



**Richtlinie für die Aufstellung und den Betrieb
von Anlagen zur Videoüberwachung
an der
Freien Universität Berlin**

Version 2.0

28. Februar 2019

Steckbrief

| | |
|-------------------------|--|
| <i>Zielsetzung</i> | Geregelte Beantragung und geregelter Betrieb von Videoüberwachungsanlagen |
| <i>Inhalt</i> | Standardisiertes Antragsverfahren zur Einrichtung und zum Betrieb von Videoüberwachungsanlagen sowie zur Verarbeitung aufgezeichneter Informationen (Videodaten) |
| <i>Zielgruppe</i> | Dekane, Verwaltungsleiter, Bereichsleiter, IT-Beauftragte, Verfahrensverantwortliche |
| <i>Geltungsbereich</i> | Alle Einrichtungen der Freien Universität Berlin |
| <i>Gültigkeitsdauer</i> | Unbegrenzt |

Autoren

Hr. Camphausen

Hr. Dräger

Hr. Dr. Haase

Fr. Heinau

Hr. Posel

Hr. Dr. Sommerer

Hr. Tietz

Fr. Dr. Wittkopf

Hr. Worch

Dieses Dokument einschließlich aller Teile ist urheberrechtlich geschützt.

Die Weitergabe (Vervielfältigung) ist ohne Zustimmung der Freien Universität Berlin unzulässig.

© 2019 Freie Universität Berlin, Kaiserswerther Str. 16/18, 14195 Berlin

Inhalt

| | |
|--|-----------|
| Inhalt | 3 |
| Präambel | 4 |
| 1 Vorbemerkung | 4 |
| 2 Begriffsdefinitionen | 5 |
| 3 Ablauf des Antragsverfahrens | 6 |
| 3.1 Phase 1 – Antragsstellung | 7 |
| 3.2 Phase 2 – Prüfung des zuständigen IT-Beauftragten | 8 |
| 3.3 Phase 3 – Eingangsprüfung durch den IT-Sicherheitsbeauftragten | 8 |
| 3.4 Phase 4 – Prüfung und Entscheidung | 8 |
| 3.5 Phase 5 – Umsetzung und Archivierung | 9 |
| 4 Auswertung von Videodaten | 10 |
| 4.1 Grundsätze | 10 |
| 4.2 Verarbeitung von Videodaten | 10 |
| 4.3 Auswertung von Videodaten | 10 |
| 4.4 Herausgabe von Videodaten an Dritte | 11 |
| 4.4.1 Datensicherung | 11 |
| 4.4.2 Prüfung | 12 |
| 4.4.3 Protokollierung | 13 |
| 4.4.4 Datenübermittlung | 13 |
| 5 Änderungen nach Antragstellung | 14 |
| 6 Bekanntgabe der Richtlinie und Inkrafttreten | 14 |
| Anlage 1: Antrag für den Einsatz von Videoüberwachungsanlagen | 15 |
| Anlage 2: Protokoll zur Einsichtnahme von Videodaten | 20 |
| Anlage 3: Protokoll zur Herausgabe von Videodaten | 21 |
| Anlage 4: Schematischer Ablaufplan | 22 |
| Anlage 5: Auszug Berliner Datenschutzgesetz | 23 |

Präambel

Das Präsidium hat nach Anhörung der Datenschutzbeauftragten der Freien Universität Berlin und des Datenschutzbeauftragten für die Zentraleinrichtung Botanischer Garten, Botanisches Museum gemäß § 6b II BerlHG am 28.02.2019 folgende Richtlinie zur Videoüberwachung erlassen.

1 Vorbemerkung

Der Einsatz von Videoüberwachungsanlagen kann ein geeignetes Mittel zum Schutz von Menschen und universitären Einrichtungen sein. Auch im wissenschaftlichen Kontext stellt Videoaufzeichnungstechnik ein wertvolles Hilfsmittel dar, beispielsweise zur Dokumentation von Versuchen oder zur Beobachtung von Prozessen. Bei nicht geregeltem Einsatz drohen jedoch Gefahren für die Freiheitsrechte der Mitglieder der Universität und unbeteiligter Dritter.

Die Freie Universität Berlin ist gehalten, beim Einsatz von Videoüberwachungsanlagen eine Abwägung insbesondere zwischen Freiheitsrechten und Sicherheitsanforderungen zu treffen. Zu beachten sind dabei insbesondere:

- das Recht auf freie Entfaltung der Persönlichkeit
- das Recht am eigenen Bild
- das Recht auf informationelle Selbstbestimmung
- die nach den Bestimmungen des Datenschutzes geforderte Verhältnismäßigkeit (Datenvermeidung, Zweckbindung, Erforderlichkeit)
- die Beachtung von Mitbestimmungsrechten der Personalvertretung, sofern Beschäftigte der Freien Universität von der Videoüberwachung erfasst werden.
- Regelungen nach dem Berliner Datenschutzgesetz (siehe Anhang)

Mit einem standardisierten Antragsverfahren wird dazu beigetragen, dass alle notwendigen Überlegungen vor Beschaffung und Einsatz einer Videoüberwachung angestellt und alle zuständigen Stellen beteiligt werden. Außerdem werden verbindliche Regeln aufgestellt und per Unterschrift bestätigt. Darüber hinaus werden Grundsätze für die Verarbeitung von Videodaten festgelegt. Dieses Verfahren ist auch dann einzuhalten, wenn eine Speicherung der aufgenommenen Daten nicht vorgesehen ist.

Ob der Einsatz von Videoüberwachung überhaupt erforderlich ist und wie dieser ggf. zu gestalten ist, muss jeweils im Einzelfall geprüft werden.

Eine Übersicht über den Ablauf des Antragsverfahrens finden Sie in der [Anlage 4: Schematischer Ablaufplan](#) auf Seite 22.

2 Begriffsdefinitionen

Videoüberwachung ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen, so die Definition im Berliner Datenschutzgesetz.

Die vorliegende Richtlinie betrifft nur Videoüberwachungsanlagen aus festinstallierten und dauerhaft mit einem Baukörper verbundenen optisch-elektronischen Einrichtungen zur Aufzeichnung von Bildern. Zu einer Videoüberwachungsanlage zählen neben dem Kamerasystem auch die zugehörigen Stromversorgungseinrichtungen (Leitungen), Datenübertragungsmedien (Leitungen, Funk), Datendosen und Hinweisschilder. Darüber hinaus sind auch alle technischen Einrichtungen zur Datenübertragung und -speicherung mit einzubeziehen.

Zum Zweck der Abschreckung kommen auch Attrappen von Videokameras (Dummys), die keine Bilder aufnehmen können, sowie Warnschilder zum Einsatz. Die Vorschriften dieser Richtlinie, insbesondere die Regelungen zur Beantragung und Dokumentation, gelten auch für den Einsatz von Dummys im vollen Umfang. Sie sind in dieser Hinsicht funktionsfähigen Videoüberwachungsanlagen gleichgestellt.

Antragsteller sind Beschäftigte der Freien Universität Berlin, die zur Beantragung von Videoüberwachungsanlagen berechtigt sind. Berechtigt sind Verwaltungsleiter/innen sowie Dekaninnen und Dekane und Prodekaninnen und Prodekane der Fachbereiche, Leiter/innen von Zentralinstituten, Abteilungsleiter/innen und Direktoren/innen von zentralen Einrichtungen.

Betriebsverantwortliche/r ist ein/e Beschäftigte/r der Freien Universität, die/der von der/vom Antragsteller/in als solche/r benannt wird.

Die Regelungen dieser Richtlinie müssen auch für Videoüberwachungsanlagen angewendet werden, die im wissenschaftlichen Kontext eingesetzt werden und nicht dem Schutz von Menschen und universitären Einrichtungen dienen. (Beispiel: Überwachung von Tieren im Fachbereich Veterinärmedizin.)

3 Ablauf des Antragsverfahrens

Das Antragsverfahren soll durch die folgende Grafik veranschaulicht werden. Die einzelnen Phasen des Ablaufs werden im Folgenden beschrieben.

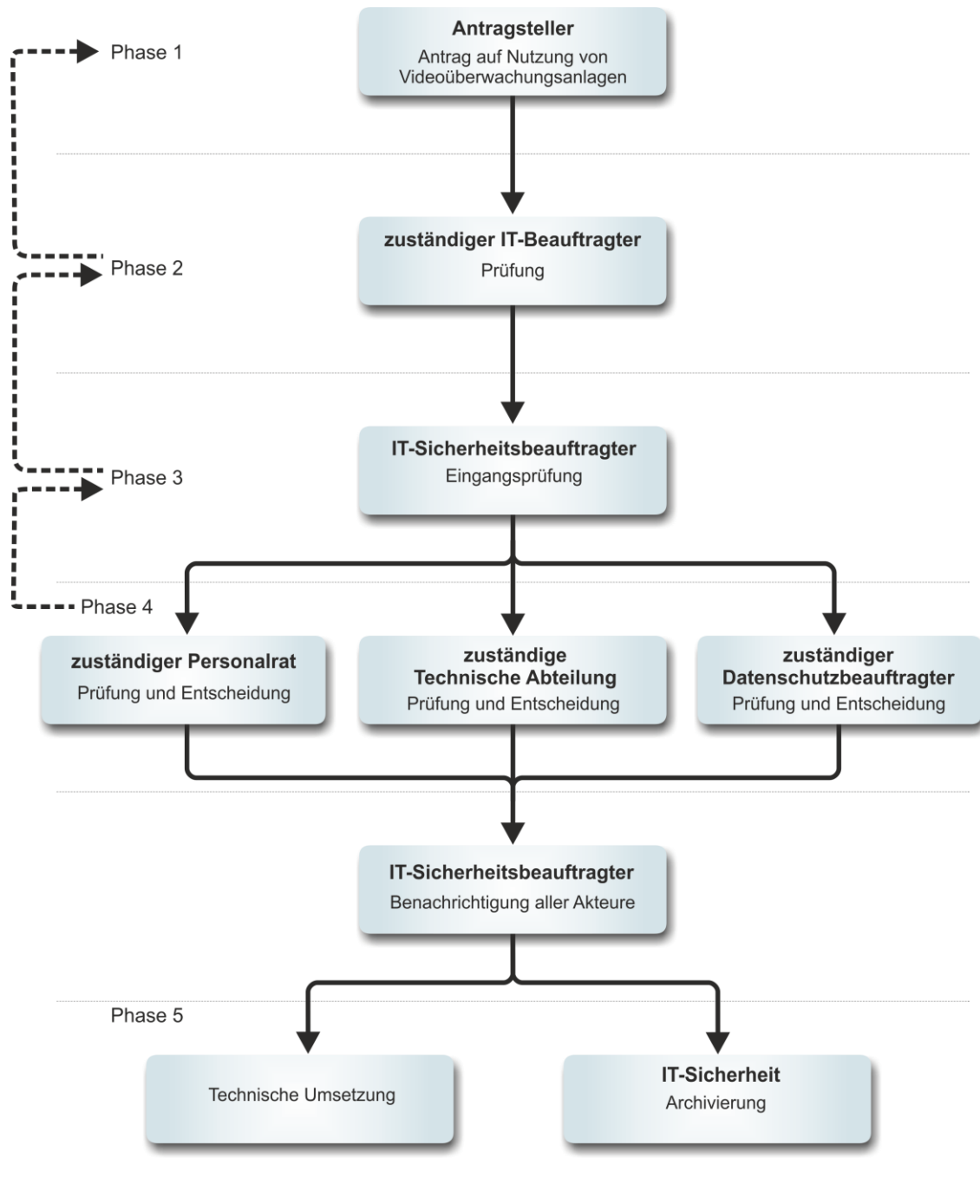


Abbildung 1: Schematische Darstellung des Ablaufs des Antragsverfahrens. Die gestrichelten Pfeile sollen andeuten, dass bei unterschiedlichen Bewertungen weitere Gespräche erfolgen.

3.1 Phase 1 – Antragsstellung

Bei Videoüberwachung und ggf. Aufzeichnungen von Personen ist in jedem Fall der Persönlichkeitsschutz zu beachten. Um an der Freien Universität Berlin eine Anlage zur Videoüberwachung in Betrieb zu nehmen, müssen vorher die Anforderungen des Datenschutzes und der Beteiligungsrechte der Personalvertretung geprüft werden.

Die Antragsteller müssen im Vorfeld prüfen, ob andere Mittel geeigneter sind, den gewünschten Gewinn an Sicherheit bzw. den gewünschten Zweck zu erzielen. Der Antrag gemäß Anlage 1 dieser Richtlinie muss vom/von der Antragsteller/in gestellt werden. Hierfür sind die jeweils geltenden Regelungen der Freien Universität Berlin sowie wirtschaftliche und technische Aspekte zu berücksichtigen, d.h. eine Kostenschätzung und eine technische Skizze muss dem Antrag beigelegt werden.

Die in dem Antragsformular der Anlage 1 dieser Richtlinie geforderten Angaben dienen u. a. als Grundlage für die Prüfung durch die zuständige Technische Abteilung, den zuständigen Personalrat und den zuständigen Datenschutzbeauftragten. Der Antrag muss nach der Prüfung der/des zuständigen IT-Beauftragten an den IT-Sicherheitsbeauftragten der Freien Universität Berlin übermittelt werden.

Unter anderem müssen die folgenden Informationen aus den Antragsunterlagen hervorgehen:

- Zweck der Videoüberwachung
- mögliche Alternativen
- Schätzung der entstehenden Kosten
- Angaben zu allen verfahrensrelevanten Rollen und Rolleninhabern
- Angaben über die Anzahl und Art von (geplanten) technischen Einrichtungen (u. a. Anzahl und Typ der Kameras, Ort der Anbringung)
- Technische Skizze (Lage- bzw. Aufstellungsplan, Erfassungswinkel)
- Angaben zu betroffenen Personen
- Angaben der Schnittstellen zu anderen IT-Verfahren, Datenübertragung
- Angaben zur Art der Speicherung, Speicherort, Speicherdauer
- Angaben der zugriffsberechtigten Personen (inkl. Angaben zum Umfang der Zugriffsrechte)
- Beabsichtigter Beginn und beabsichtigtes Ende der Maßnahme
- Zeitplan mit den wesentlichen Meilensteinen für die Einführung des Verfahrens

Insbesondere müssen alle verantwortlichen Rolleninhaber (Antragsteller, Personen mit administrativen Rechten usw.) und deren Vertreter/innen mit den vollständigen Kontaktdaten (Name, Dienstadresse, dienstliche Telefonnummer, dienstliche E-Mail-Adresse) angegeben werden. Sind externe Personen (z.B. Fremdfirmen) involviert, müssen ebenfalls alle Personen mit einer Zugriffsberechtigung auf die Systeme und/oder Daten mit ihren vollständigen Kontaktdaten angegeben werden.

Bei einer beabsichtigten Änderung von bereits genehmigten Anlagen sind die Änderungen im Einzelnen zu beschreiben.

3.2 Phase 2 – Prüfung des zuständigen IT-Beauftragten

Der/Die zuständige IT-Beauftragte prüft den Antrag. Bei Bedenken sollte mit der/dem Antragsteller/in eine einvernehmliche Lösung angestrebt werden, bevor der Antrag weitergeleitet wird.

3.3 Phase 3 – Eingangsprüfung durch den IT-Sicherheitsbeauftragten

Der IT-Sicherheitsbeauftragte der Freien Universität Berlin prüft die Angaben inhaltlich und auf Vollständigkeit. Einzelheiten können in einem Gespräch mit der/dem Antragsteller/in geklärt werden. In diesem Gespräch können Ergänzungen und Modifikationen zum Antrag vorgeschlagen werden. Die Prüfung durch den IT-Sicherheitsbeauftragten muss i. d. R. spätestens drei Wochen nach Eingang der Unterlagen abgeschlossen werden.

3.4 Phase 4 – Prüfung und Entscheidung

Nachdem der IT-Sicherheitsbeauftragte den Antrag geprüft hat, wird der Antrag mit dem Ergebnis der Prüfung an die zuständige Technische Abteilung, den zuständigen Personalrat und den zuständigen Datenschutzbeauftragten weitergeleitet. In der zuständigen Technischen Abteilung wird eine mögliche technische Realisierung geprüft, insbesondere werden Aspekte im folgenden Zusammenhang betrachtet:

- Finanzierung der Anlage
- Installation bzw. Aufbau der Anlage
- Wartung bzw. Instandsetzung der Anlage
- Veränderung der Anlage

Der zuständige Personalrat prüft den Antrag bezüglich mitbestimmungsrelevanter Tatbestände. Der zuständige Datenschutzbeauftragte prüft den Antrag in datenschutzrechtlicher Hinsicht.

Das Ergebnis der Prüfung wird in Form von schriftlichen Stellungnahmen an den IT-Sicherheitsbeauftragten der Freien Universität übermittelt. Nach Ablauf von vier Wochen informiert der IT-Sicherheitsbeauftragte die/den Antragsteller/in, den zuständigen Personalrat und den zuständigen Datenschutzbeauftragten über den aktuellen Stand des Antragsverfahrens und das Antragsverfahren läuft weiter.

Ergeben sich aus zusätzlichen Gesprächen noch weitere Informationen, so werden diese dem Antragsformular hinzugefügt bzw. wird der Antrag modifiziert. Der IT-Sicherheitsbeauftragte informiert alle anderen Akteure über die erfolgten Änderungen, damit der modifizierte Antrag erneut geprüft werden kann.

Die Videoüberwachungsanlage kann eingerichtet und in Betrieb genommen werden, wenn die folgenden Bedingungen erfüllt sind:

- Zustimmung der/des zuständigen IT-Beauftragten liegt vor
- Zustimmung des IT-Sicherheitsbeauftragten der Freien Universität Berlin liegt vor
- Zustimmung des zuständigen Personalrats liegt vor
- Zustimmung der zuständigen Technischen Abteilung liegt vor
- Zustimmung der/des zuständigen Datenschutzbeauftragten liegt vor

Wenn von einer der oben genannten Entscheidungsinstanzen nach Ablauf von vier Wochen keine Stellungnahme erfolgt ist und sonst nur Zustimmungen vorliegen, darf die/der Antragsteller/in die Videoüberwachungsanlage einrichten und in Betrieb nehmen.

3.5 Phase 5 – Umsetzung und Archivierung

Im Falle einer positiven Entscheidung erfolgt i.d.R. in Zusammenarbeit der Antragstellerin bzw. des Antragstellers mit der zuständigen Technischen Abteilung die Installation und die Inbetriebnahme in der dokumentierten Art und Weise. Wenn zum Betrieb der Videoüberwachungsanlage IT-Infrastruktur benötigt wird, muss rechtzeitig der zuständige Infrastrukturbetreiber (i.d.R. ZE-DAT) informiert und notwendige Abstimmungen eingeleitet werden.

Alle Unterlagen des Antragsverfahrens werden beim IT-Sicherheitsbeauftragten archiviert. Außerdem wird vom IT-Sicherheitsbeauftragten in der IT-Verfahrensdatenbank für jede genehmigte Videoüberwachungsanlage ein IT-Verfahren angelegt, das immer die gleiche Dokumentationsstruktur aufweist:

| Feldbezeichnung | Inhalt |
|---|--|
| Angaben zum IT-Verfahren / Bezeichnung: | „Videoüberwachung“ und ergänzend durch einen variablen Teil, bestehend aus einer Ortsangabe |
| Angaben zum IT-Verfahren / Zielsetzung und Zweck: | <ul style="list-style-type: none"> • Zusammenfassung von 1.1 des Antrags • Angabe über den Ort der Dokumentation • Status: „in Betrieb“, „stillgelegt“ oder „genehmigt“ • (Ggf. Nummerierte) „Änderung am:“ Datum der Änderung |
| Angaben zum IT-Verfahren / Datum der Erstmeldung: | Datum der Genehmigung (Benachrichtigung der Akteure durch den IT-Sicherheitsbeauftragten der Freien Universität Berlin) |
| Angaben zum IT-Verfahren / Organisationseinheit: | Organisationseinheit, in der die Videoüberwachungsanlage betrieben wird |
| Verfahrensverantwortliche: | Angaben zum Antragsteller und zum Betriebsverantwortlichen |

Darüber hinaus werden keine weiteren Informationen in der IT-Verfahrensdatenbank gespeichert. Insbesondere wird zu dem IT-Verfahren kein Geschäftsprozess angelegt.

4 Auswertung von Videodaten

In diesem Abschnitt werden die Grundsätze für die Verarbeitung bzw. die Übermittlung der von Videoüberwachungsanlagen aufgezeichneten Informationen (Videodaten) festgelegt.

4.1 Grundsätze

Die folgenden Grundsätze sind bei jeder Verarbeitung oder Herausgabe von Videodaten zu beachten:

- Zweckbindung

Prinzipiell dürfen Videodaten für den im Antrag dokumentierten Zweck verarbeitet werden. Darüber hinaus ist die Verwertung bzw. Herausgabe von Videodaten nur zulässig, wenn sich Anhaltspunkte für Straftaten oder Ordnungswidrigkeiten ergeben und die Unterrichtung der für die Verfolgung oder Vollstreckung zuständigen Behörden geboten ist.

- Berechtigte Antragsteller (Anfragende Stellen)

Im Rahmen der Dokumentation dürfen Videodaten nur auf der Grundlage von Anfragen von Sicherheitsbehörden an Sicherheitsbehörden herausgegeben werden. Die Herausgabe von Videodaten an FU-interne Stellen ist unzulässig, ausgenommen sind Anfragen vom Rechtsamt und der Personalabteilung.

4.2 Verarbeitung von Videodaten

Videodaten dürfen ausschließlich laut genehmigtem Antragsverfahren verarbeitet werden. Eine davon abweichende Verarbeitung muss ihrerseits beantragt und genehmigt werden.

4.3 Auswertung von Videodaten

Der Zugriff bzw. die Einsichtnahme und die Auswertung von Videodaten muss im Antrag deutlich und unmissverständlich beschrieben werden. (Siehe Antragsformular Abschnitt 4.3) Der Kreis der Einsichtsberechtigten ist genau anzugeben (namentlich oder Funktionsbezeichnung).

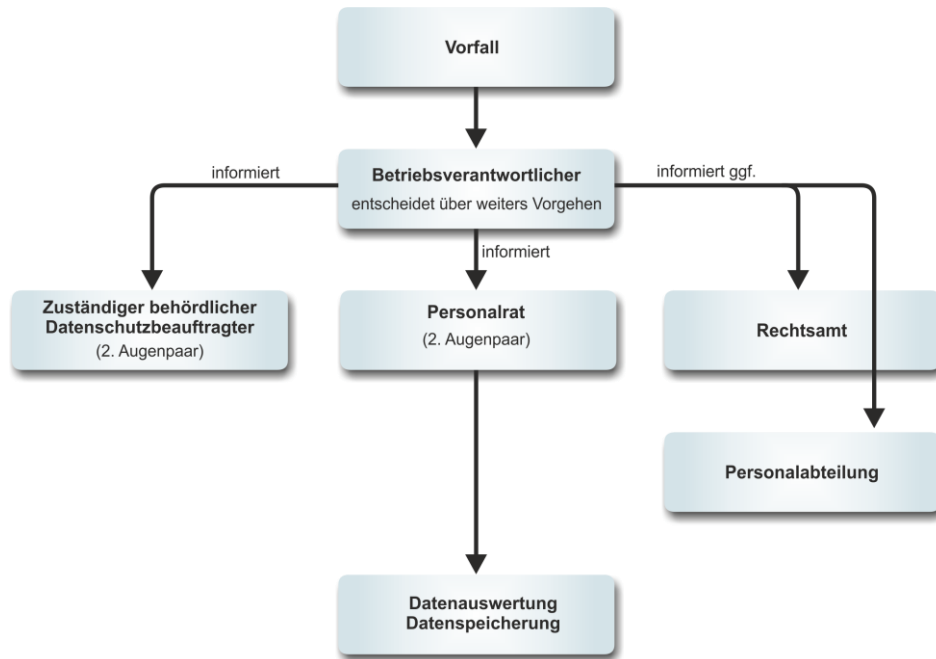


Abbildung 2: Schematische Darstellung des Ablaufs bei der Auswertung von Videodaten mit Personenbezug.

Die Auswertung von personenbezogenen Videodaten hat nach dem Vier-Augen-Prinzip zu erfolgen. In der Regel gehört das erste Augenpaar der/dem Beschäftigten, die/der vom Betriebsverantwortlichen mit der Administration der Videoüberwachungsanlage beauftragt wurde. Das zweite Augenpaar soll einer unabhängigen Stelle angehören, entweder dem zuständigen Personalrat oder dem zuständigen Datenschutzbeauftragten. Die für das Vier-Augen-Prinzip vorgesehenen Personen müssen namentlich und mit Rollenbezeichnung dokumentiert werden.

Wenn Beschäftigte der Freien Universität Berlin im Bildmaterial aufgezeichnet wurden muss der zuständige Personalrat informiert werden.

Die Auswertung muss gemäß Anlage 2: Protokoll zur Einsichtnahme von Videodaten, protokolliert werden. Die Protokollierung muss nach den Vorgaben des Abschnitts 4.4.3 erfolgen, soweit die Vorgaben auf den aktuellen Fall anwendbar sind.

4.4 Herausgabe von Videodaten an Dritte

4.4.1 Datensicherung

Wird die Herausgabe von Videodaten verlangt, sind in einem ersten Schritt die betreffenden Daten gegen Verlust zu sichern. Es muss darauf geachtet werden, dass nur die angeforderten bzw. die zur Herausgabe vorgesehenen Daten (Zeitraum, Videokamera, bei Anlagen mit mehreren Kameras) gesichert werden.

4.4.2 Prüfung

Der schematische Ablauf der Prüfung kann aus der folgenden Abbildung entnommen werden. Bei Fragen können Sie sich an den IT-Sicherheitsbeauftragten der Freien Universität Berlin wenden.

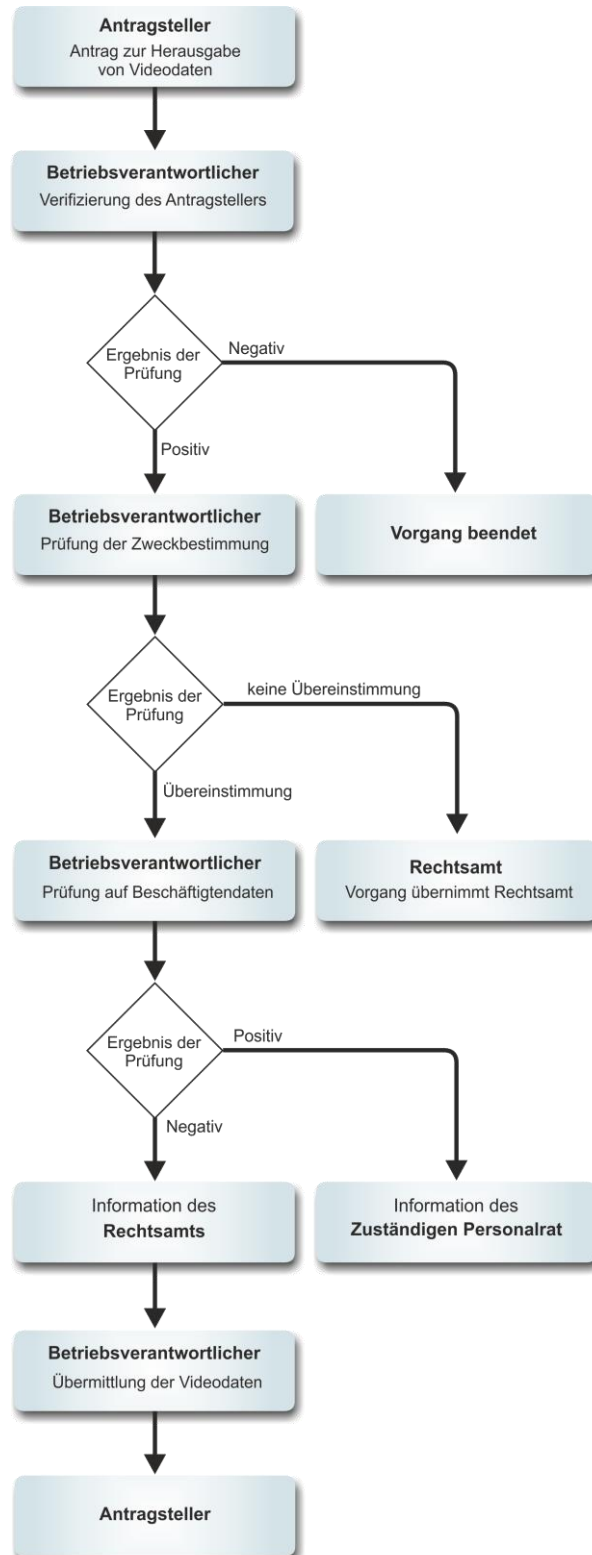


Abbildung 3: Schematische Darstellung des Ablaufs bei der Herausgabe von Videodaten.

Gespeicherte Videodaten dürfen nur nach vorheriger Prüfung durch den Betriebsverantwortlichen herausgegeben werden. Die Prüfung umfasst mindestens die folgenden Punkte:

1. Zuständigkeit und Verifizierung des Antragstellers
 - Nur Sicherheitsbehörden, in der Regel Polizei, Anwaltschaft oder Staatsanwaltschaft, dürfen die Herausgabe von Daten beantragen, in der Regel ist die Schriftform unter Nennung der Rechtsgrundlage erforderlich.
 - Der angegebene Absender muss stets überprüft werden. Dabei sind die Absenderangaben unabhängig vom eingegangenen Antrag zu prüfen. Ist beispielsweise eine Fax-Anfrage eingegangen, sollten die Angaben durch einen Telefonanruf an eine Telefonnummer überprüft werden, die unabhängig recherchiert wurde und nicht aus der Anfrage selbst stammt.
2. Prüfung der Zweckbestimmung
 - Wenn beispielsweise Videokameras zur Dokumentation eines seltenen botanischen Ereignisses (Blüte exotischer Pflanzen) installiert wurden, dürfen die Videodaten nicht ohne weiteres für andere Zwecke, wie zum Beispiel zur Aufklärung eines zufällig aufgezeichneten Vergehens, genutzt werden.
 - Ist keine Übereinstimmung zwischen der Zweckbestimmung der Videoüberwachungsanlage und dem Antrag zur Herausgabe der Videodaten erkennbar, muss das Rechtsamt einbezogen werden. Das Rechtsamt entscheidet über das weitere Vorgehen.
 - Sollte nach 30 Tagen keine Mitteilung des Rechtsamts vorliegen, fragt die betriebsverantwortliche Stelle beim Rechtsamt nach, ob die gesicherten Daten gelöscht werden können.
3. Prüfen, ob Beschäftigte der Freien Universität betroffen sind
 - Wenn in den angefragten Videodaten Beschäftigte der Freien Universität zu sehen sind, muss der zuständige Personalrat informiert werden.

4.4.3 Protokollierung

Die Herausgabe von Videodaten muss nach dem in [Anlage 3: Protokoll zur Herausgabe von Videodaten](#), wiedergegebenen Schema protokolliert werden. Das Protokoll muss von dem Betriebsverantwortlichen handschriftlich oder elektronisch¹⁾ unterschrieben werden. Das Protokoll wird bei der betriebsverantwortlichen Stelle für mindestens zwei Jahre archiviert.

4.4.4 Datenübermittlung

Videodaten dürfen grundsätzlich nicht ungeschützt übermittelt werden.

Für die Datenübermittlung kommen beispielsweise folgende Verfahren in Frage:

- Übergabe der gegen unbefugte Nutzung gesicherten Daten an vertrauenswürdigen Boten

¹⁾ Die elektronische Unterschrift muss mindestens die Anforderungen der Zertifizierungsrichtlinie der DFN-PKI erfüllen.

- Verschlüsselte E-Mail (z.B. nach dem X.509-Standard mittels eines gültigen DFN-Zertifikats)
- Ablage einer verschlüsselten²⁾ Datendatei auf eine vertrauenswürdigen Datenablageplattform und Übermittlung des Zugriffspfads sowie der notwendigen Zugriffsinformationen an den Empfänger
- Datenträger mit verschlüsselten Videodaten per Postzustellurkunde

5 Änderungen nach Antragstellung

Die Dokumentation der Videoüberwachungsanlage muss stets auf dem aktuellen Stand gehalten werden. Bei Änderungen einer Videoüberwachungsanlage muss zeitnah eine Meldung über die Art und den Umfang der Änderung an den IT-Sicherheitsbeauftragten der Freien Universität Berlin erfolgen.

Darüber hinaus sind zur Gewährleistung der Aktualität der Dokumentation alle Einrichtungen der Freien Universität Berlin verpflichtet, jährlich jeweils zum 31. März die Aktualität der Dokumentation der in ihrem Zuständigkeitsbereich betriebenen Videoüberwachungsanlagen zu prüfen. Das Ergebnis der Prüfung muss dem IT-Sicherheitsbeauftragten der Freien Universität Berlin in folgender Form mitgeteilt werden:

- Bestätigung des unveränderten Betriebs oder
- Aktualisierung der Dokumentation (Beschreibung der Art und des Umfangs der Änderung) oder
- Mitteilung über die Einstellung des Betriebs und Abbau der Videoüberwachungsanlage.

6 Bekanntgabe der Richtlinie und Inkrafttreten

Die vorliegende Richtlinie tritt am Tage nach der Veröffentlichung als Rundschreiben in Kraft. Zugleich tritt die vorhergehende Richtlinie, veröffentlicht als FU-Rundschreiben V 10/2015, außer Kraft.

²⁾ Es muss ein allgemein anerkanntes Verfahren zur starke Verschlüsselung eingesetzt werden. Das Schlüsselmanagement muss der vollständigen Kontrolle durch kompetente Stellen der Freien Universität Berlin (z.B. Hochschulrechenzentrum ZEDAT) unterliegen.

Anlage 1: Antrag für den Einsatz von Videoüberwachungsanlagen

Bei der Beantwortung der folgenden Fragen können ggf. weitere Blätter angefügt werden, falls ausführlichere Darstellungen erforderlich sind.

1 Motivation

| 1.1 | Was ist der Zweck des Videoeinsatzes? |
|---------------------------------|---|
| <input type="checkbox"/> | Abschreckung |
| <input type="checkbox"/> | Einlasskontrolle |
| <input type="checkbox"/> | Schutz von Räumen und/oder Gegenständen |
| <input type="checkbox"/> | Schutz von Personen |
| <input type="checkbox"/> | Wissenschaftliche Zwecke (z.B. Versuchsbeobachtungen) |
| <input type="checkbox"/> | Sonstige Zwecke |
| Bitte kurz den Zweck erläutern: | |
| | |

| 1.2 | Was soll überwacht werden? |
|--------------------|----------------------------|
| Überwachte Objekte | (genaue) Ortsangabe |
| | |

| 1.3 | Zu welchen Zeiten soll die Anlage in Betrieb sein? |
|------|--|
| | |

| 1.4 | Sind bereits Schäden entstanden? |
|--------------------------|----------------------------------|
| <input type="checkbox"/> | Materielle Schäden, Höhe: |
| <input type="checkbox"/> | Personenschäden, welche: |

| | |
|------------|--|
| 1.5 | Sind Alternativen zur Videoüberwachung bedacht, ggf. getestet worden? Ggf. (kurzer) Erfahrungsbericht |
| | |

2 Technik und Kosten

| | |
|---|--|
| 2.1 | Liegt eine technische Skizze zur geplanten Videoüberwachung vor? |
| <input type="checkbox"/> Ja <input type="checkbox"/> Nein, Begründung: | |

| | |
|------------|---|
| 2.2 | Welche Kameratechnologie soll angeschafft werden? |
| | |

| | |
|------------|---|
| 2.3 | Welche Software soll eingesetzt werden? |
| | |

| | |
|------------|---|
| 2.4 | Welche Leitungswege und -materialien sind erforderlich? |
| | |

| | |
|------------|--|
| 2.5 | Welche Aufzeichnungsrate ist erforderlich? |
| | |

| | |
|---|--------------------------------|
| 2.6 | Angaben zur (Server-) Hardware |
| Art, Typ: Standort: Verantwortlich für Wartung: | |

| | |
|------------|--|
| 2.7 | Angaben zu Schnittstellen zu anderen Verfahren |
| | |

| | |
|------------|---|
| 2.8 | Welche Kosten werden für die Errichtung entstehen? (Auflistung der Kostenpunkte, getrennt nach zentralen und dezentralen Mitteln) |
| | |

| | |
|------------|--|
| 2.9 | Welche Kosten werden für den laufenden Betrieb entstehen? (Auflistung der Kostenpunkte, getrennt nach zentralen und dezentralen Mitteln) |
| | |

| | |
|-------------|---|
| 2.10 | Angaben zu Betriebszeiten und ggf. zum beabsichtigten Beginn und beabsichtigtes Ende der Maßnahme |
| | |

| | |
|-------------|---|
| 2.11 | Zeitplan mit wesentlichen Meilensteinen für die gewünschte Einführung |
| | |

3 Regelungen zum Betrieb

| | |
|--|---|
| 3.1 | Existieren Regelungen für den Betrieb bzw. Einsatz der Videoüberwachungsanlage? |
| <input type="checkbox"/> Ja <input type="checkbox"/> Nein | |

| | |
|------------|--|
| 3.2 | Falls Regelungen existieren, Angabe der Regeln (Ggf. können die Regelungen als externes Dokument dem Antrag beigefügt werden.) |
| | |

4 Verantwortung

| | |
|--|--|
| 4.1 | Wer ist die/der Antragsteller/in? (Ggf. auch Kontaktdaten des Vertreters angeben.) |
| Vor- und Nachname: Bereich: Tel.: E-Mail: | |

4.2 Betriebsverantwortung

Wer ist für den Betrieb / Datenauswertung / Datenweitergabe verantwortlich? (Ggf. auch Kontaktdaten des Vertreters angeben.)

Vor- und Nachname:
Bereich:
Tel.:
E-Mail:

4.3 Wer ist vor Ort für die Kameras verantwortlich? (Ggf. auch Kontaktdaten des Vertreters angeben.)

Vor- und Nachname:
Bereich:
Tel.:
E-Mail:

4.4 Bestätigung der/des IT-Beauftragten

Über den beabsichtigten Einsatz von Videoüberwachungsanlagen wurde ich informiert.

- Dem Einsatz stimme ich zu.
- Dem Einsatz stimme ich nicht zu.
Die Begründung der Ablehnung erfolgt auf einem gesonderten Blatt.

Berlin,

Ort, Datum, Unterschrift des IT-Beauftragten

5 Datenschutz und Mitbestimmung

5.1 Werden routinemäßig Personen von den Überwachungskameras erfasst?

- Beschäftigte
- Studierende
- Externe (Gäste, Firmenangehörige, etc.)


5.2 Empfänger der Daten / Auswertungen
(Bitte beachten Sie die Hinweis in Abschnitt 4.3, Seite 10.)

- Erfolgt eine Übermittlung der gespeicherten Daten?
- Falls ja, an welche Stelle?
- Falls ja, wie erfolgt die Datenübermittlung (Art des Übermittlungsverfahrens)?

| | | |
|------------|---|------------------------------|
| 5.3 | Zugriffsrechte (Ggf. Beachtung der Regelungen zur Auftragsdatenverarbeitung und des Handlungsleitfadens "Datenzugriff durch Externe") | |
| | Zugriffsberechtigter | Art bzw. Umfang des Zugriffs |
| | | |

| | |
|------------|---|
| 5.4 | Speicherung, Archivierung (Ort, Art, Dauer) |
| | |

| | |
|------------|---------------------------------------|
| 5.5 | Löschung, Überschreiben (Löschzyklen) |
| | |

| | | |
|------------|---|---|
| 5.6 | Angaben zur Kennzeichnung der überwachten Bereiche Zum Beispiel mit Hinweisschild, siehe Abbildung rechts. Außerdem erforderlich (§ 20 Abs. 2 BInDSG): Name und Kontaktdaten der Organisationseinheit, der der Antragsteller angehört. Diese Angaben können auch in Form eines QR-Codes zur Verfügung gestellt werden. |  |
| | | |

| |
|--|
| Unterschrift der/des Antragstellerin/Antragstellers |
| Vor- und Nachname des/der Antragstellerin/Antragstellers in Druckbuchstaben: |
| |
| Berlin, |
| |
| <i>Ort, Datum, Unterschrift der/des Antragstellers/Antragstellerin</i> |

Anlage 2: Protokoll zur Einsichtnahme von Videodaten

| | |
|-------------------------|--|
| 1. | Anlass der Einsichtnahme |
| | |
| 2. | Einsehende Personen (Augenpaare) |
| Namentliche Aufzählung: | |
| | |
| 3. | Datum der Einsichtnahme |
| | |
| 4. | Unterschrift des Betriebsverantwortlichen |
| | |
| | |

Anlage 3: Protokoll zur Herausgabe von Videodaten

| | |
|--|----------|
| 1. Quelle der Videodaten | |
| Angaben zur Quelle der Videodaten (z.B. Aufnahmen der Kamera x an der Fassade des Gebäudes y): | |
| | |
| 2. Zeit der Aufzeichnung | |
| Angaben der Zeitspanne der herausgegebenen Videoaufzeichnungen (zum Beispiel: Von 11.11.2016, 23:30 Uhr – 12.11.2016, 05:15 Uhr): | |
| | |
| 3. Zweckbestimmung | |
| Die Videodaten werden <input type="checkbox"/> gemäß der Zweckbestimmung herausgegeben. <input type="checkbox"/> auf Anweisung des Rechtsamts herausgegeben. | |
| | |
| 4. Daten-Absender | |
| Angabe des Absenders der Daten (Einrichtung der Freien Universität, zum Beispiel: ZEDAT): | |
| | |
| 5. Daten-Empfänger | |
| Angabe des Datenziels (Empfänger der Daten): | |
| | |
| 6. Datenübermittlung | |
| Technische Angaben zur Datenübermittlung (z.B. Datenträger: USB-Stick): | |
| | |
| 7. Datum und Uhrzeit der Datenherausgabe | |
| Datum: | Uhrzeit: |
| | |
| 8. Name und Unterschrift des Herausgebenden | |
| Name und Unterschrift des zuständigen Beschäftigten und Angabe der herausgebenden Stelle: | |
| | |
| Quittierung des Empfängers bei persönlicher Übergabe: | |
| | |

Anlage 4: Schematischer Ablaufplan

| Nr. | Maßnahme |
|---|---|
| Antrag zum Betrieb einer Videoüberwachungsanlage | |
| 1. | Der Antragsteller übermittelt einen vollständig ausgefüllten Antrag zur Errichtung und zum Betrieb einer Videoüberwachungsanlage. |
| 2. | Der IT-Beauftragte des antragstellenden Bereichs prüft den Antrag und dokumentiert seine Zustimmung.. |
| 3. | Der Antrag wird hinsichtlich der folgenden Punkte durch den IT-Sicherheitsbeauftragten geprüft: <ul style="list-style-type: none"> • Vollständigkeit des Antrags gemäß Muster • Darlegung der Notwendigkeit • Zustimmung des zuständigen IT-Beauftragten • Abstimmung mit der Technischen Abteilung • Zustimmung des zuständigen Personalrats • Zustimmung des zuständigen Datenschutzbeauftragten • Angaben zur Sicherstellung der Finanzierung |
| 4. | Die Errichtung der Videoüberwachungsanlage erfolgt i.d.R. durch die Technische Abteilung. |
| 5. | Die Technische Abteilung ist für die 230/400 V-Stromversorgung bis zur Steckdose oder dem Festanschluss zuständig. |
| 6. | Die Datendosen und -leitungen von der Videoüberwachungsanlage zur dauerhaften Sicherung werden von der ZEDAT installiert. |
| 7. | Die Beschilderung der Anlage z.B. "Videoüberwachung" obliegt i.d.R. der Technischen Abteilung. |
| 8. | Die fertig errichtete Anlage wird mittels Übergabeprotokoll von der Technischen Abteilung übergeben. |
| 9. | Die für die Errichtung aktenführende Stelle ist die Technische Abteilung. |
| 10. | Die Mängelbeseitigung im Zuge der Anspruchszeit obliegt dem Antragsteller. |
| Betrieb einer Videoüberwachungsanlage | |
| 11. | Der Betrieb der Videoüberwachungsanlage obliegt der betriebsverantwortlichen Stelle. |
| 12. | Die Speicherung und Sicherung der Daten liegt bei der betriebsverantwortlichen Stelle. |
| 13. | Von einem Dritten beigestellte Anlagen werden vom Antragsteller der Videoanlage betrieben. |
| 14. | Sollen Videoüberwachungsanlagen verändert werden, so ist die Änderung zu dokumentieren und sofort dem IT-Sicherheitsbeauftragten mitzuteilen. |
| 15. | Die für den Betrieb aktenführende Stelle ist die betriebsverantwortliche Stelle. |
| Instandhaltung einer Videoüberwachungsanlage | |
| 16. | Die Wartung der Videoüberwachungsanlage obliegt der betriebsverantwortlichen Stelle. |
| 17. | Die Inspektion der Videoüberwachungsanlage obliegt der betriebsverantwortlichen Stelle. |
| 18. | Die Instandsetzung der Videoüberwachungsanlage obliegt der betriebsverantwortlichen Stelle. |
| 19. | Die Verbesserung (Veränderung) der Videoüberwachungsanlage obliegt der betriebsverantwortlichen Stelle. |
| 20. | Die Demontage der Videoüberwachungsanlage obliegt der Technischen Abteilung. |
| Dokumentation einer Videoüberwachungsanlage | |
| 21. | Die Dokumentation ist dem Antrag beizulegen. |
| 22. | Die Archivierung der Dokumentation obliegt dem IT-Sicherheitsbeauftragten der Freien Universität Berlin. |
| 23. | Das Führen eines Registers zum Einsatz von Videoüberwachungsanlagen obliegt dem IT-Sicherheitsbeauftragten der Freien Universität Berlin. |
| Auswertung und Herausgabe von Videodaten | |
| 24. | Die Verarbeitung der Videodaten erfolgt durch die betriebsverantwortliche Stelle. |
| 25. | Die Herausgabe von Videodaten verantwortet die betriebsverantwortliche Stelle oder das Rechtsamt. |
| 26. | Die Überprüfung der anfragenden Stelle und die Protokollierung der Herausgabe der Daten obliegen der betriebsverantwortlichen Stelle. |

Anlage 5: Auszug Berliner Datenschutzgesetz

§ 20 BlnDSG

Videoüberwachung

- (1) *Die Verarbeitung personenbezogener Daten in öffentlich zugänglichen Räumen mit Hilfe optisch-elektronischer Einrichtungen (Videoüberwachung) ist zulässig, soweit sie zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe oder zur Wahrnehmung des Hausrechts erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der betroffenen Personen überwiegen.*
- (2) *Videoüberwachte Bereiche sind so zu kennzeichnen, dass Personen vor dem Betreten über den Umstand der Videoüberwachung sowie über den Namen und die Kontaktdaten des Verantwortlichen informiert werden.*
- (3) *Eine Verarbeitung zu anderen Zwecken ist nur zulässig, soweit dies zur Abwehr von Gefahren für die öffentliche Sicherheit oder zur Verfolgung von Straftaten erforderlich ist.*
- (4) *Für die Verarbeitung personenbezogener Daten aus öffentlich zugänglichen Räumen des öffentlichen Personenverkehrs gilt abweichend von Absatz 3, dass*
 1. *sie für einen anderen Zweck nur verarbeitet werden dürfen, soweit dies für die Verhütung oder Verfolgung von Straftaten erforderlich ist, und*
 2. *für diesen Zweck ihre Übermittlung ausschließlich an den Polizeipräsidenten in Berlin und an die Strafverfolgungsbehörden zulässig ist.*

Der Verantwortliche hat durch ein mit dem Polizeipräsidenten in Berlin abzustimmendes Sicherheitskonzept zu gewährleisten, dass Aufzeichnungen spätestens nach 48 Stunden gelöscht werden, sofern deren Speicherung nicht für einen der Zwecke des Satzes 1 Nummer 1 erforderlich ist.

- (5) *Unbeschadet der Verpflichtung des Verantwortlichen zur Löschung auf Grund anderer Vorschriften sind nach Absatz 1 erhobene personenbezogene Daten unverzüglich zu löschen, wenn schutzwürdige Interessen der betroffenen Person einer weiteren Speicherung entgegenstehen.*

Berliner Datenschutzgesetz (BlnDSG) – Stand: 13. Juni 2018

<http://gesetze.berlin.de/jportal/portal/t/fin/page/bsbeprod.psml?doc.hl=1&doc.id=jlr-DSGBE2018rahmen&document-number=1&numberofresults=1&doctyp=Norm&showdoccase=1&doc.part=R¶mfromHL=true#focuspoint>