Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB
Préposé fédéral à la protection des données et à la transparence PFPDT
Incaricato federale della protezione dei dati e della trasparenza IFPDT
Incumbensà federal per la protecziun da datas e per la transparenza IFPDT

privatim
Konferenz der schweizerischen Datenschutzbeauftragten
Conférence des préposé(e)s suisses à la protection des données
Conferenza degli incaricati svizzeri per la protezione dei dati

Merkblatt

Überwachung von betreuten Personen

Datenbearbeitung mittels Videokameras und anderer in Spitälern, Pflegeheimen und vergleichbaren Einrichtungen eingesetzter Sensoren

Digitale Überwachung von Personen, die in Spitälern, Pflegeheimen oder anderen, vergleichbaren Einrichtungen betreut werden, gewinnt angesichts der technologischen Entwicklung und der Fülle entsprechender Waren- und Dienstleistungsangebote an Bedeutung. Je nachdem, welches Recht im konkreten Fall zur Anwendung gelangt, kann die Personendatenbearbeitung durch diese Einrichtungen in die Aufsichtskompetenz des eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) oder der kantonalen Datenschutzbehörden fallen. Aus diesem Grund sehen sich der EDÖB und privatim veranlasst, das vorliegende Merkblatt zur Sensibilisierung der Verantwortlichen für die mit dem Einsatz von Überwachungssensorik verbundenen datenschutzrechtlichen Herausforderungen gemeinsam zu publizieren. Das vorliegende Merkblatt bezieht sich ausschliesslich auf die Überwachung der betreuten Personen; die generelle Überwachung der Einrichtung, wie beispielsweise Kameras in den Gängen, an den Eingängen, in den Wartezimmern usw., ist davon nicht betroffen.

I. Einleitende Bemerkungen

Digitale Überwachungs- und Assistenzlösungen kommen in immer mehr Bereichen zum Einsatz (Fahrassistenz, Sicherheit, Spielzeug usw.). Inzwischen werden auf dem Markt in zunehmendem Masse multimodale Produkte mit vielfältigen Funktionen angeboten (Bewegungs- und Anwesenheitserkennung, Blickverfolgung, direkte Kommunikation, oft in Verbindung mit künstlicher Intelligenz), die auf Technologien wie optischen Kameras, Mikrofonen, Radar oder Infrarotsensoren basieren. Häufig zeichnen diese Systeme Daten (Video, Ton, Radar usw.) nicht nur auf, sondern analysieren sie in unterschiedlicher Intensität; sie erkennen automatisch Anomalien, lösen Alarme aus und ermöglichen ein Eingreifen vor Ort – sei es durch Menschen oder Algorithmen, präventiv oder reaktiv. Dieser Bereich entwickelt sich stetig weiter, und es ist absehbar, dass die angebotenen Lösungen durch die Bündelung mehrerer Technologien noch umfassender werden. Dann werden sehr weitreichende Nutzungsmöglichkeiten geboten werden, die über die eigentlichen Bedürfnisse der Nutzer weit hinausgehen. In diesem Sinne befasst sich das vorliegende Merkblatt mit der Überwachung im Bereich der Pflege. Dabei geht es nicht im Detail auf alle derzeit auf dem Markt verfügbaren Lösungen ein, ebenso wenig auf mögliche Kombinationen dieser Technologien. Vielmehr soll es anhand einiger Beispiele die Herausforderungen veranschaulichen und die wesentlichen Punkte herausarbeiten. Dennoch gelten die im Folgenden dargelegten Grundsätze allgemein, unabhängig von den eingesetzten Technologien und Lösungen.

Neben Fragen des Datenschutzes wirft die digitale Überwachung im Bereich der Pflege auch in mehreren anderen Bereichen Fragen auf, insbesondere im Arbeitsrecht, in weiteren

Bereichen des Gesundheitswesens sowie in ethischer Hinsicht. In diesem Beitrag wird die Problematik unter dem Gesichtspunkt des Datenschutzes erörtert.

Generell stellt diese Art der Überwachung eine Massnahme mit hoher Intensität dar, da sie in die Privatsphäre und sogar in die Intimsphäre der betreuten Personen eingreift, die sich oft in einer schutzbedürftigen Lage befinden. Bei Personen, die sich längerfristig in den Einrichtungen aufhalten, kann eine solche Überwachung sogar als Überwachung im privaten Zuhause der betroffenen Person angesehen werden.

Auch wenn die Intensität der Datenbearbeitung je nach Situation und eingesetzter Technologie variieren kann, sind die Grundsätze für den Einsatz solcher Mittel und die unter dem Gesichtspunkt des Datenschutzes aufgeworfenen Fragen im Grossen und Ganzen dieselben.

II. Aspekte im Hinblick auf die Technologie

Im Folgenden wird zunächst die Funktionsweise bestimmter Technologien erläutert, die in solchen Fällen zum Einsatz kommen können; anschliessend befassen wir uns mit den rechtlichen Fragen.

1. Optische Sensoren

Um bestimmte technologische Aspekte zu veranschaulichen, wird zunächst die optische Überwachung vorgestellt, bevor die Analyse auf andere Technologien ausgeweitet wird. Grob gesagt lassen sich mehrere Arten der optischen Überwachung unterscheiden:

- **Analoge direkte Überwachung:** Die Pflegekraft sitzt auf einem Stuhl im Zimmer der betreuten Person.

- **Digitale direkte Überwachung**: Im Zimmer ist eine Kamera installiert, die das Bild in Echtzeit auf einen Monitor überträgt, den das Pflegepersonal im Blick hat.

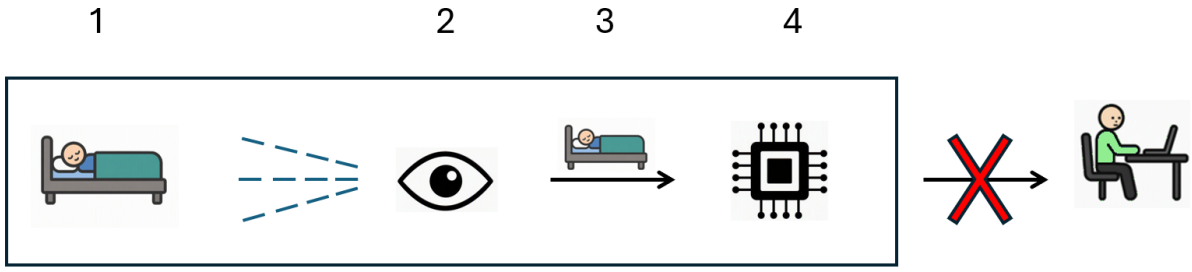
- **Digitale indirekte Überwachung**: Im Zimmer ist eine Kamera installiert, die die Bilder an eine ebenfalls im Zimmer befindliche Recheneinheit überträgt. Dort werden die Bilder in ein Piktogramm umgewandelt, das die Position oder das Verhalten des Patienten darstellt (liegend, auf dem Boden, sitzend, stehend, unruhig usw.). Das Piktogramm wird anschliessend in Echtzeit auf dem Monitor des Pflegepersonals angezeigt. Es handelt sich um eine indirekte Überwachung, weil die Rohdaten in einem Zwischenschritt von der Recheneinheit bearbeitet werden, bevor sie – in bereinigter Form – an das Pflegepersonal weitergeleitet werden.

- **Indirekte situative digitale Überwachung**: Die Situation ist wie oben, allerdings erhält das Pflegepersonal nur dann eine Meldung, wenn eine vorab konfigurierte Situation erkannt wird (z. B. ein Sturz). In einem solchen Fall sendet die Recheneinheit ein Warnsignal an das Pflegepersonal, wandelt das Bild

gegebenenfalls in ein Piktogramm um und überträgt es auf den Monitor des Pflegepersonals. Solange sich kein Vorfall ereignet, werden keine Daten übermittelt.

Die folgenden Ausführungen basieren auf dieser letztgenannten Form der Überwachung: Sie illustriert zahlreiche Überlegungen aus der Praxis und lässt Schlüsse auf den Einsatz anderer Technologien zu.

Die indirekte situative digitale Überwachung lässt sich wie folgt darstellen:



Bildunterschrift:

1: Beobachtungsobjekt, hier eine im Bett liegende Person in der Einrichtung

2: Sensor, in diesem Fall eine optische Kamera

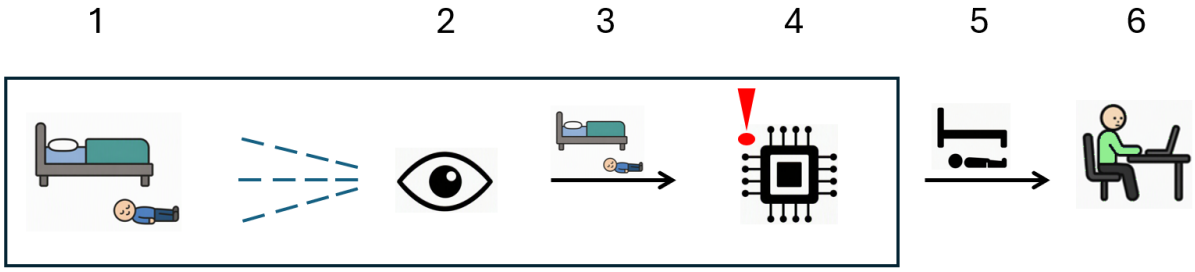
3: Rohdaten, d. h. das Bild, wie es vom Sensor erfasst und an die Recheneinheit übertragen wird

4: Im Zimmer (oder im Gehäuse des Sensors selbst) installierte Recheneinheit, die die jeweilige Situation erkennt, einen Alarm ausgibt und gegebenenfalls das Bild in ein Piktogramm umwandelt

Die Schritte 1 bis 4 finden im Zimmer statt (dargestellt durch den Rahmen).

Der Sensor (in diesem Fall eine Kamera) erfasst ein Bild, das er zur Bearbeitung (Erkennung einer bestimmten Situation) an die Recheneinheit übermittelt. In der obigen Darstellung werden keine Daten aus dem Zimmer an den Monitor übertragen, da alles «in Ordnung» ist (die Person schläft in ihrem Bett).

Im Falle eines Sturzes sieht das Schema wie folgt aus:



Die Recheneinheit hat einen Sturz erkannt. Ein Alarm wird ausgegeben, das Bild in ein Piktogramm umgewandelt (5) und auf dem Monitor des Pflegepersonals angezeigt (6 – eventuell auf einem anderen Gerät, wie Pager, Tablet usw.).

Das obige Beispiel veranschaulicht den Grundsatz der Datenminimierung (vgl. Kap. III. 4). Um Stürze oder andere Vorfälle zu erkennen, muss man nicht die Aufnahme selbst sehen. Dadurch, dass die Recheneinheit eine Filterfunktion übernimmt, werden dem Pflegepersonal nur die minimal notwendigen Daten übermittelt, d. h. entweder das Alarmsignal oder das Piktogramm (also die bereinigten Daten), und dies ausschliesslich in vordefinierten Situationen. Wenn die Situation keine Anomalie (nichts Ungewöhnliches) aufweist, werden weder Rohdaten noch bereinigte Daten aus dem überwachten Raum heraus übertragen.

2. Andere Sensoren und Auswahl der Technologie

Wie bereits erwähnt, können zur indirekten Überwachung im Bereich der Pflege auch andere Technologien wie Infrarotkameras oder Radar zum Einsatz kommen.

Infrarotkameras erfassen Temperaturunterschiede und zeigen so die im Raum befindlichen Gegenstände und Personen in Form von Silhouetten an. Radarsysteme hingegen messen die Entfernung von Objekten zum Sender; auf diese Weise erstellen sie ein Relief (das Objekte und Personen sichtbar macht) und erkennen Bewegungen.

Die erfassten Rohdaten unterscheiden sich je nach verwendetem Sensor – optisch, thermisch oder radarbasiert – und können unterschiedliche Informationen liefern. Im Gegensatz zur optischen Kamera erzeugen Wärmebild- und Radarsensoren kein fotografisches Bild. Demgegenüber können diese Geräte andere Daten erfassen, die einer optischen Kamera möglicherweise entgehen. Durch die Messung der Körpertemperatur der betreuten Person können Infrarotsensoren zusätzliche Informationen über deren Zustand liefern (Fieber, Stress usw.). Radarsysteme wiederum können bspw. Herz- und Atemfrequenz erfassen. Zu beachten ist, dass das System zwingend mit einem Zimmer oder einem Bett verknüpft sein muss, damit das Pflegepersonal im Alarmfall weiss, wo es einzugreifen hat. Die Zimmer bzw. Betten sind ihrerseits einer konkreten Person zugeordnet (wobei diese Zuordnung möglicherweise in einem anderen Informationssystem erfolgt als dem zur Überwachung). Auch wenn die Rohdaten aus Radar- und Infrarotaufnahmen *a priori* keine direkte Identifizierung einer Person ermöglichen, handelt es sich also nicht um Anonymisierung im eigentlichen Sinne, sondern um Pseudonymisierung.

Schliesslich spielt auch die Auflösung der Sensordaten eine wichtige Rolle: Unter gleichen Bedingungen (Bildfeld der Kamera, optischer Zoom usw.) erfasst eine 0,5-Megapixel-Kamera weniger Informationen als ein 10-Megapixel-Modell. Dies gilt letztlich für alle in Frage kommenden Technologien.

Die Datenschutzanforderungen im Zusammenhang mit der gewählten Überwachungs-technologie werden in Kapitel III. 5 behandelt.

III. Rechtliche Aspekte

1. Anwendbares Datenschutzrecht

Zunächst ist eine Unterscheidung hinsichtlich der Art der betreffenden Gesundheitseinrichtung zu treffen: Handelt es sich um eine öffentliche Einrichtung[1] (grundsätzlich kantonal, da das Gesundheitswesen in die Zuständigkeit der Kantone fällt), so unterliegt sie dem Legalitätsprinzip und dem Datenschutzrecht des betreffenden Kantons. Handelt es sich hingegen um eine private Einrichtung, so unterliegt sie dem Bundesgesetz über den Datenschutz (DSG) und das Legalitätsprinzip ist nicht anwendbar.

Abgesehen von der Frage der Rechtsgrundlage sind die Grundsätze, die die Durchführung solcher Überwachungsmassnahmen regeln, im Wesentlichen dieselben und sowohl in den kantonalen Gesetzen als auch im DSG vorgesehen. In den folgenden Ausführungen werden die zu beachtenden Grundsätze dargelegt.

2. Rechtmässigkeit der Datenbearbeitung und Einwilligung

Personendaten müssen rechtmässig bearbeitet werden. Wie bereits erwähnt, wird dieser Begriff je nachdem, ob es sich um eine öffentliche oder eine private Einrichtung handelt, unterschiedlich ausgelegt.

Für öffentliche Einrichtungen gilt das Legalitätsprinzip, wonach öffentliche Einrichtungen für ihr Handeln eine Rechtsgrundlage benötigen. Eine öffentliche Einrichtung darf Personendaten demnach nur bearbeiten, wenn dafür eine gesetzliche Grundlage besteht. Die Überwachung muss deshalb entweder für die Erfüllung einer gesetzlichen Aufgabe unerlässlich sein oder in einem Gesetz ausdrücklich vorgesehen sein. Eine Überwachung einer Patientin oder eines Patienten als Teil des Behandlungsplans kann sich beispielsweise auf den gesetzlichen Pflegeauftrag stützen. Eine Einwilligung kann dabei die im Sinne des Legalitätsprinzips erforderliche Rechtsgrundlage nicht ersetzen. Hinzu kommt, dass öffentliche Einrichtungen ihren Versorgungsauftrag unabhängig von einer möglichen Einwilligung in eine Datenbearbeitung zu erfüllen haben.

Private Einrichtungen unterliegen dem DSG. Gemäss Art. 30 Abs. 1 DSG darf beim Bearbeiten von Personendaten die Persönlichkeit der betroffenen Personen nicht widerrechtlich verletzt werden. In Absatz 2 wird präzisiert, dass eine Persönlichkeitsverletzung insbesondere dann vorliegt, wenn Personendaten entgegen den Grundsätzen nach den Artikeln 6 und 8 DSG bearbeitet werden, Personendaten entgegen der ausdrücklichen Willenserklärung der betroffenen Person bearbeitet werden oder Dritten

[1] Diese Einstufung hängt nicht von der Rechtsform der Einrichtung ab, sondern von ihrem Auftrag. Beispielsweise gilt eine Privatklinik, die im Auftrag des Kantons orthopädische Eingriffe durchführt, als öffentliche Einrichtung in diesem Rahmen. Zu beachten ist, dass ein und dieselbe Einrichtung für bestimmte Tätigkeiten (die sich aus einem kantonalen Auftrag ergeben) eine öffentliche Einrichtung sein kann, für die übrigen hingegen eine private.

besonders schützenswerte Personendaten bekanntgegeben werden. Wenn eine Datenbearbeitung eine widerrechtliche Persönlichkeitsverletzung verursacht, ist zu prüfen, ob ein Rechtfertigungsgrund vorliegt (Art. 31 DSG). In unserem Kontext kommen im Wesentlichen die Einwilligung der betroffenen Person und das überwiegende private Interesse in Betracht.

Von den drei oben erwähnten «klassischen» Fällen gemäss Artikel 30 Absatz 2 DSG trifft die Weitergabe von Daten an Dritte in diesem Zusammenhang *a priori* nicht zu, da die Überwachungssysteme ausschliesslich für interne Zwecke genutzt werden. Die Frage des Widerspruchs der betreuten Person wird zu einem späteren Zeitpunkt behandelt. Was die Grundsätze betrifft – insbesondere bestimmter und erkennbarer Zweck und Verhältnismässigkeit –, ist nicht ausgeschlossen, dass deren Einhaltung gewährleistet werden kann[2], wenn die betreute Person urteilsfähig ist und angesichts ihres sowohl körperlichen als auch psychischen Zustands in der Lage ist, ihre Rechte tatsächlich und zweifelsfrei geltend zu machen (insbesondere ihr Widerspruchsrecht – siehe weiter unten). In einem solchen Fall, in dem die betreute Person keine besondere Schutzbedürftigkeit aufweist, würde die Überwachung nicht zwangsläufig eine Verletzung der Persönlichkeit darstellen und daher keinen Rechtfertigungsgrund im Sinne von Artikel 31 DSG erfordern.

Dennoch ist hier Vorsicht geboten. Zunächst ist die Aufzählung der Fälle in Artikel 30 Absatz 2 DSG nicht abschliessend, wie aus dem Wortlaut *insbesondere* hervorgeht. Es sind also weitere Situationen denkbar, die eine Verletzung der Persönlichkeit zur Folge haben, zumal in einem so sensiblen und intimen Bereich wie dem hier behandelten. Hinzu kommt, dass die verantwortlichen Pflegeinstitutionen die Überwachungsmassnahmen nicht nach Massgabe der Möglichkeiten besonders vitaler Personen ausgestalten dürfen, wenn diese für die entsprechende Einrichtung nicht repräsentativ sind.

Zudem, wenn man nun davon ausgehen würde, dass keine Verletzung der Persönlichkeit vorliegt, würde dies bedeuten, dass kein Rechtfertigungsgrund und erst recht keine Einwilligung erforderlich ist. Diese Aussage gibt Anlass zu mehreren Anmerkungen.

Zu den Grundsätzen des DSG gehört der Grundsatz des erkennbaren Zwecks (Art. 6 Abs. 3 DSG), der durch die in Artikel 19 DSG verankerte Informationspflicht konkretisiert wird. Gemäss diesem Artikel muss der Verantwortliche die betroffene Person insbesondere über die Beschaffung von Personendaten und deren Zwecke informieren. Je sensibler die betreffenden Daten und je «heikler» die Situation, desto umfassender und aktiver müssen diese Informationen sein. In hier behandelten Bereich ist angesichts der Intensität der Datenbearbeitung, den die Überwachung mit sich bringen kann, davon auszugehen, dass diese Informationen der betreuten Person tatsächlich mitgeteilt und vom Personal erläutert werden müssen – ein einfaches Informationsblatt wird nicht ausreichen. Vor dem Hintergrund dieser «verstärkten» Informationspflicht kann man daher davon ausgehen, dass in der Praxis das Einholen einer («ausdrücklichen» – Art. 6 Abs. 7 DSG) Einwilligung

[2] Vereinfacht gesagt könnte dies der Fall sein, wenn die Daten für einen bestimmten Zweck bearbeitet werden, die betreute Person umfassend darüber informiert wurde und der Grundsatz der Verhältnismässigkeit gewahrt ist. Auf diese Grundsätze wird im Folgenden näher eingegangen.

zusätzlich zur «blossen» Information der betreuten Person keinen wesentlichen zusätzlichen Aufwand für die Einrichtung darstellt. (Im Übrigen stellt die Information gemäss Art. 6 Abs. 6 DSG eine notwendige Voraussetzung für die Einwilligung dar.) Es erscheint daher wünschenswert, diese wann immer möglich einzuholen – umso mehr angesichts des Vertrauensverhältnisses, das zwischen der betreuten Person und dem Pflegepersonal besteht.

Allerdings lautet die andere Voraussetzung für die Einwilligung, dass sie freiwillig erfolgt, und in dieser Hinsicht kann die Situation heikel werden. Die betreute Person befindet sich häufig in einer schutzbedürftigen Lage. Zudem kann sie sich einer Art Druck ausgesetzt fühlen, der – möglicherweise ungewollt – von der Einrichtung ausgeht, in der sie untergebracht ist. Sich auf die Einwilligung zu berufen ist daher nicht immer angemessen.

Ebenso wird sich die betreute Person nicht unbedingt in der Lage fühlen, von ihrem Widerspruchsrecht Gebrauch zu machen – auch wenn ihr der Gedanke, überwacht zu werden, Unbehagen bereitet. Daher lässt sich eine Datenbearbeitung nicht einfach als rechtmässig bezeichnen, nur weil sie die Grundsätze des DSG einhält und die betroffene Person keinen Widerspruch eingelegt hat.

Darüber hinaus kann bei betreuten Personen, die nicht urteilsfähig sind, ohnehin keine Einwilligung eingeholt werden: Angesichts des intimen Charakters der Datenbearbeitung (an einem Ort, wo die Person dauerhaft lebt) dürfte die Einwilligung *a priori* nicht durch einen Vertreter erteilt werden können (es sei denn, es handelt sich um einen medizinischen Eingriff, bei dem die Einwilligung der Angehörigen zum Tragen kommen kann).

Zusammenfassend lässt sich sagen, dass weder die Lösung mittels Einwilligung (Opt-in) noch die Lösung mittels Widerspruchs (Opt-out) als Grundlage für die Rechtfertigung einer Überwachung ausreichen – auch wenn es wünschenswert ist, die Einwilligung einzuholen, wann immer dies möglich ist. Eine Einrichtung, die eine solche Überwachung einführen möchte, muss daher ein überwiegendes Interesse nachweisen können. Obwohl Artikel 31 Absatz 1 DSG lediglich das überwiegende Interesse des für die Datenbearbeitung Verantwortlichen erwähnt, ist unbestritten, dass dieses Interesse auch das der betroffenen Person sein kann, insbesondere im Bereich der Pflege. Daher muss das vorrangige Ziel jedes Überwachungssystems darin bestehen, die Patientenversorgung zu verbessern[3]. Auf diese Frage wird im nächsten Kapitel näher eingegangen.

3. Grundsatz der Zweckmässigkeit

Dieser Grundsatz schreibt vor, dass Daten nur für einen bestimmten Zweck bearbeitet werden dürfen, der den betreffend die Datenbeschaffung erhaltenen Informationen entspricht. Bevor also ein Überwachungssystem eingerichtet wird, muss die betreffende Einrichtung die damit angestrebten Ziele klar definieren. Wie oben erwähnt, müssen diese

[3] Andere Aspekte, wie beispielsweise die Sicherheit des Personals oder anderer Patienten, können eine Rolle spielen; auf diese Frage wird in diesem Beitrag jedoch nicht näher eingegangen, da er sich auf die Betreuung der gepflegten Person konzentriert.

Ziele in erster Linie dem Wohl der betreuten Person dienen und Vorrang vor jeglicher potenziellen Verletzung ihrer Persönlichkeit haben. Aus dieser Perspektive und angesichts der Intensität der Datenbearbeitung, die diese Überwachungsmassnahmen mit sich bringen, reichen Gründe zur rein logistischen oder organisatorischen Verbesserung (z. B., um festzustellen, ob ein Bett gemacht ist oder eine Mahlzeit beendet ist usw.) jedoch nicht aus. Darüber hinaus muss ein Zweck aus konkretem Anlass verfolgt werden: Es ist nicht zulässig, eine systematische Überwachung einzuführen, ohne dass dabei die jeweilige Situation der betreuten Person berücksichtigt wird. Umso mehr darf dies am Ende nicht zu einer Verschlechterung der Betreuungsqualität führen (etwa, wenn die Pflegekräfte aufgrund des Überwachungssystems weniger im Zimmer präsent sind, wenn sich dies negativ auf die psychische Gesundheit der betreuten Person auswirkt).

Auch öffentliche Einrichtungen sind an den Grundsatz der Zweckmässigkeit gebunden. Auch sie müssen deshalb bereits vor dem Einsatz der Überwachungssysteme klar definieren, zu welchen Zwecken die Überwachung stattfinden soll. Es dürfen jedoch nur Ziele verfolgt werden, die auch von der Rechtsgrundlage abgedeckt sind. In diesem Sinne sind die zulässigen Zwecke durch die jeweiligen Rechtsgrundlagen beschränkt.

4. Grundsatz der Verhältnismässigkeit

Der Grundsatz der Verhältnismässigkeit ist von entscheidender Bedeutung. Er verlangt, dass nur jene Daten bearbeitet werden dürfen, die zum Erfüllen des angestrebten Zwecks erforderlich sind. Der Grundsatz gliedert sich in drei Elemente:

- Eignung: Das eingesetzte Mittel muss geeignet sein, den angestrebten Zweck zu erfüllen.
- Erforderlichkeit: Von denjenigen Massnahmen, mit denen der angestrebte Zweck erfüllt werden kann, ist die am wenigsten einschneidende zu wählen.
- Zumutbarkeit: Es muss ein angemessenes Verhältnis zwischen dem angestrebten Zweck und der Intensität der durchgeführten Datenbearbeitung vorliegen.

In der Praxis bedeutet dies stets, dass die Intensität der Datenbearbeitung (permanente, langfristige, in die Privatsphäre eingreifende Überwachung, hochauflösende Bilder, Echtzeitüberwachung, Ton, Kombination verschiedener Überwachungssysteme usw.) gegen deren Wirksamkeit abgewogen werden muss. Je stärker eine Datenbearbeitung in die Privatsphäre der betroffenen Person eingreift, desto grösser muss die Wirksamkeit und desto wichtiger der angestrebte Zweck sein. Wie bereits im Abschnitt «Grundsatz der Zweckmässigkeit» erwähnt, reichen rein organisatorische Verbesserungen nicht aus.

Neben der Art der eingerichteten Überwachung müssen mehrere weitere Faktoren berücksichtigt werden:

- **Datenminimierung**: Es ist wichtig, die Menge der bearbeiteten Daten so weit wie möglich zu reduzieren. Daher sind die weiter oben vorgestellten Lösungen zur indirekten Überwachung zu bevorzugen (Kap. II).
- **Konfigurationsmöglichkeiten**: Die angebotenen Lösungen verfügen möglicherweise über Funktionen, die über die Anforderungen des jeweiligen

Anwendungsfalls hinausgehen (Zoomfunktion, Tonaufnahme, Qualität der Rohdaten usw.). Falls es nicht möglich ist, zugunsten einer einfacheren Lösung darauf zu verzichten (weil diese Zusatzfunktionen beispielsweise in bestimmten Situationen erwünscht sein können), ist es unerlässlich, das System so zu konfigurieren, dass diese Zusatzfunktionen standardmässig deaktiviert werden, um keine unnötigen Daten zu generieren.

- **Datenaufbewahrung:** Die Aufbewahrung von Daten – sowohl Rohdaten als auch bereinigte Daten – über einen mehr oder weniger langen Zeitraum stellt einen erheblichen Risikofaktor dar. Grundsätzlich ist es im Rahmen der Überwachung im Bereich der Pflege nicht gerechtfertigt, die Daten über die Dauer der technischen Bearbeitung hinaus aufzubewahren (den Zeitraum also, den die IT-Prozesse benötigen, um die Daten zu bearbeiten und zu übermitteln). In jedem Fall muss eine Aufbewahrung einem konkreten und legitimen Zweck dienen; Aspekte der Praktikabilität alleine reichen nicht aus.
- **Beschränkung auf Einzelfälle**: Die Überwachung darf nicht systematisch auf alle betreuten Personen angewendet werden; jede Massnahme muss individuell begründet und regelmässig neu bewertet werden.
- **Einbindung in ein Netzwerk**: Die Möglichkeit des Zugriffs auf das System über ein (internes oder externes) Netzwerk und generell seine Einbindung in ein Netzwerk erhöhen das Risiko von Fehlern oder Cyberangriffen erheblich. Man sollte diese Möglichkeiten daher so weit wie möglich einschränken oder ganz darauf verzichten. Der Zugriff auf die Systeme muss einheitlich festgelegt und auf einen restriktiv definierten Personenkreis beschränkt sein.

Einige Beispiele:

- **Sturzmelder im Zimmer**: Die Vorrichtung muss über einen im Zimmer erreichbaren Schalter deaktiviert werden können, insbesondere bei der Anwesenheit von Pflegepersonal oder Angehörigen. Angesichts des verfolgten Zwecks ist sein Betrieb in Anwesenheit anderer Personen nicht gerechtfertigt.
- **Alarm bei einem Zwischenfall:** Wenn das System darauf ausgelegt ist, bestimmte Vorfälle wie Stürze zu erkennen, um anschliessend einen **Alarm** auszulösen, ist die Übertragung von hochauflösenden Bildern an das Pflegepersonal nicht erforderlich (vorbehaltlich besonderer Anforderungen in der Intensiv- und Akutpflege). Ein akustischer oder optischer Alarm reicht daher in den meisten Anwendungssituationen aus (siehe auch Kap. II).
- **Prävention von Stürzen aus dem Bett**: Je nach medizinischer Beurteilung der konkreten Situation kann der Einbau von versenkbaren Seitengittern eine Alternative zu Sensoren darstellen.

5. Auswahl der Technologie

Im Rahmen einer indirekten (situativen) digitalen Überwachung wirft die Auswahl der Überwachungstechnologie spezifische Fragen auf. Die Datenbearbeitung erfolgt in zwei Schritten: zuerst die Erfassung der Rohdaten, danach die Übermittlung der bereinigten

Daten. Grundsätzlich dürfen die Rohdaten nicht zugänglich sein und dienen ausschliesslich dazu, bereinigte Daten zu erstellen. Sie haben keine andere Bestimmung und dürfen auch nicht für andere Zwecke verwendet werden. Die bereinigten Daten wiederum werden entsprechend den Anforderungen aufbereitet (Piktogramme oder Alarme), und jede der oben genannten Technologien (optisch, Infrarot, Radar) stellt vergleichbare bereinigte Daten bereit.

Daher ist die Wahl der zugrunde liegenden Technologie aus Sicht der Anforderungen der Einrichtung nicht entscheidend, da jedes System ähnliche Leistungen bietet[4]. Dazu einige Anmerkungen.

Das DSG kennt den Grundsatz des Datenschutzes durch technische Ausgestaltung (*Privacy by Design*). In den kantonalen Gesetzen wird dieser Grundsatz zwar nicht ausdrücklich erwähnt; allerdings sehen diese Gesetze regelmässig die Konsultation oder sogar die Einbeziehung der kantonalen Beauftragten in die Projektentwicklung vor, sodass dieser Grundsatz dennoch Beachtung findet. Zudem überschneidet sich dieser Grundsatz teilweise mit demjenigen der Datensicherheit, der in den kantonalen Gesetzen vorgesehen ist (siehe weiter unten). Es handelt sich um einen übergreifenden Grundsatz, der den für die Datenbearbeitung Verantwortlichen verpflichtet, die jeweilige Lösung für die Datenbearbeitung so zu konzipieren, dass der Datenschutz und insbesondere die oben genannten Grundsätze gewahrt bleiben. In diesem Sinne stellt dies ebenfalls eine Möglichkeit dar, den Grundsatz der Verhältnismässigkeit zu gewährleisten.

Deshalb müssen die für die Datenbearbeitung Verantwortlichen Lösungen und Technologien wählen, die dem Stand der Technik entsprechen und der Art, dem Umfang und dem Zweck der Datenbearbeitung sowie den Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Personen angemessen sind. Dies gilt auch für die Rohdaten, die je nach verwendeter Technologie qualitative und quantitative Unterschiede aufweisen: siehe die Ausführungen im technischen Teil zu den jeweiligen Möglichkeiten und Risiken der einzelnen Technologien (Kap. II). In diesem Zusammenhang ist die Angemessenheit der Datenbearbeitung hinsichtlich der Art und des Umfangs stets in Bezug auf den konkreten Zweck zu beurteilen[5]. Die gewählte Technologie muss ein ausreichendes Mass an Zuverlässigkeit gewährleisten, um den angestrebten Zweck zu erfüllen – nämlich bei Bedarf einen Alarm auszulösen – und gleichzeitig Fehlalarme zu begrenzen, da jeder Fehlalarm einen Einsatz des Personals und möglicherweise eine ungerechtfertigte Verletzung der

[4] Hier werden «einfache» Situationen betrachtet, in denen bei Stürzen oder anderen auffälligen Verhaltensweisen Piktogramme bzw. Alarme generiert werden. Je nach Technologie können verschiedene Parameter überwacht werden, wie beispielsweise die Körpertemperatur oder die Herzfrequenz. Wenn die Einrichtung aus bestimmten Gründen tatsächlich genau diese Parameter überwachen möchte, kann die Auswahl einer bestimmten Technologie angezeigt sein. Zu beachten ist allerdings, dass diese spezifischen Parameter eben auch anders überwacht werden können (Thermometer oder am Handgelenk befestigter Pulsmesser).

[5] Eine Anmerkung zu optischen Kameras mit Übertragung in Echtzeit: Diese Lösung kann auf einer Intensivstation unter Umständen gerechtfertigt sein, wenn sie einem eindeutig festgestellten klinischen Bedarf entspricht und es dem Personal angesichts der räumlichen Gegebenheiten nicht möglich ist, die verschiedenen Patienten im Blick zu behalten.

Privatsphäre der betreuten Person zur Folge hat. Organisatorische und finanzielle Aspekte können in die Gesamtbetrachtung einfliessen, dürfen jedoch keinen Vorrang vor der Verpflichtung zum Schutz der Grundrechte haben. In diesem Sinne sind auch Massnahmen zu berücksichtigen, die ergriffen werden, um allfällige negative Folgen oder Risiken zu bewältigen, die mit einer bestimmten Wahl – beispielsweise technologischer Art – einhergehen. Die Angemessenheit einer Lösung muss daher als Ganzes und im Kontext bewertet werden.

Zudem sehen sowohl das Datenschutzgesetz des Bundes als auch die kantonalen Gesetze den Grundsatz der Datensicherheit vor. Im vorliegenden Zusammenhang bedeutet dies, dass mithilfe konkreter Massnahmen ein Zugriff auf die Rohdaten tatsächlich ausgeschlossen werden muss, auch während Wartungsarbeiten oder Software-Updates (ausgenommen sind technische Zugänge, bei denen ein direkter physischer Anschluss an den Sensor möglich ist, um dessen ordnungsgemässe Funktion zu prüfen). Die für die Datenbearbeitung Verantwortlichen müssen dies jederzeit nachweisen und sich dabei auf ausreichend detaillierte Beschreibungen der Hersteller stützen und gegebenenfalls ihre eigenen ergänzenden Überprüfungen dokumentieren können (zu den Dokumentationspflichten siehe Punkt IV weiter unten). Andernfalls ist der Einsatz der betreffenden Überwachungssensoren als unzulässig anzusehen, unabhängig davon, ob sie auf optischer, Infrarot- oder Radartechnologie basieren. Sollten hier Lücken bestehen, lässt sich dies weder durch die Einwilligung noch durch das überwiegende private oder öffentliche Interesse rechtfertigen.

Letztendlich verfügen die Einrichtungen über einen gewissen Spielraum bei der Auswahl der eingesetzten Technologien und Funktionen, die wiederum die Intensität der Datenbearbeitung und der Überwachung beeinflussen. Die Grundsätze von *Privacy by Design* und Datensicherheit erfordern, dass die getroffenen Entscheidungen im Hinblick auf die verfolgten Zwecke und die Umsetzungsbedingungen begründet und dokumentiert werden. Konkret bedeutet dies: Wenn eine Pflegeeinrichtung die Anschaffung einer solchen Lösung plant, muss das Projekt von Anfang an entsprechend gesteuert werden. Die Projektleitung muss die Schlüsselpersonen (Datenschutzberater, Rechtsabteilung, Führungskräfte, Techniker, Pflegepersonal usw.) bereits in der ersten Planungsphase einbeziehen; sie muss das für die jeweilige Situation geeignete Produkt auswählen und für jede in Betracht gezogene Alternative eine Bewertung der systemischen und spezifischen Risiken vornehmen und die Konfigurationsmöglichkeiten prüfen. Die Projektleitung darf sich nicht allein auf Marketingunterlagen verlassen, sondern muss vom Lieferanten die erforderlichen technischen Informationen einholen, um die Bearbeitung zu dokumentieren, die Risiken zu ermitteln und Massnahmen zu deren Begrenzung festzulegen. Die Projektleitung muss die Führungskräfte transparent über die Restrisiken informieren, damit diese in voller Kenntnis der Sachlage entscheiden können. Die Pflegeeinrichtung muss sich vor dem Kauf, bei der Einführung und auch danach laufend von der Datenschutzkonformität des Produkts vergewissern.

6. Chilling Effect

Unter dem Gesichtspunkt der Verhältnismässigkeit ist auch zu berücksichtigen, dass Überwachung eine Einschüchterung (*Chilling Effect*) bewirken kann. Schon allein das

Wissen, dass ein solches Überwachungssystem eingesetzt wird, kann das Verhalten der betroffenen Personen beeinflussen.

Dabei denkt man primär an die betreute Person. Auch wenn der Einsatz des Systems gerechtfertigt ist und die Person umfassend über dessen Funktionsweise und Grenzen informiert wurde, kann das Bewusstsein, überwacht zu werden, ein Unbehagen auslösen und das Verhalten der Person beeinflussen. Dies kann aber auch das Pflegepersonal und die Besucher betreffen – falls das System auch in ihrer Anwesenheit in Betrieb bleibt. Für die Pflegekräfte können die Auswirkungen besonders nachteilig sein, da das Bewusstsein einer Überwachung ihr Verhalten und letztlich die Qualität der Betreuung beeinträchtigen kann.

7. Künstliche Intelligenz

Auch bei der Überwachung im Pflegebereich kommt zunehmend künstliche Intelligenz zum Einsatz. Bei Lösungen zur indirekten Überwachung kann die Vorbearbeitung der Daten durch KI dazu beitragen, die Datenmenge zu reduzieren, die aus dem Zimmer heraus übertragen werden, und somit auch die Menge an Informationen, die das Pflegepersonal tatsächlich zur Kenntnis nimmt (ein einfaches Piktogramm oder ein Alarmsignal).

Trotz dieser Vorteile wirft der Einsatz von KI weitere Probleme und Risiken auf. Der erste Aspekt betrifft den Ort der Datenbearbeitung: Die Bearbeitung der Daten durch die KI muss so weit wie möglich lokal erfolgen, und zwar im Zimmer der betreuten Person. Der Einsatz von Cloud-Lösungen ist heikel: Er birgt nämlich spezifische Risiken im Zusammenhang mit der Zugänglichkeit der Daten (insbesondere für den Cloud-Anbieter). Es müsste somit nachgewiesen werden, dass «On-Premise»-Lösungen nicht in Frage kommen (Komplexität, Kosten usw.) und dass die Grundsätze von Verhältnismässigkeit, Sicherheit und *Privacy by Design* weiterhin gewährleistet sind. Es stellt sich zudem die Frage nach der Weiterverwendung dieser Daten für das Training von KI-Systemen. Dies bringt zusätzliche Risiken mit sich: Weitergabe von Daten ausserhalb des eigentlichen Rahmens der Pflege, Risiken der Reidentifizierung sowie Risiken im Zusammenhang mit der Speicherung und der Sicherheit der Daten. Gleichzeitig ist das KI-Training der Modelle nicht direkt auf den konkreten Bedarf der betreuten Person in ihrer aktuellen Situation ausgerichtet. Auch wenn eine solche Weiterverwendung transparent angekündigt wird, bleibt sie unter dem Gesichtspunkt der Verhältnismässigkeit problematisch, sofern diese Bearbeitung für die Betreuung der Person weder geeignet noch notwendig ist. Dies würde die Datenbearbeitung unzulässig machen, solange kein Rechtfertigungsgrund geltend gemacht werden kann. Angesichts des Kontexts und der Intensität der Datenbearbeitung dürfte es jedoch schwierig sein, diese Weiterverwendung mit einem überwiegenden Interesse zu begründen. Es bliebe also die Einwilligung der betreuten Person, wobei alle oben genannten Einschränkungen zu berücksichtigen sind[6] (vgl. Kap. III. 2).

[6] Soweit Algorithmen und künstliche Intelligenz mit Rohdaten trainiert worden sind, welche im Ausland beschafft worden sind, fällt dies in die Verantwortung der Hersteller, zumal die Rechtmässigkeit von

8. Weitere Aspekte

Im Zusammenhang mit der Überwachung sind noch weitere Aspekte zu berücksichtigen, von denen einige über den Rahmen des Datenschutzes hinausgehen. Im Folgenden werden diese Aspekte kurz umrissen, ohne jedoch näher darauf einzugehen.

Zunächst einmal sind – wie bereits erwähnt – neben den betreuten Personen auch andere Personen von solchen Überwachungsmassnahmen betroffen, insbesondere die Besucher und das Personal der Einrichtung. Auch diese müssen ordnungsgemäss über die Existenz dieser Systeme und gegebenenfalls über Möglichkeiten zu ihrer Deaktivierung informiert werden. Bezüglich des Personals sind die Vorschriften zur Überwachung im Arbeitsverhältnis zu beachten.

Es stellt sich ausserdem die Frage nach der Überwachung von Bereichen, die von mehreren betreuten Personen gemeinsam genutzt werden (insbesondere Gemeinschaftswohnungen/-zimmer und Badezimmer). Ohne näher auf die Frage einzugehen ist klar, dass solche Situationen schwierig sein können. Wie bereits erwähnt, muss die Überwachung auf den konkreten Fall abgestimmt sein. Ist die Überwachung daher für die übrigen betreuten Personen weder vom Grundsatz noch vom Umfang her gerechtfertigt, dürfte wohl darauf verzichtet werden müssen.

Weiterhin können solche Überwachungsmassnahmen unter gewissen Umständen als ärztliche Anordnungen betrachtet werden. Es sind deshalb die in solchen Fällen geltenden Vorschriften zu berücksichtigen, insbesondere was die Einwilligung betrifft (hypothetische, vermutete oder stellvertretende Einwilligung). In anderen Fällen wiederum kommen sie Zwangsmassnahmen gleich, die die Freiheit der betreuten Person einschränken. Auch hier können besondere Vorschriften zur Anwendung kommen.

Werden zur Überwachung Dritte beigezogen, bleiben die Einrichtungen für die Datenbearbeitung vollständig verantwortlich. Eine solche Auslagerung der Datenbearbeitung liegt beispielsweise vor, wenn ein Tool eines Dienstleisters für die Überwachung oder eine Cloud-Lösung eingesetzt wird. Es sind dabei die konkreten rechtlichen Voraussetzungen für die Datenbearbeitung durch Dritte zu beachten. Die beigezogenen Dritten dürfen die Daten nur so bearbeiten, wie es die Einrichtung selbst darf. Dabei können neben den Risiken durch die erweiterten Zugriffsmöglichkeiten und den grösseren Personenkreis zusätzliche Risiken entstehen, wenn die Datenbearbeitung im Ausland stattfindet. In diesen Fällen untersteht der Auftragsbearbeiter unter Umständen einer Rechtsordnung, die kein angemessenes Datenschutzniveau garantiert. Dies ist bei der Definition von technischen und organisatorischen Massnahmen einzubeziehen.

9. Datenschutz-Folgenabschätzung und Vorabkonsultation

Bearbeitungen nach ausländischem Recht für die Bearbeitungsverantwortlichen in der Schweiz schwer nachvollziehbar ist.

Mit einer Datenschutz-Folgenabschätzung (DSFA) können Datenschutzrisiken erkannt und bewertet werden. Zusätzlich kann sie helfen, die Verhältnismässigkeit einzuschätzen und Massnahmen zu ermitteln, welche die Intensität der Datenbearbeitung senken.

Sowohl das DSG als auch die meisten kantonalen Datenschutzgesetze sehen vor, dass Verantwortliche unter bestimmten Voraussetzungen eine DSFA erstellen müssen.

Private Einrichtungen, die dem DSG unterstehen, müssen gemäss Art. 22 Abs. 1 DSG eine DSFA erstellen, wenn die Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann. Ein solches Risiko kann insbesondere dadurch indiziert sein, dass in grossem Umfang besonders schützenswerte Personendaten bearbeitet werden.

Die Pflicht zur Erstellung einer DSFA für öffentliche Einrichtungen richtet sich nach den anwendbaren kantonalen Bestimmungen. Gewisse Kantone sehen vor, dass bei jeder neuen geplanten Datenbearbeitung eine DSFA erstellt werden muss, während andere Kantone analog den bundesrechtlichen Bestimmungen nur dann die Erstellung einer DSFA verlangen, wenn die geplante Datenbearbeitung voraussichtlich ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringt.

Eine DSFA enthält grundsätzlich eine Ausführung des Zwecks der Datenbearbeitung, eine Beschreibung der geplanten Bearbeitung (Auflistung der Datenbearbeitungsschritte und der Bearbeitungsorte) und eine Bewertung der Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Person (Bewertung der Eintretenswahrscheinlichkeit und des erwarteten Schadensausmasses). Für die erkannten Risiken sollten zudem Massnahmen definiert und ebenfalls in der DSFA aufgeführt werden. Mit Hilfe einer solchen DSFA können die für die Betroffenen mit der Datenbearbeitung einhergehenden Auswirkungen bereits in der Planungs- und Entwicklungsphase berücksichtigt und die Verhältnismässigkeit besser eingeschätzt werden. Die Erstellung einer DSFA kann sich insbesondere auch bei massgeblichen Veränderungen bestehender Bearbeitungen z.B. infolge der Ablösung manueller Arbeiten oder Einführung neuer Technologien als nötig erweisen. Diesfalls muss die DSFA einen quantitativen und qualitativen Vergleich der bestehenden und geplanten Bearbeitungen enthalten.

Artikel 23 Absatz 1 DSG sieht vor, dass beim EDÖB im Sinne einer Vorabkonsultation eine Stellungnahme einzuholen ist, wenn trotz der getroffenen Massnahmen noch ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen besteht. Im Bestreitungsfall kann der EDÖB eine solche auch von Amtes wegen abgeben. Auch die kantonalen Datenschutzgesetze sehen jeweils eine Vorabkontrolle vor, wobei die Voraussetzungen je nach anwendbarem Recht der kantonalen Datenschutzbehörden leicht variieren können. Da die Vorabkontrolle jeweils vor dem Beginn der geplanten Datenbearbeitung durchzuführen ist, sollte entsprechend Zeit eingeplant werden.

IV. Dokumentationspflicht und TOM

In jedem Fall müssen die für die Datenbearbeitung Verantwortlichen bereits zu Beginn des Projekts einen Vergleich der alternativen Lösungen mit einer Risikobewertung unter dem Gesichtspunkt des Datenschutzes vornehmen. Diese Arbeiten sind schriftlich zu dokumentieren und müssen im Laufe des Projekts fortlaufend ergänzt sowie nach der Einführung des Systems regelmässig überprüft werden.

Insbesondere müssen geeignete technische und organisatorische Massnahmen (TOM) umgesetzt werden (Verschlüsselung, Zugriffskontrolle, Protokollierung).

V. Checkliste

1. Ermittlung des Bedarfs, insbesondere unter dem Gesichtspunkt des Rechtfertigungsgrunds. Frühzeitige Einbindung der zuständigen Fachleute (Juristen, Datenschutzberater, IT-Fachleute, Pflegefachpersonen usw.).

2. Vergleich alternativer Lösungen, insbesondere unter dem Gesichtspunkt der zugrunde liegenden Technologie, Risikobewertung (sowohl in technischer als auch in rechtlicher Hinsicht).

3. Sicherstellung, dass die Fähigkeiten der gewählten Lösung und gegebenenfalls die Konfigurationsmöglichkeiten verstanden werden.

4. Erarbeitung eines kohärenten Umsetzungskonzepts und entsprechender Nutzungsreglemente (wann muss die Überwachung aktiviert werden, wer hat Zugriff auf die Daten, wie müssen die betreuten Personen informiert werden, allfällige Einwilligung usw.).

5. Schulung des Personals.

6. Konkrete Umsetzung (Informationstafeln usw.).

7. Konzept zur Kontrolle und Neubewertung des Systems.

Während des gesamten Prozesses: Erstellung, Ergänzung und laufende Aktualisierung der relevanten Unterlagen, insbesondere von Risikoanalysen, Reglementen usw.

16.09.2026