

## Vorbemerkung

Nach dem Berliner Datenschutzgesetz (BlnDSG) ist eine Beobachtung öffentlich zugänglicher Räume mit opto-elektronischen Einrichtungen (Videoüberwachung) nur zulässig, soweit der Einsatz der Videoüberwachung zur Aufgabenerfüllung oder zur Wahrnehmung des Hausrechts erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen (§ 31 b BlnDSG).

Dieses Formular stellt eine Arbeitshilfe zur Fertigung der Dokumentation (Dateibeschreibung) nach § 19 BlnDSG zur Verfügung.<sup>1</sup>

### 1. Dateibeschreibung für:

(Art der Überwachung)

- Videobeobachtung ohne Aufzeichnung  
(„Verlängertes Auge“ des Sekretariats, des Hausmeisters)
- Videobeobachtung mit anlassbezogener Aufzeichnungsmöglichkeit  
(„Verlängertes Auge mit Gedächtnis im Einzelfall“)
- Videobeobachtung mit Aufzeichnung  
(„Verlängertes Auge“ mit durchgehender Aufzeichnung von Bilddaten)
- Videoaufzeichnung ohne Beobachtung über Live-Monitor  
(Black-Box-Verfahren)
- Videokamera-Attrappe

---

<sup>1</sup> Diese Ausarbeitung ist in weiten Teilen dem Musterformular des Hamburger Datenschutzbeauftragten entnommen:  
[http://www.datenschutz-hamburg.de/uploads/media/Musterformular\\_Videoueberwachung\\_oeffentlicher\\_Stellen.pdf](http://www.datenschutz-hamburg.de/uploads/media/Musterformular_Videoueberwachung_oeffentlicher_Stellen.pdf)

## 2. Anschriften und Zuständigkeiten:

(1) Name und Anschrift des Schulträgers:

Bezirksamt \_\_\_\_\_ von Berlin

Abt. \_\_\_\_\_

Bezirksstadtrat/-rätin \_\_\_\_\_

\_\_\_\_\_ Berlin, \_\_\_\_\_  
(Straße)

(2) Name und Anschrift sowie Leitung der Daten verarbeitenden Stelle (Schule / Schulleitung):

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

(3) Anschrift des videoüberwachten Dienstgebäudes:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

(4) Betroffene Gebäudeteile/betroffene Außenflächen:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

## 3. Zweck der Maßnahme und Rechtsgrundlage nach 31 b BInDSG

a) Kategorien

- Abschreckung
- Einlasskontrolle
- Schutz von Räumen und / oder Gegenständen
- Schutz von Personen

b) Motivation für die Maßnahme: Welche Vorfälle gab es (Dokumentationen)?  
Welche Gefahrenlage ist zu erwarten?

---

---

---

---

c) Welche Alternativen zu der Maßnahme wurden erwogen bzw. getestet?

---

---

---

---

d) Für welchen Zeitraum ist die Maßnahme geplant?

---

---

---

e) Text des Hinweisschildes, mit dem auf die Videoanlage verwiesen wird:

---

---

---

---

f) Dauer der Überwachung:

während der Dienst- /Publikumszeiten: von \_\_\_\_\_ bis \_\_\_\_\_

außerhalb der Dienst-/Publikumszeiten: von \_\_\_\_\_ bis \_\_\_\_\_

24 h  sonstige Beobachtungs-/Aufnahmezeiten

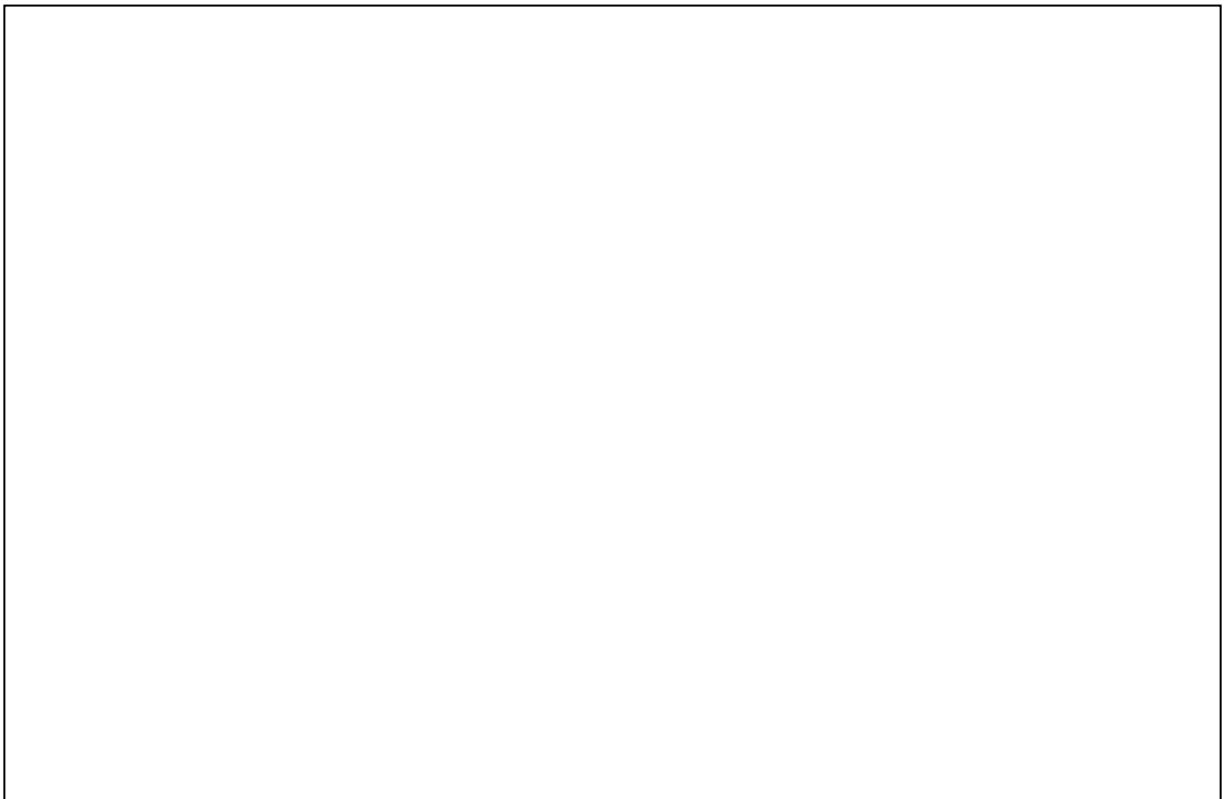
---

---

---

---

g) Perspektivfoto des räumliche Überwachungsbereichs  
(weitere Fotos im Anhang, Alternativ Skizze mit Überwachungsbereiche)



#### 4. Personengruppen

a) Welche Personengruppen sind in der Regel betroffen? Welche Personen können durch besondere Umstände betroffen sein?

---

---

---

---

---

## 5. Zugriffsberechtigungen

a) Wie sind die Zugangsberechtigungen für die Videobeobachtung geregelt?

---

---

---

---

b) Wie sind die Zugangsberechtigungen für die Videoaufzeichnungen geregelt?

---

---

---

---

c) Welche Daten werden durch wen und wann ausgewertet? (Wie ist die Kategorie Vorfall definiert? Welche Maßnahmen sind dann durch wen wie geplant?)

---

---

---

---

---

## 6. Löschung

a) Wann werden Daten gelöscht? (Welche Regelung gibt es für die Sicherung/Löschung bei Vorfällen?)

---

---

---

---

---

b) Verfahren der Löschung

---

---

---

---

---

## 7. Technisch-organisatorische Umsetzung

a) Kurzbeschreibung der Videoüberwachungsanlage (Komponenten, Anzahl der Kameras, Übertragungswege u. ä.):

Komponente der Anlage (Anzahl/Bezeichnung)	Sicherung durch ...

b)  Detailskizze siehe Anhang

c) **Nächster Prüftermin für die Maßnahme:**  
(spätestens alle zwei Jahre)

---

---

Berlin, \_\_\_\_\_

\_\_\_\_\_  
Unterschrift (Schulleitung)

## I Anlage: Technische und organisatorische Maßnahmen nach § 5 BlnDSG

(Hinweise für die Sicherheitsbetrachtung)

Systemkomponente	Schutzziel	Gefahr	Maßnahme
<b>Kamera</b>	<b>Vertraulichkeit</b>	Diebstahl, unberechtigter Zugriff, unberechtigtes Mitsehen	Zugangssicherung, Zugriffsschutz, Berechtigungssystem
	<b>Integrität</b>	Unberechtigte Eingriffe, Veränderungen, Bildbearbeitung	Protokollierung, Zugriffsschutz
	<b>Verfügbarkeit</b>	Vandalismus, Witterungseinflüsse, Diebstahl, Stromausfall	Vandalismusschutz, Alarmfunktionen bei Ausfall,
	<b>Authentizität</b>	Unzulässige Eingriffe	
	<b>Revisionsfähigkeit</b>	Unkontrollierbare Auswertung/ Nutzung der Bilddaten für andere Zwecke	Zugriffsschutz, Zugriffsprotokollierung
<b>Netz</b>	<b>Vertraulichkeit</b>	unberechtigter Zugriff, unberechtigtes Mitsehen	Verschlüsselung
	<b>Integrität</b>	Unberechtigte Eingriffe, Veränderungen,	Zugriffsschutz
	<b>Authentizität</b>	Unzulässige Eingriffe	
	<b>Verfügbarkeit</b>	Vandalismus, Witterungseinflüsse, Diebstahl von Komponenten, Stromausfall	Vandalismusschutz, Alarmfunktionen bei Ausfall / Fehler
	<b>Revisionsfähigkeit</b>		Zugriffsschutz

<b>Systemkomponente</b>		<b>Gefahr</b>	<b>Maßnahme</b>
<b>Videorekorder / Videosever</b>	<b>Vertraulichkeit</b>	Diebstahl, unberechtigter Zugriff, unberechtigtes Mitsehen	Zugangssicherung, Zugriffschutz, Berechtigungssystem
	<b>Integrität</b>	Unberechtigte Eingriffe, Veränderungen, Bildbearbeitung, Datendiebstahl	Protokollierung, Zugriffschutz
	<b>Authentizität</b>	Unzulässige Eingriffe	
	<b>Verfügbarkeit</b>	Vandalismus, Diebstahl, Stromausfall, Wasser- / Feuerschaden	Vandalismusschutz, Alarmfunktionen bei Ausfall, Monitoring
	<b>Revisionsfähigkeit</b>	Unkontrollierbare Auswertung/ Nutzung der Bilddaten für andere Zwecke	Zugriffschutz, Zugriffsprotokollierung
<b>Monitor / PC</b>	<b>Vertraulichkeit</b>	Diebstahl, unberechtigter Zugriff, unberechtigtes Mitsehen	Zugangssicherung, Zugriffschutz, Berechtigungssystem
	<b>Integrität</b>	Unberechtigte Eingriffe, Veränderungen, Datendiebstahl	Protokollierung, Zugriffschutz
	<b>Authentizität</b>	Unzulässige Eingriffe	
	<b>Verfügbarkeit</b>	Vandalismus, Diebstahl, Stromausfall, Wasser- / Feuerschaden	Vandalismusschutz, Alarmfunktionen bei Ausfall, Monitoring
	<b>Revisionsfähigkeit</b>	Unkontrollierbare Auswertung/ Nutzung der Bilddaten für andere Zwecke	Zugriffschutz, Zugriffsprotokollierung



## Anlage II: Art der Geräte, Standort und Überwachungsbereich:

### Art der Geräte:

<b>Kamera</b>	Hersteller, Typenbezeichnung sowie Darstellung der Leistungsmerkmale wie analog/digital, Lichtempfindlichkeit, Bildauflösung, Erfassungswinkel, interner Speicher, Schwenk-/Neigefunktion (mechanisch bzw. digital), Audiofunktion (Mikro integriertes bzw. extern), Signalverarbeitung, Alarmfunktion, Anbindung, mit/ohne Fernsteuerung, etc.
<b>Netz</b>	Darstellung Netzverbindungen (bspw. separate Kabelverbindung) der Einbindung in vorhandene Netze und der Schnittstellen: WLAN, ISDN/DSL, Intranet, Internet, verschlüsselte/unverschlüsselte Datenübertragung
<b>Aufnahmegerät</b>	analoger/digitaler Rekorder, PC, Server, ... Hersteller, Typenbezeichnung und/bzw. Darstellung spez. Leistungsmerkmale wie Speicherkapazität, Netzeinbindung, Audiofunktion, Zugriffsschutz, eingesetzte Videomanagementsoftware etc.
<b>Encoder (Einbindung analoger Geräte)</b>	Hersteller, Typenbezeichnung, besondere Leistungsmerkmale
<b>Monitore</b>	Hersteller, Typenbezeichnung, besondere Leistungsmerkmale