Information zur DSFA

DSFA

Videoüberwachung Polizeipräsidium Offenburg

Name des Bearbeiters

Ref. RuD, Herr FESt Stb. T, Herr

Name des Prüfers

beh. DSB

Name des Bestätigers

Behördenleitung

Bearbeitungsdatum

30.11.2018

Name des DSB

Gutachten des DSB

Die Verarbeitung scheint mit den rechtlichen Vorgaben vereinbar.

Einholung der Meinung der Betroffenen

Meinung der Betroffenen wurde nicht eingeholt.

Grund, warum die Meinung der Betroffenen nicht erfragt wurde

Die Einholung einer Stellungnahme aller von der Maßnahme betroffenen ist nicht möglich. Stellvertretend für die Beschäftigten des Polizeipräsidiums Offenburg wurde der Personalrat beteiligt.

Kontext

Überblick

Welche Verarbeitung ist geplant?

Videoüberwachung von Liegenschaften mit / ohne Aufzeichnungsfunktion an Liegenschaften des Polizeipräsidiums Offenburg

Welche Zuständigkeiten bestehen für die Verarbeitung?

Gesamtverantwortung:
Behördenleitung des Polizeipräsidiums Offenburg

Verantwortliche Fachabteilung:
Leitung der Organisationseinheit, die die Videoüberwachung durchführt

Gibt es Normen oder Standards für die Verarbeitung?

Geplante Verarbeitung:
Videoüberwachung, zum Teil mit Aufzeichnungsfunktionen

Art und Umfang der Verarbeitung:

- Erhebung personenbezogener Daten mittels Videokameras
- Speicherung des Bildmaterials gemäß der Vorgaben des § 18 V LDSG BW

Rechtsgrundlage:
Die Videoüberwachung der Dienststelle erfolgt gem. § 18 I Nr. 1 und 2 LDSG BW in Ausübung des Hausrechts.

Zweck der Videoüberwachung:

- Zugangskontrolle
- Schutz von Beschäftigten
- Ergänzung nicht vorhandener / bestehender Sicherheitsvorkehrungen
- Schutz von Dienstfahrzeugen und Führungs- und Einsatzmitteln der Polizei.
- Verhinderung und Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung sowie Straftaten
- Geltendmachung von Rechtsansprüchen

Mögliche Überwachungsbereiche:

- Zugänge und Zufahrten
- Schleusen
- schwer einsehbare Bereiche
- ungeschützter Parkraum
- nicht ausreichend gesicherte Bereiche (Abweichungen gem. RisPol)

Betroffene Personen:

- Besucherinnen und Besucher der Dienststelle
- Beschäftigte
- Personen, die sich in unmittelbarer Nähe zur Liegenschaft befinden.

Bewertung : akzeptabel

Daten, Prozesse und Unterstützung

Welche Daten werden verarbeitetet?

- Kennzeichen von Fahrzeugen, die in den Überwachungsbereich fahren
- Bildaufnahmen von Betroffenen, die sich in den Überwachungsbereich begeben
- Handlungen und Bewegungen von Personen im Überwachungsbereich

Zugriffsberechtigte Personen:

- Beschäftigte, die mit der Überwachung des Monitorbilds betraut sind
- Beschäftigte, die mit der Sicherung/Auswertung der Videoüberwachung beauftragt sind
- Beschäftigte, die mit der Systemadministration betraut sind

Empfängerkategorien:

- mit dem Vorgang betraute Beschäftigte der Dienststelle
- zuständige Strafverfolgungsbehörden und am Verfahren Beteiligte
- Vorgesetzte von betroffenen/beschuldigten Beschäftigten
- schadensregulierende Stellen, z. B. Versicherungen oder Rechtsanwälte im Wege der Akteneinsicht
- Mit der Wartung beauftragte Dienstleister

Wie verläuft der Lebenszyklus von Daten und Prozessen?

Siehe Anlage "schematische Darstellung der Verarbeitungstätigkeit Videoüberwachung"

Freundlicherweise zur Verfügung gestellt von:
Verein österreichischer betrieblicher und behördlicher Datenschutzbeauftragter - www.privacyofficers.at

Mit Hilfe welcher Betriebsmittel erfolgt die Datenverarbeitung?

Die konkrete Darstellung der vorhandenen Systeme erfolgt in den Verarbeitungsverzeichnissen der jeweiligen Liegenschaft.

Generell werden folgende Betriebsmittel unterschieden:

- Kameratyp
- Übertragungsmedium
- Monitore
- Server/Speicher
- Videoüberwachungssoftware
- Betriebssystem

Bewertung : akzeptabel

Grundlegende Prinzipien

Verhältnismäßigkeit und Notwendigkeit

Sind die Verarbeitungszwecke eindeutig definiert und rechtmäßig?

Die Verarbeitungszwecke wurden gem. § 18 I Nr. 1 und 2 LDSG BW eindeutig festgelegt (siehe Kapitel Überblick, Normen und Standards). Eine Verarbeitung zu anderen Zwecken erfolgt lediglich unter den Kriterien des § 18 III LDSG BW.

Bewertung : akzeptabel

Aufgrund welcher Rechtsgrundlage erfolgt die Verarbeitung?

§ 18 LDSG BW

Bewertung : akzeptabel

Sind die erhobenen Daten erforderlich, relevant und auf das für die Datenverarbeitung Notwendige beschränkt?

Die erhobenen Daten sind für die beschriebenen Zwecke erforderlich. Für die Zweckerreichung muss auf die Möglichkeit der Videoüberwachung zurückgegriffen werden. Mildere Mittel stehen nicht zur Verfügung. Eine lückenlose Bestreifung der Örtlichkeit ist aus personellen Gründen nicht möglich. Die Relevanz aufgezeichneter Videodaten ergibt sich aus der Notwendigkeit, als Beweismittel in einem möglichen Ordnungswidrigkeiten-/Strafverfahren eingebracht zu werden.

Die Daten werden durch die nachfolgend aufgeführten Maßnahmen auf das notwendige Maß beschränkt:

- Beschränkung der Anzahl der Kameras
- Beschränkung des Erfassungsbereich der Kameras
- zeitliche Begrenzung der Aufzeichnung falls möglich
- manuelle Aktivierung der Aufzeichnung
- Aktivierung des Monitors durch Bewegungsmelder
- Löschung der Daten gem. § 18 V LDSG BW

Das Interesse des Polizeipräsidums Offenburg überwiegend insofern das Interesse der betroffenen Personen. Die Eingriffsintensität wird lediglich in einer Höhe als rechtmäßig angesehen, wie es zur Zweckerreichung erforderlich scheint.

Bewertung : akzeptabel

Sind die Daten korrekt und auf dem neuesten Stand?

entfällt

Bewertung : akzeptabel

Welche Speicherdauer haben die Daten?

Die Speicherdauer resultiert aus § 18 V LDSG BW

Das Polizeipräsidium Offenburg beschränkt sich auf eine maximale Speicherdauer der Aufzeichnung von 72 Stunden. Danach erfolgt ein automatische Überschreibung der gespeicherten Bilddaten.

Bewertung : akzeptabel

Maßnahmen zum Schutz der Persönlichkeitsrechte der betroffenen Personen

Wie werden die betroffenen Personen über die Verarbeitung informiert?

- Hinweisschilder mit Piktogramm und Angabe der/des Verantwortlichen sowie der Kontaktmöglichkeit des behördlichen Datenschutzbeauftragten
- QR Code auf dem Hinweisschild, welches auf ein Informationsblatt zu den Betroffenenrechten verweist
- Informationsblatt zu den Betroffenenrechten im Schleusenbereich
- Benachrichtung bei Zuordnung der Aufzeichnung zu einer bestimmten Person gem. § 18 IV LDSG BW und unter Berücksichtigung des § 8 I LDSG BW

Bewertung : akzeptabel

Wenn anwendbar, wie wird die Einwilligung der betroffenen Personen eingeholt?

entfällt

Bewertung : akzeptabel

Wie können Betroffene ihre Recht auf Auskunft und Datenübertragbarkeit ausüben?

Auskunftsersuchen an Leitung der verantwortlichen Organisationseinheit oder über den behördlichen Datenschutzbeauftragten

Bewertung : akzeptabel

Wie können betroffene Personen ihr Recht auf Berichtigung und Löschung (Recht auf Vergessenwerden) ausüben?

Im Rahmen der bereits dargestellten rechtlichen Grundlagen werden die erhobenen personenbezogenen Daten automatisiert in festgelegten Zeiträumen gelöscht (Ringspeicher)

Bewertung : akzeptabel

Wie können betroffene Personen ihre Rechte auf Einschränkung oder Widerspruch der Verarbeitung ausüben?

Entsprechende Anträge sind an die Leitung der Organisationseinheit oder den behördlichen Datenschutzbeauftragten zu stellen.

Bewertung : akzeptabel

Sind die Verpflichtungen der Auftragsverarbeiter klar definiert und vertraglich geregelt?

Auf Auftragsverarbeiter wird, soweit möglich verzichtet.
Ansonsten werden mit Art. 28 DSGVO konforme Verträge (Vordruck des LfDI BW) vewendet zur Sicherstellung der genauen Modalitäten. Außerdem werden diese Verträge dem Anhang der Verarbeitungsverzeichnisse beigefügt.

Bewertung : akzeptabel

Soweit Datenübermittlungen in Länder außerhalb der Europäischen Union stattfinden, werden die Daten angemessen geschützt?

entfällt

Bewertung : akzeptabel

Risiken

Geplante oder bestehende Maßnahmen

Datentrennung

Die Videodaten werden grundsätzlich getrennt von anderen Daten gespeichert, z. B. auf:

- Stand-Alone Rechnern/Servern
- virtuellen Servern

Ein Abgleich mit anderen personenbezogenen Daten findet nicht statt.

Bewertung : akzeptabel

Logische Zugriffskontrolle

Die Zugriffskontrolle wird durch eine Rechte- und Rollenmatrix sichergestellt. In dieser wurden für das Polizeipräsidium Offenburg grundsätzlich folgende Berechtigungsprofile definiert:

- Anwender (nur Zugriff auf das dargestellte Bild)
- Administrator (lesen, exportieren, löschen, konfigurieren, zuweisen von Rollen)

Administratorrechte stehen lediglich des FESt, Stb. Technik zu. Anwender in den Liegenschaften vor Ort haben keinerlei Zugriff auf die gespeicherten personenbezogenen Daten, lediglich auf das übertragene Bild der Kamera auf den Monitor.

Bewertung : akzeptabel

Rückverfolgbarkeit (Protokollierung)

Mit Hilfe der eingesetzten Software am Polizeipräsidium Offenburg findet eine Protokollierung aller Zugriffe statt und kann nachvollzogen werden.

Bewertung : akzeptabel

Datenminimierung

Die erhobenen Daten sind für die genannten Zwecke erforderlich. Sie werden durch die nachfolgend aufgeführten Maßnahmen auf das notwendige Maß beschränkt:

- Beschränkung der Anzahl der Kameras
- Beschränkung der Erfassungsbereiche der Kameras
- zeitliche Begrenzung der Aufzeichnungsfunktion
- manuelle Aktivierung von Aufzeichnungsfunktionen
- Etablierung sogenannter Klingelschaltungen (Aktivierung bei Betätigung der Klingel, automatische Deaktivierung des Kamerasbilds nach 60 Sekunden)

Bewertung : akzeptabel

Betriebssicherheit

Turnusmäßige Wartung/Updates durch die Systemadministratoren.
Lokale Maßnahmen zur Betriebssicherheit werden in den Verarbeitungsverzeichnissen detailliert dargestellt.

Bewertung : akzeptabel

Hardware-/ Gerätewartung

Wartung und Austausch defekter Hardware erfolgt ausschließlich durch FESt, Stb. Technik bzw. in Zusammenarbeit mit möglichen Auftragsverarbeitern.

Die physische Sicherheit der Hardware wird nach den Standards der RisPol gewährleistet.

Bewertung : akzeptabel

Netzwerksicherheit

Ein Zugriff von außen auf die Videoüberwachung ist nicht möglich. Das System arbeitet autark ohne Berührungspunkte zu anderen Netzwerken.

Bewertung : akzeptabel

Zugangskontrolle

Die Zugangskontrolle wird durch örtliche Vorschriften geregelt (z. B. Hausordnung, Dienstanweisung Videoüberwachung des PP Offenburg)

Zutritt zu den kritischen Bereichen wie Serverräumen erhalten nur eine begrenzte Anzahl von Beschäftigten. Externe erhalten lediglich unter Aufsicht Zutritt zu solchen Räumlichkeiten.

Bewertung : akzeptabel

Hardware-Sicherheit

Netzwerkkomponente werden nach den Vorgaben der RisPol baulich gesichert.

Bewertung : akzeptabel

Vermeidung von Risikoquellen

Folgende Vorschriften, zu welchen regelmäßig sensibilisiert werden soll sollen Risiken vermeiden:

- Hausordnung
- örtliche Brandschutzvorschriften
- Leitlinie zur Informationssicherheit
- IT-Grundschutz

Bewertung : akzeptabel

Datenschutzorganisation

Behördlicher Datenschutzbeauftragter (Kontrolle, Überwachung)
Verantwortliche Fachabteilung (Steuerung, verantwortlich für die Einhaltung der Vorgaben)

Bewertung : akzeptabel

Management von Datenschutzrisiken

Regelmäßige Überprüfung der vorhandenen Videoüberwachung durch die verantwortliche Fachabteilung hinsichtlich Zweckerreichung inklusive Abwägung der Interessen von Betroffenen mit denen der Dienststelle.

Inbesondere bei Vorkommnissen wie bereits erfolgten Straftaten müssen turnusmäßig auf weitere Relevanz geprüft werden.

Ergeben sich Änderungen im Verfahren, muss das Verarbeitungsverzeichnis unter Einbeziehung des behördlichen Datenschutzbeauftragten angepasst werden.

Bewertung : akzeptabel

Umgang mit Datenschutzverletzungen

Hierzu werden separate Dienstanweisungen (Meldung Datenschutzpanne) erlassen.

Im Falle einer solchen Verletzung erfolgt eine rechtliche und technische Überprüfung, außerdem Beratung, wie zukünftig eine solche Panne verhindert werden kann. Verantwortlich hierfür ist die Leitung der Organisationseinheit unter Einbeziehung des Referats Recht und Datenschutz, des behördlichen Datenschutzbeauftragten sowie des FESt, Stb. Technik.

Bewertung : akzeptabel

Sensibilisierungsmaßnahmen

Im Rahmen der turnusmäßigen Belehrungen über die allgemeinen Dienstpflichten.

Bewertung : akzeptabel

Sicherheitsmaßnahmen und -regelungen für Dritte

Die Regelungen sind etwaigen Auftragsverarbeitungsverträgen zu entnehmen.

Bewertung : akzeptabel

Überwachung der Datenschutzmaßnahmen

Die Überwachung der Maßnahmen obliegt dem behördlichen Datenschutzbeauftragten.

Bewertung : akzeptabel

Unrechtmäßiger Zugriff auf Daten

Was könnten die wesentlichen Auswirkungen für die betroffenen Personen sein, wenn das Risiko eintritt?

Unbefugter Eingriff in das allgemeiner Persönlichkeitsrecht (Bekanntwerden des Aufenthalts am Überachungsort sowie dessen Umstände)

Was sind die Hauptbedrohungen, die zu dem Risiko führen könnten?

Videoüberwachungsdaten werden unrechtmäßig verarbeitet

Was sind die Risikoquellen?

Menschliches Fehlverhalten, Technische Mängel

Welche der identifizierten Maßnahmen tragen zur Bewältigung des Risikos bei?

Datentrennung, Logische Zugriffskontrolle, Datenminimierung, Betriebssicherheit, Hardware-/ Gerätewartung, Netzwerksicherheit, Zugangskontrolle, Hardware-Sicherheit, Vermeidung von Risikoquellen, Datenschutzorganisation, Management von Datenschutzrisiken, Sensibilisierungsmaßnahmen, Sicherheitsmaßnahmen und -regelungen für Dritte, Überwachung der Datenschutzmaßnahmen

Wie schätzen Sie den Risikoschweregrad ein, insbesondere hinsichtlich der möglichen Auswirkungen und geplanten Maßnahmen?

Geringfügig, Die Eintrittswahrscheinlichkeit, das Videodaten entwendet werden oder in falsche Hände geraten, ist als gering anzusehen. Die Schwere des Schadens bei Entwendung der Bilder verbleibt ebenfalls im geringfügigen Bereich, da keine kompromittierenden Aufnahmen entstehen.

Wie schätzen Sie die Eintrittswahrscheinlichkeit des Risikos ein, insbesondere hinsichtlich der Bedrohungen, Risikoquellen und geplante Maßnahmen?

Geringfügig, geringfügig, s. o.

Bewertung : akzeptabel

Unerwünschte Veränderung von Daten

Was könnten die wesentlichen Auswirkungen für die betroffenen Personen sein, wenn das Risiko eintritt?

Fehlerhafte Annahme des Aufenthalts am Überwachungsort, z. B. Manipulation des Zeitstempels

Was sind die Hauptbedrohungen, die zu dem Risiko führen könnten?

Menschliches Fehlverhalten (fahrlässig oder vorsätzlich)

Was sind die Risikoquellen?

Fehlerhafte Bedienung, Technische Mängel

Welche der identifizierten Maßnahmen tragen zur Bewältigung des Risikos bei?

Logische Zugriffskontrolle, Rückverfolgbarkeit (Protokollierung), Zugangskontrolle, Hardware-/ Gerätewartung, Netzwerksicherheit, Sensibilisierungsmaßnahmen, Betriebssicherheit, Hardware-Sicherheit

Wie schätzen Sie den Risikoschweregrad ein, insbesondere hinsichtlich der möglichen Auswirkungen und geplanten Maßnahmen?

Überschaubar, Schwere des Schadens bei Manipulation ist überschaubar. Den Betroffenen drohen u. U. deutliche Unannehmlichkeiten (z. B. falsche Verdächtigung), diese können jedoch mit gewisser Anstrengung überwunden werden, da der Nachweis der unerwünschten Datenveränderung anhand der Protokolldaten geführt werden und damit eine Rehabilitierung erfolgen kann.

Wie schätzen Sie die Eintrittswahrscheinlichkeit des Risikos ein, insbesondere hinsichtlich der Bedrohungen, Risikoquellen und geplante Maßnahmen?

Geringfügig, Auf Grund der dargestellten, den Beschäftigten bekannten, Kontrollmechanismen ist die Wahrscheinlichkeit einer Manipulation der personenebezogenen Daten als unwahrscheinlich anzusehen.

Bewertung : akzeptabel

Datenverlust

Was könnten die wesentlichen Auswirkungen für die betroffenen Personen sein, wenn das Risiko eintritt?

Bei Verlust von Daten entfällt die Möglichkeit des objektiven Nachweises, Bei Ausfall des Bildes ist die Zweckerreichung nicht mehr sichergestellt

Was sind die Hauptbedrohungen, die zu dem Risiko führen könnten?

Höhere Gewalt, Organisatorische Mängel, Menschliches Fehlverhalten, Technisches Versagen, Vorsätzliche Handlungen

Was sind die Risikoquellen?

Fehlverhalten interner oder externer Personen, technische oder organisatorische Mängel, mangelnde Sensibilität von Beschäftigten

Welche der identifizierten Maßnahmen tragen zur Bewältigung des Risikos bei?

Datentrennung, Logische Zugriffskontrolle, Betriebssicherheit, Hardware-/ Gerätewartung, Netzwerksicherheit, Zugangskontrolle, Hardware-Sicherheit, Vermeidung von Risikoquellen, Sensibilisierungsmaßnahmen

Wie schätzen Sie den Risikoschweregrad ein, insbesondere hinsichtlich der möglichen Auswirkungen und geplanten Maßnahmen?

Überschaubar, Überschaubar

- Verlust von beweiserheblichen Aufzeichnungen
- Erhöhung des Risikos der Beeinträchtigung der körperlichen Unversehrheit von Beschäftigten
- Erhöhte Wahrscheinlichkeit der Beschädigung/Verlust von FEM

Wie schätzen Sie die Eintrittswahrscheinlichkeit des Risikos ein, insbesondere hinsichtlich der Bedrohungen, Risikoquellen und geplante Maßnahmen?

Geringfügig, Die Wahrscheinlichkeit eines Ausfalls wird auf Grund der ergriffenen Maßnahmen als gering eingestuft.

Bewertung : akzeptabel

Aktionsplan

Übersicht

Grundlegende Prinzipien
- Zwecke
- Rechtsgrundlage
- Erforderlichkeit der Daten
- Korrektheit der Daten
- Speicherdauer
- Information der Betroffenen
- Einholung der Einwilligung
- Information der Betroffenen
- Recht auf Berichtigung und Löschung
- Recht auf Einschränkung und auf Widerspruch
- Auftragsverarbeitung
- Übermittlung in Drittländer

Geplante oder bestehende Maßnahmen
- Datentrennung
- Logische Zugriffskontrolle
- Rückverfolgbarkeit (Protokollierung)
- Datenminimierung
- Betriebssicherheit
- Hardware-/ Gerätewartung
- Netzwerksicherheit
- Zugangskontrolle
- Hardware-Sicherheit
- Vermeidung von Risikoquellen
- Datenschutzorganisation
- Management von Datenschutzrisiken
- Umgang mit Datenschutzverletzungen
- Sensibilisierungsmaßnahmen
- Sicherheitsmaßnahmen und -regelungen für Dritte
- Überwachung der Datenschutzmaßnahmen

Risiken
- Unrechtmäßiger Zugriff auf Daten
- Unerwünschte Veränderung von Daten
- Datenverlust

Verbesserbare Maßnahmen
Akzeptable Maßnahmen

Grundlegende Prinzipien

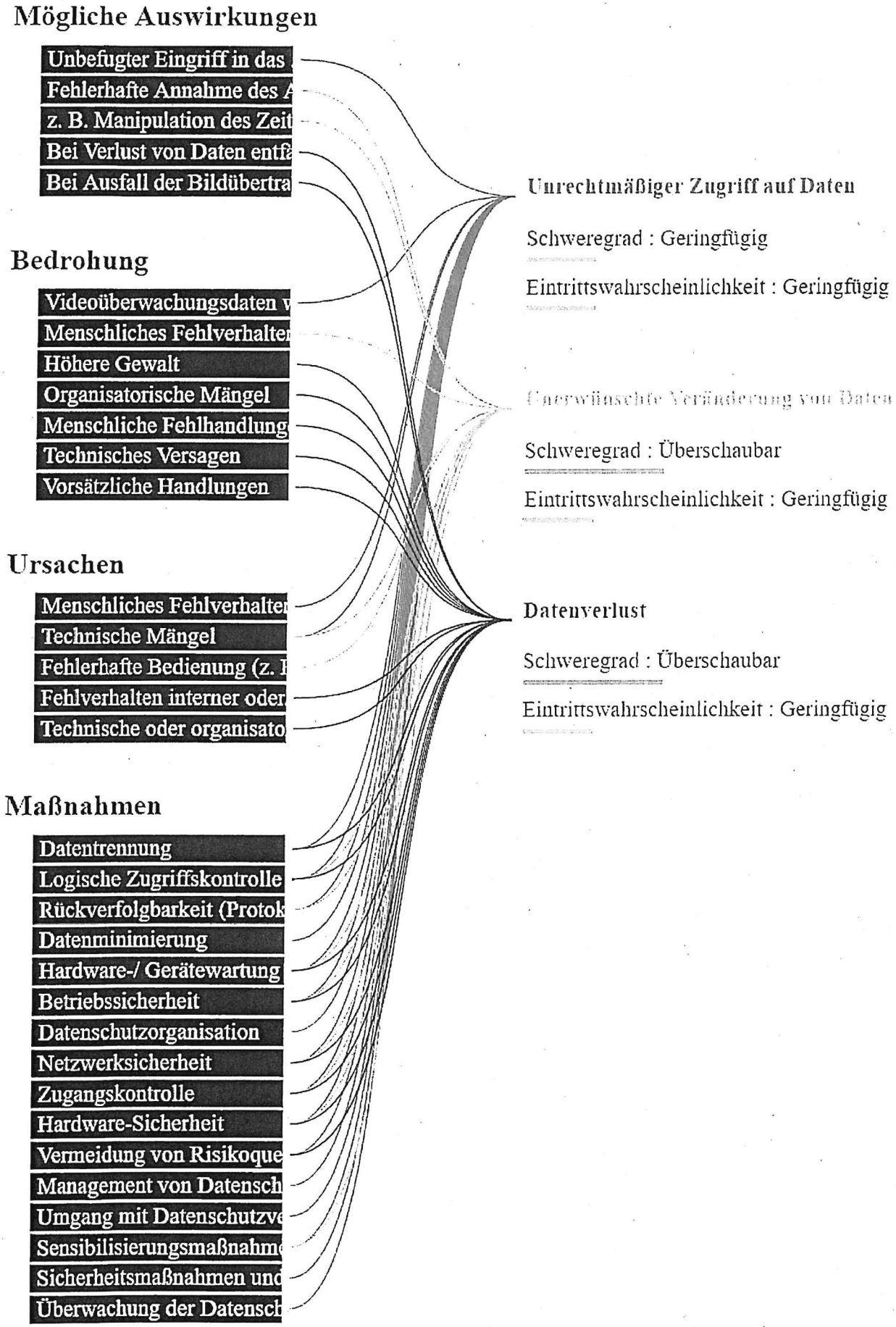
Kein Aktionsplan festgelegt.

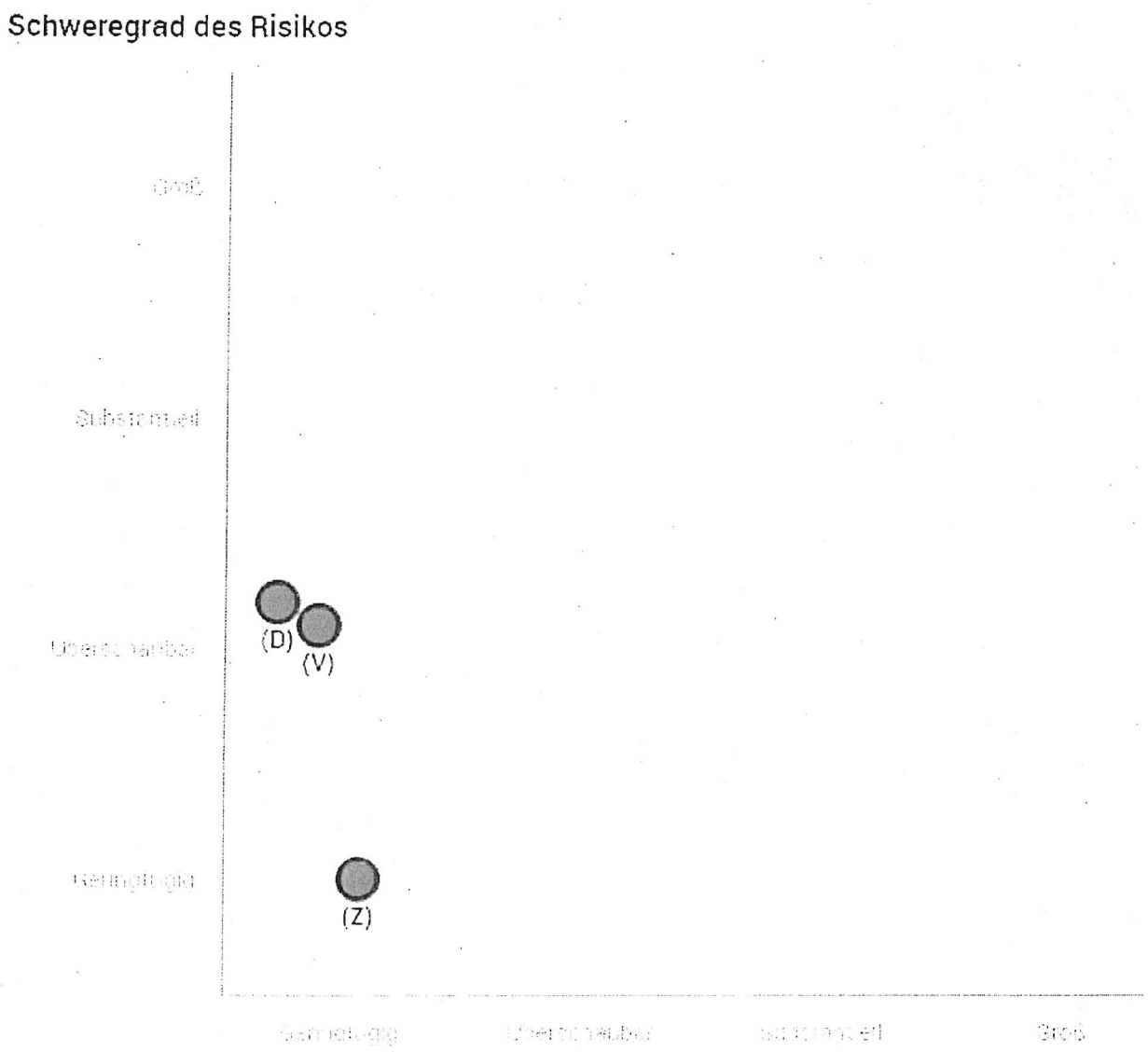
Bestehende oder geplante Maßnahmen

Kein Aktionsplan festgelegt.

Risiken

Kein Aktionsplan festgelegt.


Mögliche Auswirkungen
Unbefugter Eingriff in das
Fehlerhafte Annahme des A
z. B. Manipulation des Zeit
Bei Verlust von Daten entfä
Bei Ausfall der Bildübertra
Bedrohung
Videoüberwachungsdaten v
Menschliches Fehlverhalter
Höhere Gewalt
Organisatorische Mängel
Menschliche Fehlhandlung
Technisches Versagen
Vorsätzliche Handlungen
Ursachen
Menschliches Fehlverhalter
Technische Mängel
Fehlerhafte Bedienung (z. F
Fehlverhalten interner oder
Technische oder organisato
Maßnahmen
Datentrennung
Logische Zugriffskontrolle
Rückverfolgbarkeit (Protok
Datenminimierung
Hardware-/ Gerätewartung
Betriebssicherheit
Datenschutzorganisation
Netzwerksicherheit
Zugangskontrolle
Hardware-Sicherheit
Vermeidung von Risikoque
Management von Datensch
Umgang mit Datenschutzve
Sensibilisierungsmaßnahm
Sicherheitsmaßnahmen und
Überwachung der Datensch
Unrechtmäßiger Zugriff auf Daten
Schweregrad : Geringfügig
Eintrittswahrscheinlichkeit : Geringfügig
Unerwünschte Veränderung von Daten
Schweregrad : Überschaubar
Eintrittswahrscheinlichkeit : Geringfügig
Datenverlust
Schweregrad : Überschaubar
Eintrittswahrscheinlichkeit : Geringfügig



- Geplante oder bestehende Maßnahmen
- Mit den eingeleiteten Korrekturmaßnahmen
- (Z) Unrechtmäßiger Zugriff auf Daten
- (V) Unerwünschte Veränderung von Daten
- (D) Datenverlust

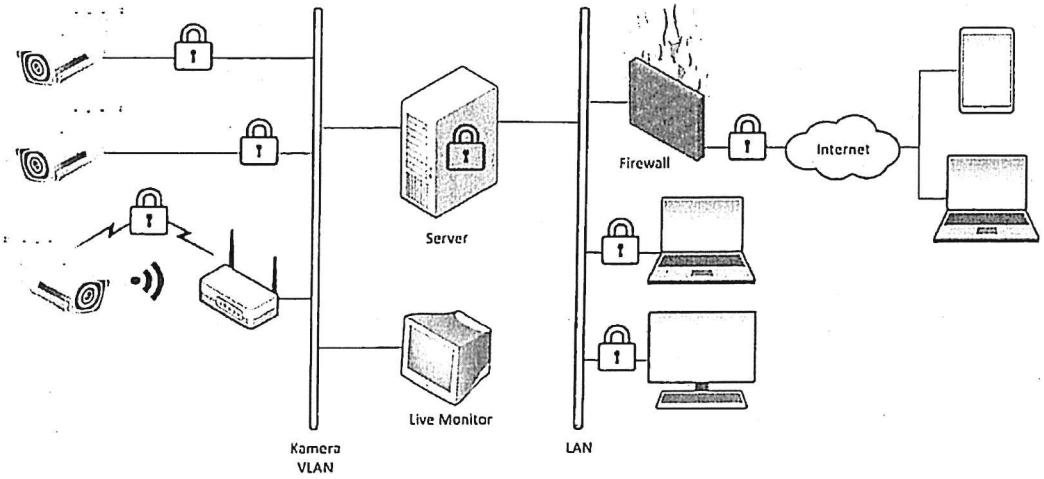


Abbildung 2: Angepasste schematische Darstellung der Verarbeitungstätigkeit „Videoüberwachung" nach Umsetzung der zusätzlichen Datensicherheitsmaßnahmen

Schlussbemerkungen

Aufgrund der Rechenschaftspflicht gemäß Artikel 5 Absatz 2 und Artikel 24 Abs 1 DSGVO, der Vorgaben gemäß Artikel 35 Absatz 11 sowie der Empfehlungen der Artikel 29-Gruppe [1, p. 22] sollte die Aktualität der DSFA in regelmäßigen Abständen überprüft werden. Laut Artikel 29-Gruppe ist die Durchführung einer DSFA keine einmalige Aufgabe, sondern ein kontinuierlicher Prozess. In jedem Fall ist eine Wiederholung der DSFA erforderlich, wenn hinsichtlich des mit den Verarbeitungsvorgängen verbundenen Risikos Änderungen eingetreten sind.

Weiterführende Informationen zur Durchführung einer DSFA:

- Leitfaden für den Prozess der Datenschutz-Folgenabschätzung gemäß ISO/IEC 29134:2017 Information technology -- Security techniques -- Guidelines for privacy impact assessment [4]
- BRD: Forum Privatheit White Paper DSFA (3. Aufl. 2017) [5]
- GDD-Praxishilfe DS-GVO X - Voraussetzungen der Datenschutz-Folgenabschätzung [6]
- Planspiel DSFA des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein und der Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern [7]
- CNIL, The open source PIA software [8]