Orientierungshilfe für die Videoüberwachung in und an staatlichen Hochschulen (Stand 08.04.2020)

I.

Grundsätze

1. Staatliche Stellen und privatwirtschaftliche Unternehmen setzen zunehmend Videoanlagen zur Überwachung öffentlicher und nicht-öffentlicher Räume ein, um Straftaten zu verhindern oder mögliche Täter zu ermitteln. Wissenschaftliche Studien belegen allerdings, dass die Videoüberwachung kein Allheilmittel ist, mit dem man überall Sicherheit und Ordnung gewährleisten kann. Vor ihrem Einsatz ist deshalb stets eine sorgfältige Prüfung erforderlich.

2. Die Videoüberwachung lässt sich in technischer Hinsicht auf unterschiedliche Weise realisieren. Von Videobeobachtung in Echtzeit (Monitoring) spricht man, wenn die aufgenommenen Bilder nur auf einen Monitor übertragen werden. Bei dieser Fallkonstellation stellt der Monitor sozusagen ein "verlängertes Auge" des Betrachters dar. Deshalb greift diese Form der Videoüberwachung auch weniger intensiv in die Rechte der Betroffenen ein als dies bei der Speicherung (Videoaufzeichnung) der Bilddaten der Fall ist. Sie ist die andere Variante der Videoüberwachung. Noch eingriffsintensiver ist die zusätzliche Speicherung und Übermittlung von so genannten Audiodaten, also von Tonaufnahmen. Sie ist deshalb grundsätzlich auch nicht erlaubt.

3. Jede Form der Videoüberwachung stellt einen Eingriff in das Persönlichkeitsrecht der davon betroffenen Personen dar. Sie ist deshalb nur zulässig, wenn es dafür eine gesetzliche Grundlage gibt oder die Betroffenen der Videoüberwachung zugestimmt haben. Dies gilt für jede Form der Videoüberwachung.

4. Im Hochschulgesetz selbst gibt es keine Regelungen zur Videoüberwachung. Diese Orientierungshilfe unterstützt die staatlichen Hochschulen bei der Einrichtung einer datenschutzkonformen Videoüberwachung nach der Datenschutz-Grundverordnung (DS-GVO) und dem § 21 Landesdatenschutzgesetz (LDSG), in dem die Videoüberwachung durch öffentliche Stellen explizit geregelt ist.

5. In bestimmten Tabubereichen ist die Videoüberwachung grundsätzlich unzulässig. Das ist immer dort der Fall, wo die Überwachung mit einem Eingriff in die Intimsphäre der Betroffenen verbunden wäre, was regelmäßig bei einer Videoüberwachung vor oder in Umkleide- oder Toilettenräumen der Fall ist.

Zugänge zu Toiletten können ausnahmsweise zur Verhinderung von Gewalt videoüberwacht werden, wenn diese Zugänge nur eingeschränkt einsehbar sind.

Auch Mensen und Cafeterien, die zur Kommunikation mit anderen Personen besucht werden, sollten prinzipiell von Videoüberwachung verschont bleiben.

6. Gegenstand dieser Orientierungshilfe sind nicht die sog. "virtuellen Hörsäle", bei denen Vorlesungen z.B. in einen anderen Hörsaal übertragen werden. Gleichwohl sollte hier nur die/der Dozent/in von der Kamera erfasst werden. Falls auch Studierende ins Blickfeld geraten, sollte darauf hingewiesen und dies auf die vorderen Sitzreihen beschränkt werden. Werden von einzelnen Veranstaltungen Aufzeichnungen beispielsweise zur wissenschaftlichen Dokumentation angefertigt, ist dies nur möglich mit Einwilligung der Teilnehmer/Innen nach vorheriger Information.

II.

Rechtliche Grundlagen

1. Als gesetzliche Grundlage kommt § 21 LDSG in Betracht. Danach ist eine Verarbeitung personenbezogener Daten mit Hilfe von optisch-elektronischen Einrichtungen (Videoüberwachung) zulässig, wenn dies

a. zur Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt,

b. zur Wahrnehmung des Hausrechts oder

c. sonst zum Schutz des Eigentums oder Besitzes oder zur Kontrolle von Zugangsberechtigungen

erforderlich ist und keine Anhaltspunkte bestehen, dass überwiegende schutzwürdige Interessen der betroffenen Personen entgegenstehen.

Eine Videoüberwachung mit Hilfe optisch-elektronischer Einrichtungen liegt vor, wenn personenbezogene Daten verarbeitet werden. Einzelne Personen müssen demnach auf den Videoaufnahmen erkennbar sein oder die Aufnahmen müssen Rückschlüsse auf deren Identität zulassen.

- Wahrnehmung einer Aufgabe im öffentlichen Interesse

  Aufgaben im öffentlichen Interesse sind Tätigkeiten öffentlicher Stellen - hier von Hochschulen -, die ihnen durch Rechtsverordnung übertragen sind.

- oder in Ausübung öffentlicher Gewalt

  alle Akte der Exekutive durch öffentliche Stellen

- zur Wahrnehmung des Hausrechts

  Das Hausrecht umfasst ein Verweisen von Personen aus einem bestimmten Raum sowie die zukünftige Untersagung des Betretens durch den Inhaber des Hausrechts. Dieser ist befugt, präventive und repressive Maßnahmen zu treffen, die zum Schutz des Objekts oder vor unbefugtem Betreten erforderlich sind.

- zum Schutz des Eigentums oder Besitzes oder zur Kontrolle von Zugangsberechtigungen

  Der Schutz des Eigentums oder Besitzes umfasst die Einwirkung auf das zu schützende Objekt von innen und außen sowie mobiler Gegenstände innerhalb des Objekts. Die Kontrolle von Zugangsberechtigungen beinhaltet z. B. die Nutzung von Parkplätzen oder den Zugang in das Objekt durch die Studierenden, Lehrenden und Beschäftigten.

Eine Unterscheidung in der Rechtsgrundlage zwischen Monitoring und Aufzeichnung gibt es nicht mehr (anders noch § 34 LDSG alt).

2. Eine Videoüberwachung nicht öffentlich zugänglicher Räume (z.B. Institutslabore, Server-Räume) in einer Hochschule richtet sich ausweislich der Gesetzesbegründung zum LDSG n.F. (Drs. 17/5703) nicht nach § 21 LDSG. Nicht öffentlich zugängliche Räume können oder dürfen nur von einem bestimmten und abschließend definierten Personenkreis betreten werden. Hier genügt es, wenn die allgemeinen Voraussetzungen für die Verarbeitung personenbezogener Daten nach § 3 LDSG eingehalten werden.

3. Als Eingriff in das allgemeine Persönlichkeitsrecht muss die Videoüberwachung immer zur Zweckerreichung geeignet, erforderlich und verhältnismäßig sein.

a. Der Grundsatz der Erforderlichkeit orientiert sich dabei an der Häufigkeit und Schwere der Vorfälle (sog. Gefährdungsprognose) und der Prüfung, ob ein milderes Mittel alternativ zum Einsatz kommen kann.

Eine für eine zulässige Videoaufzeichnung zu berücksichtigende Gefahr kann immer dann vorliegen, wenn Vorkommnisse in der Vergangenheit die Annahme rechtfertigen, dass auch künftig schwerwiegende Beeinträchtigungen der Interessen und Schutzgüter der Studierenden und der Hochschule drohen. Dabei kann es um die Sicherheit der Studierenden, der Lehrenden sowie der Beschäftigten gehen, aber auch um die Unversehrtheit von Hochschuleigentum. Sachbeschädigungen, Diebstähle und Einbrüche können daher eine Videoaufzeichnung - jedenfalls prinzipiell - ebenso rechtfertigen, wie Körperverletzungen oder sonstige Delikte gegen die körperliche Integrität der genannten Personen.

Es kann aber auch ausreichen, wenn einer nach allgemeiner Lebenserfahrung vorliegenden abstrakten Gefährdungslage nur durch den Einsatz einer Videoüberwachung wirksam begegnet werden kann.

b. Die Videoüberwachung muss außerdem auch verhältnismäßig sein. Dies ist nicht der Fall, wenn der Hochschule Mittel zur Verfügung stehen, die weniger eingriffsintensiv sind als die Videoüberwachung. Eine solche Alternative besteht in der Regel während laufender Kurs-, Seminar- oder Fortbildungsveranstaltungen, weil die soziale Kontrolle durch die Referenten, Studierenden oder Beschäftigten so hoch ist, dass es nicht zu Straftaten kommen dürfte. Mit anderen Worten: Videoüberwachung ist dann grundsätzlich unzulässig.

Als weitere mildere Mittel zum Schutz des Eigentums kommt die Sicherung von DV-Geräten gegen Gelegenheitsdiebstähle mittels Laptop-Sicherungskabeln oder Schlössern in Betracht. Gegebenenfalls kann auch die Beobachtung der Eingangstür zu einem PC-Pool genügen, um Diebstähle zu vermeiden bzw. aufzuklären. Bildschirminhalte der Arbeitsplätze in PC-Pools dürfen auf keinen Fall von der Überwachungsanlage erfasst werden. In Außenbereichen kann die Sicherheit gegebenenfalls durch den Einsatz geeigneter Beleuchtung mit Bewegungsmeldern erhöht werden.

c. Eine bloße Bildübermittlung zur unmittelbaren Betrachtung auf Monitoren ("verlängertes Auge") greift weniger intensiv in die Rechte Betroffener ein als die Speicherung solcher Bilddaten. Monitoring ist aber nur dann zweckmäßig und somit verhältnismäßig, wenn auch tatsächlich eine simultane Beobachtung der übertragenen Daten erfolgt. Zudem muss sichergestellt sein, dass bei einer für ein Rechtsgut auftretenden Gefahr von der beobachtenden Stelle ohne Verzögerung Schutzmaßnahmen eingeleitet werden können. Wurde die Videoüberwachung z.B. anlässlich eines tätlichen Übergriffes auf eine Studentin bzw. einen Studenten auf dem Campus eingerichtet, um solche Vorfälle zu vermeiden bzw. direkt eingreifen zu können, wäre die Maßnahme zur Erfüllung des Zwecks nicht geeignet und deshalb unzulässig, wenn eine Beobachtung nur zeitweise sichergestellt wäre. Ansonsten kann die Videoüberwachung den unerwünschten Effekt haben, dass auf anonyme Hilfe vertraut wird und in Gefahrensituationen Anwesende nicht selbstständig helfend intervenieren.

Das reine Monitoring von Schrankenanlagen an Zutritts-/Zufahrtsbereichen kann dann weitgehend unproblematisch gehandhabt werden, wenn die Beobachtung eng auf den jeweiligen Bereich beschränkt wird und keine sonstigen, insbesondere keine dem öffentlichen Verkehr gewidmeten Flächen außerhalb des Campus erfasst werden. Die dabei zum Einsatz kommenden Kameras sollten über keine Zoom- oder Schwenkfunktionen verfügen.

d. Weiterhin dürfen auch keine Hinweise dafür vorliegen, dass schutzwürdige Interessen der von einer Überwachungsmaßnahme betroffenen Personen die Interessen beispielsweise des Inhabers des Hausrechts überwiegen. Die Überwachung sensibler Bereiche im Sinne der Ziffer I.5 ist daher grundsätzlich ausgeschlossen.

4. In Bezug auf die systematische Überwachung kann die Einwilligung der betroffenen Person nur in Ausnahmefällen als Rechtsgrundlage dienen. Es liegt in der Natur der Überwachung, dass diese Technologie eine unbekannte Anzahl von Personen gleichzeitig überwacht. Der für die Verarbeitung Verantwortliche kann kaum nachweisen, dass die betroffene Person vor der Verarbeitung ihrer personenbezogenen Daten ihre Einwilligung erteilt hat. Unter der Annahme, dass die betroffene Person ihre Einwilligung widerruft, kann der für die Verarbeitung Verantwortliche nur schwer nachweisen, dass personenbezogene Daten nicht mehr verarbeitet werden (so auch Guidelines 3/2019 on processing of personal data through video devices, European Data Protection Board).

5. Für die Videoaufzeichnung ist gem. § 21 Abs. 6 LDSG eine Datenschutz-Folgenabschätzung durchzuführen und die Datenverarbeitung in ein Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DS-GVO) aufzunehmen.

III.

Hinweis- und Informationspflichten

1. Die formellen Vorgaben der Datenschutz-Grundverordnung sind zu beachten. Dies gilt insbesondere für die Hinweis- und Informationspflichten (Art. 12, 13 DS-GVO), die Betroffenenrechte (Art. 15 ff DS-GVO) und die Dokumentationspflichten (Art. 5 Abs. 2 DS-GVO).

2. § 21 Abs. 2 LDSG verlangt, dass auf die Umstände der Videoüberwachung sowie den Verantwortlichen (z.B. Hochschule, Studierendenwerk, Gebäudeeigentümer, selbständiges Forschungsinstitut) hingewiesen wird. Dies geschieht in der Regel durch entsprechende Piktogramme oder Hinweisschilder. Entsprechende Muster für Hinweisschilder nach Art. 13 DS-GVO befinden sich auf der Homepage des LfDI unter

https://www.datenschutz.rlp.de/de/themenfelder-themen/videoueberwachung/videoueberwachung-von-haus-und-grund/

Sie sind so anzubringen, dass sie vor dem Betreten des überwachten Bereichs mühelos (z.B. an der Eingangstür zum PC-Pool) wahrgenommen werden können. Ist die Überwachungsanlage nur während einer bestimmten Tageszeit in Betrieb, so ist auch darauf hinzuweisen.

IV.

Die Behandlung aufgezeichneter Daten

1. Ist die Videoüberwachung mit einer Aufzeichnung und Speicherung der aufgenommenen Daten verbunden, müssen diese Daten spätestens nach zwei Monaten gelöscht oder vernichtet werden, soweit diese nicht zur Verfolgung von Straftaten, zur Geltendmachung von Rechtsansprüchen oder wegen entgegenstehender schutzwürdiger Interessen betroffener Personen, insbesondere zur Behebung einer bestehenden Beweisnot, erforderlich sind (vgl. § 21 Abs. 5 LDSG) Ob eine Sicherung des Materials notwendig ist, dürfte grundsätzlich innerhalb von ein bis zwei Tagen geklärt werden können. Unter Berücksichtigung von Art. 5 Abs. 1 lit. c und e DSGVO – „Datenminimierung“ und „Speicherbegrenzung“ – sollte demnach grundsätzlich, wie bisher auch, nach 48-72 Stunden eine Löschung erfolgen, es sei denn, durch Feiertage werden längere Speicherzeiten notwendig. Über diesen Zeitraum hinaus können natürlich die Sequenzen gespeichert werden, die für polizeiliche Ermittlungen, zur Geltendmachung von Rechtsansprüchen oder wegen entgegenstehender schutzwürdiger Interessen betroffener Personen bei entsprechenden Vorfällen benötigt werden.

2. Es empfiehlt sich, die Aufzeichnungen zu verschlüsseln. Dies hat zur Folge, dass die aufgezeichneten Videodaten nur von einer bestimmten Person entschlüsselt und ausgewertet werden können. Nach Möglichkeit sollte das Schlüsselpasswort auf mehrere Personen aufgeteilt werden, so dass der Zugriff auf die Aufzeichnungen immer nach dem "Vier-Augen-Prinzip" erfolgen muss.

3. Solange die Videoaufnahmen zulässigerweise gespeichert sind, dürfen nur besonders legitimierte Personen Zugriff auf diese Daten nehmen. Dieser Personenkreis ist ausdrücklich festzulegen. Er kann variieren, je nachdem, wer für die Videoüberwachung verantwortlich ist. In jedem Falle müssen die zugriffsberechtigten Personen dem Anlass entsprechend Verantwortungsträger sein. Es sollte nur ein möglichst kleiner Personenkreis zugriffsberechtigt sein.

4. Die Weitergabe von Videoaufzeichnungen darf nur im Rahmen der mit der Videoüberwachung unmittelbar verfolgten Zwecke an Polizei, Staatsanwaltschaft oder Gerichte erfolgen. Ein polizeilicher Zugriff aus anderen Gründen ist nur auf der Grundlage gesetzlicher Befugnisse erlaubt.

5. Jeder Zugriff und jede Auswertung sind zu dokumentieren. Auf diese Weise kann auch geprüft und nachvollzogen werden, ob die Überwachungsanlage nach Ablauf einer bestimmten Frist noch erforderlich ist.

V.

Dienstanweisung

Alle mit einer Videoüberwachung zusammenhängenden Fragen und Probleme sind in einer allgemeinen Dienstanweisung der Hochschule unter Beteiligung der/des behördlichen Datenschutzbeauftragten zu regeln. Das gilt u.a. für den Zweck der Videoüberwachung und die zulässige Dauer der Videospeicherung, für den Kreis der zugriffsberechtigten Personen und die für eine Weitergabe in Betracht kommenden Anlässe. Auch die Notwendigkeit einer Dokumentation der Zugriffe ist festzulegen. Ggf. ist eine technisch mögliche Nutzung von Schwenk- oder Zoomfunktion zu untersagen. Die Muster des LfDI für eine allgemeine Dienstanweisung und eine Einzelfallanweisung im kommunalen Bereich können entsprechend verwendet werden.

VI.

Institutionelle Beteiligungen

1. Die von einer geplanten Überwachungsmaßnahme betroffenen Studierenden sind durch ihre Vertreter frühzeitig zu hören.

2. Die behördlichen Datenschutzbeauftragten sind gemäß Art. 38 DS-GVO ebenfalls rechtzeitig über geplante Videoüberwachungen zu unterrichten, damit sie auf die Einhaltung der vorstehenden Grundsätze hinwirken können.

3. Die zuständigen Personalräte sind entsprechend den Bestimmungen des Landespersonalvertretungsgesetzes zu beteiligen. In der Dienstanweisung oder einer entsprechenden Dienstvereinbarung (vgl. VI.) sollte eine ausdrückliche Erklärung enthalten sein, dass die mit der Überwachungsmaßnahme aufgezeichneten Daten nicht zu Verhaltens- und Leistungskontrollen der Beschäftigten genutzt werden dürfen.

VII.

Evaluation

Nach Ablauf eines Jahres ist zu überprüfen, ob der Grund für eine zulässige Videoüberwachung noch fortbesteht. Zu diesem Zweck ist eine Evaluation durchzuführen. Liegen keine Anhaltspunkte

für eine Gefährdung der Interessen und Schutzgüter mehr vor, ist die Maßnahme zu beenden. Die Anlagen müssen in diesem Fall nicht zwangsläufig entfernt werden. Es genügt, wenn sie gut erkennbar verhüllt sind oder i. S. v. § 21 Abs. 2 LDSG darauf hingewiesen wird, dass keine Verarbeitung personenbezogener Daten erfolgt. Liegt der Grund für eine Videoüberwachung allerdings noch vor, ist die Überprüfung regelmäßig einmal jährlich zu wiederholen.

VIII.

Kamera-Attrappen

Der Einsatz von Kamera-Attrappen ist unter den gleichen Voraussetzungen wie eine Videoüberwachung nach § 21 Abs. 1 u. 2 LDSG zulässig (vgl. § 21 Abs. 7 LDSG). Für die Kenntlichmachung gelten dieselben Anforderungen wie dies beim Einsatz funktionstüchtiger Kameras der Fall ist.