Datenschutz-Folgenabschätzung

Durchführung einer DSFA am Beispiel Videoüberwachung

Version: 1.0
Stand: Jänner 2018

Impressum: Medieninhaber, Herausgeber und Hersteller: Verein österreichischer betrieblicher und behördlicher Datenschutzbeauftragter – Privacyofficers.at, ZVR-Zahl 061847005, Wien, https://www.privacyofficers.at/impressum

Vorwort des Vereinsvorstands

Liebe Leserin, lieber Leser,

der Verein österreichischer betrieblicher und behördlicher Datenschutzbeauftragter – Privacyofficers.at freut sich, dieses praxistaugliche Beispiel zur Durchführung einer DSFA zur Verfügung stellen zu können. Unser Ziel ist es, diese Umsetzungshilfe aktuell zu halten. In der vorliegenden Version wurde das österreichische Datenschutz-Anpassungsgesetz 2018 entsprechend berücksichtigt.

Besonderer Dank für die Ausarbeitung gebührt dabei unserem Arbeitskreis Datensicherheit und allen beteiligten Vereinsmitgliedern. Frei nach dem Motto „Von Mitgliedern für Mitglieder (und darüber hinaus)" ist hier in kurzer Zeit eine übersichtliche Praxishilfe entstanden.

Das vorliegende Durchführungsbeispiel gibt einen Überblick und praxistaugliche Informationen über die Durchführung einer DSFA am Beispiel einer Videoüberwachung inkl. Risikobewertung aus Sicht der Betroffenen.

Wir dürfen darauf hinweisen, dass dieses Durchführungsbeispiel nur als Orientierungshilfe dient und die wichtigsten Inhalte der DSGVO bezüglich der Durchführung einer DSFA in kompakter und übersichtlicher Form zusammenfasst und keinen Anspruch auf vollständige Berücksichtigung aller Bestimmungen der DSGVO bzw. der nationalen Datenschutzbestimmungen erhebt. Die in diesem Dokument verwendeten Begriffe entsprechen jenen Definitionen, wie sie in der DSGVO verwendet werden. Abkürzungen sind im Abschnitt „Abkürzungen" definiert.

Privacyofficers.at hofft, dass das vorliegende Durchführungsbeispiel viele Verantwortliche bei der Durchführung der DSFA unterstützen kann, wir haben diese daher unter eine CC BY-NC-SA 4.0-Lizenz gestellt. Anregungen und konstruktive Kritik nehmen wir gerne unter office@privacyofficers.at entgegen, aktuelle Datenschutz-News finden Sie auf unserer Homepage: https://www.privacyofficers.at/.

Der Vereinsvorstand

Abkürzungen

- **BSI IT-Grundschutz:** Der vom deutschen Bundesamt für Sicherheit in der Informationstechnik entwickelte IT-Grundschutz ermöglicht es, notwendige Sicherheitsmaßnahmen zu identifizieren und umzusetzen
- **DSB:** Datenschutzbeauftragter
- **DSFA**: Datenschutz-Folgenabschätzung gemäß Artikel 35 DSGVO
- **DSG:** Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG) idF BGBl I 120/2017
- **DSGVO:** Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl L 119 vom 4.5.2016, 1–88 (LINK zum Volltext inklusive Berichtigung vom 22.11.2016)
- **DSMS:** Datenschutz-Managementsystem
- **ISMS nach ISO/IEC 27001:** Ein Informationssicherheits-Managementsystem ist eine Aufstellung von Verfahren und Regeln, um die Informationssicherheit zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern. Die international anerkannte Norm ISO/IEC 27001 spezifiziert die Anforderungen für Einrichtung, Umsetzung und Aufrechterhaltung eines dokumentierten ISMS.
- **ISO/IEC 31000:** Internationale Norm „Risk Management - Principles and Guidelines“, welche Risikomanagement in alle Unternehmensaktivitäten integriert
- **ITIL:** Die IT Infrastructure Library (ITIL) ist eine Sammlung vordefinierter Prozesse, Funktionen und Rollen, wie sie typischerweise in jeder IT-Infrastruktur mittlerer und großer Unternehmen vorkommen
- **KVP:** Kontinuierlicher Verbesserungsprozess
- **NIS-Richtlinie:** Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, ABl L 194 vom 19.7.2016, 1–30 (LINK zum Volltext)
- **pb Daten:** Personenbezogene Daten (siehe die Definition in Artikel 4 Z 1 DSGVO)
- **TOM**: Technische und Organisatorische Maßnahme zur Erfüllung der Sicherheits- und Schutzanforderungen

Inhaltsverzeichnis

Abkürzungen 3

Inhaltsverzeichnis 3

Einleitung 4

Schritt 1: Kriterien zur Prüfung, ob eine DSFA notwendig ist 5

1.1 Vorgaben aus der DSGVO 5

1.2 Empfehlungen der Artikel 29-Gruppe 5

Schritt 2: DSFA durchführen (gemäß Artikel 35 DSGVO) 8

2.1 Beschreibung und Bewertung der Vorgänge 8

2.2 Risikobewertung 12

2.3 Abhilfemaßnahmen 14

2.4 Erneute Risikobewertung unter Berücksichtigung der getroffenen Maßnahmen 15

Schlussbemerkungen 19

Literaturverzeichnis 20

Einleitung

Die Durchführung einer DSFA sollte grundsätzlich unternehmensintern stattfinden. Sofern vorhanden, ist der/die Datenschutzbeauftragte beratend hinzuzuziehen (Art 35 Abs 2, Art 39 Abs 1 lit c DSGVO). Die Zusammensetzung des durchführenden Teams wird je nach Organisationseinheit und Art der Verarbeitungstätigkeit variieren und kann daher nicht allgemein vorgegeben werden.

Für die Durchführung der DSFA und des damit gegebenenfalls verbundenen Konsultationsverfahrens mit der Datenschutzbehörde nach Art 36 DSGVO sind entsprechende Vorlaufzeiten einzuplanen. Komplexere Verfahren können einen mehrmonatigen Zeitraum in Anspruch nehmen.

Eine DSFA ist für Verarbeitungsvorgänge durchzuführen, wenn diese wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen und wenn sich deren Risiken in Hinblick auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung geändert haben [1, p. 16].

Sanktionen, Geldbußen und/oder weitere Maßnahmen werden grundsätzlich je nach den Umständen des Einzelfalls verhängt. Allgemein gilt jedoch, dass bei Verstößen gegen die Pflichten des Verantwortlichen gemäß Artikel 35 DSGVO Geldbußen von bis zu 10.000.000 EUR oder im Fall eines Unternehmens von bis zu 2% seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt werden können, je nachdem, welcher Betrag höher ist.

Schritt 1: Kriterien zur Prüfung, ob eine DSFA notwendig ist

1.1 Vorgaben aus der DSGVO

Gemäß Artikel 35 Absatz 3 DSGVO ist insbesondere in folgenden Fällen eine DSFA durchzuführen:

- ❑ **Systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen:** Erwägungsgrund 71 DSGVO erwähnt in diesem Zusammenhang automatische Ablehnungen im Rahmen von Online-Einstellungsverfahren oder Online-Kreditanträgen ohne menschliche Prüfung.

- ❑ **Umfangreiche Verarbeitung besonderer Kategorien von pb Daten gemäß Artikel 9 Absatz 1 DSGVO oder von pb Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 DSGVO:** Darunter fallen pb Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen. Zusätzlich sind biometrische und genetische Daten, Gesundheitsdaten, Daten zum Sexualleben sowie zur sexuellen Orientierung und Daten zu strafrechtlichen Verurteilungen bzw. Straftaten und damit zusammenhängende Daten über Sicherungsmaßregeln umfasst (in Anlehnung an Erwägungsgrund 75 DSGVO).

- ❑ **Systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche**: Darunter könnten Videoüberwachungsanlagen subsumiert werden, welche beispielsweise wesentliche Teile des öffentlichen Straßennetzes aufzeichnen.

1.2 Empfehlungen der Artikel 29-Gruppe

Die Artikel 29-Gruppe geht davon aus, dass bei Vorliegen von mindestens zwei der nachfolgend genannten Kriterien in den meisten Fällen eine DSFA erfolgen wird müssen. Es kann jedoch auch vorkommen, dass bereits die Erfüllung eines einzigen der unten genannten Kriterien die Pflicht zur Durchführung einer DSFA auslöst (vgl. [1, p. 12 f.]).

- ❑ **Bewerten oder Einstufen:** Darunter fallen das Erstellen von Profilen und Prognosen, insbesondere auf der Grundlage von Aspekten, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, Zuverlässigkeit oder Verhalten, Aufenthaltsort oder Ortswechsel der Person betreffen (siehe Erwägungsgrund 71 DSGVO). Dieses Kriterium erfüllt beispielsweise eine Bank, welche Datenbanken von Kreditauskunfteien und/oder Betrugsdatenbanken und/oder Geldwäschedatenbanken nach ihren Kundinnen/Kunden durchsucht bzw. auch ein Unternehmen, das anhand der Nutzung seiner Website bzw. der Navigation der Website durch die Nutzer Verhaltens- oder Marketingprofile erstellt (vgl. [1, p. 10 Punkt 1]).
- ❑ **Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung:** Darunter fallen Verarbeitungstätigkeiten, auf deren Grundlage für Betroffene Entscheidungen getroffen werden sollen, “die Rechtswirkung(en) gegenüber natürlichen Personen entfalten” oder diese “in ähnlich erheblicher Weise beeinträchtigen” (siehe Artikel 35 Absatz 3 Buchstabe a DSGVO). Dieses Kriterium ist erfüllt, wenn es zum Ausschluss oder zur Benachteiligung von Personen kommt. Verarbeitungstätigkeiten mit keinen oder wenigen Auswirkungen auf Personen fallen nicht unter dieses Kriterium. Weitere Ausführungen zu diesen Auffassungen/Vorstellungen sind in den Guidelines betreffend Profiling zu finden (vgl. [1, p. 10 Punkt 2], [2, pp. 7, 9ff.]).

- **Systematische Überwachung:** Darunter fallen Verarbeitungstätigkeiten, die die Beobachtung, Überwachung oder Kontrolle von Betroffenen zum Ziel haben und beispielsweise auf über Netzwerke erfasste Daten zurückgreifen. Ein Beispiel könnte die systematische Überwachung der Arbeitsplatzrechner von Angestellten durch den Arbeitgeber sein. Des Weiteren sind Verarbeitungstätigkeiten umfasst, die die Beobachtung, Überwachung oder Kontrolle von Betroffenen zum Ziel haben und beispielsweise auf „eine systematische [...] Überwachung öffentlich zugänglicher Bereiche“ zurückgreifen. Hier ist es für betroffene Personen oft kaum möglich, diese Verarbeitungstätigkeiten zu verhindern. Oftmals wissen die betroffenen Personen in solchen Situationen nicht einmal, wer ihre Daten wie verwendet (gemäß Artikel 35 Absatz 3 Buchstabe c DSGVO, vgl. [1, p. 10f. Punkt 3]).

- **Verarbeitung von vertraulichen Daten oder höchstpersönlichen Daten:** Damit sind einerseits jene Daten gemeint, welche in den Artikeln 9 und 10 DSGVO angeführt sind (Verarbeitung besonderer Kategorien pb Daten – wie beispielsweise Gesundheitsdaten – sowie Verarbeitung von pb Daten über strafrechtliche Verurteilungen und Straftaten). Hierunter fällt beispielsweise eine von einer Krankenanstalt geführte Patientendokumentation. Andererseits fallen darunter auch Standortdaten, Finanzdaten, persönliche Dokumente, E-Mails, Tagebücher, Notizen aus E-Readern mit Notizfunktion sowie Informationen von Life-Logging-Anwendungen (gemäß Artikel 35 Absatz 3 Buchstabe b DSGVO, vgl. [1, p. 11 Punkt 4]).

- **Datenverarbeitung im großen Umfang**: Für die Ermittlung, ob Verarbeitungstätigkeiten im großen Umfang vorliegen, sollten beispielsweise folgende Faktoren herangezogen werden: Zahl der Betroffenen, verarbeitete Datenmenge bzw. Datenelemente, Dauer der Datenverarbeitung und geografisches Ausmaß der Datenverarbeitung (vgl. [1, p. 11 Punkt 5]).

- **Abgleichen oder Zusammenführen von Datensätzen**: Damit sind Verarbeitungstätigkeiten gemeint, bei denen ein Abgleich bzw. eine Zusammenführung unterschiedlicher Datensätze zu unterschiedlichen Zwecken und/oder von verschiedenen für die Verarbeitung Verantwortlichen durchgeführt wurden. Zusätzlich muss der Abgleich bzw. die Zusammenführung in einer Weise stattfinden, der über die vernünftigen Erwartungen der Betroffenen hinausgeht (vgl. [1, p. 12 Punkt 6]).

- **Daten zu schutzbedürftigen Betroffenen**: Die Verarbeitung dieser Art von Daten stellt auf Grund des größeren Machtungleichgewichts zwischen Betroffenen und Verantwortlichen ein Kriterium dar. Hier geht es um Betroffene, die der Verarbeitung ihrer Daten nicht einfach zustimmen oder widersprechen können bzw. für die es nicht so leicht möglich ist, ihre Betroffenenrechte auszuüben. Zu den schutzbedürftigen Betroffenen gehören bspw. folgende Bevölkerungsgruppen: Kinder, Arbeitnehmer/innen, Teile der Bevölkerung mit besonderem Schutzbedarf (psychisch Kranke, Asylwerber/innen, Senioren/Seniorinnen, Patienten/Patientinnen) und Betroffene in Situationen, in denen ein ungleiches Verhältnis zwischen der Stellung des Betroffenen und der des Verantwortlichen vorliegt (vgl. [1, p. 12 Punkt 7]).

- **Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen:** Damit sind Verarbeitungstätigkeiten gemeint, die innovative Methoden der Datenverarbeitung einsetzen, wie beispielsweise die Zugangskontrolle mit Hilfe eines Fingerabdrucks in Kombination mit einer Gesichtserkennung. Der Einsatz einer neuen Technologie kann ein hohes Risiko für die Rechte und Freiheiten einer natürlichen Person mit sich bringen und Grund für die Notwendigkeit einer DSFA sein. Auch Anwendungen des “Internet der Dinge” (IoT) können sich erheblich auf den Alltag und das Privatleben von Personen auswirken und somit eine DSFA obligatorisch machen (vgl. [1, p. 12 Punkt 8]).

- ❑ **Fälle, in denen die Verarbeitung an sich "die betroffenen Personen an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags hindert"**: Dies beinhaltet Verarbeitungstätigkeiten, mit deren Hilfe Betroffenen der Zugriff auf eine Dienstleistung oder der Abschluss eines Vertrags gestattet, geändert oder verwehrt werden soll. Ein Beispiel dafür ist eine Bank, die anhand eines Abgleichs mit einer Datenbank einer Kreditauskunftei entscheidet, ob sie einem Kunden / einer Kundin einen Kredit gewährt (vgl. [1, p. 12 Punkt 9]).

Die Datenschutzbehörden haben Verordnungen zu erlassen, in denen Datenverarbeitungsvorgänge angeführt sind, für die jedenfalls eine DSFA (**Blacklist**) durchzuführen ist. Sie können zudem Listen veröffentlichen, in denen Datenverarbeitungsvorgänge angeführt sind, für die keine DSFA (**Whitelist**) durchzuführen ist (siehe Artikel 35 Absatz 4 und 5 DSGVO). Eine entsprechende Whitelist wird die österreichische Datenschutzbehörde voraussichtlich noch vor dem 25.5.2018 veröffentlichen.

Beispiel: Videoüberwachung im Eingangsbereich einer HIV-Beratungsstelle

Da von der Videoaufzeichnung vor allem Menschen mit einer HIV-Infektion betroffen sein werden, kommt es auch zu einer Verarbeitung von Daten schutzbedürftiger Betroffener. Die Verarbeitungstätigkeit hat des Weiteren die Beobachtung, Überwachung oder Kontrolle von Betroffenen zum Ziel und greift auf eine systematische Überwachung öffentlich zugänglicher Bereiche zurück, weil auch der öffentliche Gehsteig im notwendigen Ausmaß mitumfasst ist. Die Abwicklung der Videoüberwachung (Erfassung, Speicherung, Wiedergabe) findet zudem mit Hilfe einer IT-Applikation statt und erfolgt somit systematisch.

In dem hier geschilderten Fall ist es für betroffene Personen schwierig, die Verarbeitungstätigkeit zu verhindern. Viele betroffene Personen wissen nicht einmal, wer ihre Daten wie verwendet. Obwohl die Videoüberwachungsanlage nur im Zeitraum zwischen 20.00 Uhr und 6.00 Uhr aktiv ist, können und werden schutzbedürftige Betroffene auf den Videoaufzeichnungen in höchstpersönlichen Situationen zu sehen sein. Es ist nämlich davon auszugehen, dass die erste Erkundung einer HIV-Beratungsstelle gerade zu Zeiten erfolgt, an denen die HIV-Beratungsstelle nicht geöffnet ist.

Schritt 2: DSFA durchführen (gemäß Artikel 35 DSGVO)

2.1 Beschreibung und Bewertung der Vorgänge

2.1.1 Systematische Beschreibung

Bei der Durchführung der DSFA muss eine systematische Beschreibung der Verarbeitungsvorgänge erfolgen. Dazu ist es notwendig, die Verarbeitungsvorgänge (wie beispielsweise Erfassung, Speicherung, Veränderung, Übermittlung, Verknüpfung, Löschung) aufzulisten und zu erläutern. Dabei kann es hilfreich sein, schon bekannte Datensicherheitsmaßnahmen sehr allgemein bei der Beschreibung der einzelnen Verarbeitungsvorgänge anzuführen.

Referenzen:

- ❑ Artikel 4 Z 2 DSGVO
- ❑ Artikel 35 Absatz 7 Buchstabe a DSGVO

2.1.2 Zweck

Zusätzlich sind die mit der Verarbeitungstätigkeit verfolgten Zwecke anzuführen. Denn pb Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung"). Zusätzlich müssen pb Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung").

Referenzen:

- ❑ Artikel 5 Absatz 1 Buchstabe b und c DSGVO
- ❑ Artikel 35 Absatz 7 Buchstabe a DSGVO

2.1.3 Berechtigte Interessen

Stützt sich der Verantwortliche auf berechtigte Interessen, sind diese berechtigten Interessen zu erläutern. Ein berechtigtes Interesse liegt vor, wenn die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz pb Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Referenzen:

- ❑ Artikel 6 Absatz 1 Buchstabe f DSGVO
- ❑ Artikel 35 Absatz 7 Buchstabe a DSGVO

2.1.4 Bewertung der Notwendigkeit und Verhältnismäßigkeit

Des Weiteren hat eine Bewertung zu erfolgen, warum die Verarbeitungstätigkeit in ihrer konkreten Ausprägung mit den angeführten Verarbeitungsvorgängen für den genannten Zweck notwendig und verhältnismäßig ist. Dabei sollte sich der Verantwortliche die Frage stellen, ob der Zweck der Verarbeitungstätigkeit wirklich nicht durch gelindere Mittel erreichbar ist, welche mit weniger pb Daten auskommen. Außerdem sollte aus der Bewertung der Notwendigkeit und Verhältnismäßigkeit hervorgehen, dass bei der konkreten Ausgestaltung der Verarbeitungstätigkeit schon Datensicherheitsmaßnahmen zum Einsatz kommen.

Referenzen:

- ❑ Artikel 4 Z 2 DSGVO
- ❑ Artikel 35 Absatz 7 Buchstabe b DSGVO

2.1.5 Standpunkt der betroffenen Personen einholen

Der Verantwortliche sollte gegebenenfalls den Standpunkt der betroffenen Personen einholen. Dabei erscheint es sinnvoll darauf zu achten, dass man von Mitgliedern unterschiedlicher Personenkategorien (Mitarbeiter/innen, Lieferant/innen, Kund/innen) Stellungnahmen erhält, sofern diese von der

Verarbeitungstätigkeit betroffen sind. Die wesentlichen Aussagen und insbesondere Bedenken dieser Personen sollten dokumentiert werden.

Referenzen:

- ❏ Artikel 35 Absatz 9 DSGVO

2.1.6 Rat des/der Datenschutzbeauftragten einholen

Hat der Verantwortliche eine/n Datenschutzbeauftragte/n bestellt, ist diese/r frühzeitig in die DSFA einzubinden. So kann der/die Datenschutzbeauftragte bei der Durchführung der DSFA schon in der Anfangsphase der DSFA beraten.

Referenzen:

- ❏ Artikel 35 Absatz 2 DSGVO
- ❏ Artikel 39 Absatz 1 Buchstabe a und c DSGVO

Beispiel: Videoüberwachung im Eingangsbereich einer HIV-Beratungsstelle[1]

2.1.1 Systematische Beschreibung (siehe auch Abbildung 1):

- ❏ *Erfassung von Videodaten im Eingangs- und Zutrittsbereich mit IP-Kameras. Die Erfassung erfolgt an Wochentagen nur zwischen 20.00 Uhr und 6.00 Uhr. An Wochenenden und Feiertagen erfassen die IP-Kameras durchgehend Videodaten.*[2] *Im betroffenen Eingangs- und Zutrittsbereich befinden sich keine Arbeitsplätze. Die IP-Kameras sind nicht schwenkbar. Somit ist das Schwenken der IP-Kameras in die Richtung von Arbeitsplätzen nicht möglich.*
- ❏ *Verschlüsselte kabelgebundene Übertragung der Videodaten zum Server.*[3]
- ❏ ***Unverschlüsselte drahtlose Übertragung*** *der Videodaten zum Server.*
- ❏ *Verschlüsselte Speicherung der Videodaten am Server für drei Tage. Danach überschreibt das System automatisch die Videodaten. Der Server steht in einem* ***Abstellraum****. Vor allem Reinigungspersonal muss mehrmals täglich den Abstell- bzw. Serverraum betreten, um an benötigtes Reinigungsmaterial zu gelangen.*
- ❏ *Die Videodaten werden weder einem Empfänger übermittelt oder offengelegt, noch wird ein Auftragsverarbeiter mit der weiteren Verarbeitung der Daten beauftragt.*
- ❏ *Verschlüsselter Zugriff auf Videodaten über Unternehmensnetzwerk oder Internet. Die Videoaufzeichnungen können nur bestimmte Mitarbeiter/innen der IT-Abteilung und der Facility Management-Abteilung ansehen. Dafür ist für jede/n Mitarbeiter/in die Eingabe des korrekten Passworts erforderlich. Die Zugriffe, Änderungen und Löschungen hinsichtlich der Videoaufzeichnungen protokolliert das System lückenlos. Einmal jährlich erfolgt eine Kontrolle der Protokolle hinsichtlich Datenschutzverletzungen. Das heißt, es kommt zu einer Überprüfung, ob jeder Zugriff auch von einem konkreten Anlassfall abgedeckt ist.*[4]

---

[1] Gemäß Artikel 32 und Erwägungsgrund 74 DSGVO sollte der Verantwortliche die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung und das **Risiko** für die Rechte und Freiheiten natürlicher Personen berücksichtigen. Dieser risikobasierte Ansatz führt zu einer situativen Bewertung von Videoüberwachungsanlagen. Beispielsweise werden Videoaufzeichnungen des Eingangsbereichs von HIV-Beratungsstellen mit mehr Risiken verbunden sein als Videoaufzeichnungen des Eingangsbereichs eines Getränkeherstellers.

[2] Jede Verarbeitungstätigkeit muss die Grundsätze für die Verarbeitung personenbezogener Daten gemäß Artikel 5 DSGVO einhalten. Die hier beschriebene ausschließliche Aufzeichnung in den Nachtstunden und an Feiertagen bzw. Wochenenden trägt dem **Grundsatz der Datenminimierung** Rechnung. Wenn bestimmte beschriebene technische oder organisatorische Maßnahmen im Beispiel einen Grundsatz unterstützen, ist der Grundsatz in einer Fußnote angegeben.

[3] Grundsatz der Integrität und Verfügbarkeit gemäß Artikel 5 Absatz 1 Buchstabe f DSGVO.

[4] Grundsatz der Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz gemäß Artikel 5 Absatz 1 Buchstabe a DSGVO.

- ***Anmerkung/Referenz:*** *Das österreichische Datenschutzgesetz enthält in §§ 12, 13 DSG Bestimmungen zu besonderen Datensicherheitsmaßnahmen bei Bildaufnahmen. § 13 Abs 1 DSG normiert, dass der Verantwortliche dafür zu sorgen hat, dass der Zugang zur Bildaufnahme und eine nachträgliche Veränderung derselben durch Unbefugte ausgeschlossen ist. Gemäß § 13 Abs 2 DSG hat der Verantwortliche – außer bei Echtzeitüberwachung – jeden Verarbeitungsvorgang zu protokollieren. § 13 Abs 3 DSG bestimmt, dass eine länger als 72 Stunden andauernde Aufbewahrung verhältnismäßig sein muss, gesondert zu protokollieren und zu begründen ist.*

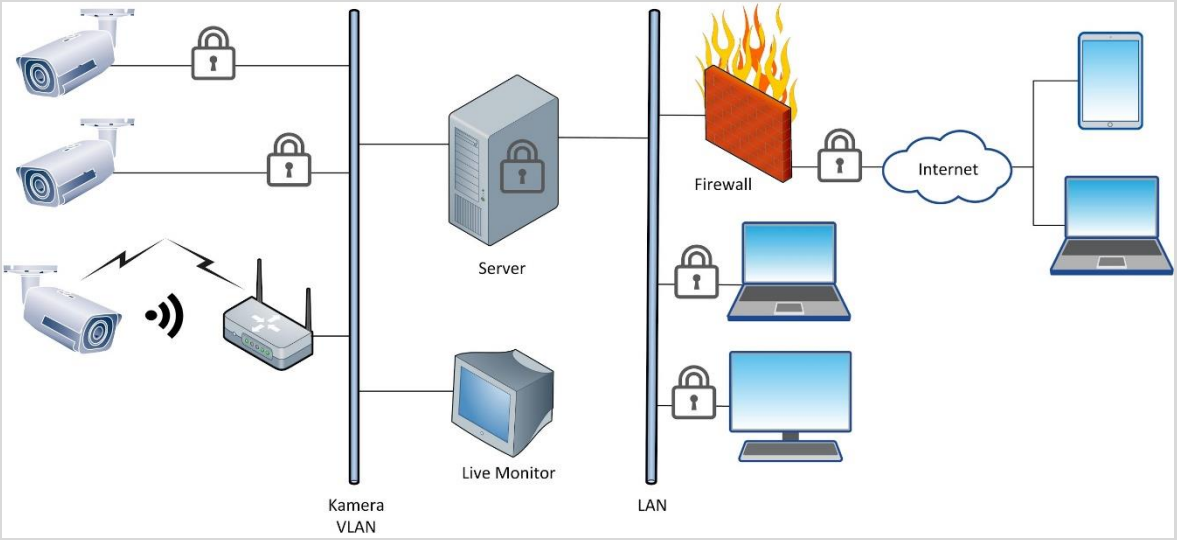

Abbildung 1: Schematische Darstellung der Verarbeitungstätigkeit „Videoüberwachung“

2.1.2 Zweck:

- *Digitale Videoüberwachung ohne Tondaten des Einganges samt Zutrittsbereich des Verwaltungsgebäudes der HIV-Beratungsstelle, Mustergasse 1, 1234 Musterort, Österreich zum Zweck des Eigentumsschutzes und des Verantwortungsschutzes, der Verhinderung, Eindämmung und Aufklärung strafrechtlich relevanten Verhaltens mit ausschließlicher Auswertung in dem durch den Zweck definierten Anlassfall.*[5]

2.1.3 Berechtigte Interessen:

- *Die HIV-Beratungsstelle geht aufgrund wiederholter Einbruchsversuche und Sachbeschädigungen in den letzten Monaten (teilweise mit Erfolg) davon aus, dass eine besondere Gefährdungslage besteht, die durch die beschriebene Videoüberwachung eingedämmt werden kann. Deswegen liegt ein berechtigtes Interesse der HIV-Beratungsstelle an der Videoüberwachung vor. Die Videoüberwachung dient dem vorbeugenden Schutz von Personen oder Sachen auf privaten Liegenschaften, die ausschließlich vom Verantwortlichen genutzt werden und reicht räumlich nicht über die Liegenschaft hinaus, mit Ausnahme einer zur Zweckerreichung unvermeidbaren Einbeziehung öffentlicher Verkehrsflächen (Gehsteig).*
- ***Anmerkung/Referenz:*** *Das österreichische Datenschutzgesetz enthält in § 12 Abs 2 Z 4 DSG iVm § 12 Abs 3 DSG eine demonstrative Aufzählung von Fällen, in denen laut dem Gesetzgeber ein überwiegendes berechtigtes Interesse eines Verantwortlichen an einer Bildverarbeitung besteht. § 12 Abs 3 Z 1 normiert, dass “[…] eine Bildaufnahme […] insbesondere dann zulässig [ist], wenn sie dem vorbeugenden Schutz von Personen oder Sachen auf privaten Liegenschaften, die ausschließlich vom Verantwortlichen genutzt werden, dient, und räumlich nicht über die Liegenschaft hinausreicht, mit Ausnahme einer zur Zweckerreichung allenfalls unvermeidbaren Einbeziehung öffentlicher Verkehrsflächen[.]”*

[5] Grundsatz der Zweckbindung gemäß Artikel 5 Absatz 1 Buchstabe b DSGVO.

2.1.4 Bewertung der Notwendigkeit und Verhältnismäßigkeit:

- ❑ *Die HIV-Beratungsstelle sichert ihren Eingangs- und Zutrittsbereich mit einem Zugangskontrollsystem ab. Zusätzlich gibt es tagsüber (von 6.00 Uhr bis 20.00 Uhr) einen Empfangsdienst. In der Nacht (von 20.00 Uhr bis 6.00 Uhr) kommt eine Alarmanlage zum Einsatz. Außerdem überprüft ein externer Sicherheitsdienstleister mehrmals, ob es sicherheitskritische Ereignisse gibt. Die Fenster im Erdgeschoß sind vergittert. Es sind Anzeigen bei der örtlichen Polizeiinspektion hinsichtlich der letzten Einbruchsversuche und Sachbeschädigungen erfolgt. Trotzdem kommt es immer wieder zu Einbruchsversuchen und Sachbeschädigungen. Deswegen ist die Videoüberwachung notwendig. Mittels eines Aushanges in der HIV-Beratungsstelle werden die Betroffenen über ihre Rechte aufklärt und die Informationspflichten erfüllt. Die konkrete Ausgestaltung der Verarbeitungsvorgänge (siehe Beschreibung oben) soll die Verhältnismäßigkeit[6] herstellen.*
- ❑ ***Kennzeichnung:** Eine verständliche Kennzeichnung weist die betroffenen Personen in Bildform darauf hin, dass die HIV-Beratungsstelle die Videoüberwachung verantwortet. Aus der Kennzeichnung ergibt sich auch, dass die HIV-Beratungsstelle die Videoaufzeichnung aufzeichnet, nur im Anlassfall auswertet und dass keine Gesichtserkennung im Rahmen der Videoüberwachung zur Anwendung kommt.[7]*
- ❑ ***Anmerkung/Referenz:** Das österreichische Datenschutzgesetz enthält in § 13 Abs. 5 DSG eine Kennzeichnungspflicht von Bildaufnahmen. Aus dieser Kennzeichnung muss zumindest die Identität des Verantwortlichen feststellbar sein. Werden entgegen Abs. 5 keine ausreichenden Informationen bereitgestellt, kann jeder von einer Verarbeitung potenziell Betroffene vom Eigentümer oder Nutzungsberechtigten einer Liegenschaft oder eines Gebäudes oder sonstigen Objekts, von dem aus eine solche Verarbeitung augenscheinlich ausgeht, Auskunft über die Identität des Verantwortlichen begehren. Die unbegründete Nichterteilung einer derartigen Auskunft ist einer Verweigerung der Auskunft nach Artikel 15 DSGVO gleichzuhalten (§ 13 Abs. 7 DSG).*

2.1.5 Standpunkt der betroffenen Personen einholen:

- ❑ *Die HIV-Beratungsstelle hat stichprobenartig den Standpunkt von betroffenen Personen eingeholt. Insgesamt hat die HIV-Beratungsstelle die in dieser Beschreibung dargelegten Informationen fünf Personen vorgelegt und um Stellungnahme gebeten. Darunter befanden sich ein Mitarbeiter der HIV-Beratungsstelle, zwei Mitarbeiterinnen von Lieferanten und zwei Personen, welche Beratungsleistungen bezogen haben. Die Rückmeldungen fielen allesamt positiv aus, da alle Personen die Notwendigkeit der Videoüberwachung nachvollziehen konnten und die konkrete Ausgestaltung ihres Erachtens auch verhältnismäßig ist. Es liegen schriftliche Gesprächsprotokolle vor.*
- ❑ ***Anmerkung/Referenz:** Im österreichischen Arbeitsverfassungsgesetz sind die Befugnisse des Betriebsrats geregelt. Für bestimmte Verarbeitungstätigkeiten hinsichtlich Mitarbeiterdaten muss der Abschluss von Betriebsvereinbarungen erfolgen. Auch wenn der Abschluss einer Betriebsvereinbarung nicht notwendig ist, hat eine frühzeitige Information des Betriebsrats über geplante Verarbeitungstätigkeiten, von denen auch Mitarbeiter/innen betroffen sind, zu erfolgen (siehe §§ 91 Abs. 2, 96 ff ArbVG). Deswegen bietet es sich auch im Rahmen der DSFA an, den Standpunkt des Betriebsrats einzuholen, wenn Daten von Mitarbeiter/innen betroffen sind und ein Betriebsrat vorhanden ist.*

2.1.6 Rat des/der Datenschutzbeauftragten einholen:

- ❑ *Die HIV-Beratungsstelle hat eine/n Datenschutzbeauftragten bestellt. Deswegen hat die HIV-Beratungsstelle auch den Rat des/der Datenschutzbeauftragten bezüglich der Videoüberwachung im Eingangsbereich eingeholt. Diese/r bat um großflächige Kennzeichnung der Videoüberwachung. Aus dieser soll zusätzlich zur verpflichtenden Angabe des Verantwortlichen hervorgehen, dass das Videoüberwachungssystem die Videos aufzeichnet (also nicht nur Echtzeitaufnahmen erfolgen), eine*

[6] Die Bewertung der Verhältnismäßigkeit bei einer **durchgehenden** Videoüberwachung (also auch tagsüber) wäre differenziert festzulegen. Unter Umständen könnte der Eingangsbereich aus datenschutzrechtlicher Sicht als „Arbeitsplatz" verstanden werden, da die Mitarbeiter beim Verlassen bzw. Betreten der Beratungsstelle aufgenommen werden, es sei denn, es gibt für die MitarbeiterInnen einen separaten Eingang.

[7] Grundsatz der Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz gemäß Artikel 5 Absatz 1 Buchstabe a DSGVO.

Auswertung nur im Anlassfall stattfindet und Gesichtserkennung nicht zur Anwendung gelangt. Diesen Vorschlag hat die HIV-Beratungsstelle umgesetzt. Die Stellungnahme des/der Datenschutzbeauftragten liegt in Textform vor.

2.2 Risikobewertung

Bei der Risikobewertung werden mögliche Risiken für die Rechte und Freiheiten der betroffenen Personen identifiziert (Risikoidentifikation) und analysiert (Risikoanalyse). Die Risikobewertung erfolgt durch den DSFA-Durchführenden.

Es wird empfohlen, zumindest folgende Risiken zu bewerten:

- Verlust der Vertraulichkeit (z. B. unbefugter Zugriff auf pb Daten)
- Verlust der Integrität (z. B. unbefugte Veränderung von pb Daten)
- Verlust der Verfügbarkeit (Belastbarkeit) (z. B. Verlust von pb Daten)

Im Zuge der Risikoanalyse wird der Risikowert ermittelt (= Höhe des identifizierten Risikos). In einem ersten Schritt werden die Eintrittswahrscheinlichkeit einer Bedrohung sowie die zu erwartenden Auswirkungen bewertet. Für die Bewertung der Eintrittswahrscheinlichkeiten und Auswirkungen werden seitens DSGVO keine Kategorien vorgegeben. Mögliche Einstufungs-Kategorien können beispielsweise wie folgt vorgegeben werden:

Beurteilung der Eintrittswahrscheinlichkeit	
Vernachlässigbar	Für die ausgewählte Risikoquelle scheint es nicht sehr wahrscheinlich zu sein, eine Schwachstelle eines unterstützenden Wertes[8] auszunutzen, um eine Bedrohung eintreten zu lassen (zum Beispiel: Diebstahl von Papierdokumenten aus einem Raum, der durch ein Ausweislesegerät und einen Zugangscode gesichert ist).
Eingeschränkt	Für die ausgewählte Risikoquelle scheint es schwierig zu sein, eine Schwachstelle eines unterstützendes Wertes auszunutzen, um eine Bedrohung eintreten zu lassen (zum Beispiel: Diebstahl von Papierdokumenten aus einem Raum, der durch ein Ausweislesegerät gesichert ist).
Signifikant	Für die ausgewählte Risikoquelle scheint es möglich zu sein, eine Schwachstelle eines unterstützenden Werts auszunutzen, um eine Bedrohung eintreten zu lassen (zum Beispiel: Diebstahl von Papierdokumenten aus einem Büro, welches nur zugänglich ist, nachdem man einen Empfang passiert hat).
Maximal	Für die ausgewählte Risikoquelle scheint es einfach zu sein, eine Schwachstelle eines unterstützenden Wertes auszunutzen, um eine Bedrohung eintreten zu lassen (zum Beispiel: Diebstahl von Papierdokumenten aus einer öffentlich zugänglichen Lobby).

Tabelle 1: Beurteilung der Eintrittswahrscheinlichkeit gemäß Bitkom-Leitfaden für "Risk Assessment & Datenschutz-Folgenabschätzung" *[3, p. 31]*

[8] Werte sind alles, was wichtig ist für eine Institution (Vermögen, Wissen, Gegenstände, Gesundheit) vgl. BSI-Glossar „Wert (englisch „asset"), Quelle: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html

Einschätzung der Auswirkungen	
Vernachlässigbar	Betroffene erleiden eventuell Unannehmlichkeiten, die sie aber mit einigen Problemen überwinden können.
Eingeschränkt	Betroffene erleiden eventuell signifikante Unannehmlichkeiten, die sie aber mit einigen Schwierigkeiten überwinden können.
Signifikant	Betroffene erleiden eventuell signifikante Konsequenzen, die sie nur mit ernsthaften Schwierigkeiten überwinden können.
Maximal	Betroffene erleiden eventuell signifikante oder sogar unumkehrbare Konsequenzen, die sie nicht überwinden können.

Tabelle 2: Generische Beschreibung der Auswirkungen gemäß Bitkom-Leitfaden für "Risk Assessment & Datenschutz-Folgenabschätzung" *[3, p. 50]*

Untenstehend sind Beispiele für die Einschätzung der Auswirkungen aus Sicht der Betroffenen angeführt. Die vollständige Auflistung aller Beispiele ist im Bitkom-Leitfaden für "Risk Assessment & Datenschutz-Folgenabschätzung" [3, p. 51f.] ersichtlich.

	Vernachlässigbar	**Eingeschränkt**	**Signifikant**	**Maximal**
Beispiele für physische Auswirkungen	Vorübergehende Kopfschmerzen	Leichte körperliche Beschwerden (z. B. leichte Krankheiten aufgrund unberücksichtigter medizinischer Kontraindikationen)	Veränderung der körperlichen Unversehrtheit z. B. nach einem Angriff, einem Unfall zu Hause oder auf der Arbeit etc.	Tod (z. B. Mord, Selbstmord, tödlicher Unfall)
Beispiele für materielle Auswirkungen	Empfang unerwünschter E-Mails (z. B. Spam)	Unrichtiges oder unangebrachtes Profiling	Verbot der Führung von Bankkonten	Erhebliche Schulden
Beispiele für moralische Auswirkungen	Angst, die Kontrolle über die eigenen Daten zu verlieren	Einschüchterung in sozialen Netzwerken	Cyber-Mobbing und Belästigung	Strafrechtliche Verurteilung

Tabelle 3: Beispiele für die Einschätzung der Auswirkungen gemäß Bitkom-Leitfaden für "Risk Assessment & Datenschutz-Folgenabschätzung" *[3, p. 51f.]*

Bei der Bewertung der Eintrittswahrscheinlichkeiten und Auswirkungen sollen alle bisher getroffenen technischen und organisatorischen Maßnahmen berücksichtigt werden.

Anschließend kann der Risikowert wie folgt berechnet werden:

Risikowert **=** *Eintrittswahrscheinlichkeit einer Bedrohung* **mal** *zu erwartende Auswirkungen*

Für die Berechnung des Risikowerts gibt die DSGVO keine Risiko-Matrix vor. Folgende Risiko-Matrix kann an dieser Stelle beispielsweise herangezogen werden:

Auswirkungen aus Sicht der Betroffenen	**Maximal**	**mittel**	**mittel**	**hoch**	**hoch**
	Wesentlich	**mittel**	**mittel**	**mittel**	**hoch**
	Eingeschränkt	**gering**	**mittel**	**mittel**	**mittel**
	Vernachlässigbar	**gering**	**gering**	**mittel**	**mittel**
		Vernachlässigbar	**Eingeschränkt**	**Wesentlich**	**Maximal**
		Eintrittswahrscheinlichkeit			

Tabelle 4: Risiko-Matrix gemäß Bitkom-Leitfaden für "Risk Assessment & Datenschutz-Folgenabschätzung" *[3, p. 32]*

Um dem laut Artikel 5 Absatz 2 DSGVO geforderten Datenschutz-Grundsatz der „Rechenschaftspflicht" nachzukommen, wird empfohlen, im Zuge der Risikobewertung folgende Informationen zu dokumentieren:

Titel und Beschreibung der Bedrohung	Kurze Beschreibung der Bedrohung (z. B. Verlust der Vertraulichkeit durch …)
Eintrittswahrscheinlichkeit inkl. Begründung	Bewertung der Eintrittswahrscheinlichkeit von Bedrohungen gemäß Tabelle 1 (inkl. Begründung in Prosa-Text)
Auswirkungen inkl. Begründung	Bewertung der Auswirkungen (= möglicher Schaden) gemäß Tabelle 2 (inkl. Begründung in Prosa-Text)
Risikowert	Angabe des laut Risiko-Matrix ermittelten Risikowerts (siehe Tabelle 4)

2.3 Abhilfemaßnahmen

Laut Artikel 35 Absatz 7 Buchstabe d DSGVO hat der Verantwortliche folgendes sicherzustellen:

> *„die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird."*

Bei der Risikobehandlung gemäß Artikel 32 Absatz 1 DSGVO wird entschieden, wie mit identifizierten Risiken umgegangen werden soll. Dabei stehen folgende vier Risikobehandlungs-Optionen zur Verfügung:

- Risikominimierung (durch Setzen von Maßnahmen)
- Risikovermeidung (durch Unterlassen der risikobehafteten Aktivität, z. B. Beendigung der Verarbeitung pb Daten in Cloud-Anwendungen)
- Risikotransfer (durch Auslagerung von Risikofolgen auf Dritte, z. B. Versicherung bei Datenverlust)
- Risikoakzeptanz (bewusste Entscheidung, keine weiteren Maßnahmen zu treffen)

Um dem laut Artikel 5 Absatz 2 DSGVO geforderten Datenschutz-Grundsatz der „Rechenschaftspflicht" nachzukommen, wird empfohlen, im Zuge der Risikobehandlung folgende Informationen zu dokumentieren:

Typ der Risikobehandlung	Risikominimierung, Risikovermeidung, Risikotransfer, Risikoakzeptanz
Begründung für die Auswahl Risikobehandlung	Beschreibung der Gründe für die Auswahl des Risikobehandlungstyps (in Prosa-Text)
Dokumentation der Maßnahmen	Verweis auf die Maßnahmendokumentation (z. B. TOMs-Dokumentation, zusätzliche Dokumentationen etc.)

Beispiele für Maßnahmenkataloge:
Nachfolgend sind gängige, dem Stand der Technik entsprechende Maßnahmenkataloge angeführt, die bei der Auswahl von risikominimierenden Maßnahmen unterstützen können:

- ISO/IEC 27001:2013 - Information security management systems - Requirements, Annex A[9]
- ISO/IEC 27002:2013 - Code of practice for information security controls[10]
- BSI IT-Grundschutz - IT-Grundschutz-Kompendium[11]
- Maßnahmenkatalog der CNIL[12]
- ISO/IEC 29151:2017 - Code of practice for personally identifiable information protection[13]
- WKO - IT-Sicherheitshandbuch für Mitarbeiterinnen und Mitarbeiter[14]

2.4 Erneute Risikobewertung unter Berücksichtigung der getroffenen Maßnahmen

In einem letzten Schritt soll das Risiko – unter Berücksichtigung der getroffenen Maßnahmen – erneut bewertet werden.

Eintrittswahrscheinlichkeit	Bewertung der Eintrittswahrscheinlichkeit von Bedrohungen laut Tabelle 1 unter Berücksichtigung der getroffenen Maßnahmen (inkl. Begründung in Prosa-Text)
Auswirkungen	Bewertung der Auswirkungen (= möglicher Schaden) laut Tabelle 2 (inkl. Begründung in Prosa-Text)
Risikowert	Angabe des Risikowerts unter Berücksichtigung der getroffenen Maßnahmen (Tabelle 3)

Wenn aus der durchgeführten DSFA hervorgeht, dass die Verarbeitung ein hohes Risiko für die Betroffenen zur Folge hätte und keine Maßnahmen zur Eindämmung des Risikos mehr getroffenen werden können, muss vor der Aufnahme der Verarbeitung die Aufsichtsbehörde konsultiert werden.

Konsultation der Aufsichtsbehörde erforderlich?	ja / nein

Nach Fertigstellung der DSFA sollten die Ergebnisse dem Management bzw. der Geschäftsführung zur Abzeichnung und Genehmigung vorgelegt werden.

[9] https://www.iso.org/standard/54534.html
[10] https://www.iso.org/standard/54533.html
[11] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html
[12] https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-3-GoodPractices.pdf
[13] https://www.iso.org/standard/62726.html
[14] http://wko.at/ic//IT_Handbuch_MA_2017.pdf

Beispiele: Videoüberwachung im Eingangsbereich einer HIV-Beratungsstelle

Risikobewertung	
Titel und Beschreibung der Bedrohung	***Verletzung des Schutzes der Vertraulichkeit*** *Daten können von unberechtigten Dritten abgegriffen werden, da die Übertragung zum Server unverschlüsselt und drahtlos erfolgt.*
Eintrittswahrscheinlichkeit inkl. Begründung	***Wesentlich*** *Da Videoüberwachung an Wochentagen zwischen 20.00 und 6.00 Uhr sowie an Wochenenden und Feiertagen erfolgt*
Auswirkungen inkl. Begründung	***Maximal*** *Unberechtigte Dritte können pb Daten abgreifen (Datenschutzverletzung)*
Risikowert	***Hohes Risiko***
Abhilfemaßnahmen/Risikobehandlung	
Typ der Risikobehandlung	***Risikominimierung***
Begründung für die Auswahl der Risikobehandlung	*Verschlüsselung der drahtlosen Übertragung der Videodaten zum Server aufgrund des hohen Schutzbedarfs der übertragenen pb Daten, Einsatz von SSL/TLS*
Dokumentation der Maßnahmen	*Wiki*
Erneute Risikobewertung unter Berücksichtigung der getroffenen Maßnahmen	
Eintrittswahrscheinlichkeit (unter Berücksichtigung der getroffenen Maßnahmen)	***Vernachlässigbar***
Auswirkungen	***Vernachlässigbar***
Risikowert (unter Berücksichtigung der getroffenen Maßnahmen)	***Geringes Risiko***
Konsultation der Aufsichtsbehörde erforderlich?	***nein***

Risikobewertung	
Titel und Beschreibung der Bedrohung	***Verletzung des Schutzes der Integrität*** *Aufzeichnungen können durch Admins jederzeit manipuliert werden (z.B. Änderung der Timestamps, Löschung von einzelnen Aufzeichnungen / Ausschnitten von Aufzeichnungen, …)*
Eintrittswahrscheinlichkeit inkl. Begründung	***Maximal*** *Admins können jederzeit Änderungen durchführen*
Auswirkungen inkl. Begründung	***Maximal*** *Falsche Behauptungen zu einem Zutritt können vorliegen*
Risikowert	***Hohes Risiko***
Abhilfemaßnahmen/Risikobehandlung	
Typ der Risikobehandlung	***Risikominimierung***
Begründung für die Auswahl der Risikobehandlung	*4-Augen-Prinzip für Änderungen erforderlich*
Dokumentation der Maßnahmen	*Wiki*
Erneute Risikobewertung unter Berücksichtigung der getroffenen Maßnahmen	
Eintrittswahrscheinlichkeit (unter Berücksichtigung der getroffenen Maßnahmen)	***Vernachlässigbar***
Auswirkungen	***Eingeschränkt***
Risikowert (unter Berücksichtigung der getroffenen Maßnahmen)	***Geringes Risiko***
Konsultation der Aufsichtsbehörde erforderlich?	***nein***

Risikobewertung	
Titel und Beschreibung der Bedrohung	***Verletzung des Schutzes der Verfügbarkeit*** *Reinigungspersonal kann Server, auf dem die Videoaufzeichnungen gespeichert sind, stehlen, da der Server in einem Abstellraum steht (zu dem u.a. auch das Reinigungspersonal Zutritt hat)*
Eintrittswahrscheinlichkeit inkl. Begründung	***Maximal*** *Personal hat durchgehenden Zutritt*
Auswirkungen inkl. Begründung	***Vernachlässigbar*** *Daten am Server sind verschlüsselt und Betroffener erfährt (voraussichtlich) keinen Schaden, wenn die Daten nicht verfügbar sind*
Risikowert	***Mittleres Risiko***
Abhilfemaßnahmen/Risikobehandlung	
Typ der Risikobehandlung	***Risikoakzeptanz***
Begründung für die Auswahl der Risikobehandlung	*Voraussichtlich kein hohes Risiko für die Rechte und Freiheiten der Betroffenen*
Dokumentation der Maßnahmen	-
Erneute Risikobewertung unter Berücksichtigung der getroffenen Maßnahmen	
Eintrittswahrscheinlichkeit (unter Berücksichtigung der getroffenen Maßnahmen)	***Maximal***
Auswirkungen	***Vernachlässigbar***
Risikowert (unter Berücksichtigung der getroffenen Maßnahmen)	***Mittleres Risiko***
Konsultation der Aufsichtsbehörde erforderlich?	***Nein***

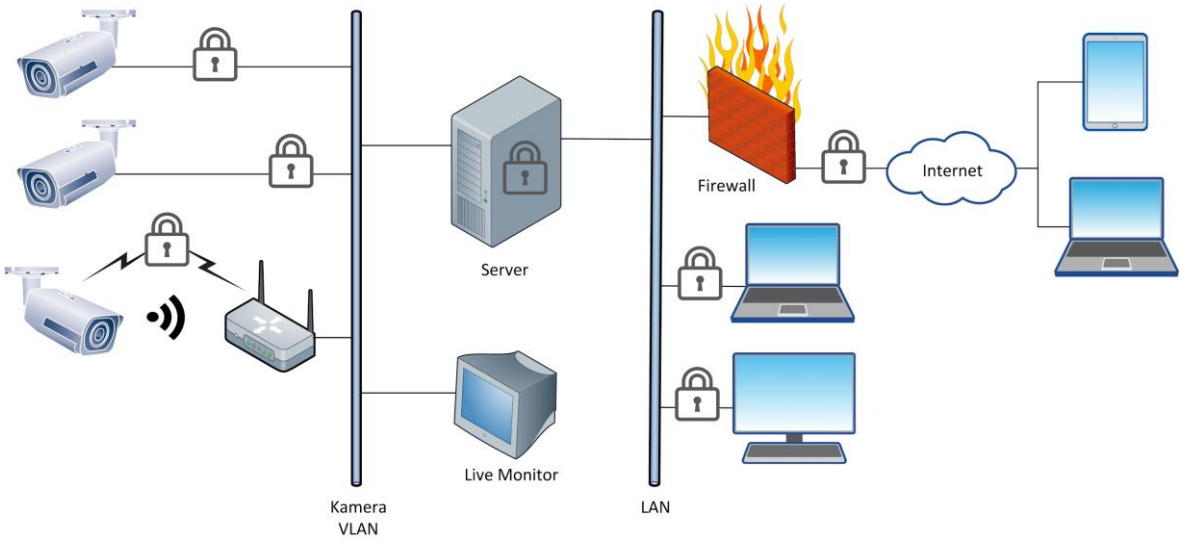

Abbildung 2: Angepasste schematische Darstellung der Verarbeitungstätigkeit „Videoüberwachung“ nach Umsetzung der zusätzlichen Datensicherheitsmaßnahmen

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]

Literaturverzeichnis

[1] Article 29 Working Party, „Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“, WP 248 Rev. 01, 17/DE,“ http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083, 4. Oktober 2017.

[2] Article 29 Working Party, „Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP 251, 17/EN,“ http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083, 3. Oktober 2017.

[3] Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (Bitkom), „Risk Assessment & Datenschutz-Folgenabschätzung: Leitfaden,“ Berlin, https://www.bitkom.org/NP-Themen/NP-Vertrauen-Sicherheit/Datenschutz/FirstSpirit-1496129138918170529-LF-Risk-Assessment-online.pdf, 2017 (abgerufen am 17.10.2017).

[4] International Organization for Standardization (ISO), „ISO/IEC 29134:2017 - Information technology -- Security techniques -- Guidelines for privacy impact assessment,“ https://www.iso.org/standard/62289.html.

[5] B. F. Privatheit, „White Paper DSFA,“ 3. Auflage 2017. [Online]. Available: https://www.forum-privatheit.de/forum-privatheit-de/publikationen-und-downloads/veroeffentlichungen-des-forums/themenpapiere-white-paper/Forum-Privatheit-WP-DSFA-3-Auflage-2017-11-29.pdf.

[6] GDD-Praxishilfe, „DS-GVO X - Voraussetzungen der Datenschutz-Folgenabschätzung,“ Version 1.0, November 2017. [Online]. Available: https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_10.pdf.

[7] „Planspiel DSFA des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein und der Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern,“ [Online]. Available: https://www.datenschutz-mv.de/static/DS/Dateien/DS-GVO/Hilfsmittel%20zur%20Umsetzung/Planspiel_Datenschutz_Folgenabschaetzung.pdf .

[8] CNIL, „The open source PIA software,“ [Online]. Available: https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment.