Einführung

Für Verarbeitungsprozesse mit hohem Risiko für Rechte und Freiheiten natürlicher Personen müssen Sie eine Folgeschabschätzung gemäß Artikel 35 DS-GVO durchführen, z.B. bei Videoüberwachung oder Fingerprint-Scannern. Wenn Sie eine Folgenabschätzung durchzuführen haben, unterliegen Sie gemäß § 38 Absatz 1 BDSG auch automatisch der Pflicht zur Bestellung eines Datenschutzbeauftragten. Gemäß Art. 35 Absatz 2 DS-GVO holen Sie den Rat Ihres Datenschutzbeauftragten bei einer Folgenabschätzung ein.

In welchen Fällen eine Datenschutz-Folgenabschätzung durchzuführen ist, kann anhand von sogenannten „Positivlisten" und der eigenen Schwellenwertprüfung ermittelt werden. Die Positivliste der Datenschutzkonferenz finden Sie zum Beispiel über den folgenden Link:

https://www.lfd.niedersachsen.de/startseite/datenschutzrecht/ds_gvo/liste_von_verarbeitungsvorgangen_nach_art_35_abs_4_ds_gvo/muss-listen-zur-datenschutz-folgenabschatzung-179663.html

Nachfolgend stellen wir zunächst vor, welchen Inhalt und Ablauf eine Folgenabschätzung haben muss und geben Ihnen im Anschluss ein Beispiel für eine Folgenabschätzung.

Dieses Muster einer Folgenabschätzung gemäß Artikel 35 DS-GVO für die Videoüberwachung im öffentlichen Raum, also dem Verkaufsraum der Apotheke, dient Ihrer Orientierung. Wir übernehmen keine Haftung oder sonstige Gewährleistung für die Richtigkeit und Vollständigkeit der folgenden Folgenabschätzung für Videoüberwachung, und weisen darauf hin, dass das Muster noch an den individuellen Betrieb angepasst werden muss. So können bei Ihnen die Kameras anders aufgestellt sein oder auch eine kurzfristige Überwachung des nichtöffentlichen Bereichs der Apotheke gegeben sein. Ihr fertig angepasstes Muster legen Sie Ihrem Verfahrensverzeichnis bei, am besten zum Verarbeitungsprozess „Videoüberwachung".

Zusätzlich hängen Sie gut sichtbar entsprechend dem mitgelieferten Beispiel der Landesbeauftragten für Datenschutz aus Niedersachsen ein Informationsblatt bzw. Hinweis auf die Videoüberwachung am Eingang Ihrer Apotheke aus.

Folgenabschätzung

(nach Koreng/Lachmann, Formularhandbuch Datenschutzrecht, 4. Auflage, 2025)

Zuständig für die Durchführung: Verantwortliche bzw. der Betriebserlaubnisinhaber

Hinzuziehung des Datenschutzbeauftragten der Apotheke erforderlich

Option: Hinzuziehung eines involvierten Auftragsverarbeiters als Wissensträger

Option: Einholung des Standpunkts betroffener Personen, sowohl einzelner konkreter Personen als auch Interessengruppen- oder Verbandsbeteiligung denkbar

Wer begleitet und dokumentiert zur Gewährleistung von Nachweispflicht und Accountability?

Zeitpunkt: vor Beginn der Verarbeitung

Haben ähnliche Verarbeitungsvorgänge ein ähnliches Gefahrenpotenzial und können zusammen einer DSFA unterzogen werden? (Beispiel: Videoüberwachung an mehreren vergleichbaren Standorten)

Kann ggf. auf eine allgemeine DSFA eines Herstellers zurückgegriffen und darauf spezifisch aufgesetzt werden?

Phase 1. Beschreibung

Systematische Beschreibung der geplanten Verarbeitungsvorgänge

- Art, Umfang, Umstände und Zwecke der Verarbeitung
- Art der personenbezogenen Daten, Empfänger und Speicherfristen
- eingesetzte Datenträger, Wissensträger und/oder Trägermedien (Hardware, Software, Netzwerke, Personen, Papier etc.)
- Branche, Rolle des Verantwortlichen und Rolle des Betroffenen
- zusammenfassend: Alle datenschutzrelevanten Sachverhaltsmerkmale und die eingesetzte Technik müssen so konkret beschrieben werden, dass sich die Phasen der Bewertung und der Bewältigung anschließen können.
- Systematische Beschreibung der Zwecke der Verarbeitung, z. B. Abrechnung, Diebstahlsschutz, Aufklärung von Straftaten
- Systematische Beschreibung der von dem Verantwortlichen verfolgten berechtigten Interessen: rechtlicher, wirtschaftlicher, ideeller oder sonstiger Art (Überschneidungen mit der Beschreibung des Zwecks möglich).
- Identifikation der maßgeblichen Rechtsgrundlagen

Phase 2. Bewertung

Systematische Prüfung der geplanten Verarbeitungsvorgänge und Bewertung der Risiken:

- Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck
  - konkret bestimmte spezifische – und legitime – Zwecke der Verarbeitung
  - Einhaltung der Zweckbindung
  - Berücksichtigung von Betroffenenrechten (Benachrichtigung, Berichtigung etc)
  - Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen
  - Welche Schutzziele sind im Rahmen des Art. 35 DS-GVO maßgeblich?
  - Vertraulichkeit
  - Integrität
  - Verfügbarkeit
  - Transparenz
  - Intervenierbarkeit
  - Nicht-Verkettung von personenbezogenen Verfahren
  - Datensparsamkeit
- Berücksichtigung und Abwägung von Betroffenenrechten und die Risiken für die Rechte und Freiheiten der Betroffenen zum verfolgten Zweck
  - unbefugter Zugriff
  - unerwünschte Veränderung von Daten

  - Verlust von Daten
- andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile
- Welche Angreifer und Risikoquellen kommen in Betracht?
- Das Risiko bemisst sich als Produkt der Faktoren „Schwere des drohenden Schadens“ und „Eintrittswahrscheinlichkeit“. Für ein hohes Risiko iSd Art. 35 Abs. 1 DS-GVO müssen in der Regel mindestens „wesentliche“ in Kombination mit „maximalen“ Faktoren aufeinandertreffen:
- Zur Bewertung der einzelnen Faktoren (nach ISO 29134, Annex A):

Bemessung der Schwere

maximal	möglicher Eintritt signifikanter, sogar irreversibler Konsequenzen, die nicht überwunden werden können (Vernichtung der wirtschaftlichen Existenz, Arbeitsunfähigkeit, dauerhafte physische oder psychische Konsequenzen, Tod)
wesentlich	möglicher Eintritt signifikanter Konsequenzen, die sich – wenn auch ggf. mit großen Anstrengungen – wieder überwinden lassen (Verlust der Kreditwürdigkeit, Verlust von Eigentum, gesundheitliche Verschlechterung)
begrenzt	möglicher Eintritt signifikanter Konsequenzen, die sich mit nur geringen Anstrengungen wieder überwinden lassen (Zusatzkosten, Stress, geringe physische Belastungen)
vernachlässigbar	Eintritt allenfalls bloßer Belästigungen, die sich ohne Probleme ertragen lassen (Ärgernisse, kurzer Zeitverlust etc.)

Bemessung der Eintrittswahrscheinlichkeit

maximal	Realisierung der Bedrohung erscheint aufgrund der gewählten Ressourcen sehr leicht möglich (z. B. Aufbewahrung im öffentlich zugänglichen Bereich)
wesentlich	Realisierung der Bedrohung erscheint aufgrund der gewählten Ressourcen möglich (z. B. Aufbewahrung im öffentlich zugänglichen Bereich mit leicht umgehbarer Zutrittskontrolle/-beschränkung)
begrenzt	Realisierung der Bedrohung erscheint aufgrund der gewählten Ressourcen schwer möglich (z. B. einfache Zugangssicherung)
vernachlässigbar	Realisierung der Bedrohung erscheint aufgrund der gewählten Ressourcen nicht möglich (z. B. doppelte Zugangssicherung)

Phase 3. Bewältigung der identifizierten Risiken

- Beschreibung der zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt wird:
- Welche Maßnahmen können getroffen werden, um den Schutz personenbezogener Daten sicherzustellen, Garantien, Sicherheitsvorkehrungen etc.?
- Wer ist wann für die Maßnahmen zuständig?
- Woran wird der Erfolg/die Effektivität der Maßnahmen gemessen

- Berücksichtigung der bereits gem. Art. 32 DS-GVO für die Sicherheit der Verarbeitung zu beachtenden technischen und organisatorischen Maßnahmen für ein dem Risiko angemessenes Schutzniveau:
  – Pseudonymisierung und Verschlüsselung
  – Sicherstellung von Vertraulichkeit
  – Verfügbarkeit und Belastbarkeit der Systeme
  – rasche Wiederherstellungsmöglichkeit von Verfügbarkeit und Zugang nach einem Zwischenfall
  – regelmäßige Überprüfung und Bewertung der Maßnahmen.
- Orientiert am jeweils verfolgten Schutzziel und erwarteten Bedrohungsszenario sind ferner Maßnahmen der Risikobewältigung für die Schutzziele gemäß Standarddatenschutzmodell bzw. Art. 5 DS-GVO zu entwickeln, z. B.:

Schutzziel	**denkbare Schutzmaßnahme gegen Bedrohung**
Vertraulichkeit	• Rollen- und Rechtekonzept mit regelmäßiger Prüfung und beschränkten Admin-Rechten • Beschränkung des User-eigenen Hardware- und Software-Einsatzes • Mandantentrennung, Partitionierung • Verschlüsselung • Protokollierung, Log-Dateien aller Anfragen und Server-Aktivitäten • IT und Privacy-Compliance-Richtlinie/Einbeziehung in Code of Conduct: z.B. Sperrbildschirm bei Verlassen des Arbeitsplatzes aktivieren • Schulungen • Verpflichtungs- und Vertraulichkeitserklärungen, NDAs der involvierten Personen • Risikohinweise, z.B. auf Social Engineering, neue Angriffsformen • gut sichtbare Warnhinweise auf in Dokumenten oder Dateien enthaltene personenbezogene Daten, ggf. sogar besonderer Kategorie gem. Art. 9 DS-GVO
Integrität	• Hash-Werte • Zugriffskontrollen • elektronische Signaturen • Schreibschutz • Lösch- und Korrekturkonzept • Auditierung • Protokollierung, Log-Dateien aller Anfragen und Server-Aktivitäten
Verfügbarkeit	• Zugriffskontrollen • Redundanz • Virenscanner-Einsatz • Firewalls • Partitionierung • angemessene Speichermedien und -Umstände (Schutz gegen Feuer, Korrosion etc.) • Vermeidung von Speicher-/Server-Standort mit geographischen, tektonischen, aber auch rechtlichen Herausforderungen (letzteres z. B. bei plötzlichem Wegfall des angemessenen Schutzniveaus)

Schutzziel	**denkbare Schutzmaßnahme gegen Bedrohung**
Nichtverkettbarkeit und Zweckbindung	• Schulungen • Rollen- und Rechtekonzepte, u. a. Grenzen von Admin-Rechten • Anonymisierung • Pseudonymisierung
Transparenz	• Dokumentation • Protokollierung, auch von Änderungen, z. B. der Konfiguration
Intervenierbarkeit	• Zugriff zur Ausübung von Betroffenenrechten, unmittelbar oder über geeignete Kontaktperson/Hotline/Helpdesk

Muster einer Folgenabschätzung

für

Videoüberwachung im öffentlichen Bereich der Apotheke (Verkaufsraum)

Zuständig für die Durchführung: Verantwortlicher bzw. der Betriebserlaubnisinhaber

Hinzuziehung des Datenschutzbeauftragten der Apotheke erforderlich

Ggf. Hinzuziehung des Dienstleisters (Auftragnehmers) für die Software der Videoüberwachung

Standorte der Videoüberwachung: Verkaufsraum der Apotheke

Zeitpunkt: vor Beginn der Verarbeitung

Phase 1. Beschreibung

Im öffentlichen Raum bzw. Verkaufsraum unserer Apotheke führen wir eine Videoüberwachung durch. Dazu sollen 3 Videokameras im Verkaufsraum positioniert werden, die den Eingangsbereich, den Regalbereich und die Umgebung des HV-Tisches, jedoch nicht den HV-Tisch selbst aufnehmen. Es werden durch die drei Videokameras Bildaufzeichnungen von Mitarbeitern, Lieferanten, Vertretern und Patienten/Kunden der Apotheke oder anderen Besuchern der Apotheke gemacht. Auf den Aufnahmen werden auch Kunden bei Auswahl von Artikeln im Verkaufsraum und beim Warten in der Nähe der HV-Tische zusehen sein. Ebenso wird die Arbeitsweise der Beschäftigten zum Teil dokumentiert, soweit sie Regale einräumen, putzen, Kunden im Verkaufsraum beraten und ähnliche typische Situationen in der Apotheke.

Die Videoaufnahmen werden gespeichert und durch den Verantwortlichen oder einen seiner Filialleiter gesichtet und ausgewertet. Es findet keine Weiterleitung oder ein Zugriff Dritter statt. Der Zugang zu den Videos selbst innerhalb des Netzwerks der Apotheke ist Passwort geschützt. Die Software zum Schutz vor unberechtigtem Zugriff wird auf dem neusten Stand gehalten. Die wiederum Passwort gesicherten Computer, über die ein Zugriff auf das Netzwerk und die Videoaufnahmen möglich ist, befinden sich im nichtöffentlichen, internen Bereich der Apotheke, zu dem der Zutritt ausschließlich den Mitarbeitern der Apotheke sowie – nach Absprache mit dem Verantwortlichen oder einem Mitarbeiter der Apotheke - bestimmten Dritten, wie Zulieferern, Vertretern und Putzkräften, vorbehalten ist.

Die Videoüberwachung erfolgt auf Grundlage unseres Hausrechtes und § 4 BDSG, um uns gegen bereits wiederholt aufgetretene Diebstähle und andere Straftaten zu schützen sowie diese aufzuklären und straf- und zivilrechtlich zu verfolgen. Die Videoaufzeichnungen werden unmittelbar nach Sichtung der Aufzeichnung, eine Sichtung erfolgt durch den Verantwortlichen oder durch einen berechtigen Mitarbeiter in der Regel einmal pro Woche, gelöscht. Sofern die Begehung eines Diebstahls oder einer anderen Straftat aufgezeichnet wird, wird diese Sequenz an die Strafverfolgungsbehörden übergeben und erst mit Abschluss der Verfolgung unserer Rechtsansprüche gelöscht.

Phase 2. Bewertung

Durch die Videoüberwachung werden die Patienten/Kunden, Lieferanten, Mitarbeiter und andere Besucher der Apotheke in ihrem Grundrecht auf informationelle Selbstbestimmung verletzt. Es

werden durch die Videoaufnahmen personenbezogene Daten besonderer Kategorien gemäß Artikel 9 Absatz 1 DS-GVO ohne Einwilligung der Betroffenen verarbeitet, denn es wird aufgezeichnet, welche freiverkäuflichen und apothekenüblichen Produkte wie Apothekenkosmetik, Verbandsmaterial, Nahrungsergänzungsmittel oder ähnliches der Patient/Kunde betrachtet und auswählt. Auch ist es bei hochauflösenden Aufnahmen unter Umständen möglich, zu erkennen, welche Arznei- oder Hilfsmittel auf einem Rezept verschrieben wurden, das der Patient beim Warten in der Apotheke möglicherweise in der Hand hält. Dies lässt Rückschlüsse auf den Gesundheitszustand zu, weshalb somit personenbezogene Daten besonderer Kategorien gemäß Artikel 9 Absatz 1 DS-GVO erhoben werden. Dazu wird meist allein der Umstand des Besuchs einer Apotheke schon als Datum mit Gesundheitsbezug angesehen. Ebenso wäre es möglich, Bewegungsprofile regelmäßig erscheinender Kunden zu erstellen.

Es wird die Arbeitsweise der Beschäftigten im Bereich des Verkaufsraumes dokumentiert, welches bei Fehlverhalten arbeitsrechtliche Konsequenzen haben könnte.

Ohne Zugriffskontrolle und die weiteren schon beschriebenen Sicherheitsmaßnahmen besteht ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen mit einer hohen Eintrittswahrscheinlichkeit. Besonders wenn auch der HV-Tisch gefilmt werden würde, bestünde ein besonders hohes Risiko für einen Schaden durch die Verletzung von Rechten und Freiheiten der Betroffenen, der mit wesentlicher Eintrittswahrscheinlichkeit zu wesentlichen Konsequenzen führen könnte. Wenn gefilmt wird, welche Arzneimittel oder ähnliches von Betroffenen bezogen werden, lässt dies einfach Rückschlüsse auf ihren Gesundheitszustand und somit auf ihre Arbeitsfähigkeit, Erwerbsfähigkeit, Familienplanung, Lebenserwartung und Kreditwürdigkeit zu. Daher muss von einem direkten Filmen des HV-Tisches Abstand genommen werden

Dem gegenüber steht der legitime Zweck, sich vor Diebstählen zu schützen und diese und andere Straftaten verfolgen zu können. Der Verantwortliche hat zum einen das Hausrecht und möchte sein Eigentum schützen. Mithin handelt es sich bei Verkaufsräumen mit Ausnahme des HV-Tisches nicht um Räumlichkeiten, in denen Betroffene in ihrer Intimsphäre betroffen sind. Vielmehr handelt es sich bei Verkaufsräumen um öffentlich-zugängliche Räume, in denen unterschiedlichste Menschen aufeinandertreffen und eine Überwachung seit vielen Jahren immer üblicher wird.

Phase 3. Bewältigung der identifizierten Risiken

Maßnahmen:

- Information der Kunden durch gut sichtbares Hinweisschild am Eingang der Apotheke
- Unterrichtung der Mitarbeiter darüber, in welchen Bereichen der Apotheke eine Videoüberwachung erfolgt,
- Datenschutzhinweise für alle betroffenen Personen durch Aushang in der Apotheke
- Löschung (nach Löschkonzept, sofern eins vorhanden ist; Hinweis der Datenschutzkonferenz (DSK) max. 48 h) der Aufzeichnungen unmittelbar nach Sichtung der Aufzeichnung, eine Sichtung erfolgt durch den Verantwortlichen oder durch einen berechtigen Mitarbeiter in der Regel einmal pro Woche,
- nur Aufnahmen in Bereichen, die von hohem Diebstahlrisiko betroffen sind,
- Zugriff und Auswertung nur durch den Verantwortlichen oder einen Filialleiter,
- Zugriff auf Videoaufnahmen ist Passwort geschützt, Computer / Zugang zum Netzwerk ist Passwort geschützt, Computer stehen nur im nichtöffentlichen Bereich der Apotheke
- Keine Aufnahmen des HV-Tischs, um sicherzustellen, dass intime Gesundheitsdaten, wie von Rezepten und verkauften Arzneimitteln etc. nicht zusätzlich verarbeitet werden

- Regelmäßige Überprüfung, ob eine Videoüberwachung noch notwendig ist bzw. ihre tatsächlichen und rechtlichen Voraussetzungen gegeben sind