



Multimedia Kontor
Hamburg

Ausfüllhilfe

für das MMKH-Muster

„Vorgelagertes Hinweisschild bei Videoüberwachung“

Erklärungen, Beispiele und Hinweise zum Ausfüllen des *MMKH-Musters für das vorgelagerte Hinweisschild bei Videoüberwachung*.

Multimedia Kontor Hamburg gGmbH (MMKH)
Version 1.0 | Juli 2026

Hinweis

Diese Ausfüllhilfe ersetzt keine rechtliche Beratung im Einzelfall. Stand: Juli 2026.



Ein Unternehmen der
Hamburger Hochschulen

1. Einleitung

Diese Ausfüllhilfe erläutert, wie das MMKH-Muster für das vorgelagerte Hinweisschild bei einer möglichen Videoüberwachung an Hamburger Hochschulen korrekt ausgefüllt und angebracht werden kann. Sie richtet sich an Datenschutzkoordinatorinnen und -koordinatoren sowie Datenschutzbeauftragte der Hochschulen und dient als ausführliche Ergänzung zum MMKH-Muster „Vorgelagertes Hinweisschild bei Videoüberwachung“, das den Hamburger Hochschulen über die Infothek unter hh-datenschutz.de bereitgestellt wird.

Das Muster enthält bereits kurze Erläuterungen zu den einzelnen Feldern. Diese Ausfüllhilfe vertieft die Hintergründe, bietet zusätzliche Beispielszenarien aus dem Hochschulkontext und erläutert die rechtlichen Zusammenhänge.

Was ist ein vorgelagertes Hinweisschild?

Art. 13 DSGVO verlangt bei jeder Erhebung personenbezogener Daten eine Vielzahl von Angaben — vom Verantwortlichen über die Rechtsgrundlage bis hin zu den Betroffenenrechten, die den Betroffenen transparent zur Verfügung gestellt werden. All das auf einem einzelnen Schild (oder Dokument) unterzubringen, ist weder praktikabel noch im Sinne der Transparenz. Das vorgelagerte Hinweisschild löst das, indem es die Pflichtangaben auf zwei Stufen verteilt:¹

- **Stufe 1 (Hinweisschild):** Die notwendigen Kernangaben auf dem physischen Schild — kompakt und auf einen Blick erfassbar.
- **Stufe 2 (Separate Datenschutzinformation):** Vollständige Informationen gemäß Art. 13 Abs. 1 und 2 DSGVO, erreichbar über einen QR-Code, einen Link oder als physischen Aushang.

Achtung

Das bloße Betreten des videoüberwachten Bereichs nach Kenntnisnahme des Schildes stellt ausdrücklich keine datenschutzrechtliche Einwilligung dar.² Die Rechtfertigung für die Verarbeitung ergibt sich ausschließlich aus der auf dem Schild dargestellten Rechtsgrundlage.

Darstellung des gestuften Informationsmodells

Zwei Darstellungen veranschaulichen das Stufenmodell:

¹Dieses Vorgehen wird in offiziellen Handreichungen auch als „layered approach“ oder „gestuftes Informationsmodell“ bezeichnet — so der Europäische Datenschutzausschuss (EDSA/EDPB) in den Guidelines 3/2019 on processing of personal data through video devices (unter Verweis auf WP260 rev.01). In der deutschen Praxis ist auch von „Medienbruch“ die Rede, wenn die Stufen tatsächlich auf verschiedene Medien verteilt werden (z. B. physisches Schild und digitale Webseite) — das ist jedoch nur eine mögliche Umsetzungsform des Stufenmodells. Die DSK hat das Modell in ihrer Orientierungshilfe Videoüberwachung (Juli 2020) für nicht-öffentliche Stellen übernommen; für öffentliche Stellen ist das Stufenmodell unstreitig ebenfalls anwendbar. Die Zulässigkeit der gestuften Informationserteilung wird von den Aufsichtsbehörden in der Regel bejaht.

²Vgl. Art. 4 Nr. 11, Art. 7 DSGVO. Das Betreten ist keine „eindeutig bestätigende Handlung“ im Sinne der DSGVO.



Gestuftes Informationsmodell (Layered Approach)

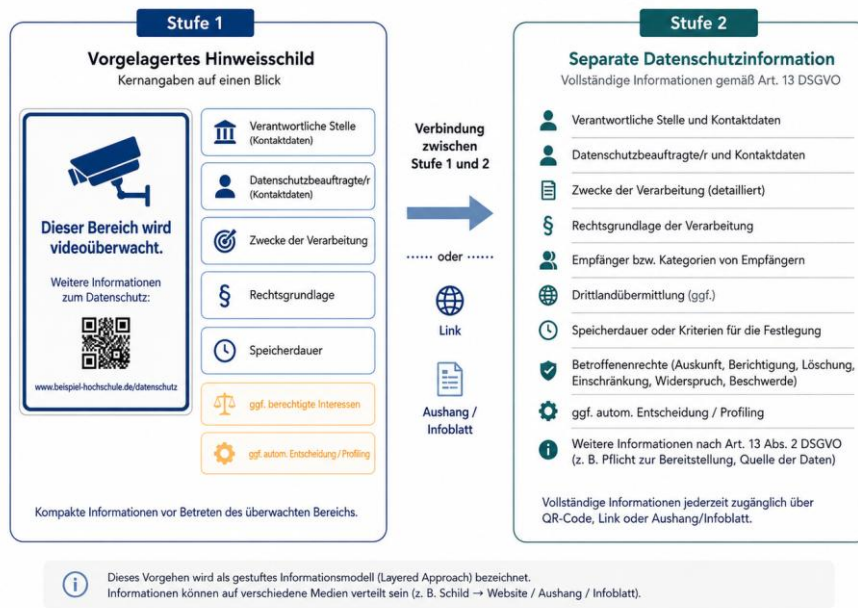


Abb. 1a: Gestuftes Informationsmodell als farbiges Strukturdiagramm.



Abb. 1b: Erweiterte Illustration mit ausgefülltem Schild, Smartphone und physischem Infoblatt. Das Infoblatt muss nicht als gedrucktes Blatt bereitliegen — die vollständige Information (Stufe 2) kann auch über eine Webseite bereitgestellt werden; ein zusätzlicher analoger Zugang wird empfohlen (siehe Abschnitt 4.7).

2. Pflichtangaben auf dem Hinweisschild (Stufe 1)

Art. 13 DSGVO verlangt bei jeder Erhebung personenbezogener Daten bestimmte Informationen. Auf dem vorgelagerten Hinweisschild (Stufe 1) sind folgende Kernangaben zu machen:

- Piktogramm / Umstand der Beobachtung — erfüllt durch ein eindeutiges Kamerasymbol
- Identität des Verantwortlichen (Name und Kontaktdaten)
- Kontaktdaten des Datenschutzbeauftragten (sofern benannt, dann zwingend)
- Zwecke und Rechtsgrundlage der Verarbeitung
- Speicherdauer
- Hinweis auf Zugang zu den weiteren Pflichtinformationen (Link, QR-Code)

Hinweis: Art. 13 Abs. 1 lit. d DSGVO verlangt zusätzlich die Angabe der berechtigten Interessen, wenn sich die Verarbeitung auf Art. 6 Abs. 1 lit. f DSGVO stützt. Für Hamburger Hochschulen als öffentliche Stellen ist dieser Punkt in der Regel nicht einschlägig, da die Rechtsgrundlage hier Art. 6 Abs. 1 lit. e DSGVO i. V. m. § 9 HmbDSG ist (siehe Abschnitt 4.4).

Alle übrigen Informationen nach Art. 13 Abs. 1 und 2 DSGVO — insbesondere die Betroffenenrechte, Empfänger und ggf. Angaben zu Drittlandübermittlungen — gehören in die vollständige Datenschutzinformation (Stufe 2). Siehe dazu Abschnitt 5 dieser Ausfüllhilfe.

Beispiel für ein vollständig ausgefülltes Hinweisschild

Das folgende Beispiel zeigt, wie ein Hinweisschild mit allen Pflichtangaben konkret aussehen kann. Das gezeigte Beispiel bezieht sich auf das Szenario „Bibliothek / Schutz vor Diebstahl“:

 Dieser Bereich wird videüberwacht. Weitere Informationen zum Datenschutz:  Kontaktdaten der/des Verantwortlichen: Beispiel-Hochschule Musterstraße 1 20095 Hamburg E-Mail: info@beispiel-hochschule.de Die Beispiel-Hochschule ist eine Körperschaft des öffentlichen Rechts. Sie wird gesetzlich vertreten durch den/die Präsident/in der Beispiel-Hochschule. Kontaktdaten des/der Datenschutzbeauftragten: Datenschutzbeauftragte/r der Beispiel-Hochschule Musterstraße 1 20095 Hamburg E-Mail: datenschutz@beispiel-hochschule.de	 Zwecke der Datenverarbeitung: • Schutz von Eigentum und Personen • Durchsetzung des Hausrechts • Aufklärung entsprechender Vorfälle und Beweissicherung im Anlassfall  Rechtsgrundlage: Art. 6 Abs. 1 lit. e DSGVO i. V. m. § 9 Abs. 1 und Abs. 2 HmbDSG  Speicherdauer: Die Aufnahmen werden grundsätzlich 72 Stunden gespeichert. Anschließend werden sie automatisch gelöscht, sofern keine längere Speicherung im Einzelfall zur Beweissicherung erforderlich ist.  Weitere Hinweise: Alle weiteren Informationen, insbesondere zu Ihren Rechten als betroffene Person, erhalten Sie über den QR-Code oder den oben genannten Link.
--	---

Abb. 2: Beispiel für ein vollständig ausgefülltes Hinweisschild (hier: Szenario Bibliothek / Diebstahlschutz).

3. Typische Fehler in der Praxis

Bei der Umsetzung der Informationspflichten zur Videoüberwachung kommen in der Praxis immer wieder dieselben Fehler vor — sowohl auf dem vorgelagerten Hinweisschild (Stufe 1) als auch in der verlinkten, vollständigen Datenschutzinformation (Stufe 2). Die folgende Zusammenstellung hilft, sie zu vermeiden.

Unvollständige oder zu pauschale Zweckangaben

Ein besonders häufiger Fehler ist eine zu pauschale Zweckangabe wie „Sicherheit“, „Hausrecht“ oder „Zum Schutz unseres Eigentums“ (siehe Abb. 3). Die Zwecke müssen konkret und auf den jeweiligen Kamerastandort bezogen formuliert werden. Auch Angaben wie „for your safety“ reichen als Zweckbestimmung nicht aus. Das folgende Beispiel verdeutlicht den Unterschied:

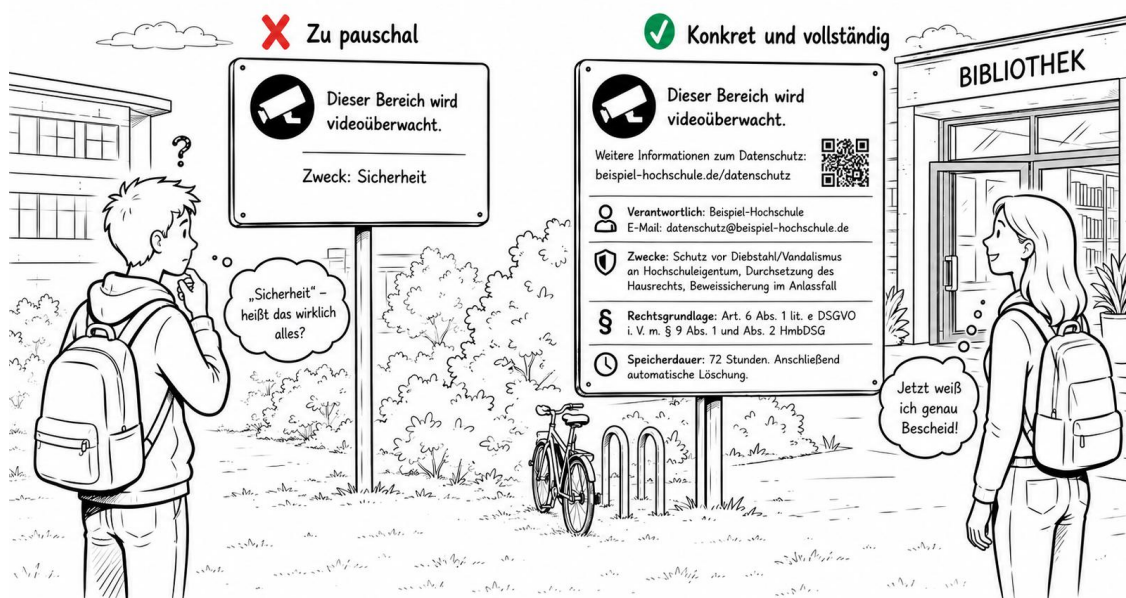


Abb. 3: Unzureichendes vs. vollständiges Hinweisschild.

Fehlendes Piktogramm

Ein reines Textschild ohne Piktogramm oder Kamerasymbol ist problematisch, weil es die Videoüberwachung nicht auf einen Blick erkennbar macht. Das Piktogramm ist zwar nicht zwingend vorgeschrieben (eine konkrete Norm verlangt kein bestimmtes Symbol), entspricht aber dem Gebot der transparenten und leicht zugänglichen Information nach Art. 12 Abs. 1 DSGVO und ist gute fachliche Praxis.

Nur Piktogramm ohne Pflichtangaben

Der umgekehrte Fehler ist ebenso verbreitet: Ein Schild zeigt lediglich ein Kamerasymbol, ohne die in Art. 13 DSGVO geforderten Pflichtangaben zu nennen (Verantwortlicher, Zweck, Rechtsgrundlage, Speicherdauer, Verweis auf Stufe 2). Ein solches Schild erfüllt die Informationspflicht nicht. Das Piktogramm ist eine Ergänzung, kein Ersatz für die Pflichtangaben.

Falsche Platzierung des Schildes

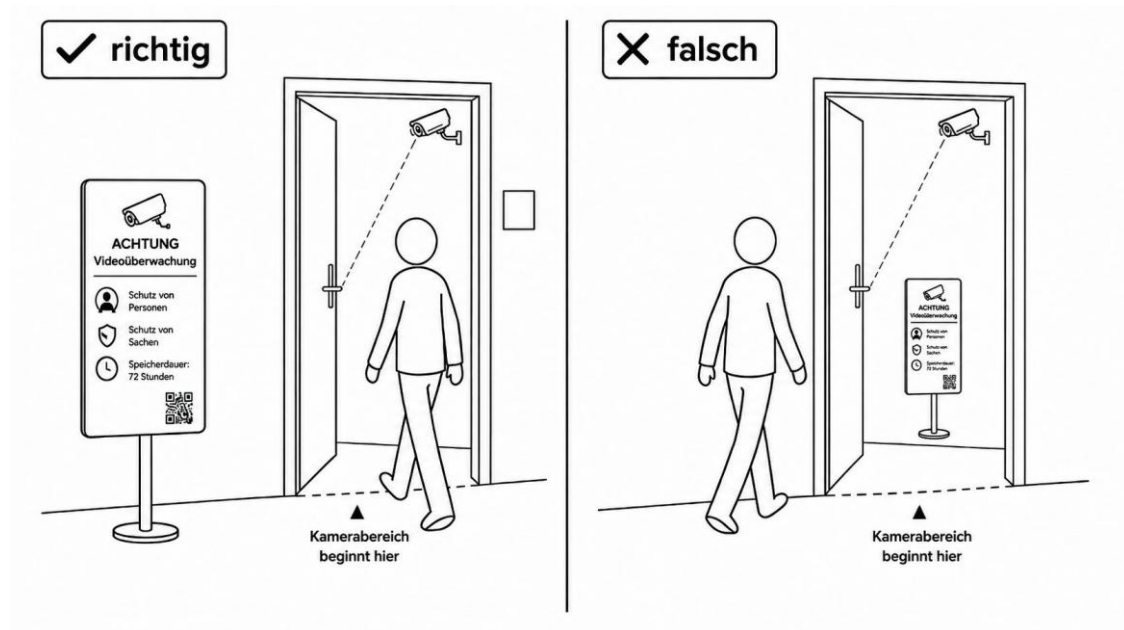
Ein Schild, das erst im bereits überwachten Bereich sichtbar wird, verletzt Art. 13 DSGVO und § 9 Abs. 3 HmbDSG (Kennzeichnung zum frühestmöglichen Zeitpunkt). Das Hinweisschild muss so platziert werden, dass betroffene Personen die Information zur Kenntnis nehmen können, bevor sie den von der Kamera erfassten Bereich betreten (siehe Abb. 4). Es muss so angebracht sein, dass es nicht übersehen werden kann — auf Augenhöhe, gut lesbar und in ausreichender Größe.

i Hinweis

Das bloße Betreten des Bereichs nach Kenntnisnahme des Schildes ist keine datenschutzrechtliche Einwilligung. Das Schild dient ausschließlich der Erfüllung der Informationspflicht, nicht der Rechtfertigung der Verarbeitung.

Bei mehreren Zugängen zum überwachten Bereich ist an jedem Zugang ein Schild anzubringen (vgl. § 9 Abs. 3 HmbDSG — die Kennzeichnung hat zum frühestmöglichen Zeitpunkt durch geeignete Maßnahmen zu erfolgen).

Abb. 4: Richtige vs. falsche Platzierung des Hinweisschildes



Fehlender oder nicht funktionierender Zugang zu weiteren Informationen

Wenn ein QR-Code, Link oder sonstiger Verweis auf die vollständige Datenschutzinformation fehlt, zum Abrufzeitpunkt ins Leere führt, auf die allgemeine Startseite der Hochschule verweist oder eine veraltete Seite anzeigt, ist die Informationspflicht nach Art. 13 DSGVO nicht erfüllt. Der Verweis muss regelmäßig überprüft werden und direkt zur vollständigen Datenschutzinformation führen.

Falsche Rechtsgrundlage

Häufig wird als Rechtsgrundlage Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse) angegeben — das ist für Hamburger Hochschulen als öffentliche Stellen regelmäßig falsch (siehe Abschnitt 4.4). Ebenso wenig taugt die Einwilligung (Art. 6 Abs. 1 lit. a DSGVO), da das bloße Betreten des überwachten Bereichs keine wirksame Einwilligung im Sinne des Art. 4 Nr. 11 DSGVO darstellt.

Zu lange Speicherdauer ohne Begründung

Speicherfristen von mehreren Wochen oder gar Monaten ohne dokumentierte Begründung sind ein häufiger Beanstandungspunkt der Aufsichtsbehörden. Als praxistaugliche Obergrenze gelten 72 Stunden; längere Fristen erfordern eine konkrete, fallbezogene Begründung (siehe Abschnitt 4.5).

Fehlender gesonderter Widerspruchsrechts-Hinweis auf Stufe 2

Bei Verarbeitung auf Grundlage von Art. 6 Abs. 1 lit. e DSGVO (der Standardfall für Hochschulen) verlangt Art. 21 Abs. 4 DSGVO, dass die betroffene Person auf das Widerspruchsrecht ausdrücklich und in einer von anderen Informationen getrennten Form hingewiesen wird. Dieser gesonderte Hinweis fehlt in der Praxis häufig auf der verlinkten Datenschutzhinweise (Stufe 2).

4. Erläuterungen zu den einzelnen Feldern des Musters

4.1 Piktogramm / Umstand der Beobachtung

Das Piktogramm auf dem Hinweisschild dient dazu, den Umstand der Videoüberwachung auf einen Blick erkennbar zu machen — noch bevor der Text gelesen wird.

Die MMKH-Mustervorlage stellt ein eigenes Piktogramm bereit. Dieses kann verwendet oder durch ein hochschuleigenes Symbol ersetzt werden. Eine Verpflichtung zur Verwendung eines bestimmten Piktogramms besteht nicht. Insbesondere ist die DIN 33450 in Deutschland grundsätzlich freiwillig — DIN-Normen werden erst bindend, wenn ein Gesetz, eine Verordnung oder ein Vertrag ausdrücklich auf sie verweist. Die DSGVO verlangt transparente Informationen nach Art. 13, schreibt aber kein bestimmtes Bildsymbol vor.

4.2 Name und Kontaktdaten des Verantwortlichen

Anzugeben sind der vollständige Name und die Kontaktdaten (postalische Anschrift, E-Mail-Adresse) der verantwortlichen Stelle. Bei Hochschulen als Körperschaften des öffentlichen Rechts ist die gesetzliche Vertretung durch den/die Präsident/in anzugeben.

Beispiel: *Hochschule für Angewandte Wissenschaften Hamburg, Berliner Tor 5, 20099 Hamburg, E-Mail: info@haw-hamburg.de. Die HAW Hamburg ist eine Körperschaft des öffentlichen Rechts. Sie wird gesetzlich vertreten durch den Präsidenten der HAW Hamburg.*

4.3 Kontaktdaten des Datenschutzbeauftragten

Sofern ein Datenschutzbeauftragter benannt ist — was bei Hochschulen als öffentlichen Stellen regelmäßig der Fall ist —, sind dessen Kontaktdaten zwingend auf dem Hinweisschild anzugeben (Art. 13 Abs. 1 lit. b DSGVO). Mindestens eine E-Mail-Adresse ist erforderlich; Name und postalische Anschrift sind empfehlenswert.

4.4 Zwecke und Rechtsgrundlage der Verarbeitung

Rechtsgrundlage für Hamburger Hochschulen

Hamburger Hochschulen sind Körperschaften des öffentlichen Rechts. Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse) kommt daher als Rechtsgrundlage grundsätzlich nicht in Betracht — Art. 6 Abs. 1 UAbs. 2 DSGVO schließt die Anwendung für Verarbeitungen durch Behörden in Erfüllung ihrer Aufgaben ausdrücklich aus.³

³Vgl. auch ErwGr. 47 DSGVO: „Da es dem Gesetzgeber obliegt, per Rechtsvorschrift die Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch die Behörden zu schaffen, sollte diese Rechtsgrundlage nicht für Verarbeitungen durch Behörden gelten, die diese in Erfüllung ihrer Aufgaben vornehmen.“ Es gibt begrenzte Ausnahmen: Wenn die Hochschule in einem rein privatrechtlichen Kontext handelt — also nicht in Erfüllung einer öffentlichen Aufgabe, sondern z. B. beim Betrieb eines kommerziellen Cafés durch eine Tochter-GmbH —, könnte Art. 6 Abs. 1 lit. f DSGVO anwendbar sein. Die Abgrenzung hängt von der Art der Tätigkeit ab, nicht vom Status der Institution. Für private Hochschulen als nicht-öffentliche Stellen ist die Anwendbarkeit von Art. 6 Abs. 1 lit. f DSGVO grundsätzlich nicht verschlossen. Solche Fälle sind individuell zu prüfen.



Auch auf eine Einwilligung lässt sich die Videoüberwachung nicht stützen. Das bloße Betreten des überwachten Bereichs nach Kenntnisnahme des Schildes ist keine „eindeutig bestätigende Handlung“ im Sinne des Art. 4 Nr. 11 DSGVO und damit keine wirksame Einwilligung.

Die einschlägige Rechtsgrundlage ist **Art. 6 Abs. 1 lit. e DSGVO** (Wahrnehmung einer Aufgabe im öffentlichen Interesse) **in Verbindung mit § 9 HmbDSG**, der die Videoüberwachung für Hamburger Behörden konkretisiert. Die Videoüberwachung ist danach nur zulässig, wenn:

- sie zur Erfüllung der rechtmäßig übertragenen Aufgaben der Hochschule erforderlich ist oder zur Wahrnehmung des Hausrechts (beide Alternativen sind eigenständig),
- keine mildereren Mittel verfügbar sind (z. B. Alarmanlagen, Zutrittskontrollen, bessere Beleuchtung), und
- schutzwürdige Interessen der Betroffenen nicht überwiegen.

Dies erfordert eine vorab durchgeführte Risikoanalyse, in der das Bedrohungspotential dokumentiert wird — etwa durch vergangene Vorfälle wie Diebstähle oder Vandalismus.

Hausrecht als eigenständige Grundlage

§ 9 Abs. 1 Satz 1 HmbDSG nennt zwei gleichrangige Alternativen: die Aufgabenerfüllung öffentlicher Stellen oder die Wahrnehmung des Hausrechts. In vielen Fällen ist das Hausrecht die einfachere und tragfähigere Begründung — insbesondere, wenn es um den Schutz vor unbefugtem Zutritt, Sachbeschädigungen oder Störungen des Hochschulbetriebs geht. Für Hamburger Hochschulen ergibt sich das Hausrecht aus § 81 Abs. 4 HmbHG (Zuweisung an den Präsidenten/die Präsidentin). Es empfiehlt sich, in der Zweckdokumentation sowohl die Aufgabenerfüllung als auch das Hausrecht zu prüfen und diejenige Alternative heranzuziehen, die am besten zum konkreten Überwachungszweck passt — häufig sind auch beide parallel einschlägig.

Videobeobachtung und Videoaufzeichnung — zwei getrennte Prüfungen

§ 9 HmbDSG unterscheidet terminologisch und dogmatisch klar zwischen zwei Vorgängen: § 9 Abs. 1 HmbDSG regelt die Videobeobachtung — also die reine Live-Übertragung des Kamerabildes ohne Speicherung. § 9 Abs. 2 HmbDSG regelt die Videoaufzeichnung — also die Speicherung und weitere Verwendung der erhobenen Daten. Beide Vorgänge benötigen eine jeweils eigenständige Erforderlichkeitsprüfung: Auch wenn eine Videobeobachtung nach Abs. 1 zulässig ist, folgt daraus nicht automatisch, dass auch eine Aufzeichnung nach Abs. 2 zulässig wäre. Dies hat unmittelbare Konsequenzen für die Praxis: Reine Live-Beobachtung ist regelmäßig weniger eingriffsintensiv und leichter zu rechtfertigen als eine Aufzeichnung. Wo immer möglich, sollte daher zuerst geprüft werden, ob die Live-Beobachtung den Zweck bereits erfüllt.

Eine zweckändernde Verwendung der Aufzeichnungen ist nach § 9 Abs. 2 Satz 2 HmbDSG zudem nur zulässig, wenn dies zur Verfolgung von Straftaten oder zur Abwehr von Gefahren für Leib, Leben oder Freiheit einer Person oder für bedeutende Sach- oder Vermögenswerte erforderlich ist. Eine darüber hinausgehende Nutzung der Aufnahmen — etwa zur allgemeinen Verhaltens- oder Leistungskontrolle von Beschäftigten — ist damit gesetzlich ausgeschlossen.



Öffentlich und nicht öffentlich zugängliche Bereiche

§ 9 Abs. 1 HmbDSG unterscheidet zwischen öffentlich zugänglichen und nicht öffentlich zugänglichen Bereichen. Für nicht öffentlich zugängliche Bereiche (z. B. interne Labors, Lager, Serverräume, Personalräume) stellt Satz 2 zusätzliche und strengere Anforderungen: Die Überwachung ist dort nur zulässig, soweit und solange sie zur Abwehr von Gefahren für Leib, Leben oder Freiheit einer Person oder für bedeutende Sach- oder Vermögenswerte erforderlich ist. Die Überwachung nicht öffentlich zugänglicher Bereiche ist also nicht ausgeschlossen, aber an eine qualifizierte Gefahrenlage geknüpft. Die Erforderlichkeit ist sorgfältig zu dokumentieren und regelmäßig zu überprüfen.

Die Zwecke müssen konkret formuliert werden

Die Zweckangabe auf dem Hinweisschild darf nicht pauschal gehalten sein. „Sicherheitszwecke“ oder „zum Schutz unseres Eigentums“ allein genügt nicht. Die Zwecke müssen auf den jeweiligen Kamerastandort bezogen formuliert werden.

Die folgenden Beispiele dienen der Orientierung und dürfen nicht ohne Anpassung an den Einzelfall übernommen werden.

Überblick über vier Beispielszenarien

Die folgende Tabelle fasst die vier nachfolgend ausführlich erläuterten Beispielszenarien kompakt zusammen. Die Rechtsgrundlagen sind bewusst verkürzt — die vollständige Herleitung findet sich in den ausführlichen Beispielen unten in diesem Abschnitt. Die Liste ist nicht abschließend; andere Konstellationen sind im Einzelfall denkbar und eigenständig zu prüfen.

Zweck	Beispielhafter Einsatzort	Rechtsgrundlage	Zu beachten
Bsp. 1: Schutz vor Diebstahl und Vandalismus an Hochschuleigentum	Bibliotheken, Computerpools, Lagerräume für Forschungsgeräte	Art. 6 Abs. 1 lit. e DSGVO i. V. m. § 9 Abs. 1 HmbDSG, § 6 Abs. 2 Nr. 2 HmbHG	Keine Leistungs- oder Verhaltenskontrolle von Mitarbeitenden
Bsp. 2: Schutz von Personen in konkret gefährdeten Teilbereichen	Schlecht einsehbare Parkplätze, Zugangspunkte mit Vorfallshistorie	Art. 6 Abs. 1 lit. e DSGVO i. V. m. § 9 Abs. 1 HmbDSG, § 81 Abs. 4 HmbHG (Hausrecht)	Mildere Mittel vorab prüfen (Beleuchtung, Security); DSFA regelmäßig erforderlich
Bsp. 3: Schutz des Hochschulbetriebs vor Störungen	Labors mit gefährlichen Stoffen, Zugang zu sensiblen Betriebsbereichen, Eingangsbereiche bei dokumentierter Vorfallslage	Art. 6 Abs. 1 lit. e DSGVO i. V. m. § 9 Abs. 1 HmbDSG, § 81 Abs. 4 HmbHG	Zweck eng fassen; keine anlasslose Verhaltens- oder Leistungskontrolle; Zugriff nur anlassbezogen
Bsp. 4: Schutz sensibler Forschungseinrichtungen und -ergebnisse	Forschungslabors, Archive, Datenräume	Art. 6 Abs. 1 lit. e DSGVO i. V. m. § 9 Abs. 1 HmbDSG, § 81 Abs. 4 HmbHG (Hausrecht)	Zweck eng fassen; keine anlasslose Verhaltensbeobachtung der Beschäftigten



i Wichtiger Hinweis zu den Abbildungen

Die auf den folgenden Illustrationen dargestellten Hinweisschilder sind bewusst verkürzte Musterformulierungen zur visuellen Orientierung. Sie enthalten NICHT alle Pflichtangaben nach Art. 13 DSGVO und eignen sich daher nicht als Vorlage. Ein vollständig ausgefülltes Hinweisschild mit sämtlichen Pflichtangaben findet sich in Abschnitt 2 (Abb. 2).

Beispiel 1: Schutz vor Diebstahl und Vandalismus an Hochschuleigentum

Zweck: Die Videoüberwachung dient der Prävention und Aufklärung von Diebstählen oder Beschädigungen an Eigentum der Hochschule, z. B. in Bibliotheken, Computerpools oder Lagerräumen für Forschungsgeräte. Denkbar ist etwa der Einsatz von Kameras in Eingangsbereichen, um unbefugten Zugriff zu verhindern.

Rechtsgrundlage: Art. 6 Abs. 1 lit. e DSGVO i. V. m. § 9 Abs. 1 HmbDSG, § 6 Abs. 2 Nr. 2 HmbHG. Letzterer definiert die Verwaltung von Grundstücken und Einrichtungen als staatliche Auftragsangelegenheit der Hochschule, was den Schutz dieses Eigentums einschließt.

Praktische Hinweise: Die Überwachung darf nicht zur Leistungs- oder Verhaltenskontrolle von Mitarbeitenden eingesetzt werden. Es empfiehlt sich, die Videoüberwachung zusätzlich in einer Dienstvereinbarung zu regeln, in der dies ausdrücklich festgelegt wird.

Beispiel 2: Schutz von Personen in konkret gefährdeten Teilbereichen

Zweck: Die Überwachung dient dem Schutz von Studierenden, Beschäftigten und Besucherinnen und Besuchern in konkret gefährdeten Teilbereichen des Campus — etwa an einem schlecht einsehbaren Parkplatz außerhalb der Öffnungszeiten oder an einem Zugangspunkt mit dokumentierter Vorfallshistorie. Ziel ist die Vorbeugung und Aufklärung von Übergriffen, unbefugtem Zutritt und Sachbeschädigungen. Das Szenario ist eng auf den jeweiligen Standort zuzuschneiden; eine flächendeckende Überwachung belebter Bereiche wie Hörsäle oder Cafeterias zur allgemeinen Sicherheit ist mit § 9 HmbDSG regelmäßig nicht vereinbar.

Rechtsgrundlage: Art. 6 Abs. 1 lit. e DSGVO i. V. m. § 9 Abs. 1 HmbDSG, § 81 Abs. 4 HmbHG (Hausrecht). Der Schutz von Personen gehört zu den anerkannten Zwecken, die sich tragfähig auf das Hausrecht der Hochschulleitung stützen lassen. Bei der Überwachung nicht öffentlich zugänglicher Teilbereiche sind zusätzlich die strengeren Anforderungen des § 9 Abs. 1 Satz 2 HmbDSG zu beachten (qualifizierte Gefahrenlage für Leib, Leben oder Freiheit).

Praxishinweis: Vor Einrichtung der Kamera sind mildere Mittel zu prüfen, etwa bessere Beleuchtung, bauliche Maßnahmen oder zeitweise Sicherheitspräsenz. Bei systematischer und umfangreicher Überwachung öffentlich zugänglicher Bereiche ist regelmäßig eine Datenschutz-Folgenabschätzung (Art. 35 DSGVO) zu prüfen. Auf dem Schild sollte der konkrete Bereich benannt werden, etwa: Die Videoüberwachung im Bereich [konkreter Standort] dient dem Schutz vor Übergriffen und unbefugtem Zutritt sowie der Aufklärung entsprechender Vorfälle. Bei reiner Videobeobachtung ohne Speicherung ist die Formulierung entsprechend anzupassen; bei Aufzeichnung kann der Zusatz zur Beweissicherung im Anlassfall passen.



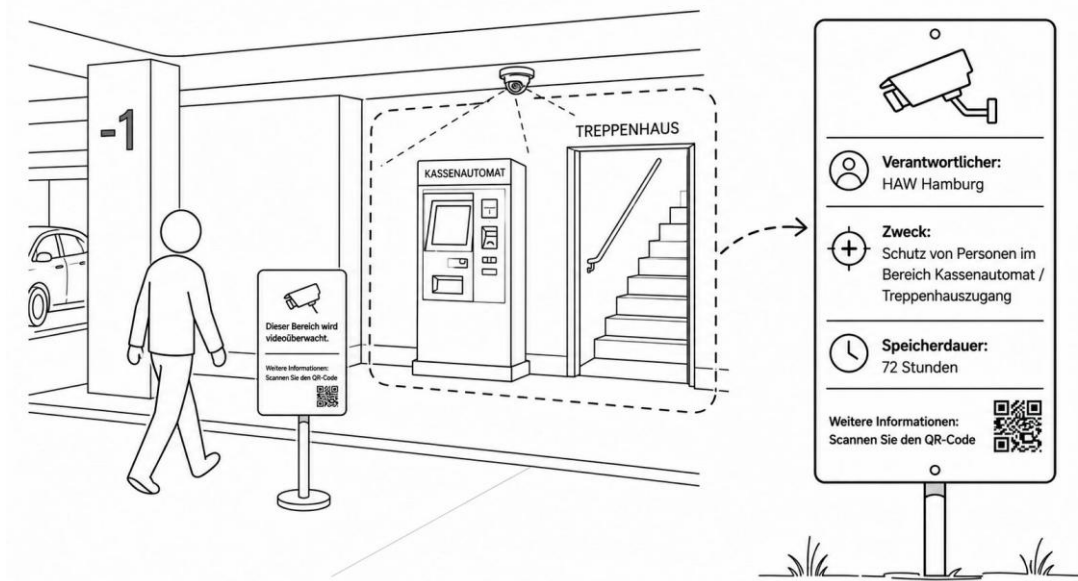


Abb. 5: Tiefgarage — Schutz von Personen in gefährdeten Teilbereichen.

Beispiel 3: Schutz des Hochschulbetriebs vor Störungen

Zweck: Die Videoüberwachung kann dem Schutz besonders störungsanfälliger Bereiche dienen, etwa von Laborzugängen, Chemikalienlagern oder technischen Betriebsräumen. Zulässig ist eine solche Überwachung nur, wenn ein konkreter Schutzbedarf besteht und der Zweck standortbezogen beschrieben wird.

Rechtsgrundlage: Art. 6 Abs. 1 lit. e DSGVO i. V. m. § 9 Abs. 1 HmbDSG, § 81 Abs. 4 HmbHG. Das Hausrecht und die Ordnungsgewalt der Hochschulleitung können eine Videoüberwachung tragen, wenn sie zur Verhinderung oder Aufklärung konkreter Störungen erforderlich ist.

Praxishinweis: Eine Risikoanalyse sollte dokumentieren, ob entsprechende Störungen in der Vergangenheit aufgetreten sind oder warum der Bereich besonders schutzbedürftig ist. Die Kamera darf nicht zur allgemeinen Kontrolle von Beschäftigten, Studierenden oder Besuchenden eingesetzt werden. Der Zugriff auf Aufzeichnungen sollte organisatorisch beschränkt und nur anlassbezogen erfolgen; eine Auswertung im Vier-Augen-Prinzip kann die Revisionssicherheit erhöhen. Die Verarbeitung ist im Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DSGVO) zu dokumentieren.

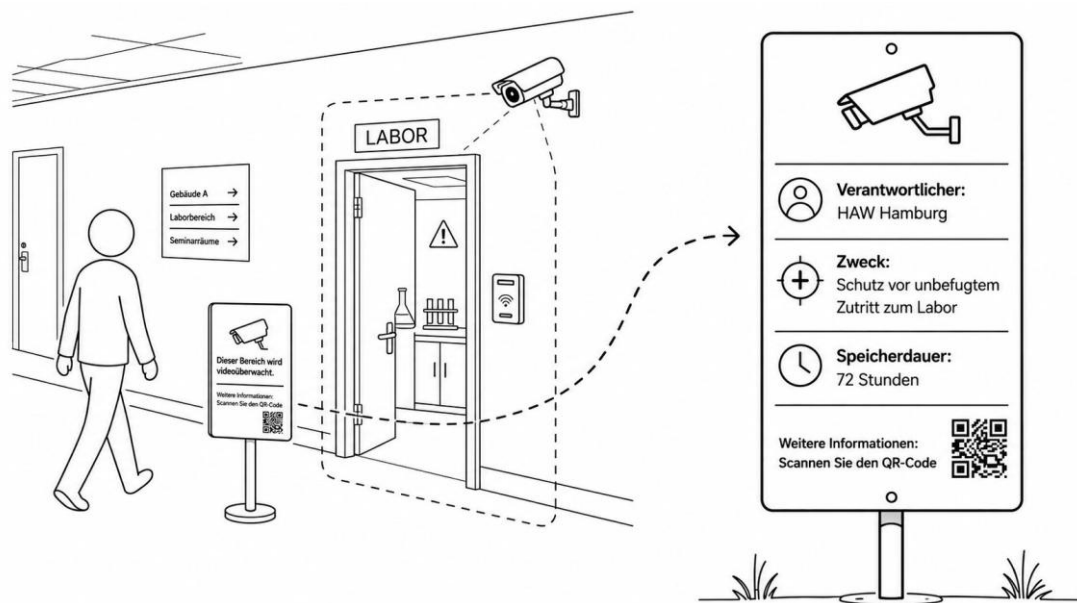


Abb. 6: Laboreingang — Schutz des Hochschulbetriebs vor Störungen / Schutz vor unbefugtem Zutritt.

Beispiel 4: Schutz sensibler Forschungseinrichtungen und -ergebnisse

Zweck: Die Überwachung schützt Forschungsräume vor unbefugtem Zugriff, z. B. in Labors oder Archiven, um Diebstahl intellektuellen Eigentums oder Beschädigung von Experimenten zu verhindern. Dies ist besonders relevant für Hochschulen mit Unternehmenskooperationen.

Rechtsgrundlage: Art. 6 Abs. 1 lit. e DSGVO i. V. m. § 9 Abs. 1 HmbDSG und § 81 Abs. 4 HmbHG (Hausrecht). Der Schutz von Forschungsräumen, Laboren und Archiven lässt sich tragfähig auf das Hausrecht der Hochschulleitung stützen. Handelt es sich um nicht öffentlich zugängliche Bereiche (Innenlabore, Archivräume), gelten zusätzlich die strengeren Anforderungen des § 9 Abs. 1 Satz 2 HmbDSG (qualifizierte Gefahrenlage für bedeutende Sach- oder Vermögenswerte). Der Zweck muss eng gefasst sein, um eine unzulässige, anlasslose Verhaltensbeobachtung der Beschäftigten auszuschließen.



4.5 Speicherdauer

Auf dem Hinweisschild ist die konkrete Speicherdauer anzugeben — oder die Kriterien, nach denen sie festgelegt wird. Eine gesetzlich vorgeschriebene Frist gibt es nicht. In der Aufsichtspraxis lassen sich etwaige Schäden in der Regel innerhalb weniger Tage feststellen; ab 72 Stunden besteht ein deutlich erhöhter Begründungsaufwand. 72 Stunden gelten daher als praxistaugliche Obergrenze und Orientierungsgröße — nicht als starre Frist.

Längere Speicherfristen sind möglich, erfordern aber eine konkrete Begründung. Je länger die Speicherfrist, desto höher der Begründungsaufwand. Mögliche Begründungen sind etwa die dokumentierte Häufigkeit von Schadensfällen oder die besondere Schutzbedürftigkeit bestimmter Bereiche. Eine automatische Löschung ist einzurichten — das folgt aus dem Grundsatz der Speicherbegrenzung (Art. 5 Abs. 1 lit. e DSGVO).

Beispielformulierung: „Die Aufnahmen werden grundsätzlich nach 72 Stunden automatisch gelöscht. In Ausnahmefällen, etwa bei Verdacht auf Straftaten oder Vandalismus, werden relevante Daten bis zur Klärung des Vorfalls aufbewahrt.“

4.6 Empfänger und Drittlandübermittlung

Die Angabe von Empfängern oder Kategorien von Empfängern der Videodaten sowie die Absicht einer Datenübermittlung in ein Drittland sind Pflichtangaben nach Art. 13 DSGVO.

Ob diese Angaben bereits auf dem Hinweisschild (Stufe 1) oder erst in der vollständigen Datenschutzhinweisung (Stufe 2) aufgeführt werden, ist im Einzelfall zu entscheiden. In der Regel genügt es, diese Angaben in Stufe 2 zu machen — es sei denn, es liegt eine für die betroffene Person besonders wesentliche Konstellation vor, etwa eine Übermittlung in ein Drittland.

Neben den eigentlichen externen Empfängern — etwa Polizeibehörden im Fall einer Strafanzeige, Gerichte zur Beweissicherung oder Versicherungen zur Schadensregulierung — werden in der Praxis auch Auftragsverarbeiter im Sinne des Art. 28 DSGVO (z. B. externe Sicherheitsdienste oder IT-Dienstleister, die das Videosystem warten) mit den Daten in Berührung kommen.

Auftragsverarbeiter sind nach Art. 4 Nr. 9 DSGVO ebenfalls Empfänger, werden in der Informationspflicht aber üblicherweise als eigene Kategorie dargestellt, weil sie nicht zu eigenen Zwecken verarbeiten, sondern weisungsgebunden für den Verantwortlichen tätig werden. In Stufe 2 sollten beide Gruppen transparent gemacht werden — Empfänger im engeren Sinn und Auftragsverarbeiter —, insbesondere wenn ihre Beteiligung für die betroffene Person absehbar ist.

4.7 Weitere Informationen — Verweis auf Stufe 2

Das Hinweisschild muss einen funktionierenden Verweis auf die vollständige Datenschutzhinweisung enthalten. Üblich ist eine Kombination aus Link und QR-Code, damit die Information sowohl mobil als auch am Computer abgerufen werden kann.

Betroffene Personen müssen die Informationen der Stufe 2 abrufen können, ohne den videoüberwachten Bereich betreten zu müssen. Der QR-Code bzw. der Link muss zum Zeitpunkt des Abrufs funktionieren und auf eine Seite verweisen, die tatsächlich die vollständigen Pflichtinformationen enthält — nicht auf die allgemeine Startseite der Hochschule.



Empfehlung: Darüber hinaus sollten die Informationen der Stufe 2 nach Möglichkeit auch ohne digitales Endgerät erreichbar sein — etwa durch einen Aushang im Eingangsbereich oder ein Infoblatt an einer zentralen, frei zugänglichen Stelle. Dies ist eine Empfehlung der Aufsichtsbehörden, keine zwingende Pflicht.

Beispielformulierung: „Weitere Informationen, insbesondere zu Ihren Rechten als betroffene Person, finden Sie unter [Link/QR-Code].“



5. Hinweis zu Stufe 2 — Vollständige Datenschutzinformation

Die vollständige Datenschutzinformation (Stufe 2), die über den QR-Code oder Link erreichbar sein muss, enthält alle in Art. 13 Abs. 1 und 2 DSGVO geforderten Angaben. (Für die Erstellung stellt das MMKH ein eigenes Muster samt Ausfüllhilfe bereit — Näheres am Ende dieses Abschnitts.) Dies umfasst die Wiederholung der Informationen von Stufe 1 sowie die folgenden zusätzlichen Angaben:

- **Empfänger oder Kategorien von Empfängern** — externe Stellen, an die Videodaten weitergegeben werden können (z. B. Polizei, Gerichte, Versicherungen). Auch Auftragsverarbeiter im Sinne des Art. 28 DSGVO (z. B. externe Sicherheitsdienste, IT-Dienstleister für die Wartung) sind nach Art. 4 Nr. 9 DSGVO Empfänger; in der Informationspflicht werden sie jedoch üblicherweise als eigene Kategorie dargestellt, weil sie nicht zu eigenen Zwecken verarbeiten, sondern weisungsgebunden für den Verantwortlichen tätig werden.
- **Drittlandtransfer** — falls Daten an Empfänger außerhalb der EU/des EWR übermittelt werden (z. B. bei Nutzung von Cloud-Speichern US-amerikanischer Anbieter), sind die Rechtsgrundlage (z. B. Angemessenheitsbeschluss, Standardvertragsklauseln) und die Garantien zum Schutz der Daten zu nennen.
- **Speicherdauer** — die konkrete Speicherdauer bzw. die Kriterien für ihre Festlegung (Art. 13 Abs. 2 lit. a DSGVO). Die Angabe erscheint zwar schon auf dem Schild, ist aber in Stufe 2 ggf. ausführlicher zu begründen.
- **Betroffenenrechte** — Recht auf Auskunft (Art. 15 DSGVO), Berichtigung (Art. 16 DSGVO), Löschung (Art. 17 DSGVO) und Einschränkung der Verarbeitung (Art. 18 DSGVO). Das Recht auf Datenübertragbarkeit (Art. 20 DSGVO) ist bei Videoüberwachung auf Grundlage von Art. 6 Abs. 1 lit. e DSGVO regelmäßig nicht einschlägig, da es nur für die Rechtsgrundlagen lit. a und lit. b gilt.
- **Widerspruchsrecht und Hinweispflicht** — das Recht auf Widerspruch gegen die Verarbeitung nach Art. 21 DSGVO. Nach Art. 21 Abs. 4 DSGVO ist auf dieses Recht spätestens zum Zeitpunkt der ersten Kommunikation ausdrücklich hinzuweisen, und zwar in einer verständlichen und von anderen Informationen getrennten Form. Dieser gesonderte Hinweis ist in Stufe 2 klar sichtbar anzubringen.
- **Beschwerderecht** — der Hinweis auf das Recht, eine Beschwerde bei einer Datenschutzaufsichtsbehörde einzulegen (Art. 13 Abs. 2 lit. d DSGVO). Die Nennung einer konkreten Behörde ist nicht zwingend, wird aber zur besseren Ausübung des Rechts empfohlen. Für Hamburger Hochschulen ist dies der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI).
- **Bestehen einer automatisierten Entscheidungsfindung** — Angabe nur, wenn ausschließlich automatisiert entschieden wird, einschließlich Profiling nach Art. 22 DSGVO. Der Einsatz biometrischer Technologien allein begründet noch keine automatisierte Entscheidung im Sinne des Art. 22 DSGVO — entscheidend ist, ob eine rechtliche oder ähnlich erhebliche Wirkung für die betroffene Person ohne menschliches Zutun erzeugt wird. In der Praxis ist dies bei Hochschul-Videoüberwachung regelmäßig nicht der Fall.



- **Angabe nach Art. 13 Abs. 2 lit. e DSGVO** — Hinweis darauf, ob die Bereitstellung der Daten gesetzlich oder vertraglich vorgeschrieben ist und welche Folgen die Nichtbereitstellung hätte. Bei Videoüberwachung ergibt sich dies aus dem Umstand, dass die Aufnahme bereits durch das Betreten des Bereichs erfolgt — eine Nichtbereitstellung ist praktisch nur durch Meidung des Bereichs möglich.

Für die Erstellung der vollständigen Datenschutzinformation steht in der Infothek unter hh-datenschutz.de ein separates Muster („Datenschutzrechtliche Informationspflichten“) mit zugehöriger Ausfüllhilfe zur Verfügung.



6. Checkliste — Vor dem Aufhängen

Inhalt des Schildes:

- ☐ Piktogramm / Kamerasymbol
- ☐ Verantwortlicher: Name, Anschrift, E-Mail
- ☐ DSB: Name oder Bezeichnung, Kontaktdaten
- ☐ Zwecke konkret formuliert (kein pauschales „Sicherheit“)
- ☐ Rechtsgrundlage genannt
- ☐ Speicherdauer angegeben
- ☐ Verweis auf Stufe 2 (Link / QR-Code)

Anbringung:

- ☐ Vor dem überwachten Bereich platziert
- ☐ Auf Augenhöhe, gut lesbar
- ☐ Nicht übersehbar
- ☐ Jeder Zugang mit eigenem Schild versehen

Begleitende Pflichten:

- ☐ Risikoanalyse durchgeführt
- ☐ DSFA geprüft (Art. 35 DSGVO — bei systematischer und umfangreicher Überwachung öffentlich zugänglicher Bereiche regelmäßig erforderlich)
- ☐ Verarbeitung in VVT dokumentiert (Art. 30 DSGVO)
- ☐ Stufe 2 vorhanden und funktionsfähig
- ☐ Personalrat beteiligt (§ 88 Abs. 1 Nr. 32 HmbPersVG — Videoüberwachung unterliegt der Mitbestimmung des Personalrats. Eine Dienstvereinbarung ist eine häufige, aber nicht die zwingend einzige Form der Beteiligung.)
- ☐ Freigabe durch Datenschutzstelle der Hochschule



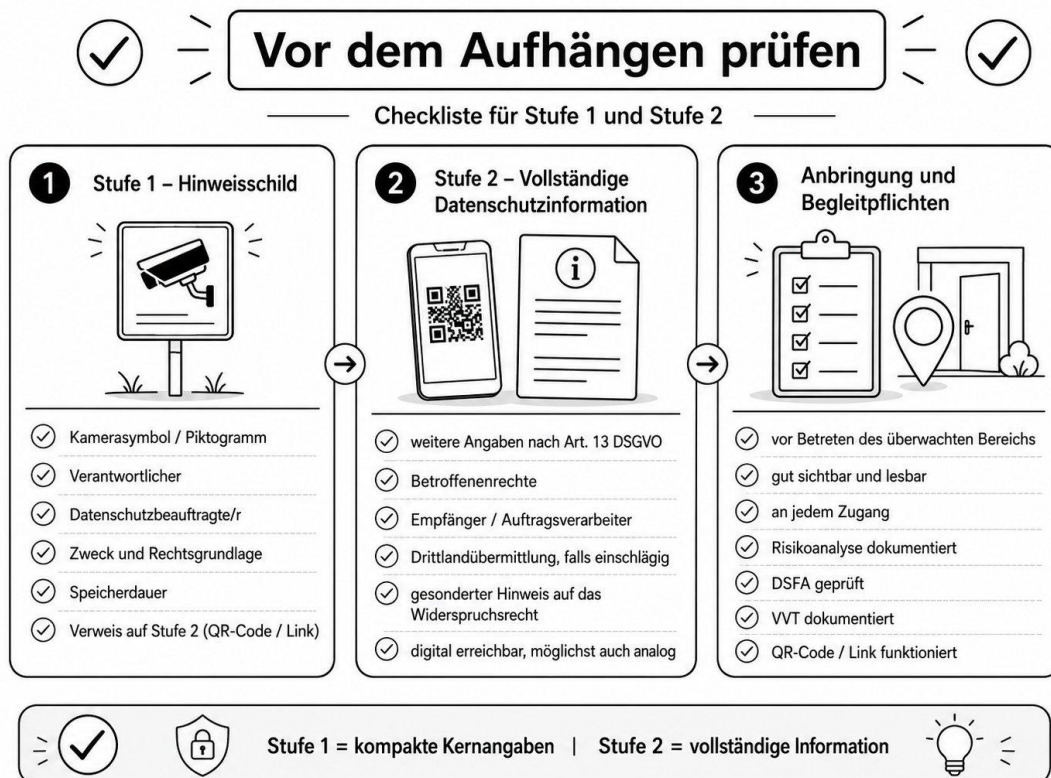


Abb. 7: Die Checkliste im Überblick — maßgeblich ist die vollständige Checkliste oben.

Abschließend:

Vor Verwendung bzw. Anbringung des Hinweisschildes lassen Sie dieses durch die zuständige Datenschutzstelle Ihrer Hochschule prüfen und freigeben. Prüfen Sie vor Inbetriebnahme der Videoüberwachung, ob eine Datenschutz-Folgenabschätzung (DSFA) gem. Art. 35 DSGVO erforderlich ist. Nach Art. 35 Abs. 3 lit. c DSGVO ist eine DSFA bei systematischer und umfangreicher Überwachung öffentlich zugänglicher Bereiche regelmäßig erforderlich.

Bei Fragen können Sie uns gerne jederzeit über das Funktionspostfach datenschutz@mmkh.de kontaktieren.

Stand: Juli 2026