Bundesamt
für Sicherheit in der
Informationstechnik

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Common Criteria Protection Profile
Software zur Verarbeitung[1] von personenbezogenen Bilddaten

BSI-PP-0023

Version 2.0, 15.01.2007

[1] Verarbeitung umfasst das Erheben, Speichern, Löschen und Nutzen.

Inhaltsverzeichnis

1 PP-Einführung

1.1 PP-Identifikation

1	PP-Name:	Schutzprofil (Protection Profile) für Software zur Verarbeitung[2] von personenbezogenen Bilddaten
2	Zertifizierungs-ID:	BSI-CC-PP-0023
3	PP-Version:	2.0
4	Datum:	15.01.2007
5	Antragsteller:	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Bonn
6	Autoren:	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Bonn Bundesamt für Sicherheit in der Informationstechnik, Bonn
7	EVG-Name:	Software zur Verarbeitung von personenbezogenen Bilddaten
8	CC-Version:	2.3

1.2 PP-Übersicht

9 Dieses auf den Common Criteria basierende Schutzprofil (Protection Profile – PP) thematisiert die Mindestanforderungen, die an die Software zur Verarbeitung von personenbezogenen Bilddaten gestellt werden, um einerseits den datenschutzrechtlichen Bestimmungen zu genügen und andererseits eine anwenderfreundliche Bedienung der IT-Sicherheit moderner Videoüberwachungsanlagen zu ermöglichen.

10 Die in diesem Dokument charakterisierte datenschutzkonforme Videoüberwachungsanlage kann Bilddaten von an den EVG angeschlossenen Signalaufnahmekomponenten empfangen und auf Authentizität (Herkunft der Daten) prüfen. Einmal gespeicherte Bilddaten stehen unter der Kontrolle des EVG, bis sie gemäß der maximalen Aufbewahrungsfrist automatisch gelöscht werden. In dieser Zeit können über den EVG nur registrierte Benutzer auf die Bilddaten zugreifen. Abhängig von der Rolle des jeweiligen Benutzers (z.B. Beobachter oder Revisor/bDSB) erlaubt der EVG den Export von Bilddaten aus dem EVG heraus oder auch das Löschen einzelner Bilddaten. Für alle datenschutzrelevanten Benutzer-Aktionen fordert der EVG vor Durchführung der Aktion zur Eingabe einer Begründung auf, welche in den Protokolldaten gespeichert wird. Neben diesen Benutzer-Aktionen und Begründungen protokolliert der EVG auch seinen Start und seinen Stopp sowie Beginn und Ende eines Bildausfalls einer Signalaufnahmekomponente.

---

[2] Verarbeitung umfasst das Erheben, Speichern, Löschen und Nutzen.

11 Die Protokolldaten stehen nach der Erzeugung und Speicherung unter der Kontrolle des EVG. Der EVG ist dazu in der Lage, nicht autorisierte Manipulationen an den Protokolldaten zu erkennen.

12 Der hier beschriebene EVG schützt die Bilddaten erst nach dem Empfang. Die EVG Umgebung muss dafür sorgen, dass die Bilddaten vertraulich und integer sowie authentisch (Aufnahme aus zulässigem Bereich und Kamera hat Realität erfasst) beim EVG ankommen. Weiterhin vertraut der EVG auf einer physikalisch abgesicherten Einsatzumgebung, korrekte Konfiguration der Hardware und auf vertrauenswürdiges Bedienpersonal.

13 Ein Schutzprofil stellt dabei gemäß [CC-Teil1] eine implementierungsunabhängige Menge von Sicherheitsanforderungen an eine Kategorie von IT-Produkten oder IT-Systemen zusammen, die besondere Bedürfnisse der Anwender erfüllen. Relevante Eigenschaften, die bei einer konkreten Hersteller-Lösung über diese im Schutzprofil formulierten Mindestanforderungen hinausgehen, können in den Sicherheitsvorgaben (Security Target – ST) spezifiziert werden, welche die Basis für eine Zertifizierung eines konkreten Produktes darstellen und die Konformität zu diesem Schutzprofil postulieren können.

14 Die softwaregestützte automatisierte Verarbeitung von Bilddaten umfasst gemäß §3 Bundesdatenschutzgesetz ([BDSG]) die Erhebung (also die Aufnahme), die Verarbeitung (vorrangig Speichern und Löschen) und die Nutzung (z. B. die Auswertung/Suche) von Bilddaten.

15 Die Anforderungen an die Vertrauenswürdigkeit, welche vom EVG erfüllt werden müssen, entsprechen der Vertrauenswürdigkeitsstufe EAL1.

1.3 PP-Organisation

16 Die wesentlichen Bestandteile des Schutzprofils (Protection Profile – PP) sind

- die EVG-Beschreibung,
- die EVG-Sicherheitsumgebung,
- die Sicherheitsziele,
- die IT-Sicherheitsanforderungen und
- der Erklärungsteil.

17 Die EVG-Beschreibung (Abschnitt 2) liefert allgemeine Informationen über den Evaluationsgegenstand (EVG), wie etwa den beabsichtigten Gebrauch und die Darstellung der zu schützenden Werte. Sie ist die Voraussetzung zum Verständnis der Sicherheitsanforderungen. Dabei ist zu beachten, dass sich ein PP in der Regel nicht auf eine spezielle Implementierung bezieht, sondern eine Klasse gleichartiger Produkte beschreibt.

18 Die EVG-Sicherheitsumgebung (Abschnitt 3) legt in den Annahmen die Sicherheitsauflagen an die Umgebung, in der der Evaluationsgegenstand eingesetzt werden soll, dar. Dieses Kapitel kann als Auflagenkatalog an den Betreiber des EVG angesehen werden. In den Abschnitten Bedrohungen und organisatorische Sicher-

heitspolitiken werden die vom EVG abzuwehrenden Bedrohungen und die umzusetzenden Sicherheitspolitiken aufgeführt, welche sich aus den datenschutzrechtlichen Rahmenbedingungen (vgl. Anhang A) ableiten.

19 Abschnitt 4 definiert die Sicherheitsziele für den EVG und dessen Umgebung. Die Sicherheitsziele müssen auf alle identifizierten Sicherheitsumgebungsaspekte eingehen. Die Sicherheitsziele müssen die dargelegte Absicht widerspiegeln und geeignet sein, allen identifizierten Bedrohungen entgegenzuwirken und alle organisatorischen Politiken und Annahmen abzudecken.

20 Die IT-Sicherheitsanforderungen (Abschnitt 5) beinhalten funktionale Sicherheitsanforderungen an den EVG und seine Umgebung und Anforderungen an die Vertrauenswürdigkeit.

21 Der Erklärungsteil (Abschnitt 6) des PP stellt den Nachweis zur Prüfung und Bewertung des PP dar. Dieser Nachweis unterstützt die Postulate, dass das PP eine vollständige und in sich geschlossene Menge von Anforderungen ist und dass ein zu diesem PP konformer EVG eine wirksame Menge von IT-Sicherheitsmaßnahmen in der festgelegten Sicherheitsumgebung bereitstellt.

22 Die Anhänge sind nicht mehr Bestandteile der Schutzprofilkapitel nach CC. Sie referenzieren die gesetzlichen Texte, die bei der Erstellung dieses Schutzprofils relevant waren. Hinweise zu den datenschutzrechtlichen Rahmenbedingungen sind im Anhang A aufgeführt.

23 Ein den Common Criteria genügendes Schutzprofil erfüllt gewisse Anforderungen hinsichtlich Form, Notation und Aufbau. Ein Glossar mit Erläuterungen zu den wichtigsten Abkürzungen der CC findet sich in den Abschnitten 1.4 und 1.5.

24 Zum besseren Verständnis des Schutzprofils sind Anwendungsbemerkungen eingearbeitet. Diese richten sich an den Leser eines PP und beinhalten Informationen, die nicht der Evaluation des Schutzprofils unterliegen und nur kommentierenden Charakter haben.

1.4 Abkürzungen

BD	Bilddaten
bDSB	betrieblicher/behördlicher Datenschutzbeauftragter
BDSG	Bundesdatenschutzgesetz
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BSI	Bundesamt für Sicherheit in der Informationstechnik
CC	Common Criteria
EAL	Evaluation Assurance Level (Vertrauenswürdigkeitsstufe)
EVG	Evaluationsgegenstand (Target of Evaluation – TOE)
PD	Protokolldaten
PP	Protection Profile (Schutzprofil)

SFP	funktionale Sicherheitspolitik
ST	Security Target (Sicherheitsvorgaben)
TOE	Target of Evaluation (Evaluationsgegenstand – EVG)
TSC	TSF Scope of Control (Anwendungsbereich der TSF-Kontrolle)
TSF	TOE Security Function (EVG-Sicherheitsfunktionen)

1.5 Glossar

Authentizität der Bilddaten — Mit diesem Attribut eines empfangenen Bildes kann festgestellt werden, von welcher angeschlossenen Signalaufnahmekomponente das Bild aufgenommen wurde.

Bildschirmarbeitsplatz — Der Bildschirmarbeitsplatz kann in Abhängigkeit von der Rolle, die sich eingeloggt hat, für folgende 3 Aufgaben benutzt werden:

- Bildschirmarbeitsplatz für Beobachtung: Der EVG bietet einem autorisierten Beobachter auf diesem Bildschirmarbeitsplatz die Möglichkeit, den EVG zu nutzen (vgl. Abschnitt 3.1).
- Bildschirmarbeitsplatz für Administration: Der EVG bietet einem Administrator die Möglichkeit, auf diesem Bildschirmarbeitsplatz den EVG zu konfigurieren (vgl. Abschnitt 3.1).
- Bildschirmarbeitsplatz für Revision: Der EVG bietet einem Revisor oder betrieblichem/behördlichen Datenschutzbeauftragtem (bDSB) die Möglichkeit, auf diesem Bildschirmarbeitsplatz Beobachter und Administratoren zu kontrollieren, ihm vorbehaltene Einstellungen wie Löschfristen der Bilddaten zu ändern sowie einzelne (auf Anfrage des Betroffenen) Bilddaten zu löschen (vgl. Abschnitt 3.1).

Beobachter — Ein Beobachter kann die laufend angezeigten Bilddaten beobachten und kann eine Bildsuche entsprechend konkret einstellbarer Kriterien inklusive Anzeige durchführen. Er kann Bilddaten aus dem EVG exportieren und ausdrucken (als Spezialfall des Bilddatenexports).

Betriebsraum — Raum, in dem sich der Rechner befindet, auf dem der EVG läuft, und zu dem nur der Beobachter, der Administrator, der Revisor/bDSB und Fremdpersonal Zutritt haben.

Bilddaten — Bilddaten sind einzelne (live oder aufgezeichnete) Videobilder.

Attribute — Attribute sind alle Eigenschaften, die Bedingungen zur Verarbeitung von Bilddaten beinhalten wie etwa Datum, Uhrzeit, Kameranummer, Begründung etc.

Evaluationsgegenstand — Dieser, den CC entnommene Begriff (engl.: TOE – Target of Evaluation) bezeichnet das IT-Produkt, die IT-Komponente oder das

	IT-System, das auf Erfüllung aller Sicherheitsanforderungen zu evaluieren ist (vgl. Abschnitt 2).
Fremdpersonal	Personen, die Zutritt zum Betriebsraum des EVG haben müssen, aber keine Zugangs- oder Zugriffsberechtigung auf den EVG und EVG-Daten besitzen. Beispielsweise könnte es sich hier um Reinigungspersonal handeln.
Kamera	Siehe Signalaufnahmekomponente
Konfigurationsdaten	Die Konfigurationsdaten steuern die Benutzung des Systems (etwa durch Zugriffsrechte und Passwörter) sowie den Umfang der Protokollierung.
Löschzyklus	Bild- und Protokolldaten sind gemäß gesetzlicher bzw. betrieblicher Anforderungen zu einem gewissen Zeitpunkt zu löschen. Dieser Zeitpunkt wird „Löschzyklus“ genannt. Der Zeitpunkt kann sich nach einem Zeitintervall richten (z.B. nach 2 Wochen nach Erfassung der Daten) oder nach anderen Kriterien (z.B. wenn mehr als 2 GByte an Daten vorliegen)Die Löschzyklen für Bild- und Protokolldaten sind voneinander völlig unabhängig.
Passwort	Ein Passwort wird als Authentisierungsmerkmal eingesetzt und kann auch durch andere Mechanismen realisiert werden – etwa eine PIN oder biometrische Merkmale.
personenbezogen	Personenbezogene Daten sind nach §3 Abs. 1 BDSG „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).“
Protokolldaten	Protokolldaten erfassen, welcher Beobachter, Administrator resp. Revisor/bDSB den EVG wann zu welchem Zweck genutzt hat. Weiterhin werden wichtige Ereignisse (z.B. Start des EVG oder Ausfall einer Kamera) erfasst.
Sicherheitsfunktionen	EVG-Sicherheitsfunktionen ist der Teil des EVG, der zur Durchsetzung der Sicherheitspolitik verantwortlich ist.
Signalaufnahmekomponente	Da der übliche Begriff „Kamera“ häufig mehr beinhaltet als die reine Signalaufnahme, wird der Begriff Signalaufnahmekomponente eingeführt.
TSF-Daten	Von und für den EVG erstellte Daten, die den Betrieb des EVG beeinflussen können.
Videosequenzen	Mehrere zu einer Folge zusammengefügte Videobilder. Videosequenzen werden nicht anders als Bilddaten behandelt.

2 EVG-Beschreibung

25 Die EVG-Beschreibung enthält neben der Darstellung des Evaluationsgegenstandes (EVG) allgemeine Informationen über den EVG, wie etwa den beabsichtigten Gebrauch und die Darstellung der zu schützenden Werte.

2.1 EVG-Umfang

26 Der Evaluationsgegenstand (EVG) ist eine Softwarekomponente zur Verarbeitung und Speicherung der von Videoüberwachungskameras aufgenommenen Bilddaten. Der EVG läuft als Anwendung auf einem Rechner und benötigt selbst den Schutz durch die darunterliegende Plattform (wird in dem Kapitel *Annahmen* genauer erläutert).

27 Damit gehören die Videokameras selbst als reine Signalaufnahmekomponenten und mögliche Bildübertragungsstrecken explizit nicht zum EVG, aber zur IT-Einsatzumgebung des EVG, da ohne diese Komponenten der EVG keine Daten erhält. Weitere wichtige Komponenten der IT-Einsatzumgebung sind die IT-Plattform, auf der der EVG läuft, sowie die Bildschirmarbeitsplätze der Benutzer.

28 Zur Benutzung des EVG werden von ihm drei Schnittstellen zu Bildschirmarbeitsplätzen angeboten:

- Bildschirmarbeitsplatz für Beobachtung, mit dem ein Beobachter den EVG nutzen kann (vgl. Abschnitt 3.1)
- Bildschirmarbeitsplatz für Administration, in dem der Administrator den EVG konfigurieren kann (vgl. Abschnitt 3.1)
- Bildschirmarbeitsplatz für Revision (vgl. Abschnitt 3.1)

Anwendungsbemerkung 1 *Die Bildschirmarbeitsplätze können sowohl als eigenständige Softwarekomponenten als auch als Teil der Software realisiert sein, die den EVG enthält. Im letzteren Fall bedarf es in konkreten Sicherheitsvorgaben einer klaren Abgrenzung zwischen EVG Anteil und nicht-EVG Anteil der Software.*

Anwendungsbemerkung 2 *Die oben angeführten drei Schnittstellen stellen lediglich abstrakt die unterschiedlichen Zugriffsmöglichkeiten der unterschiedlichen Benutzer-Rollen dar. Auf einer konkreteren (technischen) Ebene kann es sich hierbei durchaus um eine einzige Schnittstelle handeln, wobei der EVG anhand der Benutzerdaten (z.B. Authentisierungsmerkmale) über die Verfügbarkeit bzw. Zulässigkeit von Funktionen entscheidet.*

Anwendungsbemerkung 3 *Das Schutzprofil geht von einem monolithischen EVG aus, so dass Bild- und Protokolldaten innerhalb des EVG sicher transferiert werden. Falls der EVG als verteiltes System realisiert wird, ist dies in den herstellerspezifischen Sicherheitsvorgaben zu berücksichtigen.*

29 Nicht zum Umfang des EVG gehören:

- die Komponenten zur Signalaufnahme (Objektiv, Bildauflösung, optionale Kamerasteuerung, etc.)
- die Übertragungswege zwischen Signalaufnahme und EVG
- Schalter/Sensoren/Sensorik, die über eine Schnittstelle von außen Signale an den EVG liefern – etwa zum Aufschalten einer externen Komponente zur Signalaufnahme oder Starten einer Aufzeichnung
- Managementsysteme, die über eine Schnittstelle Informationen mit dem EVG austauschen
- Drucker (wird als Datenexport auf einen Drucker angesehen, der nicht mehr unter der EVG-Kontrolle steht)
- Monitore
- interne Speichermedien (z.B. die Festplatten des Rechners, auf denen der EVG die Bilddaten speichert). Hierbei ist anzumerken, dass diese Speichermedien nicht Teil des EVG sind, die darauf gespeicherten Bild- und Protokolldaten sich jedoch noch im Anwendungsbereich der TSF-Kontrolle (TSC) befinden und damit unter der Kontrolle des EVG stehen.
- externe Speichermedien (etwa Videobänder, USB-Massenspeicher usw.) Abspeichern von Bilddaten auf diese Medien wird als Datenexport nach außen angesehen, also außerhalb der EVG-Kontrolle. Einmal exportierte Bilddaten werden nicht mehr vom EVG bzw. dessen Funktionen geschützt.

> ***Anwendungsbemerkung 4*** *Die in den Sicherheitsvorgaben einer konkreten Realisierung genutzte herstellerspezifische Nomenklatur für die Bestandteile des Evaluationsgegenstandes kann – mit entsprechenden Hinweisen – von den hier genannten Begriffen abweichen.*

30 Der EVG verfügt über die folgenden Typen von externen Schnittstellen:

- externe Schnittstelle für Empfang von Bilddaten
- externe Schnittstelle für Weitergabe sowie das Einlesen von abgespeicherten Bilddaten zwecks Verarbeitung
- externe Schnittstelle für Weitergabe sowie das Einlesen von abgespeicherten Protokolldaten zwecks Auswertung
- externe Schnittstelle für sonstige Signale (für Schalter, Sensoren, Sensorik, Managementsysteme u. ä.)
- externe Schnittstellen zum Benutzer (s.o. Bildschirmarbeitsplätze)

31 Der EVG ist in Abbildung 1 auf Seite 13 illustriert.

2.2 EVG-Sicherheitsleistung

32 Die Verarbeitung von personenbezogenen Bilddaten umfasst als automatisierte Verarbeitung gemäß §3 Bundesdatenschutzgesetz ([BDSG])

- das Erheben von Bilddaten (also die Aufnahme),
- das Verarbeiten von Bilddaten (vorrangig Speichern und Löschen) sowie
- das Nutzen von Bilddaten (z. B. die Auswertung/Suche).

33 Die Datenschutzbestimmungen zur Videoüberwachung enthalten dabei einerseits Aspekte, die technisch vom Evaluationsgegenstand und andererseits der Umgebung – technisch und organisatorisch – umzusetzen sind. Das Schutzprofil fordert zur Unterstützung eines gesetzeskonformen Umganges mit den Bilddaten einen Mindestsatz an Sicherheitseigenschaften.

34 Die Aufgabenbeschreibung an den EVG sieht wie folgt aus:

35 Außerhalb des EVG werden in der Signalaufnahmekomponente Bilddaten erzeugt. Um zu gewährleisten, dass bei der Übertragung zum EVG diese „*personenbezogenen Daten […] nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können*“ (Zugriffskontrolle gemäß Anlage zu § 9 Nr. 3 BDSG), werden zum Schutz der Bilddaten Anforderungen an einen vertrauenswürdigen Kanal gestellt. Nach erfolgreicher Prüfung der Authentizität der Bilddaten durch den EVG können die Bilddaten im Anwendungsbereich der TSF gespeichert und durch den EVG weiterverarbeitet werden, während bei fehlerhafter Prüfung dieses Ereignis (je nach Konfiguration) protokolliert und ein entsprechender Hinweis an den Beobachter, Administrator oder Revisor/bDSB gegeben wird. Der EVG ist weiterhin in der Lage, die Integrität gespeicherter Bilddaten zu prüfen und identifizierte Unstimmigkeiten (Manipulation, Löschen) je nach Konfiguration zu protokollieren sowie dem Benutzer zu melden.

> ***Anwendungsbemerkung 5*** *Maßnahmen in der Einsatzumgebung für sichere Übertragungswege sind beispielsweise bauliche Maßnahmen (Verlauf der Kommunikation in geschützten Räumen/Gebäuden) oder Einsatz einer geeigneten Verschlüsselung, die nicht Bestandteil des EVG sind.*

36 Die Bilddaten werden nach Ablauf der jeweiligen Speicherfrist automatisch gelöscht. Sollen Bilddaten über die vorgegebene Speicherdauer hinaus aufbewahrt werden, müssen diese vor dem automatischen Löschen vom Beobachter oder Administrator aus dem Anwendungsbereich der TSF heraus exportiert werden.

37 Unter der Annahme, dass die Plattform einen unerlaubten Zugriff auf den EVG und die EVG Daten verhindert, setzt der EVG auch eine Zugriffskontrolle auf die EVG Daten, hier insbesondere die Bild- und Protokolldaten, durch. Ausschließlich über den EVG autorisierte Benutzer erhalten über den EVG die ihrer Benutzerrolle entsprechenden Zugriffsmöglichkeiten.

38 Der Rolle **Beobachter** stehen Recherchemöglichkeiten im Bilddatenbestand zur Verfügung, um bestimmte Vorfälle genauer zu analysieren.

39 Datenschutzrechtlich relevant ist der Export zur Weitergabe von Bilddaten aus dem Anwendungsbereich der TSF heraus, da diese Bilddaten dann nicht mehr vom EVG

kontrollierbar sind. Dem Beobachter steht grundsätzlich diese Möglichkeit zum Export zur Verfügung. Der Export ist zulässig, sofern „*nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind*“ (Eingabekontrolle gemäß Anlage 1 zu §9 Satz 1 BDSG; vgl. auch Anhang A). Daher erzwingt der EVG eine Begründung für jeden Export von Bilddaten und protokolliert diesen auch. Dadurch unterstützt der EVG die Gewährleistung der Zweckbestimmung der Datenverarbeitung und Dokumentation durch die erzwungene Begründung bei Zweckänderung von „Auswerten“ auf „Ausdrucken“ oder „Exportieren“ (Zweckbindung) gemäß §6b Nr. 1 BDSG (vgl. auch Anhang A).

40 Die Rolle **Administrator** hat typischerweise den EVG zu installieren und die Plattform und den vertrauenswürdigen Kanal für die Übertragung so einzurichten, dass der EVG und alle relevanten Daten angemessen geschützt sind. Für Wartungsarbeiten benötigt der Administrator zur Kontrolle der korrekten Funktion des EVG die Auswertungs- und Exportmöglichkeiten des Beobachters.

41 Die Einrichtung der verschiedenen Benutzer zur Rolle Beobachter wird ebenfalls vom Administrator durchgeführt. Er kann weiterhin das Passwort für den Revisor/bDSB initialisieren. Er ist für die Administration der IT-Einsatzumgebung verantwortlich. Sicherheitsrelevante Änderungen an der EVG Konfiguration sowie die Einrichtung von Benutzeraccounts und das Rücksetzen von Passwörtern werden je nach Konfiguration vom EVG protokolliert.

42 Die Rolle des **Revisors**, die dem betrieblichen Datenschutzbeauftragten (bDSB) zugedacht ist, ist im EVG fest eingerichtet und nicht vom Administrator beeinflussbar. Der Revisor hat als Einziger die Einstellung aller relevanten Parameter bezüglich der Löschzyklen für die Bilddaten sowie des Umfangs der Protokollierung (nur des konfigurierbaren Anteils) vorzunehmen. Diese Konfigurationsänderungen werden protokolliert. Der Revisor ist auch der Einzige, der Bilddaten nach Eingabe einer ausreichenden Begründung löschen kann, wenn ein Betroffener seinen individuellen Löschungsanspruch auf Bilddaten geltend macht (vgl. Eingabekontrolle gemäß Anlage 1 Nr. 5 BDSG; vgl. auch Anhang A). Hierfür stehen dem Revisor auch die Recherchemöglichkeiten des Beobachters zur Verfügung. Der Revisor ist nicht berechtigt, Bilddaten zu exportieren.

43 Aus Sicht des Betreibers einer Videoüberwachungsanlage ist die korrekte Funktion der Komponenten zur Signalaufnahme, zur Übertragung und Speicherung wichtig: Ein unbemerktes zu frühes oder unautorisiertes Löschen oder gar eine unbemerkte Manipulation der gespeicherten Bilddaten muss ausgeschlossen werden, was der EVG sicherzustellen hat. Auch möchte der Betreiber im Zweifelsfall mit Hilfe der Protokolldaten den Nachweis erbringen können, dass mit den Bilddaten gesetzeskonform verfahren wurde. Daher wird an die Erzeugung der Protokolldaten gleichwertige Anforderungen bezüglich Verfügbarkeit und Integrität wie an die Bilddaten gestellt, was ebenfalls der EVG umzusetzen hat. Der Schutz der bereits gespeicherten Protokolldaten wird mit Unterstützung der zugrunde liegenden Plattform erreicht. Der EVG ist nur in der Lage, Manipulationen an den gespeicherten Protokolldaten zu erkennen. Der Umfang der Protokollierung wird über den EVG per Parameter gesteuert.

44 Zudem soll ein Ausfall sowie die wiederhergestellte Verfügbarkeit des Bildsignals von einzelnen Signalaufnahmekomponenten vom EVG erkannt, protokolliert und an den Benutzer gemeldet werden.

2.3 Datenarten und Werte

45 Aus der bisherigen Beschreibung heraus werden folgende Werte betrachtet, die durch den EVG unter den genannten Aspekten zu schützen sind:

- **Bilddaten**: Bilddaten umfassen einzelne (live oder aufgezeichnete) Videobilder[3], Bilddaten können als „Rohdaten“, d. h. unverändert und ohne Komprimierung[4], oder in einem (standardisierten) Format vorliegen. Die Bilddaten werden außerhalb des EVG aber im TSC gespeichert.

  Personenbezogene Bilddaten stellen den zentralen Wert für den EVG dar.

  Damit der EVG ein Löschen oder Verändern dieser Daten erkennen kann, werden diese gespeicherten Bilddaten über vom EVG erzeugte Integritätsmerkmale geschützt.

  Anwendungsbemerkung 6 *Falls eine Konfiguration der Integritätsmerkmale für gespeicherte Bilddaten notwendig ist, darf dies nur durch den Revisor/bDSB konfiguriert werden.*

  Anwendungsbemerkung 7 *Ein Backup der Bilddaten wird in diesem PP nicht berücksichtigt, da dies wegen der Kurzlebigkeit dieser Daten üblicherweise nicht durchgeführt wird. Sollte diese Fähigkeit gefordert werden, dürfen die auf den Backupmedien liegenden Bilddaten nach Erreichen der Löschfrist nicht mehr verfügbar sein. Ein Backup der Protokolldaten ist dagegen möglich und ohne Auswirkungen auf zusätzliche Sicherheitsanforderungen.*

- **Protokolldaten** für oben genannte Aktivitäten – und insbesondere zum Nachweis aller datenschutzrelevanten Aktionen.

  Die Protokolldaten werden vom EVG erzeugt sofort nach der Erzeugung auf der zugrunde liegenden Plattform (außerhalb des EVG) aber noch im TSC gespeichert. Damit der EVG ein Löschen oder Verändern dieser Daten erkennen kann, werden diese gespeicherten Protokolldaten über vom EVG erzeugte Integritätsmerkmale geschützt.

  Anwendungsbemerkung 8 *Falls eine Konfiguration des Integritätsmerkmals für Protokolldaten notwendig ist, darf dies nur durch den Revisor/bDSB konfiguriert werden.*

- **Konfigurationsdaten für den EVG**, die die Benutzung des EVG steuern – etwa Zugriffsrechte und Passwörter.

---

[3] Vgl. Videosequenzen im Glossar in Abschnitt 1.5.

[4] Zur Nutzung von Rohdaten kann – etwa aufgrund eines proprietären Datenformats – ein dedizierter Player benötigt werden.

- **Konfigurationsdaten für den Umfang der Protokollierung**. Der Umfang der Protokollierung ist durch den Revisor/bDSB in eingeschränktem Maße konfigurierbar; die Protokollierung aller datenschutzrechtlich relevanten Aktionen wird erzwungen.

46 Der EVG zur Verarbeitung der von Videoüberwachungskameras aufgenommenen Bilddaten mitsamt seinen externen Schnittstellen sowie die Zuordnung der Datenarten zwischen den logischen funktionalen Komponenten sind in Abbildung 1 dargestellt.

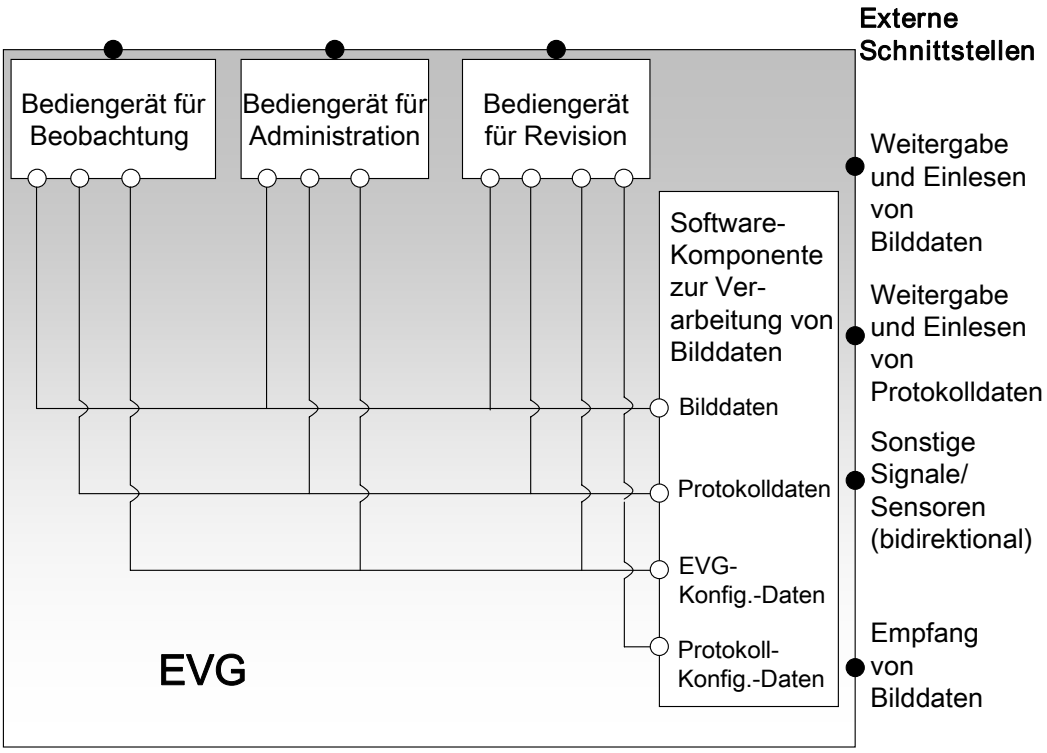

Abbildung 1: Darstellung des EVG mit externen Schnittstellen

Abbildung 2 stellt nochmals graphisch den Anwendungsbereich der TSF (TSC) und den eigentlichen EVG dar. EVG Schnittstellen sind hier nicht eingezeichnet.

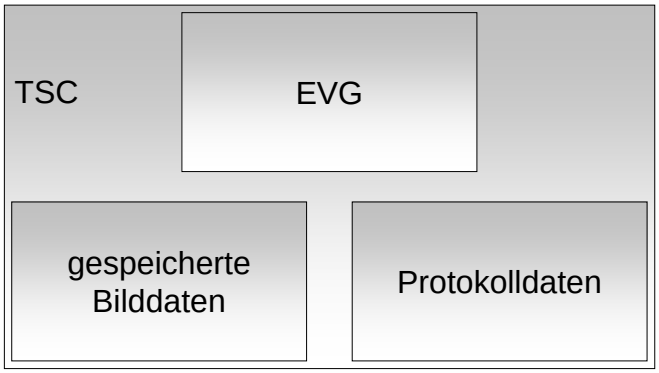

Abbildung 2: Darstellung des Anwendungsbereich der TSF-Kontrolle (TSC)

3 EVG-Sicherheitsumgebung

47 Die EVG-Sicherheitsumgebung beschreibt Annahmen an die Umgebung, in der der Evaluationsgegenstand eingesetzt werden soll, die damit Auflagen an den Betrieb darstellen. Des Weiteren werden im Abschnitt 3.3 alle vom EVG abzuwehrenden Bedrohungen und im Abschnitt 3.4 die zu berücksichtigenden organisatorischen Sicherheitspolitiken aufgeführt. Die Bedrohungen thematisieren einerseits die datenschutzrechtlichen Rahmenbedingungen und andererseits die IT-Sicherheit.

3.1 Rollen im EVG

48 Es gibt die folgenden, im Kontext des Evaluationsgegenstands zu berücksichtigenden Rollen mit den nachfolgend aufgeführten Eigenschaften:

- **Beobachter (S1):**
  - Zutritt zum Betriebsraum des EVG sowie Zugang und Zugriff zum EVG;
  - Auswertung von Bilddaten, d. h. Durchführen einer Bildsuche entsprechend konkret einstellbarer Kriterien inklusive Anzeige (kann auch ein Zoomen oder Schwenken beinhalten)
  - Exportieren von Bilddaten aus dem EVG heraus zwecks Weitergabe (dazu zählt auch das Ausdrucken von Bilddaten)
  - Ändern seines Passwortes
  - Lesen von Protokolldaten[5]

  Der Beobachter hat Fachkenntnisse zur Bedienung des EVGs und grundlegende IT-Kenntnisse.

[5] Da die Protokolldaten auch die Begründungen für ein Exportieren, Ausdrucken oder vorzeitiges Löschen von Bilddaten enthalten, sollen Protokolldaten für jeden Beobachter, Administrator und Revisor/bDSB sichtbar sein.

- **Administrator (S2):**
  - Er hat Zutritt zum Betriebsraum des EVG sowie Zugang und Zugriff zum EVG
  - Konfigurieren von Beobachter- und Administratorenaccounts im EVG einschließlich der Passwörter
  - Prüfen von Beobachter-Aktivitäten durch Auswertung der Protokolldaten – wichtig beim Auftreten technischer Probleme
  - Ändern seines eigenen Passwortes
  - Initialisieren (Rücksetzen) des Passwortes des Revisor/bDSB.
  - Einstellen und Konfigurieren des EVG zur Gewährleistung des Betriebs. Den Umfang der Protokollierung durch den EVG oder den Löschzyklus für Bilddaten kann der Administrator nicht beeinflussen.
  - zur Konfiguration und zur Prüfung der Funktionsfähigkeit des EVG verfügt der Administrator zusätzlich über die Rechte als Beobachter (S1)

  Der Administrator hat Fachkenntnisse zur Bedienung und Administration des EVGs und professionelle IT-Kenntnisse.

- **Revisor/bDSB (S3):**
  - Zutritt zum Betriebsraum des EVG sowie Zugang und Zugriff zum EVG
  - Kontrollieren des Beobachters und des Administrators des EVG durch Auswertung der Protokolldaten
  - Ändern des Revisor-Passwortes
  - Einstellen des Löschzyklus' für die Bilddaten gemäß der zulässigen Speicherdauergrenzen für Bilddaten
  - Konfigurieren des Umfangs der Protokollierung[6]
  - Auswertung von Bilddaten, d. h. Durchführen einer Bildsuche entsprechend konkret einstellbarer Kriterien inklusive Anzeige (kann auch ein Zoomen oder Schwenken beinhalten); diese Funktionalität wird dem Revisor/bDSB zugewiesen, um diejenigen Bilddaten heraussuchen zu können, die explizit gelöscht werden sollen
  - Löschen von Bilddaten auf begründete Anforderung (individueller Löschungsanspruch)

  Der Revisor/bDSB hat Fachkenntnisse zur Bedienung des EVGs und grundlegende IT-Kenntnisse.

[6] Der Umfang der Protokollierung muss für den Revisor/bDSB konfigurierbar gestaltet sein: Die Anforderungen an die Protokollierung richten sich dabei nach der Eingabekontrolle der Anlage zu § 9 Nr. 5 BDSG. Von minimaler Protokollierung (An-/Abmeldung am System) über die Protokollierung beim Erkennen besonderer Ereignisse bis hin zur Protokollierung aller Aktivitäten. Der Umfang muss so gewählt werden, dass die Vorgabe der Eingabekontrolle erfüllt werden können und wesentliche Aktionen erfasst und eine Auswertung der Protokollspeicher ermöglicht wird.

- **Fremdpersonal (S4):**
  - kein logischer Zugang zum EVG, darf den EVG also nicht nutzen. Physikalischer Zugang zum Rechner, auf dem der EVG läuft, ist jedoch möglich.
  - Zutritt zum Betriebsraum des EVG[7]

  Für das Fremdpersonal werden höchstens grundlegende IT-Fachkenntnisse angenommen.

- **Außenstehender (S5):**
  - Kein Zutritt zum Betriebsraum des EVG und damit auch keinen direkten Zugang oder Zugriff auf den EVG oder dessen Daten.
  - Zugang zu den Übertragungsstrecken, wenn dies nicht durch Maßnahmen der Umgebung verhindert wird (z.B. baulich geschützte Leitungsführung).

  Der Außenstehende hat Profi-Expertise.

3.2 Annahmen

49 Im Abschnitt Annahmen werden die Sicherheitsauflagen an die Umgebung angeführt, in der der Evaluationsgegenstand eingesetzt werden soll und deren Umsetzung angenommen wird. Dieser Abschnitt kann als Auflagenkatalog an den Betreiber des EVG angesehen werden. Jeder Annahme wird zur eindeutigen Referenzierbarkeit ein Name mit dem Anfangsbuchstaben A (Assumption) zugeordnet.

50 Eine Erklärung für die Annahmen findet sich im Erklärungsteil dieses Schutzprofils in Abschnitt 6.1.

51 A.Alle — Es wird vorausgesetzt, dass alle Personen der Rollen Administrator, Beobachter, Revisor/bDSB und Fremdpersonal auf das Datengeheimnis verpflichtet sind und dementsprechend auch eine Verschwiegenheit ausüben und auch ihre Passworte sicher verwahren und sorgsam nutzen. Es wird weiterhin vorausgesetzt, dass alle Personen der Rolle Administrator dahingehend vertrauenswürdig sind, dass sie keine gezielten Angriffe gegen den EVG, die EVG Daten oder die Einsatzumgebung ausführen.

52 A.Backup — Die EVG-Daten mit Ausnahme der Bilddaten (vgl. A.NoBackup) sowie die Protokolldaten werden regelmäßig gesichert. Bei einem möglichen Recovery werden die gesicherten Daten unverändert in das System wieder eingespielt.

---

[7] Fremdpersonal hat keinen Zugang zum EVG – kann den EVG also nicht für Auswertungszwecke benutzen – aber Zutritt zum geschützten Bereich des EVG und den Monitoren, die die aktuellen Aufnahmen zeigen; das Fremdpersonal gehört zum Personal derjenigen Stelle, bei der der EVG betrieben wird (etwa Personal für andere Anwendungen oder Reinigungspersonal).

53 A.BD.Zuordnung Es wird davon ausgegangen, dass die IT-Einsatzumgebung (z.B. die Signalaufnahmekomponente) vor dem Versand an den EVG in die erzeugten Bilddaten einen eindeutigen und korrekten Verweis auf die entsprechende Signalaufnahmekomponente sowie das Datum und die Uhrzeit des Aufnahmezeitpunktes einfügt.

54 A.Betrieb Der EVG wird auf einem Rechner betrieben, der in einem geschützten Bereich steht und zu dem nur Beobachter, Administrator, Revisor/bDSB und Fremdpersonal Zutritt haben. Alle zum Betrieb des EVG notwendigen IT-Komponenten[8] befinden sich ausschließlich in diesem Bereich und sind nicht von außerhalb dieses Bereiches zugänglich. Ein Zugang zu den Hardware-Schnittstellen des EVG (bzw. des entsprechenden Systems auf welchem der EVG läuft) ist nur in diesem Bereich möglich. Nur in diesem Bereich sind an den EVG angeschlossene Monitore aufgestellte, und zwar so, dass Einsicht von Außen nicht möglich ist.

55 A.Kamera Es wird davon ausgegangen, dass die von der Komponente zur Signalaufnahme aufgenommenen Bilddaten unverfälscht[9] sind und nur zulässige Bilder aufgenommen werden (vgl. Anhang A zur datenschutzrechtlichen Zulässigkeit).

56 A.NoBackup Es wird kein Backup für Bilddaten durchgeführt.

> ***Anwendungsbemerkung 9*** *Ein Backup für Bilddaten hätte die Konsequenz, dass im produktiven System bereits gelöschte Bilddaten von den Backup-Medien wiedereingespielt werden können. Sollte ein Backup der Bilddaten notwendig sein, ist durch zusätzliche Sicherheitseigenschaften und Annahmen für den Umgang mit den Backupmedien das Wiedereinspielen gelöschter Bilddaten zu verhindern und die Lesbarkeit dieser Bilddaten auf den Backup-Medien ebenfalls zu verhindern.*

57 A.Plattform Es wird davon ausgegangen, dass in den Systemen, auf die der EVG aufbaut[10], ein Zugriffsberechtigungssystem existiert und die Zugriffsberechtigungen auf den EVG und die EVG-Daten so gesetzt sind, dass Zugriffe auf alle EVG-Daten nur über den EVG möglich sind. Der Protokollspeicher ist ebenfalls durch die Mechanismen der zugrunde liegenden Plattform ausreichend vor unautorisiertem Zugriff geschützt. Von der Plattform, auf der der EVG selbst läuft, gehen keine Bedrohungen wie Viren oder Trojaner aus. Auf der Plattform wird ausschließlich der EVG betrieben.

---

[8] Hardware (z.B. Server) und Netzwerke (Leitungen, Netzwerkkomponenten)

[9] Die Kamera lässt sich z.B. nicht durch ein vorgehaltenes Foto täuschen.

[10] Z.B. Betriebssystem, Datenbank, Dateisystem, etc.

58 A.Schnittstellen An die externen Hardware-Schnittstellen des EVG (bzw. des Systems auf dem der EVG läuft) sind alle benötigten IT-Komponenten aus der Umgebung wie z.B. Signalaufnahmekomponenten, externe transportable Speicher für den Export, Drucker oder die Steuerungskomponenten für die Kameras korrekt angeschlossen.

59 A.Speicher Es wird angenommen, dass der Speicher für die Bild- und Protokolldaten ausreichend groß dimensioniert ist.

60 A.Überlastung Die Übertragungsleitungen und die Plattform, auf welcher der EVG läuft, sind so dimensioniert, dass eine Überlastung des EVG durch zu hohes Bilddatenaufkommen nicht auftreten kann.

61 A.Übertragung Der Übertragungsweg von den Signalaufnahmekomponenten zum EVG muss bezüglich der Vertraulichkeit, Integrität und Authentizität der Bilddaten geschützt werden.

Anwendungsbemerkung 10 *Wird der Übertragungsweg durch den EVG geschützt, so ist diese Annahme durch die Formulierung einer Bedrohung zu ersetzen, die den Angriff auf die Übertragungsstrecke zulässt.*

62 A.Uhrzeit Die IT-Umgebung muss allen Komponenten des Systems eine korrekte Uhrzeit bereitstellen, damit der Aufnahmezeitpunkt der Bilddaten erfassbar ist und die Protokolleinträge mit dem Zeitpunkt des Ereignisses versehen werden können. Weiterhin ist die korrekte Uhrzeit für das automatische Löschen von Bilddaten relevant.

3.3 Bedrohungen

63 Im Abschnitt Bedrohungen werden die Bedrohungen als konkrete Ereignisse aufgeführt, die der EVG selbst abzuwehren hat. Jeder Bedrohung wird zur eindeutigen Referenzierbarkeit ein Name mit dem Anfangsbuchstaben T (Threat) zugeordnet.

64 Die Bedrohungen ergeben sich z. T. aus den datenschutzrechtlichen Anforderungen (vgl. Anhang A).

65 T.BD.Ausfall Der EVG bemerkt nicht, dass von einer Komponente zur Signalaufnahme keine Bilddaten mehr ankommen (vgl. Verfügbarkeit gemäß Anlage zu §9 Satz 1 BDSG; Anhang A). Der EVG bemerkt nicht, dass von einer ausgefallenen Signalaufnahmekomponente wieder Bilddaten geliefert werden.

66 T.BD.Import Die an den EVG gelieferten Bilddaten wurden von einer nicht autorisierten Signalaufnahmekomponente erzeugt. Ein beispielhafter Angriff könnte sein, dass ein Außenstehender die eigentliche Kamera durch einen Videorecorder ersetzt hat.

67 T.BD.Lösch Beobachter oder Administrator löschen unbemerkt Bilddaten.

68 T.BD.Veränd Beobachter, Administrator oder Revisor/bDSB verändern unbemerkt gespeicherte Bilddaten.

69 T.Einspielen Es werden über eine Schnittstelle am Rechner, auf dem der EVG läuft, zusätzliche Bilddaten in den EVG importiert. Zum Beispiel könnte der Anschluss der Übertragungsstrecke vom Rechner getrennt und der Rechner mit einem Bildabspielgerät (z.B. Videorecorder) verbunden werden. Damit sollen falsche Tatsachen vorgetäuscht werden oder durch Überlauf des Bilddatenspeichers die weitere Aufzeichnung von Ereignissen verhindert werden. Als Angreifer kommen alle in Frage, die Zutritt zum Betriebsraum und physikalischen Zugang zum Rechner haben, auf welchem der EVG läuft. (siehe Rollenbeschreibung in Kapitel 3.1).

70 T.KonfigS3 Beobachter oder Administrator führt Tätigkeiten durch, die nur dem Revisor/bDSB zugewiesen sind. Er kann damit Bilddaten löschen oder die Protokollkonfiguration zum Vertuschen eines unkorrekten Handelns mit den Bilddaten ändern.

71 T.Löschung Fremdpersonal, Beobachter, Administrator oder Revisor/bDSB können auf logisch aber nicht physikalisch gelöschte Bilddaten zugreifen.

72 T.Nachvollz Beobachter oder Administrator schalten zum Vertuschen eines unkorrekten Handelns mit den Bilddaten die Protokollierung ab oder verändern den Umfang der Protokollierung, so dass die zu protokollierenden Aktionen zwecks Vertuschens eines unkorrekten Handelns mit den Bilddaten nicht nachvollziehbar wären.
Revisor/bDSB schaltet die Protokollierung ab oder verändert den Umfang der Protokollierung so, dass Veränderungen der Löschzyklen für Bilddaten nicht mehr nachvollziehbar sind.

73 T.PD.Veränd Beobachter, Administrator oder Revisor/bDSB verändern oder löschen unbemerkt zum Vertuschen eines unkorrekten Handelns mit den Bilddaten einzelne Protokolldatensätze, z.B. durch direkten Zugriff auf den Datenspeicher.

74 T.S3Aktion Revisor/bDSB setzt die Löschzyklen für die Bilddaten außerhalb seines Konfigurationsspielraums (eine Mindest- und eine Maximalspeicherdauer für Bilddaten ist gesetzlich vorgegeben). Dies könnte u.a. der Vertuschung eines unkorrekten Handelns mit den Bilddaten dienen.

75 T.Zugriff Fremdpersonal oder Außenstehender erlangt Zugriff zum EVG und führt Aktivitäten der Rollen Beobachter, Administrator oder Revisor/bDSB aus. Der Angreifer hat damit z.B. die Möglichkeit zum unbefugten Löschen oder Exportieren von Bilddaten oder der Manipulation der Konfiguration.

76 Motivation für Angriffe von Beobachter, Administrator, Revisor/bDSB, Fremdpersonal und Außenstehendem: Auf Bildmaterial oder Protokolldaten dokumentiertes (Fehl-)verhalten soll vertuscht oder kompromittierende Bilddaten sollen veröffentlicht bzw. weitergegeben werden. Weitere Gründe können sein: Erpressungsversuch, Rache, Rufschädigung, Erlangung finanzieller Vorteile.

77 Alle Rollen haben grundsätzlich jederzeit Gelegenheit, absichtlich (bis auf Administrator) und auch unabsichtlich Angriffe durchzuführen.

Anwendungsbemerkung 11 *Es ist nicht weiter möglich, die Angriffmethoden und die dafür notwendigen Ressourcen genauer zu beschreiben, da diese stark von der konkreten Implementierung abhängig sind. Falls nicht anders angegeben, bietet der EVG selbst die Möglichkeiten für die Angriffe.*

3.4 Organisatorische Sicherheitspolitiken (OSP)

78 Im Abschnitt Organisatorische Sicherheitspolitiken werden die relevanten Gesetze, deren Einhaltung oder Umsetzung der EVG zu gewährleisten hat, aufgeführt.

79 P.Begründ Folgende datenschutzrechtlich relevanten Aktionen müssen von unten angegebenen Benutzern vor Ausführung begründet werden. Der EVG hat dem Benutzer eine Auswahl zulässiger Begründungen zur Verfügung zu stellen und eine Begründung zu erzwingen. Die Begründungen sind zusammen mit dem Ereignis zu protokollieren:

- Beobachter und Administrator: Exportieren von Bilddaten
- Revisor/bDSB: Löschen von Bilddaten

80 P.KonfigS2 Beobachter oder Revisor/bDSB dürfen keine Tätigkeiten durchführen, die nur dem Administrator zugewiesen sind (vgl. Rollendefinition in Kapitel 3.1).

81 P.Löschgarantie Der EVG hat die Bilddaten unmittelbar nach der jeweiligen vom Revisor/bDSB vorgegebenen Löschfrist zu löschen (gemäß §6b BDSG).

82 P.S3Export Der EVG muss gewährleisten, dass der Revisor auf die gesetzlich vorgegebene Kontroll- und Löschfunktion eingeschränkt ist. Insbesondere darf der Revisor keine Bilddaten exportieren können.

4 Sicherheitsziele

83 Dieses Kapitel legt produktunabhängig dar, wie der EVG den zuvor genannten Bedrohungen begegnet. Jedem Sicherheitsziel wird zur eindeutigen Referenzierbarkeit ein Name mit dem Anfangsbuchstaben O (von engl. „Objective“) zugeordnet. Sicherheitsziele für die Umgebung werden mit OE gekennzeichnet. Diese Ziele können weiterhin in Ziele für die IT-Umgebung (IT) und die nicht-IT-Umgebung (NI) unterschieden werden und sind entsprechend gekennzeichnet.

4.1 Sicherheitsziele für den EVG

84 O.BD.Ausfall Der EVG muss erkennen, wenn keine Bilddaten mehr von einer externen Komponente zur Signalaufnahme ankommen. Der EVG muss erkennen, dass von einer Signalaufnahmekomponente nach einem Ausfall wieder Bilddaten geliefert werden.
Beide Ereignisse sind vom EVG zu protokollieren und dem Benutzer anzuzeigen.

85 O.BD.Import Der EVG muss vor der Speicherung aller empfangenen Bilddaten diese auf Authentizität prüfen. Dies hat mittels eines in den Bilddaten vorhandenen Authentizitätsmerkmals zu erfolgen. Optional ist das Resultat der Prüfung zu protokollieren. Fehler sind in jedem Fall dem Benutzer zu melden.

86 O.BD.Lösch Der EVG darf den Rollen Administrator und Beobachter keine Möglichkeit anbieten, gespeicherte Bilddaten zu löschen. Werden Bilddaten unter Umgehung des EVG gelöscht, muss er dies mit Hilfe eines Integritätsmerkmals erkennen können. Optional ist das Resultat der Prüfung zu protokollieren. Fehler sind in jedem Fall dem Benutzer zu melden. Der EVG muss über alle von ihm gespeicherten Bilddaten ein Integritätsmerkmal erzeugen.

> ***Anwendungsbemerkung 12*** *Es ist zulässig, dass der EVG dieses Integritätsmerkmal auch indirekt über alle Bilddaten erstellt, z.B. nur über eine Liste von momentan gespeicherten Bilddaten, nicht über die Bilddaten selbst.*

87 O.BD.Veränd Der EVG darf den Rollen Administrator, Beobachter und Revisor/bDSB keine Möglichkeit anbieten, gespeicherte Bilddaten zu verändern. Werden Veränderungen unter Umgehung des EVG durchgeführt, muss er dies mit Hilfe eines Integritätsmerkmals erkennen können. Optional ist das Resultat der Prüfung zu protokollieren. Fehler sind in jedem Fall dem Benutzer zu melden. Der EVG muss die von ihm gespeicherten Bilddaten sofort mit einem Integritätsmerkmal versehen.

88 O.Begründ Das Datenschutzrecht gibt vor, dass Beobachter, Administrator und Revisor/bDSB datenschutzrechtlich relevante Aktionen begründen müssen, bevor sie diese ausführen. Der EVG muss bei jeder datenschutzrechtlich relevanten Aktionen hierfür eine Textliste mit den zulässigen Begründungen (mit möglichem zusätzlichen Freitextfeld für weitere Informationen) zur Verfügung stellen und dafür sorgen, dass bei jeder datenschutzrechtlich relevante Aktionen eine der vorgegebenen Begründung ausgewählt oder ggf. eine eigene Begründung eingegeben wird. Die Begründungen sind zusammen mit dem Ereignis vom EVG zu protokollieren. Im Einzelnen sind dies:

- Beobachter und Administrator: Exportieren von Bilddaten
- Revisor/bDSB: Löschen von Bilddaten

89 O.Einspielen Der EVG darf über keine Funktion verfügen, die einen manuellen Import von Bilddaten erlaubt.

90 O.KonfigS2 Der EVG muss gewährleisten, dass der Beobachter und der Revisor/bDSB EVG-Funktionen des Administrators nicht ausführen können.

91 O.KonfigS3 Der EVG muss gewährleisten, dass der Administrator und der Beobachter folgende, exklusiv dem Revisor/bDSB zugeordneten EVG-Funktionen nicht ausführen können:

- Löschen von Bilddaten (vgl. auch O.BD.Lösch)
- Konfiguration der Löschzyklen für die Bilddaten
- Konfiguration des Umfangs der Protokollierung
- Nur Beobachter: Setzen/Verändern des Revisor/bDSB-Passwortes

92 O.Löschgarantie Der EVG muss Bilddaten nach Ablauf der vorgegebenen jeweiligen Löschfrist automatisch löschen.

93 O.Löschung Der EVG muss gewährleisten, dass gelöschte Bilddaten (sowohl automatisch gelöschte Bilddaten gemäß Löschzyklus als auch von Revisor/bDSB gelöschte Bilddaten bei individuellem Löschungsanspruch eines Betroffenen) beim Löschen physikalisch überschrieben werden.

94 O.Nachvollz Der EVG muss gewährleisten, dass die Erzeugung von Protokolldaten für datenschutzrelevante oder den Betrieb beeinflussende Ereignisse nicht abgeschaltet oder außerhalb der zulässigen Grenzwerte gesetzt werden kann.

95 O.PD.Veränd Der EVG muss gewährleisten, dass gespeicherte Protokolldaten von Administrator, Beobachter und Revisor/bDSB nicht unbemerkt verändert werden können, indem er Manipulationen an den Protokolldaten mit Hilfe eines Integritätsmerkmals erkennen kann. Der EVG muss die von ihm erzeugten Protokolldaten sofort mit einem Integritätsmerkmal versehen. Optional ist das Resultat der Prüfung zu protokollieren. Fehler sind in jedem Fall dem Benutzer zu melden.

96 O.S3Aktion Der EVG muss gewährleisten, dass die Löschzyklen zur automatischen Löschung für die Bilddaten nur innerhalb der gesetzlich vorgegebenen Grenzen durch den Revisor/bDSB geändert werden können.

97 O.S3Export Der EVG muss gewährleisten, dass der Revisor auf die gesetzlich vorgegebene Kontroll- und Löschfunktion eingeschränkt ist. Insbesondere darf der Revisor keine Bilddaten exportieren können.

98 O.Zugriff Der EVG muss gewährleisten, dass sich jeder eindeutig und erfolgreich gegenüber dem EVG identifizieren und authentisieren muss, um Zugriff zum EVG und dessen Daten zu erlangen.

4.2 Sicherheitsziele für die Umgebung

4.2.1 Sicherheitsziele für die IT Umgebung

99 OE.IT.BD.Zuordnung Die IT-Einsatzumgebung muss gewährleisten, dass eine Zuordnung von Bilddaten zur entsprechenden Signalaufnahmekomponente und zum Zeitpunkt der Aufnahme alleine durch die vom EVG empfangenen Bilddaten möglich ist. Die Bilddaten selbst müssen also die notwendigen Informationen enthalten.
Eventuell notwendige eindeutige Kennzeichnungen aller Signalaufnahmekomponenten sowie dezentrale und/oder zentrale Speicherung dieser Identifikationsdaten ist darin inbegriffen.

100 OE.IT.Kamera Da die Komponenten zur Signalaufnahme (Objektiv, Bildauflösung, optionale Kamerasteuerung, etc.) außerhalb des EVG liegen, muss die IT-Umgebung dafür sorgen, dass nur authentische[11] Bilder aus einem zulässigen Bereich von der Kamera versendet werden.

[11] Damit ist gemeint, dass die Kamera z.B. nicht durch Fotos getäuscht werden kann.

101 OE.IT.Plattform Es muss gewährleistet sein, dass auf der Plattform, auf der der EVG läuft, ein Zugriffsberechtigungssystem existiert und die Zugriffsberechtigungen auf den EVG und die EVG-Daten so gesetzt sind, dass Zugriffe auf alle EVG-Daten nur über den EVG möglich sind. Die Berechtigungen auf die Bilddaten müssen dem EVG das Speichern neuer Bilddaten sowie das Auslesen und das Löschen bestehender Bilddaten erlauben. Die Berechtigungen auf die Protokolldaten müssen dem EVG das Erzeugen neuer Protokolldaten sowie das Lesen bestehender Protokolldaten erlauben. Unautorisierte Zugriffe auf die Bild- und Protokolldaten (auch unter Umgehung des EVG) sind durch die Plattform zu verhindern. Es ist durch technisch/organisatorische Maßnahmen sicherzustellen, dass von der technischen Plattform, auf der der EVG selbst läuft, keine Bedrohungen wie Viren oder Trojaner ausgehen. Möglichen Bedrohungen durch andere Software wird dadurch begegnet, dass auf der Plattform ausschließlich der EVG betrieben wird.

> ***Anwendungsbemerkung 13*** *Da der Administrator keinen technischen Beschränkungen durch das Betriebssystem unterliegt, muss seine Administrationstätigkeit organisatorisch reglementiert werden. (siehe OE.NI.Alle)*

102 OE.IT.Uhrzeit Damit der EVG die automatische Löschung von Bilddaten sowie die Eintragung der Uhrzeit- und Datumsangaben für die Protokolldaten vornehmen kann, muss das korrekte Datum und die korrekte Uhrzeit von der IT-Umgebung bereitgestellt werden.

> ***Anwendungsbemerkung 14*** *Es liegt in der Entscheidung des Herstellers, ob die Signalaufnahmekomponente oder das Betriebssystem, auf dem der EVG aufsetzt, zum Bestimmen der Uhrzeit benutzt wird.*

4.2.2 Sicherheitsziele für die nicht-IT Umgebung

103 OE.NI.Alle Da der EVG nicht verhindern kann, dass die im Rahmen ihrer Tätigkeit gewonnenen Informationen weitergegeben werden, ist organisatorisch Folgendes festzulegen: Der Administrator, die Beobachter, der Revisor/bDSB und das Fremdpersonal dürfen die aus den Bilddaten gewonnenen Informationen nicht weitergeben. Sie müssen ihre Passworte sicher verwahren und sorgsam nutzen. Es ist weiterhin organisatorisch sicherzustellen, dass nur vertrauenswürdiges Personal administrative Privilegien erhält, so dass absichtliche Angriffe dieses Personenkreises gegen den EVG, die EVG Daten oder die Einsatzumgebung unberücksichtigt bleiben können. Dieser Personenkreis ist darauf hinzuweisen, dass eine Manipulation oder das Löschen des EVG, von EVG Daten oder von Protokolldaten nicht zulässig ist.

104 OE.NI.Backup Die EVG-Daten mit Ausnahme der Bilddaten (vgl. OE.NI.NoBackup) und die Protokolldaten sind regelmäßig zu sichern, damit bei einem Hardware-Ausfall protokollierte Ereignisse dennoch nachvollziehbar sind. Es ist sicherzustellen, dass die gesicherten Daten nicht verändert werden (können), so dass ein mögliches Recovery den Originalzustand wiederherstellt.

105 OE.NI.Betrieb Der EVG sowie alle zum Betrieb des EVG notwendigen IT-Komponenten[12] müssen in einem geschützten Bereich betrieben werden, zu dem nur Beobachter, Administrator, Revisor/bDSB und Fremdpersonal Zutritt haben. Die betroffenen IT-Komponenten dürfen nicht von außerhalb dieses Bereiches zugänglich sein. Es ist weiterhin sicherzustellen, dass nur in diesem geschützten Bereich an den EVG angeschlossene Monitore aufgestellt werden, die auch von außerhalb des Bereiches nicht eingesehen werden können.

106 OE.NI.NoBackup Es ist technisch/organisatorisch sicher zu stellen, dass von den Bilddaten keine Backups angefertigt werden.

107 OE.NI.Schnittstellen Es muss gewährleistet sein, dass an die Hardware-Schnittstellen des Systems, auf welchem der EVG läuft, die benötigten IT-Komponenten aus der Umgebung wie Signalaufnahmekomponenten, externe transportable Speicher für den Export, Drucker und die Steuerungskomponenten für die Kameras korrekt angeschlossen sind. Es muss weiterhin gewährleistet sein, dass unbefugtes Ändern dieser Hardware-Konfiguration nicht möglich ist.

108 OE.NI.Speicher Damit eine Auslagerung auf externe Datenträger von noch zu speichernden Bilddaten vermieden werden kann und alle anfallenden Bilddaten aufgenommen und hinreichend lange gespeichert werden können, muss der Speicher für die Bilddaten ausreichend groß dimensioniert sein.
Der Speicher für die Protokolldaten muss ebenfalls ausreichend groß dimensioniert sein. Durch rechtzeitiges Auslagern bzw. Löschen von Protokolldaten, die nicht mehr im direkten Zugriff stehen müssen, kann die Einsatzumgebung ein Überlaufen des Protokollspeichers verhindern.

109 OE.NI.Übertragung Es muss sichergestellt sein, dass die Bilddaten auf dem Übertragungsweg zwischen Signalaufnahmekomponente und EVG derart geschützt sind, dass sie vertraulich, integer und authentisch beim EVG ankommen.

[12] Hardware (z.B. Server) und Netzwerke (Leitungen, Netzwerkkomponenten)

Anwendungsbemerkung 15 *Wird das Ziel OE.NI.Übertragung durch die IT-Umgebung erreicht, so ist dieses Ziel der IT-Umgebung zuzuordnen. Das Kapitel Sicherheitsanforderungen an die IT-Umgebung ist dann um die Komponente FTP_ITC zu ergänzen. Wird das Ziel vom EVG umgesetzt, so ist es dem EVG zuzuordnen und im Erklärungsteil auf die dadurch abgewehrte Bedrohung zurückzuführen. Das Kapitel Funktionale Sicherheitsanforderungen an den EVG ist dann um die Komponente FTP_ITC zu ergänzen.*

110 OE.NI.Überlastung Damit der EVG alle von den Signalaufnahmekomponenten zugesandten Bilder aufnehmen kann, müssen die Übertragungsleitungen und die Plattform, auf welcher der EVG läuft, so dimensioniert werden, dass eine Überlastung des EVG durch zu hohes Bilddatenaufkommen nicht auftreten kann.

5 IT-Sicherheitsanforderungen

111 Die IT-Sicherheitsanforderungen stellen die funktionalen Anforderungen an den EVG und seine Umgebung dar und definieren die Anforderungen an die Vertrauenswürdigkeit.

112 Die im Folgenden aufgeführten funktionalen Sicherheitsanforderungen entstammen dem Teil 2 der CC [CC-Teil2], in dem die Anforderungen bausteinartig in hierarchische Strukturen definiert sind. Die Notation der Anforderungen entspricht der in den Common Criteria. In den Elementen ausgeführte Operationen „Zuweisung“ und „Auswahl“ sind *kursiv* dargestellt, während „Verfeinerungen“ unterstrichen gedruckt sind. Iterationen erfolgen grundsätzlich auf Ebene von Komponenten. Die Kurzbezeichnungen der iterierten Komponenten sind um Postfixe ergänzt.

5.1 Sicherheitsanforderungen an den EVG

5.1.1 Definition der funktionalen Sicherheitspolitik für Videoflusskontrolle

113 Der EVG darf alle von Signalaufnahmekomponenten empfangenen Bilddaten speichern, wenn diese erfolgreich auf Authentizität geprüft werden konnten.

114 Jeder authentisierte Beobachter, Administrator und Revisor/bDSB darf alle vom EVG verwalteten Bilddaten lesen und auswerten.

115 Nur die Rollen Beobachter und Administrator dürfen Bilddaten aus dem Anwendungsbereich der TSF exportieren, wenn zuvor eine hierfür ausreichende Begründung eingegeben wurde. Dies schließt auch Drucken mit ein. Dem Revisor/bDSB ist dies explizit verboten.

116 Nur der Rolle Revisor/bDSB ist das manuelle Löschen von Bilddaten erlaubt, wenn zuvor eine hierfür ausreichende Begründung eingegeben wurde.

117 Die Bilddaten werden vom EVG automatisch gelöscht, wenn die entsprechende Löschfrist erreicht wurde.

118 Ein anderer Transfer von Bilddaten als oben erlaubt ist explizit verboten. Dies schließt auch das Speichern von nicht erfolgreich geprüften Bilddaten oder ein Verändern von bereits gespeicherten Bilddaten mit ein.

5.1.2 Funktionale Sicherheitsanforderungen an den EVG

119 Im Folgenden werden die funktionalen Sicherheitsanforderungen für den EVG dargestellt.

120 Die Komponente FAU_GEN.1 wird iteriert, um die Unterscheidung von optional protokollierbaren Ereignissen und verpflichtend zu protokollierenden Ereignissen zu strukturieren. Die Protokollierung der optionalen Ereignisse kann vom Revisor/bDSB konfiguriert werden. Die verpflichtenden Ereignisse werden immer protokolliert (nicht konfigurierbar).

121 Die Instanzen der Komponente FDP_SDI.1 definieren die unterschiedlichen Integritätsmerkmale, die der EVG zur Erkennung von Manipulationen an Daten erzeugen muss.

122 Die Komponenten FMT_MTD.1 wurde ebenfalls iteriert, um die verschiedenen Berechtigungen zur Verwaltung von TSF-Daten abzubilden.

5.1.2.1 FAU_GEN.1 (Optional) Generierung der Protokolldaten

123 Ist hierarchisch zu: Keinen anderen Komponenten.

124 FAU_GEN.1.1 Die TSF müssen in der Lage sein, für folgende protokollierbaren Ereignisse eine Protokollaufzeichnung zu generieren:

a) Starten und Beenden der Protokollierungsfunktionen;

b) Alle protokollierbaren Ereignisse für den *nicht angegebenen* Protokollierungsgrad[13]; und-

c)

- *Fehlerhafte Prüfung der Authentizität von empfangenen Bilddaten*
- *fehlerhafte Prüfung des Integritätsmerkmals von gespeicherten Bilddaten*
- *fehlerhafte Prüfung des Integritätsmerkmals der Protokolldaten*
- *Auswerten von Bilddaten*
- *Modifizierungen von Benutzeraccounts (hier: Beobachter, Administrator, Revisor/bDSB) einschließlich dem Zurücksetzen des Passworts*
- *Veränderung von EVG-Parametern*

125 FAU_GEN.1.2 Die TSF müssen innerhalb jeder Aufzeichnung mindestens die folgenden Informationen speichern:

a) Datum und Uhrzeit des Ereignisses, Art des Ereignisses, Identität des Beobachter, Administrator oder Revisor/bDSB und das Ergebnis (Erfolg oder Mißerfolg) des Ereignisses; und

b) basierend auf den Definitionen der in PP/ST eingebundenen protokollierbaren Ereignisse, für jede Art von Protokollierungsereignissen

- *Für Auswertungen von Bilddaten die vom Benutzer eingegebenen Auswahlkriterien.*

[13] Die Wortstellung wurde zu Gunsten eines korrekten Satzes umgestellt. Dies wird jedoch nicht als Verfeinerung betrachtet.

- *Bei Modifikationen von Benutzeraccounts die Bezeichnung des modifizierten Benutzeraccounts.*
- *Bei Veränderung von EVG-Parameter mindestens den Namen des Parameters.*

126 Abhängigkeiten: FPT_STM.1 Verlässliche Zeitstempel

5.1.2.2 FAU_GEN.1 (Pflicht) Generierung der Protokolldaten

127 Ist hierarchisch zu: Keinen anderen Komponenten.

128 FAU_GEN.1.1 Die TSF müssen für folgende protokollierbaren Ereignisse eine Protokollaufzeichnung generieren:

a) Starten und Beenden der Protokollierungsfunktionen;

Anwendungsbemerkung 16 *Da diese Protokollierungsfunktion im EVG nicht abschaltbar ist, ist dieser Protokolleintrag gleichbedeutend mit dem Start und der Beendigung des EVG*

b) Alle protokollierbaren Ereignisse für den *nicht angegebenen* Protokollierungsgrad[14]; und

c)

- *Exportieren von Bilddaten*
- *Löschen von Bilddaten auf Anforderung des Betroffenen*
- *Konfiguration der Löschzyklen für Bilddaten*
- *Konfiguration der Protokolldateien*
- *Misslungener Gebrauch des Authentisierungsmechanismus*
- *Misslungener Gebrauch des Benutzeridentifikationsmechanismus*
- *Alle Modifizierungen von Werten der Sicherheitsattribute*
- *Alle Modifizierungen des Anfangswertes von Sicherheitsattributen*
- *Protokollierung eines Signalausfalls*
- *Protokollierung, wenn der Signalausfall beendet ist*

129 FAU_GEN.1.2 Die TSF müssen innerhalb jeder Aufzeichnung mindestens die folgenden Informationen speichern:

a) Datum und Uhrzeit des Ereignisses, Art des Ereignisses, Identität des Subjektes und das Ergebnis (Erfolg oder Mißerfolg) des Ereignisses; und

[14] Die Wortstellung wurde zu Gunsten eines korrekten Satzes umgestellt. Dies wird jedoch nicht als Verfeinerung betrachtet.

b) basierend auf den Definitionen der in PP/ST eingebundenen protokollierbaren Ereignisse, für jede Art von Protokollierungsereignissen.

- *Beim Exportieren von Bilddaten die Begründung.*
- *Beim manuellen Löschen von Bilddaten die Begründung.*

130 Abhängigkeiten: FPT_STM.1 Verlässliche Zeitstempel

5.1.2.3 FAU_SAR.1 Durchsicht der Protokollierung

131 Diese Komponente stellt den autorisierten Benutzern die Fähigkeit zur Erlangung und Interpretation von Informationen bereit. Im Fall von menschlichen Benutzern müssen diese Informationen in einer für Menschen verständlichen Form dargestellt werden. Im Fall von externen IT-Einheiten muß die Information eindeutig in elektronischer Form dargestellt werden.

132 Ist hierarchisch zu: Keinen anderen Komponenten.

133 FAU_SAR.1.1 Die TSF müssen für *Beobachter, Administrator und Revisor/bDSB* die Fähigkeit bereitstellen, *alle protokollierten Ereignisse* aus den Protokollaufzeichnungen zu lesen.

134 FAU_SAR.1.2 Die TSF müssen die Protokollaufzeichnungen in einer für die Interpretation der Informationen durch Beobachter, Administrator und Revisor/bDSB geeigneten Art und Weise bereitstellen.

135 Abhängigkeiten: FAU_GEN.1 Generierung von Protokolldaten
hier
FAU_GEN.1 (Pflicht) Generierung der Protokolldaten
FAU_GEN.1 (Optional) Generierung der Protokolldaten

5.1.2.4 FDP_IFC.1 Teilweise Informationsflußkontrolle

136 Ist hierarchisch zu: Keinen anderen Komponenten.

137 FDP_IFC.1.1 Die TSF müssen die *funktionale Sicherheitspolitik für Videoflusskontrolle* für *Signalaufnahmekomponenten, Beobachter, Administrator und Revisor/bDSB für Empfangen und Speichern, Lesen und Auswerten, Exportieren und Löschen von Bilddaten* durchsetzen.

138 Abhängigkeiten: FDP_IFF.1 Einfache Sicherheitsattribute

5.1.2.5 FDP_IFF.1 Einfache Sicherheitsattribute

139 Ist hierarchisch zu: Keinen anderen Komponenten.

140 FDP_IFF.1.1 Die TSF müssen die *funktionale Sicherheitspolitik für Videoflusskontrolle* auf Grundlage folgender Arten von Subjekt- und Informations-Sicherheitsattributen:

- *Signalaufnahmekomponenten*
  - *Liste der Attribute: Kamera-ID*
- *Beobachter, Administrator und Revisor/bDSB*
  - *Liste der Attribute: Rollenzugehörigkeit*
- *Bilddaten*
  - *Liste der Attribute: Authentizitätsmerkmal der Bilddaten, Aufnahmedatum, -zeit, Kamera-ID, Integritätsmerkmale*
- *Protokolldaten*
  - *Liste der Attribute: Integritätsmerkmal*

Anwendungsbemerkung 17 *Unter „Authentizitätsmerkmal" kann hier z.B. die in das Bild eingeblendete ID der Kamera verstanden werden.*

durchsetzen.

141 FDP_IFF.1.2 Die TSF müssen einen über eine kontrollierte Operation erfolgenden Informationsfluß zwischen einem kontrollierten Subjekt und den kontrollierten Informationen erlauben, wenn die folgenden Regeln zutreffen:

SFP-Regel .1 *Aufzeichnung aller vom EVG empfangenen Bilddaten, wenn diese auf Authentizität erfolgreich geprüft werden konnten.*

SFP-Regel .2 *Lesen und Auswerten von aufgezeichneten Bilddaten an Beobachter, Administrator oder Revisor/bDSB, wobei die Bilddaten anhand der Attribute Aufnahmedatum, -zeit und/oder Kameraidentifikation zu bestimmen sind.*

SFP-Regel .3 *Exportieren von aufgezeichneten Bilddaten aus dem Anwendungsbereich der TSF durch Beobachter oder Administrator, wenn eine Begründung hierfür angegeben wurde.*

142 FDP_IFF.1.3 Die TSF müssen *keine zusätzliche SFP-Regeln* durchsetzen.

143 FDP_IFF.1.4 Die TSF müssen folgende *zusätzliche SFP-Fähigkeiten* bereitstellen:

SFP-Regel .4 *Erkennung eines Signalausfalls und Benachrichtigung eines Beobachters, Administrators oder Revisor/bDSB.*

SFP-Regel .5 *Erkennung, dass der Signalausfall beendet ist und Benachrichtigung eines Beobachters, Administrators oder Revisor/bDSB.*

SFP-Regel .6 *Benachrichtigung eines Beobachters, Administrators oder Revisor/bDSB, falls empfangene Bildda-*

ten nicht erfolgreich auf Authentizität geprüft werden konnten.

SFP-Regel .7 *Benachrichtigung eines Beobachters, Administrators oder Revisor/bDSB, wenn gespeicherte Bilddaten nicht erfolgreich auf Integrität geprüft werden konnten.*

SFP-Regel .8 *Benachrichtigung eines Beobachters, Administrators oder Revisor/bDSB, wenn gespeicherte Protokolldaten nicht erfolgreich auf Integrität geprüft werden konnten.*

SFP-Regel .9 *Automatisches Löschen von Bilddaten, wenn diese ihre konfigurierte Löschfrist erreicht haben.*

SFP-Regel .10 *Löschen von Bilddaten durch den Revisor/bDSB, wenn er eine Begründung hierfür angegeben hat.*

144 FDP_IFF.1.5 Die TSF müssen einen Informationsfluß auf Grundlage folgender Regeln explizit autorisieren:

SFP-Regel .11 keine

145 FDP_IFF.1.6 Die TSF müssen einen Informationsfluß auf Grundlage folgender Regeln explizit verweigern:

SFP-Regel .12 *Ein anderer Transfer von Bilddaten als oben explizit erlaubt ist verboten. Dies schließt ein Speichern nicht erfolgreich geprüfter empfangener Bilddaten oder ein Verändern von gespeicherten Bilddaten und Protokolldaten mit ein.*

146 Abhängigkeiten: FDP_IFC.1 Teilweise Informationsflußkontrolle
FMT_MSA.3 Initialisierung statischer Attribute

5.1.2.6 FDP_ITC.2 Import von Benutzerdaten mit Sicherheitsattributen

147 Ist hierarchisch zu: Keinen anderen Komponenten.

148 FDP_ITC.2.1 Die TSF müssen die *funktionale Sicherheitspolitik für Videoflusskontrolle* beim Import von unter Kontrolle der SFP stehenden Bilddaten von außerhalb des TSC durchsetzen.

149 FDP_ITC.2.2 Die TSF müssen die mit den importierten Bilddaten verknüpften Sicherheitsattribute benutzen.

Anwendungsbemerkung 18 *Die in FDP_ITC.2.2 erwähnten Sicherheitsattribute von Bilddaten können z.B. die KameraID oder der Aufnahmezeitpunkt sein.*

150 FDP_ITC.2.3 Die TSF müssen sicherstellen, daß das benutzte Protokoll eine Möglichkeit zur eindeutigen Verknüpfung zwischen den Sicherheitsattributen und den empfangenen Bilddaten bereitstellt.

151 FDP_ITC.2.4 Die TSF müssen sicherstellen, daß die Interpretation der Sicherheitsattribute von importierten Bilddaten so erfolgt, wie es vom Sender der Benutzerdaten vorgesehen ist.

152 FDP_ITC.2.5 Die TSF müssen die folgenden Regeln beim Import unter Kontrolle der SFP stehender Bilddaten von außerhalb des TSC durchsetzen:

- *Keine weiteren als bei FDP_IFF.1*

153 Abhängigkeiten: [FDP_ACC.1 Teilweise Zugriffskontrolle,
oder
FDP_IFC.1 Teilweise Informationsflußkontrolle]

[FTP_ITC.1 Inter-TSF Vertrauenswürdiger Kanal,
oder
FTP_TRP.1 Vertrauenswürdiger Pfad]

FPT_TDC.1 Einfache Inter-TSF TSF-Datenkonsistenz

5.1.2.7 FDP_RIP.1 Teilweiser Schutz bei erhalten gebliebenen Informationen

154 Ist hierarchisch zu: Keinen anderen Komponenten.

155 FDP_RIP.1.1 Die TSF müssen sicherstellen, dass der frühere Informationsinhalt eines persistenten Speichers für Bilddaten bei *automatischem oder manuellem Löschen des Speicherplatzes der gelöschten Bilddaten* nicht verfügbar ist.

156 Abhängigkeiten: Keine Abhängigkeiten

5.1.2.8 FDP_SDI.1 (Bild.L) Überwachung der Integrität der gespeicherten Daten

157 Ist hierarchisch zu: Keinen anderen Komponenten.

158 FDP_SDI.1.1 Die TSF müssen die innerhalb des TSC gespeicherten Bilddaten auf *nicht autorisiertes Löschen* bei allen Objekten auf Basis *eines vom EVG zu erzeugenden Integritätsmerkmals über alle Bilddaten* überwachen.

159 Abhängigkeiten: Keine Abhängigkeiten

Anwendungsbemerkung 19 *Es ist zulässig, dass der EVG dieses Integritätsmerkmal auch indirekt über alle Bilddaten erstellt, z.B. nur über eine Liste von momentan gespeicherten Bilddaten, nicht über die Bilddaten selbst.*

Anwendungsbemerkung 20 *Der EVG muss diese Überwachung nicht permanent durchführen. Eine sporadische Prüfung oder eine Prüfung auf Anforderung des Benutzers ist ausreichend.*

5.1.2.9 FDP_SDI.1 (Bild.V) Überwachung der Integrität der gespeicherten Daten

160 Ist hierarchisch zu: Keinen anderen Komponenten.

161 FDP_SDI.1.1 Die TSF müssen die innerhalb des TSC gespeicherten Bilddaten auf *Manipulation* bei allen Objekten auf Basis *eines vom EVG zu erzeugenden Integritätsmerkmal für Bilddaten* überwachen.

162 Abhängigkeiten: Keine Abhängigkeiten

Anwendungsbemerkung 21 *Der EVG muss diese Überwachung nicht permanent durchführen. Eine sporadische Prüfung oder eine Prüfung auf Anforderung des Benutzers ist ausreichend.*

5.1.2.10 FDP_SDI.1 (Prot.) Überwachung der Integrität der gespeicherten Daten

163 Ist hierarchisch zu: Keinen anderen Komponenten.

164 FDP_SDI.1.1 Die TSF müssen die innerhalb des TSC gespeicherten Protokolldaten auf *Manipulation* bei allen Objekten auf Basis *eines vom EVG zu erzeugenden Integritätsmerkmals für Protokolldaten* überwachen.

165 Abhängigkeiten: Keine Abhängigkeiten

Anwendungsbemerkung 22 *Der EVG muss diese Überwachung nicht permanent durchführen. Eine sporadische Prüfung oder eine Prüfung auf Anforderung des Benutzers ist ausreichend.*

5.1.2.11 FIA_UAU.2 Benutzerauthentisierung vor jeglicher Aktion

166 Ist hierarchisch zu: FIA_UAU.1

167 FIA_UAU.2.1 Die TSF müssen erfordern, daß jeder Beobachter, Administrator und Revisor/bDSB erfolgreich authentisiert wurde, bevor diesem jegliche andere TSF-vermittelte Aktionen erlaubt werden.

168 Abhängigkeiten: FIA_UID.1 Zeitpunkt der Identifikation
hier
FIA_UID.2 Benutzeridentifikation vor jeglicher Aktion

5.1.2.12 FIA_UID.2 Benutzeridentifikation vor jeglicher Aktion

169 Ist hierarchisch zu: FIA_UID.1

170 FIA_UID.2.1 Die TSF müssen erfordern, daß sich jeder Beobachter, Administrator und Revisor/bDSB identifiziert, bevor für diesen jegliche andere TSF-vermittelte Aktionen erlaubt werden.

171 Abhängigkeiten: Keine Abhängigkeiten

5.1.2.13 FMT_MSA.1 Management der Sicherheitsattribute

172 Ist hierarchisch zu: Keinen anderen Komponenten.

173 FMT_MSA.1.1 Die TSF müssen die *funktionale Sicherheitspolitik für Videoflusskontrolle* zur Beschränkung der Fähigkeit zum *Standardvorgabe ändern, Abfragen und Modifizieren* der Sicherheitsattribute *Löschzyklen für Bilddaten* auf *den Revisor/bDSB* durchsetzen.

174 Abhängigkeiten: [FDP_ACC.1 Teilweise Zugriffskontrolle
oder
FDP_IFC.1 Teilweise Informationsflußkontrolle]

FMT_SMF.1 Spezifikation von Management-Funktionen

FMT_SMR.1 Sicherheitsrollen

5.1.2.14 FMT_MSA.3 Initialisierung statischer Attribute

175 Ist hierarchisch zu: Keinen anderen Komponenten.

176 FMT_MSA.3.1 Die TSF müssen die *funktionale Sicherheitspolitik für Videoflusskontrolle* zur Bereitstellung von vorgegebenen Standardwerten mit *einschränkenden Eigenschaften* für Sicherheitsattribute, die zur Durchsetzung der SFP benutzt werden, durchsetzen.

177 FMT_MSA.3.2 Die TSF müssen dem *Revisor/bDSB* gestatten, beim Empfangen eines Bildes alternative aber gesetzlich zulässige Löschzyklen zu spezifizieren, die die vorgegebenen Standardwerte ersetzen.

178 Abhängigkeiten: FMT_MSA.1 Management der Sicherheitsattribute

FMT_SMR.1 Sicherheitsrollen

> ***Anwendungsbemerkung 23*** *Die hier angesprochenen gesetzlich zulässigen Löschzyklen geben die minimale und/oder maximale Speicherdauer von Bilddaten an. Diese Werte dürfen sich nur in den gesetzlich vorgegebene Grenzwerte bewegen.*

5.1.2.15 FMT_MTD.1 (Einrichtung) Management der TSF-Daten

179 Ist hierarchisch zu: Keinen anderen Komponenten.

180 FMT_MTD.1.1 Die TSF müssen die Fähigkeit zum

- *Einrichten* von *Beobachteraccounts*
- *Vorgabe von Initialpasswörtern sowie Rücksetzen* der *Passwörter*

auf *den Administrator* beschränken.

181 Abhängigkeiten: FMT_SMF.1 Spezifikation von Management-Funktionen
FMT_SMR.1 Sicherheitsrollen

Anwendungsbemerkung 24 *Die Rolle Revisor/bDSB ist fest vorgegeben und kann nicht vom Administrator administriert werden. Wenn keine Modifikationen an der Rolle Revisor möglich sind, ist diese Forderung erfüllt.*

Anwendungsbemerkung 25 *Es wird gefordert, dass mindestens ein Administratoren-Account vorhanden ist. Die Möglichkeit zur Erzeugung weiterer Administratoren-Accounts ist optional.*

5.1.2.16 FMT_MTD.1 (Passwörter) Management der TSF-Daten

182 Ist hierarchisch zu: Keinen anderen Komponenten.

183 FMT_MTD.1.1 Die TSF müssen die Fähigkeit zum *Modifizieren von eigenen Passwörtern* auf *den damit verknüpften Beobachter, Administrator oder Revisor/bDSB* beschränken.

184 Abhängigkeiten: FMT_SMF.1 Spezifikation von Management-Funktionen
FMT_SMR.1 Sicherheitsrollen

5.1.2.17 FMT_MTD.1 (Prot.) Management der TSF-Daten

185 Ist hierarchisch zu: Keinen anderen Komponenten.

186 FMT_MTD.1.1 Die TSF müssen die Fähigkeit zum *Modifizieren* von

- *Parameter zur Behandlung der Protokolldatei*
- *Umfang der Protokollierung*

auf *den Revisor/bDSB* beschränken.

187 Abhängigkeiten: FMT_SMF.1 Spezifikation von Management-Funktionen
FMT_SMR.1 Sicherheitsrollen

5.1.2.18 FMT_SMF.1 Spezifikation von Management-Funktionen

188 Ist hierarchisch zu: Keinen anderen Komponenten.

189 FMT_SMF.1.1 Die TSF müssen in der Lage sein, die folgenden Sicherheitsmanagementfunktionen auszuführen:

- *Standardvorgabe ändern, Abfragen und Modifizieren der Sicherheitsattribute Löschzyklen für Bilddaten*
- *Einrichten von Beobachteraccounts*
- *Vorgabe von Initialpasswörtern sowie Rücksetzen der Passwörter anderer Benutzer*
- *Ändern des eigenen Passwortes*

- *Ändern der Parameter zur Behandlung der Protokolldatei*
- *Ändern des Umfangs der Protokollierung*

190 Abhängigkeiten: Keine Abhängigkeiten

5.1.2.19 FMT_SMR.1 Sicherheitsrollen

191 Ist hierarchisch zu: Keinen anderen Komponenten.

192 FMT_SMR.1.1 Die TSF müssen die Rollen *Beobachter, Administrator und Revisor/bDSB* erhalten.

193 FMT_SMR.1.2 Die TSF müssen Benutzer mit Rollen verknüpfen können.

194 Abhängigkeiten: FIA_UID.1 Zeitpunkt der Identifikation
hier
FIA_UID.2 Benutzeridentifikation vor jeglicher Aktion

5.1.2.20 FPT_TDC.1 Einfache Inter-TSF TSF-Datenkonsistenz

195 Ist hierarchisch zu: Keinen anderen Komponenten.

196 FPT_TDC.1.1 Die TSF müssen die Fähigkeit zur konsistenten Interpretation von *Bilddaten* bereitstellen, wenn diese von den TSF und einem anderen vertrauenswürdigen IT-Produkt gemeinsam genutzt werden.

197 FPT_TDC.1.2 Die TSF müssen [Zuweisung: *Liste der von den TSF anzuwendenden Interpretationsregeln*] benutzen, wenn diese die TSF-Daten von einem anderen vertrauenswürdigen IT-Produkt interpretieren.

198 Abhängigkeiten: Keine Abhängigkeiten

Anwendungsbemerkung 26 *Die bei FPT_TDC.1.2 einzufügende Liste von Interpretationsregeln soll die verwendeten Grafikformate (z.B. GIF, JPG, MPEG4, etc.) enthalten.*

5.1.3 Anforderungen an die Vertrauenswürdigkeit des EVG

199 Die Anforderungen an die Vertrauenswürdigkeit, welche vom EVG erfüllt werden müssen, sind in nachfolgender Tabelle (Tabelle 1: Maßnahmen zur Erfüllung von EAL1) aufgeführt. Sie entsprechen der Vertrauenswürdigkeitsstufe EAL1 aus [CC-Teil3].

Tabelle 1: Maßnahmen zur Erfüllung von EAL1

Anforderungen gemäß EAL1		Maßnahmen der Entwickler und Evaluatoren
Konfigurations-management	ACM_CAP.1	Kennzeichnung des EVG mit einem eindeutigen Verweisnamen

Anforderungen gemäß EAL1		Maßnahmen der Entwickler und Evaluatoren
Auslieferung und Betrieb	ADO_IGS.1	Dokumentation der zum Schutz des EVG bei Auslieferung, Installation und Anlauf getroffenen Maßnahmen
Entwicklung	ADV_FSP.1	Definition von Anforderungen gemäß CC an die Abstraktionsstufen des EVG
	ADV_RCR.1	
Handbücher	AGD_ADM.1	Erstellung eines Systemverwalter- und Benutzer-handbuchs
	AGD_USR.1	
Testen	ATE_IND.1	unabhängiges Testen durch den Evaluator

5.2 Sicherheitsanforderungen an die IT-Umgebung

200 Im Folgenden werden die funktionalen Sicherheitsanforderungen an die IT-Umgebung aufgelistet.

- FDP_ACC.2 Vollständige Zugriffskontrolle
- FDP_ACF.1 Zugriffskontrolle basierend auf Sicherheitsattributen
- FDP_ETC.2 Export von Benutzerdaten mit Sicherheitsattributen
- FDP_IFC.1 Teilweise Informationsflusskontrolle
- FDP_IFF.1 Einfache Sicherheitsattribute
- FMT_MSA.1 Management der Sicherheitsattribute
- FMT_MSA.3 Initialisierung statischer Attribute
- FPT_STM.1 Verlässliche Zeitstempel

Anwendungsbemerkung 27 *Es ist zulässig, die Zeit vom unterliegenden System oder von den Komponenten zur Signalaufnahme zu übernehmen, die bei kritischen Anwendungen um weitere Sicherheitsmechanismen ergänzt werden können.*

6 Erklärung

201 Der Erklärungsteil eines Schutzprofils stellt eine Art von Qualitätskontrolle des Schutzprofil-Verfassers dar, in der eine Analyse der bisherigen Kapitel hinsichtlich Vollständigkeit, Angemessenheit und Widerspruchsfreiheit durchgeführt wird.

202 Die Erklärung zeigt, dass das Schutzprofil eine vollständige und zusammengehörige Menge von IT-Sicherheitsanforderungen ist und dass ein konformer EVG die Sicherheitserfordernisse wirksam ansprechen würde.[15]

6.1 Erklärung der Sicherheitsumgebung und der Sicherheitsziele

203 In diesem Teil der Erklärung wird dargelegt, dass die Aspekte der Sicherheitsumgebung durch die Sicherheitsziele abgedeckt werden. Darüber hinaus wird die Sicherheitsumgebung dargelegt.

204 Die Zuordnung der Sicherheitsumgebung (Annahmen, Bedrohungen und organisatorische Sicherheitspolitiken) zu den Sicherheitszielen für den EVG und die Umgebung ist in Tabelle 2 dargelegt.

Tabelle 2: Abdeckung der Sicherheitsumgebung durch Sicherheitsziele

Sicherheitsumgebung	Sicherheitsziele
A.Alle	OE.NI.Alle
A.Backup	OE.NI.Backup
A.BD.Zuordnung	OE.IT.BD.Zuordnung, OE.IT.Uhrzeit
A.Betrieb	OE.NI.Betrieb
A.Kamera	OE.IT.Kamera
A.NoBackup	OE.NI.NoBackup
A.Plattform	OE.IT.Plattform
A.Schnittstellen	OE.NI.Schnittstellen
A.Speicher	OE.NI.Speicher
A.Überlastung	OE.NI.Überlastung
A.Übertragung	OE.NI.Übertragung
A.Uhrzeit	OE.IT.Uhrzeit
T.BD.Ausfall	O.BD.Ausfall
T.BD.Import	O.BD.Import

[15] Verfügt ein konkretes System zusätzlich über die Funktion, bestimmte Bereiche auszublenden, sind im Erklärungsteil der ST entsprechende Angaben nachzuziehen.

Sicherheitsumgebung	Sicherheitsziele
T.BD.Lösch	O.BD.Lösch, OE.IT.Plattform, OE.NI.Alle
T.BD.Veränd	O.BD.Veränd, OE.IT.Plattform, OE.NI.Alle
T.Einspielen	O.Einspielen, OE.NI.Schnittstellen
T.KonfigS3	O.KonfigS3
T.Löschung	O.Löschung
T.Nachvollz	O.Nachvollz
T.PD.Veränd	O.PD.Veränd, OE.IT.Plattform, OE.NI.Alle
T.S3Aktion	O.S3Aktion
T.Zugriff	O.Zugriff
P.Begründ	O.Begründ
P.KonfigS2	O.KonfigS2
P.Löschgarantie	O.Löschgarantie
P.S3Export	O.S3Export

6.1.1 Abdeckung der Annahmen

205 **A.Alle**: Es wird angenommen, dass der Administrator, die Beobachter, der Revisor/bDSB und das Fremdpersonal aus den Bilddaten gewonnene Informationen nicht weitergeben – also beispielsweise keine Bildinhalte abfotografieren – Darüber hinaus verwahren sie ihr Passwort sicher und nutzen es sorgsam. Das Sicherheitsziel für die Umgebung **OE.NI.Alle** deckt diese Annahme ab.

206 **A.Backup**: Es wird angenommen, dass die EVG-Daten mit Ausnahme der Bilddaten (vgl. A.NoBackup) regelmäßig gesichert werden, so dass ein Hardware-Ausfall des Massenspeichers nicht dazu führt, dass protokollierte Ereignisse nicht nachvollziehbar wären. Weiterhin ist eine Manipulation der gesicherten Daten (insbesondere der Konfigurationsdaten) ausgeschlossen. Das Sicherheitsziel für die Umgebung **OE.NI.Backup** deckt diese Annahme ab.

207 **A.BD.Zuordnung:** Gemäß der Annahme soll die IT-Einsatzumgebung die erzeugten Bilddaten vor dem Versand an den EVG mit der Kamera-ID und Datum/Uhrzeit der Aufnahme versehen. Durch **OE.IT.BD.Zuordnung** wird diese Annahme vollständig umgesetzt. **OE.IT.Uhrzeit** unterstützt hierbei durch die Bereitstellung der korrekten Uhrzeit.

208 **A.Betrieb**: Es wird angenommen, dass der Rechner mit allen Komponenten (incl. Monitore), von denen die Durchsetzung der SFP des EVG abhängt, in einem Bereich eingesetzt wird, zu dem nur Beobachter, Administrator, Revisor/bDSB und Fremdpersonal Zutritt haben. Der logische und physikalische Zugang zu den IT-Komponenten (schließt ihre Hardware-Schnittstellen mit ein) muss ebenfalls auf diesen Bereich eingeschränkt sein. Das Sicherheitsziel für die Umgebung **OE.NI.Betrieb** deckt diese Annahme ab.

209 **A.Kamera**: Es wird angenommen, dass die Komponenten zur Signalaufnahme authentische Bilder aus zulässigen Bereichen liefern. Manipulationen an der Kamera, die nicht zu einem kompletten Ausfall führen – etwa ein Verstellen/Verändern von Objektiv, Zoom oder Perspektive – sind ebenfalls inbegriffen. Das Sicherheitsziel für die Umgebung **OE.IT.Kamera** deckt diese Annahme ab.

210 **A.NoBackup**: Da der EVG keine Kontrolle über ausgelagerte Bilddaten hat, wird angenommen, dass kein Backup für die Bilddaten durchgeführt wird. Das Sicherheitsziel für die Umgebung **OE.NI.NoBackup** deckt diese Annahme ab.

211 **A.Plattform**: Damit der EVG seine SFP durchsetzen kann, muss die Plattform, auf der der EVG betrieben wird, so eingerichtet sein, dass keine Zugriffe auf die vom EVG zu schützenden Objekte und die Protokolldaten direkt über die Plattform möglich sind und dass auch keine Bedrohungen auf den EVG oder die zu schützenden Objekte von der Plattform (etwa durch Viren, Trojaner oder andere Software) selbst ausgehen. Das Sicherheitsziel für die Umgebung **OE.IT.Plattform** deckt diese Annahme ab.

212 Mit **A.Schnittstellen** wird angenommen, dass die externen Hardware-Komponenten vollständig und korrekt mit dem EVG System verbunden sind. Dies wird durch **OE.NI.Schnittstellen** gewährleistet.

213 **A.Speicher**: Es wird angenommen, dass der Speicher für die Bild- und Protokolldaten ausreichend groß dimensioniert ist. Das Sicherheitsziel für die Umgebung **OE.NI.Speicher** fordert eine ausreichende Dimensionierung der Speicher für Bild- und Protokolldaten und stellt den Überlauf des Protokollspeichers durch rechtzeitiges Bereinigen sicher. Damit ist die Annahme vollständig abgedeckt.

214 **A.Überlastung**: Gemäß der Annahme ist die Kapazität der Übertragungsleitungen und die Leistungsfähigkeit der EVG Plattform derart abzustimmen, dass selbst ein maximales Bilddatenaufkommen nicht zu einer Überlastung des EVG führen kann. Dies fordert das Umgebungsziel **OE.NI.Überlastung** und deckt damit die Annahme vollständig ab.

215 **A.Übertragung**: Es wird angenommen, dass der Übertragungsweg der Bilddaten so geschützt ist, dass ein Mitlesen, gezieltes Verändern (beispielsweise durch ein Entfernen oder Hinzufügen von Bildausschnitten) und Einspielen falscher Bilddaten nicht möglich ist. Diese Annahme wird durch das Sicherheitsziel **OE.NI.Übertragung** umgesetzt.

216 **A**.**Uhrzeit**: Die Bereitstellung der korrekten Uhrzeit wird von der IT-Einsatzumgebung mit **OE.IT.Uhrzeit** zu dem Zweck angepeilt, den Aufnahmezeitpunkt von Bilddaten mit diesen verknüpfen sowie die Protokolleinträge mit der korrekten Zeit des Ereignisses versehen zu können und den Löschzeitpunkt für die Bilddaten ermitteln und einhalten zu können.

6.1.2 Begegnung der Bedrohungen

217 **T.BD.Ausfall**: Eine Bedrohung besteht darin, dass vom EVG nicht bemerkt wird, wenn keine Bilddaten von einer einzelnen Signalaufnahmekomponente mehr zum EVG geliefert werden. Ebenfalls ist das Nicht-Erkennen des Endes eines Ausfalls eine Bedrohung. Das Sicherheitsziel **O.BD.Ausfall** deckt beide Bedrohungen ab.

218 **T.BD.Import:** Die Bedrohung „Einschleusen nicht authentischer Bilddaten“ wird durch das Ziel „Authentisierungsprüfung aller Bilddaten bei Empfang“ vollständig begegnet. Die Authentisierungsprüfung soll über ein in den Bilddaten enthaltenes Authentizitätsmerkmal erfolgen, dass bei nicht authentischen Bilddaten nicht oder fehlerhaft vorhanden ist. Ein Nachweis der Authentizität ist damit möglich.

219 **T.BD.Lösch**: Diese Bedrohung zielt auf den datenschutzrechtlichen Aspekte „Gewährleistung, dass Bilddaten nicht unzulässig gelöscht werden“ ab. Einzig dem Revisor/bDSB ist es erlaubt, Bilddaten – nachvollziehbar auf Anforderung eines Betroffenen (vgl. P.Begründ) – zu löschen. (vgl. Anhang A). Die Bedrohung besteht also darin, dass Bilddaten vom Beobachter oder Administrator unbemerkt gelöscht werden. Das Sicherheitsziel **O.BD.Lösch** deckt diese Bedrohung ab. Über **OE.IT.Plattform** und **OE.NI.Alle** wird sichergestellt, dass der EVG und seine Zugriffsbeschränkungen nicht umgangen werden.

220 **T.BD.Veränd**: Bilddaten dürfen von niemandem (weder Beobachter, noch Administrator oder Revisor/bDSB) verfälscht oder manipuliert werden. Da der Administrator unter Umgehung des EVG Bilddaten verändern könnte, muss der EVG dies erkennen können. Das Sicherheitsziel **O.BD.Veränd** deckt diese Bedrohung vollständig ab. Über **OE.IT.Plattform** und **OE.NI.Alle** wird zusätzlich sichergestellt, dass der EVG und seine Zugriffsbeschränkungen nicht umgangen werden.

221 Die Bedrohung **T.Einspielen** wird durch die Ziele **O.Einspielen** und **OE.NI.Schnittstellen** abgewehrt. O.Einspielen verhindert, dass am Rechner mittels EVG-Funktionen Bilddaten eingespielt werden können. OE.NI.Schnittstellen verhindert das Einspielen von Bilddaten durch Manipulationen an den Hardware-Schnittstellen des EVG Systems.

222 **T.KonfigS3**: Diese Bedrohung zielt darauf ab, dass Beobachter oder Administrator Tätigkeiten ausführen, die sie gemäß Rollendefinition nicht ausführen dürfen, sondern nur der Revisor/bDSB. Diese Bedrohung wird durch das Sicherheitsziel **O.KonfigS3** abgedeckt.

223 **T.Löschung**: Diese Bedrohung zielt darauf ab, dass auf nur logisch gelöschte Bilddaten physikalisch bis zu einem gewissen Grad dennoch zugegriffen werden kann. Diese Bedrohung wird durch das Sicherheitsziel **O.Löschung** abgedeckt.

224 **T.Nachvollz**: Alle datenschutzrechtlich relevanten Beobachter-, Administrator- und Revisor/bDSB-Aktionen müssen protokolliert werden bzw. werden können. Eine Bedrohung besteht darin, dass diese Aktionen durch Abschalten oder Veränderung des Umfangs der Protokollierung nicht mehr nachvollziehbar sind. In **O.Nachvollz** wurde aus dieser Bedrohung heraus ein Sicherheitsziel formuliert, in dem präzisiert wurde, dass für alle datenschutzrelevanten Ereignisse zuverlässig Protokolldaten erzeugt werden müssen bzw. erzeugt werden können.

225 **T.PD.Veränd**: Protokolldaten dürfen von niemandem (weder Beobachter, noch Administrator oder Revisor/bDSB) verfälscht oder manipuliert werden. Da der Administrator unter Umgehung des EVG Protokolldaten verändern könnte, muss der EVG dies erkennen können. Das Sicherheitsziel **O.PD.Veränd** deckt diese Bedrohung vollständig ab. Über **OE.IT.Plattform** und **OE.NI.Alle** wird zusätzlich sichergestellt, dass der EVG und seine Zugriffsbeschränkungen nicht umgangen werden.

226 **T.S3Aktion**: Löschfristen für die Bilddaten sind datenschutzrechtlich korrekt zu konfigurieren. Eine Bedrohung besteht darin, dass der Revisor/bDSB die Löschfristen für die Bilddaten außerhalb des Konfigurationsspielraumes setzt. Das Sicherheitsziel **O.S3Aktion** deckt diese Bedrohung derart ab, dass der EVG gesetzeskonforme Konfigurationsgrenzen setzt.

227 **T.Zugriff**: Die Bedrohung, dass der EVG von Fremdpersonal oder Außenstehenden genutzt wird (d. h. Durchführung von Aktionen, die den Rollen Beobachter, Administrator und Revisor/bDSB zugewiesen sind), welche dadurch insbesondere Zugriff auf Bilddaten erhalten würden, wird durch das Sicherheitsziel **O.Zugriff** abgedeckt, in dem formuliert ist, dass sich jeder, der den EVG nutzen möchte, gegenüber dem EVG erfolgreich authentisieren und identifizieren muss.

6.1.3 Umsetzung der Sicherheitspolitiken

228 **P.Begründ**: Das BDSG legt fest, dass datenschutzrechtlich relevante Aktionen, die unter den Begriff „Zweckänderung“ fallen, immer nur mit Begründung ausgeführt werden dürfen. Darunter fallen insbesondere die Aktionen „Exportieren von Bilddaten“ durch den Beobachter/Administrator und „Löschen von Bilddaten“ bei individuellem Löschungsanspruch (vgl. Anhang A) durch den Revisor/bDSB. Diese Vorgabe, formuliert als Sicherheitspolitik für den EVG, wird durch das Sicherheitsziel **O.Begründ** vollständig abgedeckt.

229 **P.KonfigS2**: Diese OSP zielt darauf ab, dass Beobachter oder Revisor/bDSB Tätigkeiten ausführen, die sie gemäß Rollendefinition nicht ausführen dürfen, sondern nur der Administrator. Das Sicherheitsziel **O.KonfigS2** deckt diese Bedrohung ab.

230 **P.Löschgarantie**: Um die datenschutzrechtlichen Anforderungen an personenbezogene Bilddaten zu gewährleisten, müssen diese Daten nach der jeweils konfigurierten Löschfrist automatisch gelöscht werden. **O.Löschgarantie** setzt dies um.

231 **P.S3Export**: Gemäß der Rollendefinition darf der Revisor/bDSB keine Bilddaten exportieren oder ausdrucken. Das Sicherheitsziel **O.S3Export** setzt diese Vorgabe vollständig um.

6.2 Erklärung der Sicherheitsanforderungen

6.2.1 Erklärung der EVG-Sicherheitsanforderungen

232 Tabelle 3 zeigt, dass die in Abschnitt 4.1 aufgeführten EVG-Sicherheitsziele durch die in Abschnitt 5.1 dargelegten funktionalen Sicherheitsanforderungen abgedeckt werden.

Tabelle 3: Abdeckung der Sicherheitsziele durch Sicherheitsanforderungen

Sicherheitsziel	Funktionale EVG-Sicherheitsanforderungen	
	direkt	unterstützend
O.BD.Ausfall	FAU_GEN.1 (Pflicht) FDP_IFF.1	
O.BD.Import	FAU_GEN.1 (Optional) FDP_IFC.1 FDP_IFF.1	
O.BD.Lösch	FAU_GEN.1 (Optional) FDP_IFC.1 FDP_IFF.1 FDP_SDI.1 (Bild.L)	FIA_UAU.2 FIA_UID.2 FMT_SMR.1
O.BD.Veränd	FAU_GEN.1 (Optional) FDP_IFC.1 FDP_IFF.1 FDP_SDI.1 (Bild.V)	
O.Begründ	FAU_GEN.1 (Pflicht) FDP_IFC.1 FDP_IFF.1	FIA_UAU.2 FIA_UID.2 FMT_SMR.1
O.Einspielen	FDP_IFF.1	
O.KonfigS2	FMT_MTD.1 (Einrichtung) FMT_SMF.1	FIA_UAU.2 FIA_UID.2 FMT_SMR.1
O.KonfigS3	FMT_MSA.1 FMT_MSA.3 FMT_MTD.1 (Prot.) FMT_SMF.1	FIA_UAU.2 FIA_UID.2 FMT_SMR.1
O.Löschgarantie	FDP_IFF.1 FDP_ITC.2	FPT_TDC.1 FPT_STM.1 (in IT-Umgebung)
O.Löschung	FDP_RIP.1	

Sicherheitsziel	Funktionale EVG-Sicherheitsanforderungen	
	direkt	unterstützend
O.Nachvollz	FAU_GEN.1 (Optional) FAU_GEN.1 (Pflicht) FMT_MSA.1 FMT_MSA.3 FMT_SMF.1	FIA_UAU.2 FIA_UID.2 FMT_SMR.1 FPT_STM.1 (in IT-Umgebung)
O.PD.Veränd	FAU_SAR.1 FDP_IFC.1 FDP_IFF.1 FDP_SDI.1 (Prot.)	FAU_GEN.1 (Optional)
O.S3Aktion	FMT_MSA.1 FMT_MSA.3 FMT_SMF.1	FIA_UAU.2 FIA_UID.2 FMT_SMR.1
O.S3Export	FDP_IFC.1 FDP_IFF.1	FIA_UAU.2 FIA_UID.2 FMT_SMR.1
O.Zugriff	FIA_UAU.2 FIA_UID.2 FMT_SMF.1	FMT_MTD.1 (Passwörter)

233 Im Folgenden wird dargelegt, weshalb jedes in Abschnitt 4.1 identifizierte Sicherheitsziel durch die in Abschnitt 5.1 aufgeführten funktionalen Sicherheitsanforderungen abgedeckt wird (vgl. Tabelle 3).

234 **O.BD.Ausfall**: Durch die Eigenschaften der in FDP_IFF.1 definierten Informationsflusskontrolle wird gewährleistet, dass ein ausgefallener Empfang von Bilddaten sowie ein Ende des Ausfalls erkannt werden. FAU_GEN.1 (Pflicht) sichert die Protokollierung dieser Ereignisse.

235 **O.BD.Import**: FDP_IFF.1 und FDP_IFC.1 legen den zulässigen Informationsfluss von Bilddaten fest. Dies schließt u.a. auch eine verpflichtende Prüfung der Authentizität der Bilddaten beim Empfang und vor der weiteren Verarbeitung mit ein. Weiterhin wird hier festgelegt, dass der Benutzer im Fall der fehlerhaften Prüfung zu informieren ist. Über FAU_GEN.1 (Optional) erfolgt (je nach Konfiguration) die Protokollierung der Resultate der Prüfungen.

236 **O.BD.Lösch**: FDP_IFF.1 und FDP_IFC.1 legen den zulässigen Informationsfluss von Bilddaten fest. Dies schließt u.a. auch das Löschen von Bilddaten mit ein. Nur dem Revisor/bDSB ist es erlaubt Bilddaten zu löschen. Demnach ist es für alle an-

deren Rollen verboten. FIA_UAU.2 und FIA_UID.2 unterstützen dies, da jeder Benutzer sich selbst identifizieren und authentisieren muss. FMT_SMR.1 stellt sicher, dass jedem Benutzer eindeutig eine Rolle zugeordnet werden kann. Über FDP_SDI.1 (Bild.L) erzeugt der EVG ein Integritätsmerkmal über alle Bilddaten und kann damit auch erkennen, wenn Bilddaten unter Umgehung des EVG gelöscht wurden. In FDP_IFC.1 ist festgelegt, dass der Benutzer im Fall der fehlerhaften Prüfung zu informieren ist. Über FAU_GEN.1 (Optional) erfolgt (je nach Konfiguration) die Protokollierung der Resultate der Prüfungen.

237 **O.BD.Veränd**: FDP_IFC.1 und FDP_IFF.1 fordern, dass der EVG selbst keine Möglichkeit anbietet, Bilddaten zu verändern. FDP_SDI.1 (Bild.V) fordert die Generierung und die Möglichkeit zur Prüfung eines Integritätsmerkmals von bereits gespeicherten Bilddaten. Veränderungen können somit über den EVG nicht durchgeführt und können bei Umgehung des EVG sicher erkannt werden. In FDP_IFC.1 ist festgelegt, dass der Benutzer im Fall der fehlerhaften Prüfung zu informieren ist. Über FAU_GEN.1 (Optional) erfolgt (je nach Konfiguration) die Protokollierung der Resultate der Prüfungen.

238 **O.Begründ**: Bei den Aktionen „Exportieren von Bilddaten“ sowie „manuelles Löschen von Bilddaten“ wird durch FDP_IFF.1 und FDP_IFC.1 gewährleistet, dass diese Aktionen nur von den hierfür berechtigten Rollen und bei ausreichender Begründung durchgeführt werden dürfen. Die Anforderungen FIA_UAU.2 und FIA_UID.2 unterstützen die Durchsetzung von Zugriffsrechten, da jeder Benutzer sich selbst identifizieren und authentisieren muss. FMT_SMR.1 stellt sicher, dass jedem Benutzer eindeutig eine Rolle zugeordnet werden kann. FAU_GEN.1 (Pflicht) sorgt für die zuverlässige Protokollierung der Begründungen sowie des ausführenden Benutzers.

239 Das Einspielen falscher Bilder direkt an einer Schnittstelle zum EVG gemäß **O.Einspielen** wird dadurch verhindert, dass in FDP_IFF.1 genau dieser Informationsfluss explizit verhindert ist.

240 **O.KonfigS2**: FMT_MTD.1 (Einrichtung) stellt sicher, dass bestimmte Aktionen auf die Rolle Administrator beschränkt sind. FMT_SMF.1 stellt diese administrativen Funktionen zur Verfügung. Damit die Aktivitäten einzelnen Personen zugeordnet werden können, erzwingen FIA_UAU.2 und FIA_UID.2 eine Benutzeridentifikation und Authentisierung. FMT_SMR.1 stellt sicher, dass jedem Benutzer eindeutig eine Rolle zugeordnet werden kann.

241 **O.KonfigS3**: FMT_MTD.1 (Prot.), FMT_MSA.1 und FMT_MSA.3 stellen sicher, dass bestimmte Aktionen auf die Rolle Revisor/bDSB beschränkt sind. FMT_SMF.1 stellt diese administrativen Funktionen zur Verfügung. Damit die Aktivitäten einzelnen Personen zugeordnet werden können, erzwingen FIA_UAU.2 und FIA_UID.2 eine Benutzeridentifikation und Authentisierung. FMT_SMR.1 stellt sicher, dass jedem Benutzer eindeutig eine Rolle zugeordnet werden kann.

242 **O.Löschgarantie**: FDP_IFF.1 definiert die Regeln für das automatische Löschen von aufgezeichneten Bilddaten. Die Löschfrist wird dabei aus dem Aufnahmezeitpunkt errechnet, der durch FDP_ITC.2 und FPT_TDC.1 zuverlässig und korrekt von den Signalaufnahmekomponenten in den EVG importiert wurde. Die Umgebung stellt per FPT_STM.1 die erforderliche aktuelle Uhrzeit und das aktuelle Datum zur Verfügung.

243 **O.Löschung**: Über FDP_RIP.1 wird sichergestellt, dass von einmal gelöschten Bilddaten keine Restinformationen auf dem Speichermedium verbleiben.

244 **O.Nachvollz**: Durch FAU_GEN.1 (Pflicht) und FAU_GEN.1 (Optional) werden die Protokolldaten für die zu protokollierenden Aktionen des Beobachters, Administrators und Revisors/bDSB generiert. FAU_GEN.1 (Pflicht) sorgt dafür, dass die datenschutzrelevanten Ereignisse immer protokolliert werden (Protokollierung dieser Ereignisse kann nicht deaktiviert werden). Nur der Revisor/bDSB ist durch FMT_MSA.1 und FMT_MSA.3 in der Lage, die zu protokollierenden Ereignisse zu konfigurieren. FMT_SMR.1 unterstützt dies durch die Zuordnung von Benutzern zu Rollen. FMT_SMF.1 stellt diese administrativen Funktionen zur Verfügung. FIA_UAU.2 und FIA_UID.2 sorgen für eine zuverlässige Identifikation und Authentifizierung aller Benutzer, was ebenfalls für die eigentlichen Protokolldaten relevant ist. Die durch die Umgebung bereitgestellte Uhrzeit und Datum (FPT_SMT.1) vervollständigt die Protokolldaten.

245 **O.PD.Veränd**: FDP_SDI.1 (Prot.) zwingt den EVG zur unmittelbaren Erzeugung eines Integritätsmerkmals für die generierten Protokolldaten. Der EVG muss ebenfalls in der Lage sein, dieses Merkmal zu prüfen. Im Fall einer fehlerhaften Prüfung ermöglich FAU_GEN.1 (Optional) die Protokollierung dieses Ereignisses und FDP_IFC.1 und FDP_IFF.1 legen fast, dass dieser Fehler dem Benutzer zu melden ist. FAU_SAR.1 ermöglicht den Benutzern die Durchsicht der gespeicherten Protokolldaten in einem für sie verständlichen Format, was evtl. Einfluss auf das verwendete Integritätsmerkmal hat.

246 **O.S3Aktion**: Durch FMT_MSA.1 und FMT_MSA.3 wird sichergestellt, dass die Konfiguration der Löschzyklen von Bilddaten auf den Revisor/bDSB beschränkt ist und nur innerhalb der gesetzlich gültigen Grenzen erfolgen kann. FMT_SMR.1 unterstützt dies durch die Zuordnung von Benutzern zu Rollen. FMT_SMF.1 stellt diese administrativen Funktionen zur Verfügung. FIA_UAU.2 und FIA_UID.2 sorgen für eine zuverlässige Identifikation und Authentifizierung aller Benutzer.

247 **O.S3Export**: Über die Eigenschaften der Informationsflusskontrolle (definiert in FDP_IFC.1 und FDP_IFF.1) ist der Revisor auf die Kontroll- und Löschfunktionen eingeschränkt. FMT_SMR.1 unterstützt dies durch die Zuordnung von Benutzern zu Rollen. FIA_UAU.2 und FIA_UID.2 sorgen für eine zuverlässige Identifikation und Authentifizierung aller Benutzer.

248 **O.Zugriff**: FIA_UAU.2 und FIA_UID.2 sorgen für eine zuverlässige Identifikation und Authentifizierung aller Benutzer. FMT_MTD.1 (Passwörter) garantiert, dass Jeder Benutzer sein Passwort ändern kann, so dass das Wissen über Passwörter auf den Benutzer beschränkt sein sollte. FMT_SMF.1 stellt diese administrative Funktion zur Verfügung.

6.2.2 Erklärung der Sicherheitsanforderungen an die IT-Umgebung

249 Die funktionalen Sicherheitsanforderungen an die Umgebung unterstützen die funktionalen Sicherheitsanforderungen des EVG.

Tabelle 4: Abdeckung der Sicherheitsziele an die Umgebung durch Sicherheitsanforderungen an die IT-Umgebung

Sicherheitsziel an die IT-Umgebung	Funktionale Sicherheitsanforderungen an die IT-Umgebung	
	direkt	unterstützend
OE.IT.BD.Zuordnung	FDP_ETC.2	
OE.IT.Kamera	FDP_IFC.1 FDP_IFF.1	
OE.IT.Plattform	FDP_ACC.2 FDP_ACF.1	FMT_MSA.1 FMT_MSA.3
OE.IT.Uhrzeit	FPT_STM.1	

OE.IT.BD.Zuordnung wird durch FDP_ETC.2 umgesetzt. Die Signalaufnahmekomponente muss gemäß der Sicherheitsanforderung in der Lage sein, die benötigten Sicherheitsattribute KameraID und Aufnahmezeitpunkt direkt mit den Bilddaten zu verknüpfen, bevor diese Bilddaten an den EVG gesendet (exportiert aus Sicht der Kamera) werden. Die Merkmale für die spätere Authentizitätsprüfung durch den EVG müssen also schon beim Senden in den Bilddaten enthalten bzw. fest mit ihnen verknüpft sein (bevor sie in den sicheren Kanal für die Übertragung gelangen).

OE.IT.Kamera wird durch FDP_IFC.1 und FDP_IFF.1 umgesetzt. Diese beiden Anforderungen erzwingen die Umsetzung einer Informationsflusspolitik auf Seiten der Signalaufnahmekomponenten, wodurch nur authentische Bilder aus einem zulässigen Bereich aufgenommen werden. Über FDP_IFF.1 werden die Attribute und Regeln definiert, mit denen die für Aufnahmen zulässigen räumlichen Bereiche bestimmt und die Authentizitätskontrolle für aufgenommene Bilddaten beschrieben wird. Die Summe dieser Regeln ergibt eine Informationsflusspolitik, die durch FDP_IFC.1 durchgesetzt wird.

OE.IT.Plattform wird durch FDP_ACC.2 und FDP_ACF.1 umgesetzt. Diese Sicherheitsanforderungen setzen über das Zugriffsberechtigungssystem der Plattform eine umfassende Zugriffsbeschränkung auf den EVG und die EVG Daten durch. In FDP_ACF.1 sind die erlaubten bzw. explizit verbotenen Zugriffe zu beschreiben. Die Summe dieser Regeln ergibt eine Zugriffskontrollpolitik über alle EVG Objekte und Operationen darauf, die über FDP_ACC.2 durchgesetzt wird. Unterstützend wirken hierbei noch FMT_MSA.1 und FMT_MSA.3 durch die Definition der Management-Berechtigungen, also welche Rolle bzw. Benutzer der Plattform die Berechtigung hat, die Zugriffsregeln auf der Plattform zu verwalten.

> ***Anwendungsbemerkung 28*** *Sollte der EVG auf einer Plattform aufsetzen, die mehrere Stufen von Zugriffsberechtigungen kennt (z.B. Datenbank und Betriebssystem), ist zu bedenken, ob diese unterschiedlichen Zugriffskontrollen und auch Managementfunktionen in mehreren Iterationen der genannten Komponenten zu definieren sind.*

OE.IT.Uhrzeit wird durch FPT_STM.1 umgesetzt. Eine beliebige Komponente aus der IT-Umgebung beliefert alle anderen Komponenten und den EVG mit einer zuverlässigen Uhrzeit.

6.2.3 Erklärung der Abhängigkeiten

250 Durch die Wahl der vorgegebenen Vertrauenswürdigkeitsstufe EAL1 ist die Auflösung der Abhängigkeiten der Anforderungen an die Vertrauenswürdigkeit automatisch gegeben.

251 In folgender Tabelle 5 sind in der zweiten Spalte alle von [CC-Teil2] pro funktionaler Sicherheitsanforderung vorgegebenen Abhängigkeiten aufgelistet. In der rechten Spalte finden sich Kommentare bezüglich der Berücksichtigung dieser Abhängigkeiten.

Tabelle 5: Abhängigkeiten

Funktionale Sicherheits-anforderungen	**Abhängigkeiten**	**Umsetzung**
FAU_GEN.1 (Optional)	FPT_STM.1	Durch die IT-Umgebung
FAU_GEN.1 (Pflicht)	FPT_STM.1	Durch die IT-Umgebung
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1 (Optional) FAU_GEN.1 (Pflicht)
FDP_SDI.1 (Bild.L)	keine	
FDP_SDI.1 (Bild.V)	keine	
FDP_SDI.1 (Prot.)	keine	
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1 FMT_MSA.3
FDP_ITC.2	[FDP_ACC.1 oder FDP_IFC.1] [FTP_ITC.1 oder FTP_TRP.1] FPT_TDC.1	FDP_IFC.1 Durch die Non-IT-Umgebung[16] FPT_TDC.1
FDP_RIP.1	keine	
FIA_UAU.2	FIA_UID.1	FIA_UID.2 (Hierarchisch zu FIA_UID.1)
FIA_UID.2	keine	

[16] Bietet der EVG selbst oder die IT-Umgebung des EVG den Schutz der Übertragungsstrecke an, so muss hier die Abhängigkeit erfüllt werden.

Funktionale Sicherheits-anforderungen	Abhängigkeiten	Umsetzung
FMT_MSA.1	[FDP_ACC.1 oder FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	FDP_IFC.1 FMT_SMF.1 FMT_SMR.1
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 FMT_SMR.1
FMT_MTD.1 (Einrichtung)	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
FMT_MTD.1 (Passwörter)	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
FMT_MTD.1 (Prot.)	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
FMT_SMF.1	keine	
FMT_SMR.1	FIA_UID.1	FIA_UID.2 (Hierarchisch zu FIA_UID.1)
FPT_TDC.1	keine	

Die nicht-Auflösung der Abhängigkeit der Komponente FDP_ITC.2 nach FTP_ITC.1 in der nicht-IT-Umgebung kann wie folgt begründet werden:

Im Rahmen dieses Schutzprofils kann nicht festgelegt werden, wie ein konkretes Produkt bzw. der Hersteller die Absicherung der Übertragungsleitung realisiert. Es kann also sowohl von z.B. baulichen Maßnahmen (welche der nicht-IT-Umgebung zuzuordnen wären) oder von IT-Maßnahmen (z.B. Verschlüsselung, was der IT-Umgebung zuzuordnen wäre) ausgegangen werden. Dieses Schutzprofil möchte nun nicht die eine oder andere Lösung ausschließen, jedoch bei der Absicherung durch IT-Maßnahmen bereits das entsprechende Modell aus den CC Teil 2 bieten können. Daher wird die Komponente FTP_ITC.1 in diversen Anwendungsbemerkungen bereits aufgeführt. Eine formale Modellierung in der nicht-IT-Umgebung ist jedoch nicht zulässig.

6.2.4 Erklärung zur Widerspruchsfreiheit und gegenseitigen Unterstützung

252 Die Anforderungen an die Vertrauenswürdigkeit des EVG stören sich nicht gegenseitig, da sie der Vertrauenswürdigkeitsstufe EAL1 der Common Criteria, Teil 3 [CC-Teil3] entsprechen.

253 Die Anforderungen an die Vertrauenswürdigkeit und die funktionalen Sicherheitsanforderungen an den EVG stören sich nicht gegenseitig, da es keinerlei Abhängigkeiten zwischen diesen beiden Gruppen gibt.

254 Die funktionalen Sicherheitsanforderungen an den EVG und die IT-Umgebung unterstützen sich gegenseitig wie folgt:

255 Den zentralen Faktor bildet die funktionale Sicherheitspolitik für Videoflusskontrolle, welche in FDP_IFF.1 und FDP_IFC.1 definiert ist. Diese Politik deckt den gesamten Lebenszyklus der Bilddaten im EVG ab, vom Empfang durch den EVG bis hin zur Vernichtung.

- Die beiden Anforderungen an die IT-Umgebung FDP_IFC.1 und FDP_IFF.1 sorgen dafür, dass die Signalaufnahmekomponenten nur Bilder aus zulässigen Bereichen aufnehmen und an den EVG senden. Weiterhin werden hier auch Regeln für eine Authentizitätsprüfung der aufgenommenen Bilder festgelegt, welche durch die Signalaufnahmekomponente durchzusetzen sind.
- FDP_ETC.2 aus der Umgebung stellt sicher, dass alle relevanten Zusatzinformationen mit den Bilddaten verknüpft an den EVG versendet werden. FPT_STM.1 aus der Umgebung stellt hier sicher, dass die korrekte Aufnahmezeit mit den Bilddaten verknüpft wird.
- Die nicht-IT Umgebung sichert die Bilddaten während der Übertragung durch einen sicheren Kanals (FTP_ITC.1).
- FPT_TDC.1 und FDP_ITC.2 stellen sicher, dass der EVG alle relevanten Zusatzinformationen zu den Bilddaten korrekt importiert und interpretiert. Dies betrifft vor allem den Aufnahmezeitpunkt. Mittels dieser Zusatzinformationen kann die Prüfung auf Authentizität vom EVG durchgeführt werden (FDP_IFF.1). Zusammen mit einer aktuellen Zeitinformation von FPT_STM.1 aus der Umgebung kann damit auch später der jeweilige Löschzeitpunkt für die automatische Löschung bestimmt werden.
- FDP_SDI.1 (Bild.L) und FDP_SDI.1 (Bild.V) sorgen dafür, dass der EVG nach dem Empfang und beim Speichern der Bilddaten Integritätsmerkmale für diese Daten generiert, so dass unbefugtes Veränderungen und Löschen erkannt werden kann.
- FDP_RIP.1 stellt sicher, dass von einmal gelöschten Bilddaten keine Restinformationen auf dem Datenträger erhalten bleiben.

256 Die Möglichkeiten der einzelnen Benutzer innerhalb des EVG sollen eingeschränkt werden:

- Die IT-Umgebung verhindert eine Umgehung der EVG mittels der durch FDP_ACC.2 und FDP_ACF.1 durchgesetzten Zugriffskontrollpolitik auf den EVG und die EVG Daten. Mittels der Umgebungs-Anforderungen FMT_MSA.1 und FMT_MSA.3 wird festgelegt, welche Rolle bzw. Benutzer aus der Umgebung das Recht hat, die Zugriffsberechtigungen zu verwalten.
- FMT_SMF.1 stellt diverse EVG Funktionen für die Benutzer des EVG generell bereit.

- FMT_MTD.1 (Einrichtung) schränkt einige Funktionen auf die Rolle Administrator ein. FMT_MTD.1 (Prot.) schränkt eine Funktion auf die Rolle Revisor/bDSB ein. FMT_MSA.1 und FMT_MSA.3 schränken den Wertebereich für diese Funktion auf die gesetzlichen Grenzen ein. FMT_MTD.1 (Passwörter) erlaubt das Setzen des eigenen Passworts für jeden Benutzer. Die Zuordnung der Funktionen zu Rollen ist eindeutig und widerspruchsfrei.
- FMT_SMR.1 trifft eine Zuordnung zwischen Rollen und Benutzern.
- Mittels FIA_UIA.2 und FIA_UAU.2 wird eine zuverlässige Identifikation und Authentisierung der Benutzer erzwungen.

257 Neben der Behandlung von Bilddaten sind vom EVG noch die Protokolldaten zu verarbeiten:

- Mittels FAU_GEN.1 (Pflicht) und FAU_GEN.1 (Optional) werden zu bestimmten sicherheits- oder datenschutzrechtlich relevanten Ereignissen (zur Unterstützung der Informationsflusspolitik und der Einschränkung der Benutzer bzw. der dort relevanten funktionalen Sicherheitsanforderungen) Protokolldaten erzeugt. Unterstützt werden sie von FIA_UIA.2 und FIA_UAU.2, wodurch in den Protokolldaten ein Bezug zu Benutzern hergestellt werden kann. Weiterhin unterstützt hier FPT_STM.1 aus der IT-Umgebung durch die Bereitstellung einer Zeitinformation.
- Durch FDP_SDI.1 (Prot.) erzeugt der EVG ein Integritätsmerkmal zu diesen Protokolldaten und ermöglicht auch eine Prüfung dieses Merkmals. Unzulässige Manipulationen oder Löschen von Einträgen können so erkannt werden.
- FAU_SAR.1 stellt sicher, dass die Benutzer alle gespeicherten Protokolldaten in einem für sie lesbaren Format darstellen können.

258 Damit wurde gezeigt, dass die einzelnen funktionalen Sicherheitsanforderungen in keinem Widerspruch zueinander stehen, da sie generell unterschiedliche Ziele verfolgen. Sie unterstützen sich teilweise gegenseitig zur Erreichung dieser Ziele.

6.2.5 Erklärung der Vertrauenswürdigkeitsstufe

259 Die Anforderungen an die Vertrauenswürdigkeit gemäß der gewählten Vertrauenswürdigkeitsstufe EAL1 sind im Hinblick auf die verarbeiteten Bilddaten und datenschutzrechtlichen Anforderungen gemäß § 6b BDSG (vgl. Anhang A) für den EVG angemessen, da der EVG vollständig in einer geschützten Umgebung betrieben wird.

260 Der Wert der Daten und damit der Nutzen für die möglichen Angreifer wird nicht so hoch eingestuft, dass eine Schwachstellenanalyse zu rechtfertigen wäre. Daher ist der Nachweis der korrekten Funktionalität das Vertrauenswürdigkeitskriterium, das für den Anwender des Produktes mindestens vorzuweisen ist.

Anwendungsbemerkung 29 *Sollte die Übertragungsstrecke in konkreten Sicherheitsvorgaben ebenfalls durch den EVG zu schützen sein, muss auf das hohe Angriffspotential der dort möglichen Angreifer Rücksicht genommen werden.*

Anwendungsbemerkung 30 *Falls die Übertragungsstrecke mit dem dort angenommenen hohen Angriffspotential in den EVG aufgenommen wird, stellt dies generell einen Widerspruch zur Vertrauenswürdigkeitsstufe EAL1 dar. EAL1 ist nicht geeignet zu zeigen, dass der EVG einem hohen Angriffspotential standhalten kann (Wirksamkeit) sondern nur, dass die beschriebenen Sicherheitsfunktionen in beschriebener Weise funktionieren (Funktion). Die Sicherheitsvorgaben zu einem konkreten Produkt müssen diese Inkonsistenz in angemessener Weise berücksichtigen, z.B. über eine nachvollziehbare Begründung für EAL1 auch auf der Übertragungsstrecke oder durch die Wahl einer angemessenen Vertrauenswürdigkeitsstufe.*

Anwendungsbemerkung 31 *Bei einer spezifischen Hersteller-Lösung kann in den Sicherheitsvorgaben auch unabhängig vom Schutz der Übertragungsstrecke durch den EVG eine höherwertige Vertrauenswürdigkeitsstufe gefordert werden.*

7 Referenzen

[BDSG] Bundesdatenschutzgesetz, Januar 2002.

[CC-Teil1] „Common Criteria – Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik, Teil 1: Einführung und allgemeines Modell“. Version 2.3.

[CC-Teil2] „Common Criteria – Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik, Teil 2: Funktionale Sicherheitsanforderungen“. Version 2.3.

[CC-Teil3] „Common Criteria – Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik, Teil 3: Anforderungen an die Vertrauenswürdigkeit“. Version 2.3.

Anhang A Hinweise zur Auslegung der datenschutzrechtlichen Rahmenbedingungen

261 Es gibt verschiedene bundes- und landesrechtliche Regelungen hinsichtlich der datenschutzrechtlichen Anforderungen zur Videoüberwachung. Polizeirechtliche Regelungen der Länder, die in der Regel Vorgaben über den Einsatz optischer Überwachungsgeräte beinhalten, werden in diesem Zusammenhang aus Gründen der Übersichtlichkeit nicht berücksichtigt.

7.1 A.1 Regelungen

262 Die bundesrechtliche Umsetzung der europarechtlichen Vorgaben zur Videoüberwachung ist mit § 6b BDSG erfolgt.

§ 6b BDSG Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen

(1) Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit sie
1. zur Aufgabenerfüllung öffentlicher Stellen,
2. zur Wahrnehmung des Hausrechts oder
3. zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke
erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

(2) Der Umstand der Beobachtung und die verantwortliche Stelle sind durch geeignete Maßnahmen erkennbar zu machen.

(3) Die Verarbeitung oder Nutzung von nach Absatz 1 erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Für einen anderen Zweck dürfen sie nur verarbeitet oder genutzt werden, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist.

(4) Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, ist diese über eine Verarbeitung oder Nutzung entsprechend den §§ 19a und 33 zu benachrichtigen.

(5) Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.

263 Darüber hinaus ist im Zusammenhang mit § 6b BDSG auch §9 BDSG sowie die zugehörige Anlage 1 zu berücksichtigen.

§ 9 BDSG Technische und organisatorische Maßnahmen

Öffentliche und nicht öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Anlage 1 zu § 9 Satz 1 BDSG

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),

2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),

3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),

4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),

5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),

6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),

7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),

8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

264 Der EVG ist in der Lage, die folgenden datenschutzrechtlichen Anforderungen zu erfüllen:

1. Gewährleistung der zuverlässigen Löschung (inkl. individuellem Löschungsanspruch) gemäß § 6b Abs. 5 BDSG: „Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen“), wobei der EVG zusätzlich gewährleistet, dass die Löschzyklen nicht außerhalb des Konfigurationsspielraumes gesetzt werden können;
2. Zugangskontrolle gemäß Anlage 1 Nr. 2 BDSG, um „zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können“;
3. Zugriffskontrolle gemäß Anlage 1 Nr. 3 BDSG, um „zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können“;
4. Weitergabekontrolle gemäß Anlage 1 Nr. 4 BDSG, um „zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist“;
5. Eingabekontrolle gemäß Anlage 1 Nr. 5 BDSG, um „zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind“;
6. Gewährleistung der Zweckbestimmung der Datenverarbeitung und Dokumentation der Begründung bei Zweckänderung von „Auswerten“ auf „Ausdrucken“ oder „Exportieren“ (Zweckbindung) gemäß § 6b Nr. 1 BDSG;
7. Verfügbarkeitskontrolle gemäß Anlage 1 Nr. 7 BDSG, um „zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind“.

265 In folgenden Ländern gibt es landes(datenschutz)rechtliche Regelungen (polizeirechtliche Regelungen sind nicht aufgeführt):

- Berlin;
- Brandenburg;
- Bremen;
- Mecklenburg-Vorpommern;

- Niedersachsen;
- Nordrhein-Westfalen;
- Rheinland-Pfalz;
- Sachsen;
- Sachsen-Anhalt;
- Schleswig-Holstein.

7.2 A.2 Wesentliche Kriterien (Auslegungsrichtlinien) des § 6b BDSG

266 Aufgrund des komplexen Regelungszusammenhangs, insbesondere der jeweils unterschiedlichen örtlichen und sachlichen Rahmenbedingungen, stellen die folgenden Ausführungen lediglich beispielhafte Erläuterungen zur Rechtslage dar und erheben daher keinen Anspruch auf Vollständigkeit.

267 Aus diesem Grund empfiehlt es sich, beim Betrieb einer Videoüberwachungsanlage stets die zuständige Aufsichtsbehörde zu unterrichten und Hinweise zum Betrieb einzuholen.

268 Grundsätzlich:

- Anwendungsbereich:
  - öffentliche Stellen des Bundes;
  - private Stellen (wenn private Stellen im Auftrag des Bundes eine Videoüberwachung durchführen, sind sie selbst verantwortliche Stelle, wenn sie auch die Auswertung der Bilder übernehmen);
  - Beobachtung erfolgt nicht im Rahmen persönlicher oder familiärer Tätigkeiten (wenn Zweck geschäftlich, dann § 6b BDSG);
  - unerheblich, ob bloße Überwachung oder auch Aufzeichnung;
  - stationäre oder mobile Kameras;
  - Medienprivileg gemäß § 41 BDSG gilt nur, wenn Aufnahmen zu journalistisch-redaktionellen Zwecken erstellt werden;
- Beobachtung öffentlich(e) (zugänglicher) Räume:
  - Definition: für den öffentlichen Verkehr gewidmet oder dazu bestimmt, von unbestimmten Personen genutzt oder betreten zu werden;
  - wenn Zugänglichkeit nach allgemeinen Merkmalen bestimmt, die von jeder Person erfüllt werden kann, so auch, wenn z. B. Eintrittsgeld gefordert wird;
  - unerheblich, ob überdacht oder unter freiem Himmel (z. B. auch Parks oder umgrenzte Plätze);
  - unerheblich, wer Eigentümer ist;
  - in Arbeitsverhältnissen gilt § 6b BDSG nur, wenn die entsprechenden Arbeitsbereiche öffentlich zugänglich sind (z. B. Verkaufsräume), ansonsten ist das BetrVG – sofern einschlägig – anwendbar.

269 Zweckbestimmungen:

- Aufgabenerfüllung öffentlicher Stellen:
  - erforderlich ist eine Erfüllung der gesetzlichen Aufgaben der öffentlichen Stellen des Bundes;
  - Videoüberwachung muss die Aufgabenerfüllung im weitesten Sinne unterstützen (keine finale Bedeutung);
  - Videoüberwachung muss die Funktionsfähigkeit öffentlich zugänglicher Räume (des Bundes) gewährleisten, die zur Aufgabenerfüllung der öffentlichen Stelle verwendet werden;
- Wahrnehmung des Hausrechts:
  - in der Regel können Betroffene davon ausgehen, dass sie aufgrund öffentlicher Zugänglichkeit von Flächen nicht in den besonders geschützten Bereich einer privaten Stelle eindringen mit der Folge, dass die Zulässigkeitsvoraussetzung „Hausrecht“ insoweit nicht gilt;
  - Hausrecht-Grund auch nur insoweit bestandsfähig, wenn Überwachung ohne Technikeinsatz nicht mehr ausreichend gewährleistet werden kann;
  - es muss konkrete Sicherheitsgefahr bestehen, der durch den Kameraeinsatz tatsächlich auch begegnet werden kann;
  - Verhältnismäßigkeit muss gegeben sein;
  - bei Delegation auf private Sicherheitsdienste sind diese verantwortliche Stelle;
- Wahrnehmung berechtigter Interessen:
  - alle legitimen Interessen erfasst (verfassungsrechtlich bedenklich weit gefasst);
  - reduzierende (geltungserhaltende) Auslegung erforderlich: rein kommerzielle Gründe oder sonstige private, einseitig definierte Zwecke reichen nicht, es muss stets um eine Gefährdung von Sicherheitsbelangen gehen;
  - Zwecke müssen konkret festgelegt sein;
  - allgemein muss eine begründbare Gefährdungslage für öffentliche oder private Rechte vorliegen.

270 Notwendig:

- Interessenabwägung:
  - Interessenabwägung zugunsten der Videoüberwachung in Bereichen, an denen eine Entfaltung der Persönlichkeit oder die Wahrnehmung von Freiheitsrechten eher untypisch ist (z. B. Vorräume von Banken, Durchgangszonen von Bahnhöfen, Tankstellen etc.);
  - Gegensatz: Restaurants, Fußgängerzonen, Erholungs- und Unterhaltungsräume, auch Verkehrsmittel;

- Aufzeichnung der Aufnahmen ist schwerwiegenderer Eingriff und bedarf besonderer Rechtfertigung, strenge Zweckbindung und erneute Interessenabwägung;
- Zweckänderung ausschließlich zur Abwehr von Gefahren / Straftaten und nur bei konkreten Anhaltspunkten;

- Erkennbarkeit der Videoüberwachung / Kenntlichmachung der verantwortlichen Stelle:
  - Umstand der Videoüberwachung erkennbar, wenn hierauf durch ein Schild hingewiesen wird oder wenn die Kamera für eine durchschnittliche Person zweifelsfrei als solche erkennbar, bevor die Person davon erfasst;
  - erkennbar auch, wenn der Bildschirm für jedermann erkennbar ist;
  - Schilder müssen auffällig angebracht sein, so dass kein Suchen erforderlich;
  - Kenntlichmachung der verantwortlichen Stelle durch Hinweisschild mit Kontaktangaben;
- Benachrichtigungspflicht der Betroffenen bei Herstellung von Personenbezug:
  - es besteht individueller Löschungsanspruch, wenn Interessen der Betroffenen einer weiteren Speicherung entgegenstehen;
- Speicherung/Löschung von Aufzeichnungen:
  - Löschfristen nach Möglichkeit standardisiert festzulegen (Ideal: automatische Löschung nach festgelegtem Zeitraum);
  - Löschung unzulässig, wenn Aufbewahrungspflicht besteht oder die Löschung den Interessen der Betroffenen zuwider laufen würde (wenn Betroffener die Aufzeichnung zum Beweis im Falle von möglichen Schadensersatzanspruch benötigt);
- Sonstige Erfordernisse:
  - für automatisierte Verfahren besteht – soweit kein Datenschutzbeauftragter bestellt ist – Meldepflicht gemäß § 4d Abs. 1 BDSG;
  - für bestimmte Arten der Videoüberwachung ist eine Vorabkontrolle gemäß § 4d Abs. 5 BDSG erforderlich, nämlich wenn besondere Risiken für die Rechte und Freiheiten der Betroffenen bestehen. Dies ist der Fall bei:
    - Zusammenschaltung mehrerer Kameras mit der Möglichkeit der (Bewegungs-) Profilerstellung;
    - Einsatz von Überwachungskameras in größerer Zahl bei zentraler Kontrolle;
    - Möglichkeit hoher Auflösung biometrischer Merkmale;
    - Abgleich der Aufnahmen mit anderen personenbezogenen Daten (Gesichter);
    - unverschlüsselter Übertragung der Daten per Funk;

- o auch bei der Auswahl und Gestaltung der technischen Einrichtungen ist der Grundsatz der Datenvermeidung und Datensparsamkeit zu beachten (z. B. bei der Einrichtung von Zugriffsberechtigungen, Speicherdauer, routinemäßigem Überschreiben).

7.3 A.3 Wesentliche Kriterien der Landesregelungen

271 Die rechtlichen Rahmenbedingungen der Bundesländer für den Einsatz von Videoüberwachung sind – soweit vorliegend – in vielen Punkten ähnlich bzw. sogar gleich. Übereinstimmend lassen sich in den vorhandenen landesrechtlichen Regelungen folgende gemeinsame Zulässigkeitsvoraussetzungen, also eine Art roter Faden, feststellen:

- zulässig zur Aufgabenerfüllung der öffentlichen Stelle (Diese Zulässigkeitsvoraussetzung muss für die Länder Bremen, Mecklenburg-Vorpommern, Niedersachsen und Nordrhein-Westfalen allerdings eingeschränkt werden: Hier ist die Videoüberwachung nicht zulässig, sofern es lediglich der Aufgabenerfüllung der öffentlichen Stelle dient.);
- zulässig zur Wahrnehmung des Hausrechts;
- Interessenabwägung zwischen verfolgtem Zweck und der Einschränkung des Persönlichkeitsrechts der Betroffenen ist obligatorisch;
- Zweckänderung nur in engen Grenzen zulässig: nur zur Abwehr von Gefahren für die öffentliche Sicherheit;
- Beobachtung muss erkennbar sein;
- Aufzeichnungen nur zulässig, wenn zwingend zur Erreichung des Zwecks erforderlich;
- wenn Aufzeichnungen best. Personen zugeordnet werden, müssen diese benachrichtigt werden;
- gespeicherte Aufnahmen sind unverzüglich nach Zweckerreichung zu löschen, maximale gesetzlich genannte Speicherfrist 2 Monate (Sachsen).

272 Hinsichtlich der in Abschnitt 2 genannten Einsatzszenarien ist das Beobachten aus datenschutzrechtlicher Sicht ein „Erheben“ personenbezogener Daten (vgl. § 3 Abs. 3 BDSG), soweit aus der Beobachtung eine einzelne Person bereits bestimmbar ist.[17] Aufzeichnen und Auswerten stellen hingegen das Verarbeiten gemäß § 3 Abs. 4 BDSG dar: „Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten”.

[17] Eine Referenz auf eine Person ist notwendig. Existiert keine Referenz zu einer bestimmbaren Person, handelt es sich damit nicht um ein Erheben im Sinne des Datenschutzes.

7.4 A.4 Zusammenfassung

273 Der EVG ist durch seine Technik geeignet, die bei Videoüberwachungsanlagen einschlägigen datenschutzrechtlichen Anforderungen

- zur Löschung bzw. zur zulässigen Speicherdauer (inkl. individuellem Löschungsanspruch),
- zur Einschränkung auf einen Personenkreis, der den EVG in zulässiger Weise nutzt,
- zur Gewährleistung der Zweckbestimmung und Dokumentation der Begründung bei Änderung der Zweckbindung (vom „Auswerten“ auf „Ausdrucken“ oder „Exportieren“) und
- zur Gewährleistung, dass Bilddaten nicht unzulässig gelöscht werden,

technisch zu unterstützen. Zusätzlich ist das datenschutzrechtliche Prinzip der Datensparsamkeit und -vermeidung zu berücksichtigen.

Die datenschutzrechtlichen Anforderungen, die nicht durch die Technik des EVG realisiert werden können, sind in den Anwendungsbemerkungen beschrieben.

> ***Anwendungsbemerkung 32*** *Es wird angenommen, dass der EVG beim Einsatz in öffentlichen Räumen – d. h. Räumen, die für den öffentlichen Verkehr gewidmet oder dazu bestimmt sind, von unbestimmten Personen genutzt oder betreten zu werden – unter Beachtung der folgenden datenschutzrechtlichen Anforderungen eingesetzt wird:*

- o Die Zulässigkeitskriterien sind erfüllt:
  - Die Videoüberwachung erfolgt
    - zur Erfüllung gesetzlicher Aufgaben (gilt nur für öffentliche Stellen) – mit den oben gemachten Einschränkungen (vgl. Rd.-Nr. 271) – ,
    - zur Durchsetzung des Hausrechts oder
    - zur Wahrung berechtigter Interessen für konkret festgelegte Zwecke.
  - Es erfolgt eine Interessenabwägung zwischen dem durch den Betreiber verfolgten Zweck bzw. Interesse und der Einschränkung des Persönlichkeitsrechts der Betroffenen.
- o Die Verarbeitung personenbezogener Daten, die ausschließlich zu vorher definierten – zulässigen – Zwecken er folgt, beinhaltet insbesondere folgende Aspekte:
  - Ausrichtung der Kamera, d. h. die Bereiche bzw. Bildausschnitte, die die Kamera erfassen kann;
  - Detailgrad der Aufnahmen (Wie detailliert sind die Aufnahmen? Können Personen erkannt werden?);

        - Einsatzdauer (Rund-um-die-Uhr? Nur während der Arbeitszeit von 8-20h? Nur nachts? Nur bei Veranstaltungen?).
    - Die Videoüberwachung ist erkennbar.
    - Ist bei einer Aufzeichnung ein Personenbezug herstellbar bzw. wird im Rahmen einer Auswertung der Aufzeichnung ein solcher Personenbezug hergestellt, erfolgt eine Benachrichtigung.
    - Soweit der Betreiber keinen Datenschutzbeauftragten bestellt hat, wird die Meldepflicht gem. § 4d Abs. 1 BDSG für automatisierte Verfahren erfüllt.
    - Die für bestimmte Arten von Videoüberwachungen notwendige Vorabkontrolle gem. § 4d Abs. 5 BDSG – erforderlich, wenn besondere Risiken für die Rechte und Freiheiten der Betroffenen bestehen – wird durchgeführt.
    - Das Gebot der Datensparsamkeit und -vermeidung wird beachtet.

Soweit die Videoüberwachung im Unternehmensbereich eingesetzt werden soll, ist neben der Zweckbindung und den Löschfristen insbesondere die Mitarbeiterbeteiligung (§ 87 Abs. 1 Nr. 6 BetrVG) – sofern institutionalisiert – zu beachten.