum
 - () _____ () _____ () _____
 - ⇒ Diese Bereiche unterliegen dem Personaldatenschutz!
- () missbräuchliche Datenerhebungen in privaten Bereichen
 - () Arztpraxis () Gartenkolonie () Geschäftsraum
 - () Geschäftsgrundstück () Hotel () Krankenhaus
 - () Privatgrundstück () Wohnung () _____
 - ⇒ Diese Bereiche sind durch Artikel 13 Grundgesetz besonders geschützt!
- () unzulässige Datenerhebung während versammlungsrechtlicher Aktionen
 - () vor der Versammlung / auf dem Weg zur Versammlung
 - () während der Versammlung / am Versammlungsort
 - () nach der Versammlung / auf dem Rückweg von der Versammlung
 - ⇒ Versammlungen unterliegen dem Schutz von Artikel 8 Grundgesetz!
- () unzulässige Datenübermittlung an Dritte
 - () durch fehlende Verschlüsselung bei drahtloser Übertragung
 - () durch unzureichende Verschlüsselung bei drahtloser Übertragung
 - () durch unsachgemäßen Umgang mit Passwörtern
 - () durch unberechtigten Zugang zu Sicherheitszentralen
 - () durch unberechtigten Zugang zum Server- / Technikraum
 - () durch ungehinderten und unberechtigten Zugriff auf die Aufzeichnung
 - () über einsehbare Überwachungsmonitore
 - () über einsehbare Videowand
 - () über das Internet
 - () über das Intranet
 - () über sonstige interne Netzwerke
 - () über Ausdruck einzelner Bilder
 - () über Kopien auf mobilen Datenträger

3.2 eigenes Personal / organisatorische Regelungen

- () Personalauswahl
 - () zuverlässige Mitarbeiter () zuverlässige Servicekräfte
 - () verpflichtete Wartungskräfte () Sicherheitsüberprüfung
- () Zugriffsberechtigungen
 - () ohne Kennung () Gruppenkennung () Einzelkennung
 - () ohne Protokolldatei () mit Protokolldatei
 - () Chip- / Magnetkarten () elektronische Signatur () PIN

- ☐ Zugangsberechtigungen
 - ☐ Schlüssel
 - ☐ Generalschlüssel ☐ Schlüsselmanagement
 - ☐ Sicherheitsschlüssel
 - ☐ Chip- / Magnetkarten ☐ elektronische Signatur ☐ PIN

3.3 Netzwerkverbindungen / -übertragungen

- ☐ gewollte Übertragung in das
 - ☐ Internet
 - ☐ Intranet
 - ☐ Ausfall der Übertragung
 - ☐ Ausfall der Unterbrechung bei der Nutzung der Zoomfunktion
- ☐ ungewollte Übertragung in das
 - ☐ Internet
 - ☐ Intranet
 - ☐ Anlage mit Verbindung zu internen oder öffentlichen Netzwerken
 - ☐ Anlage ohne Verbindung zu internen oder öffentlichen Netzwerken

3.4 Wartung durch Fremdunternehmen

Bei einer Wartung durch externe Kräfte sind entsprechende vertragliche Regelungen zu treffen und eine Vertraulichkeitsvereinbarung zu unterzeichnen.

Es ist zu beachten, dass die Verantwortung für den sachgerechten und rechtmäßigen Umgang mit personenbezogenen Daten bei der verantwortlichen Stelle für die Videoüberwachung (Auftraggeber) bleibt.

4. Risikoanalyse

4.1 Wahrscheinlichkeit eines Schadenseintritts

Die Wahrscheinlichkeit eines Schadenseintritts ist jeweils nach dem Missbrauchsinteresse des Schädigers, dem Aufwand zur Herbeiführung des Schadens, dem Risiko entdeckt zu werden und der Verarbeitungshäufigkeit bzw. des -umfangs der Daten zu bewerten.

4.2 Ausmaß des Schadens / Schutzstufen

Um technische und organisatorische Maßnahmen zur Wahrung des Rechts auf informationelle Selbstbestimmung sachgerecht bewerten zu können, ist es erforderlich, das mögliche Schadenspotential zu bestimmen. Hierzu sollte das Schutzstufenkonzept des LfD Niedersachsen herangezogen werden.

4.2.1 Schutzstufe A

Die personenbezogenen / -beziehbaren Daten sind frei zugänglich.

- ⇒ Eine einzelne Überwachungskamera ohne Aufzeichnung wird lediglich als Ersatz für ein menschliches Auge eingesetzt (z. B. Zutrittskontrolle Nebeneingang).

4.2.2 Schutzstufe B

Die unsachgemäße Handhabung von personenbezogenen / -beziehbaren Daten lässt keine besondere Beeinträchtigung erwarten, weil eine rechtliche Grundlage für den anwendende Stelle vorhanden ist.

⇒ Anlage zur allgemeinen Überwachung der Außenhaut, der Ein- / Ausgänge und des Parkplatzes eines öffentlichen Gebäudes.

4.2.3 Schutzstufe C

Die unsachgemäße Handhabung der personenbezogenen / -beziehbaren Daten könnten den Betroffenen in seiner gesellschaftlichen Stellung oder in seinem wirtschaftlichen Verhältnissen beeinträchtigen (Ansehensschaden).

⇒ Unzulässige Überwachung einer Raucherecke für eigenes Personal.

4.2.4 Schutzstufe D

Die unsachgemäße Handhabung der personenbezogenen / -beziehbaren Daten könnten den Betroffenen in seiner gesellschaftlichen Stellung oder in seinem wirtschaftlichen Verhältnissen erheblich beeinträchtigen (Existenzbedrohung).

⇒ Grundlose Mitarbeiterüberwachung durch langfristiges Erstellen von Bewegungsprofilen mittels komplexer Videoüberwachungsanlagen, um Gründe für ein Disziplinarverfahren oder eine Entlassung zu finden.

4.2.5 Schutzstufe E

Die unsachgemäße Handhabung der personenbezogenen / -beziehbaren Daten könnten Gesundheit, Leben oder Freiheit des Betroffenen beeinträchtigen.

⇒ Missbrauch von komplexen Videoüberwachungsanlagen mit Aufzeichnungsfunktion in sicherheitsrelevanten Bereichen (z. B. für die Vorbereitung einer Geiselnahme in einer Justizvollzugsanstalt).

4.3 Risiko

4.3.1 Risiko bis Schutzstufe C (Grundsutzbereich)

- | | | | | |
|-----------------------------|------------|------------|----------|---------------|
| () Verarbeitungshäufigkeit | () gering | () mittel | () hoch | () sehr hoch |
| () Verarbeitungsumfang | () gering | () mittel | () hoch | () sehr hoch |
| () Missbrauchsinteresse | () gering | () mittel | () hoch | () sehr hoch |

4.3.2 Risiko bei den Schutzstufen D oder E

- | | | | | |
|-----------------------------|------------|------------|----------|---------------|
| () Verarbeitungshäufigkeit | () gering | () mittel | () hoch | () sehr hoch |
| () Verarbeitungsumfang | () gering | () mittel | () hoch | () sehr hoch |
| () Missbrauchsinteresse | () gering | () mittel | () hoch | () sehr hoch |

5. Datenschutzkonzept

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) und der Bundesbeauftragte für den Datenschutz (BfDI) haben die Informationsbroschüre „Common Criteria Protection Profile – Software zur Verarbeitung von personenbezogenen Bilddaten“ (Version 2.0 vom 15.01.2007) herausgegeben, welche die Mindestanforderungen für eine sachgerechte Videoüberwachungsanlage thematisiert.

Je komplexer eine Anlage ist oder über eine hohe Eingriffstiefe in die Grundrechte verfügt desto umfangreicher muss das Datenschutzkonzept sein. Grundsätzlich sind technische Lösungen den organisatorischen Regelungen vorzuziehen.

Durch entsprechende technische und organisatorische Maßnahmen sind die beschriebenen Gefahren auf ein Minimum zu reduzieren.

Grundsätzliche Aspekte können auch schon auf Behördenebene durch eine allgemeine Dienstanweisung zum Datenschutz bzw. zur Videoüberwachung geregelt sein. Diese Regeln ersetzen kein individuelles Datenschutzkonzept für eine bestimmte Anlage; Verweisungen auf einzelne Passagen dieser Dienstanweisungen sind aber möglich und auch sinnvoll.

5.1 Personaldatenschutz

- () Beteiligung der Personalvertretung
 - () durch Mitbestimmungsrecht
 - () durch Dienstvereinbarung

5.2 Kernbereich privater Lebensgestaltung

Die schutzwürdigen Bereiche nach § 201 a StGB dürfen von den Videoüberwachungsmaßnahmen nicht betroffen sein. Sofern sich im Ausnahmefall Überschneidungen zwischen zulässig und nicht zulässig überwachten Bereichen ergeben, ist eine partielle ... vorzunehmen.

- () Ausblendung mittels technischer Lösung (z. B. Verpixelung)
- () Ausblendung mittels manueller Lösung (z. B. Blende)
- () Beschränkung des Schwenkbereiches
- () Beschränkung der Zoomfähigkeit (lediglich Übersichtsaufnahme zulässig)

5.3 Unverletzlichkeit der Wohnung

Die Unverletzlichkeit der Wohnung und vergleichbarer Örtlichkeiten (so genannter Privatzonen) wird durch ... gewährleistet.

- () Ausblendung mittels technischer Lösung (z. B. Verpixelung)
- () Ausblendung mittels manueller Lösung (z. B. Blende)
- () Beschränkung des Schwenkbereiches
- () Beschränkung der Zoomfähigkeit (lediglich Übersichtsaufnahme zulässig)

Die Unverletzlichkeit der Wohnung gemäß Artikel 13 Grundgesetz lediglich mit einer Dienstanweisung zur Videoüberwachung zu regeln, ist nicht zulässig.

5.4 Zugriffs- und Zugangskontrolle

- () Allgemein
 - () Protokolldateien
 - () Rollen- und Berechtigungskonzept
 - () Schlüsselgewalt / Schlüsselmanagement
 - () Zugriffsberechtigungen
- () Beobachtung
 - () Beschränkung auf einen ausgewählten Personenkreis
 - () Einarbeitung / Einweisung neuer Mitarbeiter
 - () sorgfältige Personalauswahl für die Beobachtungsplätze
 - () Vertraulichkeitsvereinbarung mit externen Mitarbeitern
 - () wiederkehrende Belehrungen
- () Aufzeichnung / Auswertung
 - () Umgang mit mobilen Datenträgern
 - () Vier-Augen-Prinzip im Auswertungsfall – je nach Fallgestaltung – unter
 - () Beteiligung Administrator
 - () Beteiligung behördlicher Datenschutzbeauftragter
 - () Beteiligung Personalabteilung
 - () Beteiligung Personalvertretung
 - () Beteiligung Sicherheitsbeauftragter
- () Kontrolle
 - () regelmäßige Überprüfung der Protokolldateien
 - () regelmäßige Überprüfung der Sicherheitsmaßnahmen
- () Wartung
 - () Regelungen für den Einsatz von Fremdpersonal
 - () vertragliche Vereinbarung mit Wartungsfirma
 - () Vertraulichkeitsvereinbarung mit Wartungsfirma
- () Datenübermittlung an Dritte
 - () Dokumentation der Datensicherung
 - () Dokumentation der Datenübermittlung

5.5 Funktionsfähigkeit der Anlage

- () Schutz der technischen Anlage vor Ausfall durch höhere Gewalt
 - () Blitzableiter
 - () Feuermelder
 - () Sprinkleranlage
 - () Vermeidung von Brandlasten
 - () Feuerlöscher
 - () Notstromaggregat
 - () Überspannungsschutz
 - () _____
- () Schutz der technischen Anlage vor vorsätzliches Handeln / Manipulation
 - Monitor(e)
 - () Beobachtungsplätze ohne Publikumsverkehr
 - () Bereithalten von Ersatzmonitoren
 - () _____
 - Kamera(s)
 - () Anbringung in ausreichender Höhe
 - () regelmäßige Reinigung der Optik bzw. Verglasung
 - () vandalismussichere Schutzgehäuse für Kameras
 - Datenübertragung
 - () kabellose Verbindung
 - () offene Kabelführung
 - () mit Verschlüsselung _____
 - () mit Verschlüsselung nach BSI-Standard
 - () in ausreichender Höhe
 - () in manipulationssicheren Gehäusen

- ☐ verdeckte Kabelführung
- ☐ in Kabelschächten
- ☐ unter Putz

Aufzeichnung – Server- / Technikraum

- ☐ Sicherung der Fenster durch
 - ☐ beschusssicheres Glas
 - ☐ einbruchshemmendes Glas
- ☐ Sicherung der Zugangstür durch
 - ☐ Codeschloss
 - ☐ Sicherheitsschloss
 - ☐ Brandschutztür
 - ☐ Stahltür
- ☐ sonstige Sicherungsmaßnahmen
 - ☐ Sicherungskasten / -schrank
 - ☐ _____

Sicherheitszentralen / Lagezentren

- ☐ Gegensprechanlage
- ☐ Sicherheitsschleuse
- ☐ Sicherung der Fenster und Türen durch
 - ☐ beschusssicheres Glas
 - ☐ einbruchshemmendes Glas
 - ☐ _____
- ☐ Schutz der technischen Anlage vor sonstigen Ausfällen
 - ☐ Einhaltung und Dokumentation von Kontrollintervallen
 - ☐ durch zuständigen Administrator
 - ☐ durch den behördlichen Datenschutzbeauftragten
 - ☐ einmal im Monat
 - ☐ alle zwei Monate
 - ☐ einmal im Quartal
 - ☐ Einhaltung und Dokumentation von Wartungsintervallen
 - ☐ durch hauseigenes Personal _____
 - ☐ durch andere Behörde _____
 - ☐ durch Fremdunternehmen _____
 - ☐ einmal im Monat
 - ☐ alle zwei Monate
 - ☐ einmal im Quartal
- ☐ Klimaanlage als Überhitzungsschutz

5.6 unzulässige Datenübermittlung an Dritte

- ☐ Verhinderung der Einsichtsmöglichkeit durch
 - ☐ Aufstellung / Anbringung der Monitore
 - ☐ Anbringung einer TFT-Folie
 - ☐ Einsatz von Sichtblenden
 - ☐ Sperrung der Monitore bei temporärer Abwesenheit
- ☐ Verhinderung der Übermittlung über Intranet / Internet
 - ☐ eigenständige Anlage ohne Anbindung an zentrale hauseigene Netzwerke
 - ☐ eigenständige Anlage ohne Intranet- / Internetverbindungen
 - ☐ Übertragung von Bildern in das Internet nur als Übersichtsaufnahmen
- ☐ Verhinderung der Übermittlung im Rahmen Doppelnutzung / Verbundanlage
 - ☐ Begründung und Protokollierung Übernahme einer Kamera / einer Anlage
 - ☐ eigenständige Speicherkomponente

- ☐ räumliche Trennung der verantw. Stellen in gemeinsamen Leitstellen
 - ☐ Bundesbehörde ☐ Bundespolizei
 - ☐ Feuerwehr / Rettungsdienst ☐ Kommunalverwaltung
 - ☐ Landesbehörde ☐ Landespolizei
 - ☐ nicht-öffentliche Stelle ☐ _____
- ☐ Rollen- und Berechtigungskonzept
- ☐ Unterbrechung der Verbindung zum originären Rechteinhaber
- ☐ Verhinderung einer Parallelnutzung für den gleichen Zweck
- ☐ Vorrangschaltung für hoheitliches Tätigwerden
- ☐ vertragliche Regelungen mit Fremdunternehmen bezüglich
 - ☐ Vernichtung von Datenträgern
 - ☐ Wartung der Anlage
- ☐ Zugangsbeschränkungen / -kontrollen für
 - ☐ Aufzeichnungsbereiche
 - ☐ Beobachtungsplätze
 - ☐ Lage- und Führungszentrum
 - ☐ Server- / Technikraum
 - ☐ Sicherheitszentrale

6. Beherrschung von Gefahren / Restrisiko

Das Ergebnis der Vorabkontrolle – einschließlich sachgerechter Alternativen und eines verbliebenen Restrisikos – ist festzuhalten.

6.1 Alternativen

Die Verwaltungsvorschrift zu § 7 NDSG schreibt vor, dass die alle Verfahrensalternativen zur angestrebten Lösung aufzuzeigen sind.

Folgende Beispiele sind u. a. in die Erwägungen einzubeziehen. Die alternativen Lösungen sind gegebenenfalls auch in kombinierter Weise zu berücksichtigen. Vor dem Einsatz einer optisch-elektronischen Überwachungsanlage sind nach dem Verhältnismäßigkeitsgrundsatz zunächst alle anderen möglichen Maßnahmen – mit keiner bzw. mit geringerer Eingriffstiefe – zu prüfen.

- ☐ Einsatz von zusätzlichem Behördenpersonal (u. a. Sicherheitspartnerschaften)
 - ☐ Mediator ☐ Ordnungsamt ☐ Polizei
 - ☐ Sprachmittler ☐ Straßensozialarbeit ☐ _____
- ☐ Einsatz eines privaten Sicherheitsdienstes
 - ☐ konstant vor Ort ☐ 24 Stunden
 - ☐ während der Betriebs- / Geschäftszeiten
 - ☐ außerhalb der Betriebs- / Geschäftszeiten
- ☐ nach Alarmauslösung
- ☐ regelmäßige Kontrollen
- ☐ sonstige technische Lösungen
 - ☐ Alarmanlage ☐ akustischer Alarm
 - ☐ optischer Alarm
 - ☐ stummer Alarm
- ☐ Beleuchtung
- ☐ Bewegungsmelder

- ☐ sonstige Lösungen
- ☐ Einzäunung des Geländes
- ☐ Einsatz von Schutz- / Wachhunden
- ☐ Verwendung von Spiegeln
- ☐ Verwendung von Zugangs- / Zufahrtsberechtigungen
- ☐ _____

Die folgende Alternativen wurden in der Vergangenheit bereits erfolglos eingesetzt:

- ☐ _____
- ☐ _____
- ☐ _____

Die folgenden Alternativen wurden bisher noch nicht eingesetzt:

- ☐ _____
- ☐ _____
- ☐ _____

Die folgenden Alternativen scheiden aufgrund von ... aus:

- ☐ _____
- ☐ _____
- ☐ _____

6.2 Beherrschung der Gefahren / Restrisiko

Bei der Beurteilung der möglichen Folgen von missbräuchlicher Verwendung der Daten oder auch Ausfall der Anlage sind insbesondere folgende Faktoren zu berücksichtigen:

- ⇒ Ansehens- / Vertrauensverlust in der Öffentlichkeit
- ⇒ Schadensersatzansprüche durch Dritte
- ⇒ wesentlicher Nachteil für unmittelbar Betroffene

Seitens der verantwortlichen Stellen sind aufgrund des Datenschutzkonzeptes die notwendigen Maßnahmen getroffen worden, dass ...:

- ⇒ ein hoher Aufwand erforderlich ist, um einen Schaden herbeizuführen.
- ⇒ ein hohes Risiko besteht, entdeckt zu werden.
- ⇒ eine hohe Wahrscheinlichkeit besteht, Mängel zeitnah zu erkennen.

- ☐ Das Restrisiko wird insgesamt als ... eingestuft.
☐ gering ☐ mittel ☐ hoch ☐ sehr hoch
- ☐ Die Gefahren für die Rechte der Betroffenen können ... werden.
☐ nicht beherrscht ☐ wirksam beherrscht

7. Ergebnis

Zur abschließenden Beurteilung einer gesetzeskonformen optisch-elektronischen Anlage wird auf die allgemeine Orientierungshilfe zur Videoüberwachung durch öffentliche Stellen, die speziellen Orientierungshilfen zur Videoüberwachung an öffentlichen Schulen sowie für Fußballspiele und sonstige Großveranstaltungen des Landesbeauftragten für den Datenschutz Niedersachsen verwiesen.

Als behördliche(r) Datenschutzbeauftragte(r) erkläre ich die vorhandene bzw. vorgesehene Videoüberwachungsmaßnahme für

- ☐ zulässig.
☐ zulässig, wenn folgende Voraussetzungen erfüllt sind:

- ☐ zurzeit nicht zulässig, weil folgende Alternativen bisher nicht genutzt wurden:

- ☐ nicht zulässig, weil folgende Voraussetzungen fehlen:

- ☐ Rechtsgrundlage
- ☐ Erforderlichkeit
- ☐ Geeignetheit
- ☐ Verhältnismäßigkeit

8. Sonstiges

8.1 Wesentliche Änderungen

Unter Hinweis auf § 7 Abs. 3 NDSG ist bei jeder wesentlichen Änderung an der Videoüberwachungsanlage – auch temporärer Art – in eine erneute Prüfung einzutreten. Dem behördlichen Datenschutzbeauftragten sind alle erforderlichen Fakten umgehend mitzuteilen. Zu den wesentlichen Änderungen einer optisch-elektronischen Überwachungsanlage gehören u. a.:

- ☐ Austausch von Videokameras mit höherwertigen Leistungsmerkmalen
- ☐ Ergänzung der Anlage mit weiteren Videokameras
- ☐ Ergänzung der Anlage mit Zusatztechnik (z. B. Bewegungsmelder)
- ☐ Veränderung der Löschfrist

8.2 Regelmäßige Überprüfung der Erforderlichkeit

Die Videoüberwachungsmaßnahmen sind in regelmäßigen Abständen einer Evaluation zu unterziehen, um sicherzustellen, dass es auch zukünftig keine milderen Mittel zur Zweckerfüllung gibt. Sofern zwischenzeitlich alternative Konzepte zur Verfügung stehen, die den gleichen Zweck erfüllen und weniger bis gar nicht in das Recht auf informationelle Selbstbestimmung – auch in Form der Anonymisierung oder Pseudonymisierung – eingreifen, ist die Überwachung mittels optisch-elektronischer Einrichtungen umgehend einzustellen.

Die Evaluation hat die zur Einführung von Beobachtung und Aufzeichnung mittels Videotechnik erforderlichen Eckdaten (z. B. Kriminalitätsbelastungszahlen) ebenfalls zu umfassen. Dazu liefert der verantwortliche Stelle mindestens einmal im Jahr die entsprechenden Fakten. Sobald die entsprechenden Eckdaten nicht mehr erfüllt werden, ist die Videoüberwachung grundsätzlich ebenfalls einzustellen, da der Zweck nicht oder nicht mehr erfüllt wird.

9. Anlagen

()	Datenblatt Videokamera	Anlage Ziffer 9. ____
()	Datenblatt Aufzeichnungsgerät	Anlage Ziffer 9. ____
()	Dienstanweisung Videoüberwachung	Anlage Ziffer 9. ____
()	Dienstvereinbarung Videoüberwachung	Anlage Ziffer 9. ____
()	Muster für die Kennzeichnung	Anlage Ziffer 9. ____
()	Netzwerkplan	Anlage Ziffer 9. ____
()	Skizze / Übersichtsplan Kamerastandorte	Anlage Ziffer 9. ____
()	Skizze / Übersichtsplan Erfassungsbereiche	Anlage Ziffer 9. ____
()	Skizze / Übersichtsplan Schwenkbereiche	Anlage Ziffer 9. ____
()	_____	Anlage Ziffer 9. ____
()	_____	Anlage Ziffer 9. ____

Der Landesbeauftragte für den Datenschutz Niedersachsen

Brühlstraße 9, 30169 Hannover

Tel.: 0511 - 120 4500 / Fax: 0511 - 120 4599

E-Mail: poststelle@lfd.niedersachsen.de

Stand: Mai 2011