Anforderungen an ein Datenschutz-Cockpit

Eine Zusammenarbeit von

Berufsverband der Datenschutzbeauftragten Deutschlands e. V.

Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V.
Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“

Gesellschaft für Datenschutz und Datensicherheit e. V.
Arbeitskreis „Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen“

Autor(en)

Backer-Heuveldop, Andrea	ds² Unternehmensberatung GmbH & Co. KG
Gindera, Sarah	CURACON GmbH
Koeppe, David	Vivantes - Netzwerk für Gesundheit GmbH
Letter, Michael	5medical management GmbH
Mempel, Lukas	Sana Kliniken AG
Mönter, Johannes	CURACON GmbH
Schrenk, Nikolaus	Kliniken des Bezirks Oberbayern – Kommunalunternehmen AdöR
Schütze, Dr. Bernd	Deutsche Telekom Healthcare and Security GmbH

Version 1.0
Stand: 08.05.2020

Haftungsausschluss

Das vorliegende Werk ist nach bestem Wissen erstellt, der Inhalt wurde von den Autoren mit größter Sorgfalt zusammengestellt. Dennoch ist diese Ausarbeitung nur als Standpunkt der Autoren aufzufassen, eine Haftung für die Angaben übernehmen die Autoren nicht. Die in diesem Werk gegebenen Hinweise dürfen daher nicht direkt übernommen werden, sondern müssen vom Leser für die jeweilige Situation anhand der geltenden Vorschriften geprüft und angepasst werden.

Die Autoren sind bestrebt, in allen Publikationen die Urheberrechte der verwendeten Texte zu beachten, von ihnen selbst erstellte Texte zu nutzen oder auf lizenzfreie Texte zurückzugreifen.

Alle innerhalb dieses Dokumentes genannten und ggf. durch Dritte geschützten Marken- und Warenzeichen unterliegen uneingeschränkt den Bestimmungen des jeweils gültigen Kennzeichenrechts und den Besitzrechten der jeweiligen eingetragenen Eigentümer. Allein aufgrund der bloßen Nennung ist nicht der Schluss zu ziehen, dass Markenzeichen nicht durch Rechte Dritter geschützt sind!

Copyright

Für in diesem Dokument veröffentlichte, von den Autoren selbst erstellte Objekte gilt hinsichtlich des Copyrights die folgende Regelung:

Geschlechtergerechte Sprache

Hinweis bzgl. geschlechtsneutraler Formulierung im gesamten Text:

> Eine gleichstellungsgerechte Gesellschaft erfordert eine geschlechterneutrale Sprache. Geschlechterneutrale Sprache muss im deutschen Umfeld drei Geschlechtern gerecht werden: Divers, Frauen und Männern.
>
> Im folgenden Text wird, soweit möglich und sinnvoll, entsprechende Formulierungen genutzt (z. B. Paarformeln, Ableitungen). Personenbezeichnungen, bei denen es sich um juristische Fachbegriffe handelt, die sowohl natürliche als auch juristische Personen bezeichnen können, werden im folgenden Text nicht durch Paarformeln ersetzt. Dies gilt auch für technische Fachbegriffe, Definitionen und Zitate aus Normen (z. B. DIN EN ISO) und gesetzlichen Vorschriften. Entsprechende Begriffe sind im Sinne der Gleichbehandlung geschlechtsneutral zu interpretieren.
>
> Wo aus Gründen der leichteren Lesbarkeit bei personenbezogenen Substantiven und Pronomen nur ein Geschlecht dargestellt wurde, impliziert dies jedoch keine Benachteiligung der anderen beiden Geschlechter, sondern soll im Sinne der sprachlichen Vereinfachung als geschlechtsneutral verstanden werden.

Inhaltsverzeichnis

1 Einführung in die Thematik

1.1 „Datenschutz-Cockpit“?

Gerade bei sensiblen Gesundheitsdaten ist es unerlässlich, dass Verantwortliche und insbesondere deren Datenschutzbeauftragte einen umfassenden (oder: ganzheitlichen) Überblick über die Verarbeitung der Gesundheitsdaten behalten:

- Wie können die Rechte von betroffenen Personen gewährleistet und deren Anfragen bearbeitet werden? Z.B.
  - Wer hat wann aus welchen Gründen auf welche Daten von welchen Patienten zugegriffen?
  - Welche Daten müssen gelöscht oder gesperrt werden?
- Gibt es zu erledigende Aufgaben?
- Wie viele und welche in dem Informationssystem integrierten Verarbeitungstätigkeiten benötigen die Aufmerksamkeit des oder der Datenschutzbeauftragten?

Kurz: Analog zu einem Cockpit im Flugzeug, welches einem Piloten alle Informationen und Aufgaben übersichtlich zur Verfügung stellt, soll der Datenschutzbeauftragte in „seinem“ Cockpit eine Unterstützung bei der Bearbeitung und Erfüllung der aus dem Datenschutz resultierenden Aufgaben erhalten.

1.2 Betroffener Personenkreis

Unabhängig von Patientendaten werden bei einem Unternehmen wie einem Krankenhaus oder einer Arztpraxis weitere personenbezogene Daten verarbeitet wie beispielsweise Daten von Beschäftigten- oder Bewerberdaten bzw. auch Daten von Dritten wie z. B. Lieferanten, Angehörigen oder anderen Besuchern. Werden IT-Systeme für die Verarbeitung von deren Daten wie beispielsweise SAP Human Capital Management (HCM) bzw. SAP Human Experience Management (HXM), wie es künftig heißt, eingesetzt, so gelten dieselben Anforderungen an ein Datenschutz-Cockpit entsprechend auch für diese Systeme. D. h. wenn im Folgenden von „Patientendaten“ gesprochen wird, so dient dies nur der besseren Lesbarkeit. Die beschriebenen Anforderungen müssen natürlich auch bei Beschäftigten- sowie allen weiteren personenbezogenen Daten umsetzbar sein.

1.3 Ganzheitlicher Überblick erforderlich

Um einen Überblick hinsichtlich der Verarbeitung der personenbezogenen Daten eines Patienten zu erhalten, ist es erforderlich, dass Daten aus den verschiedenen, notwendigerweise eingesetzten Informationssystemen, wie z. B. Krankenhaus-Informations-System (KIS), Labor-Informations-System (LIS) oder eines Archivsystems wie ein Picture Archiving and Communication System (PACS), zusammen ausgewertet werden können. Insbesondere die Protokolle der einzelnen informationstechnischen Systeme sollten zentral auswertbar sein.

Es ist daher zu fordern, dass Hersteller von derartigen, in der Gesundheitsversorgung eingesetzten informationstechnischen Systemen sich auf

a) einen einheitlichen Standard hinsichtlich der Protokollierungsfunktionalität,
b) auf inhaltliche Vorgaben, die eine semantische Interoperabilität ermöglichen, sowie
c) auf einen einheitlichen Austauschmechanismus, welcher die Zusammenführung der Protokolldaten aus den verschiedenen Informationssystemen ermöglicht

einigen.

2 Bestandteile eines Datenschutz-Cockpits

Ein Datenschutz-Cockpit muss die grundsätzlichen Funktionalitäten bereitstellen, welche die Erfüllung der datenschutzrechtlichen Verpflichtungen, insbesondere hinsichtlich der Dokumentations- und Rechenschaftspflichten, ermöglichen. Dies sind insbesondere:

- Gewährleistung der Betroffenenrechte
- Auswertungsmöglichkeiten
- Reporting

2.1 Betroffenenrechte

Als „betroffene Personen“ im Sinne von Art. 4 Ziff. 1 DS-GVO sind sowohl Patienten und Beschäftigte als auch Bewerber oder Dritte anzusehen, wenn von diesen Personengruppen personenbezogene Daten verarbeitet werden. Hinsichtlich der Sensibilität und Kritikalität der Daten beinhalten Patientendaten immer personenbezogene Daten der in Art. 9 Abs. 1 DS-GVO definierten besonderen Kategorien. Beschäftigtendaten beinhalten – zumindest in den hier besprochenen Systemen – regelhaft Informationen, welche eine Zuordnung der Zugriffsrechte ermöglichen, also Daten wie

- Name,
- Organisationszugehörigkeit wie z. B. „Station 23“ oder
- im Unternehmen eingesetzte Funktion wie beispielsweise Ärztin oder Pfleger.

Sie fallen regelmäßig nicht unter die in Art. 9 Abs. 1 DS-GVO genannten besonderen Kategorien personenbezogener Daten.

Ein Datenschutz-Cockpit muss hinsichtlich der Gewährleistung der Betroffenenrechte insbesondere folgende Funktionalitäten bereitstellen:

- Erteilung einer Auskunft entsprechend Art. 15 Abs. 1 DS-GVO
    - Welche Daten sind wo über den jeweiligen Betroffenen erfasst?
    - Wer hat wann aus welchen Gründen auf welche Daten zugegriffen?
    - Wer hat was wann warum geändert? Oder eingeschränkt?
- Erteilung einer Kopie für den Betroffenen entsprechend Art. 15 Abs. 3 DS-GVO bzw. – sofern die Erstellung selbst nicht ermöglicht werden kann – die Erteilung und Zuweisung eines Auftrags zur Erstellung einer Kopie.
- Beauftragung der Überprüfung der Richtigkeit der Daten bzw. Beauftragung der Korrektur fehlerhafter Daten entsprechend Art. 16 DS-GVO
- Beauftragung der Löschung personenbezogener Daten gemäß Art. 17 DS-GVO
- Beauftragung einer Einschränkung der Verarbeitung („Sperrung“) der Daten entsprechend Art. 18 DS-GVO
- Überprüfung, ob der in Art. 19 DS-GVO verankerten Mitteilungspflicht bei Berichtigung, Verarbeitungseinschränkung oder Löschung personenbezogener Daten genügt wurde, inklusive Einsichtnahme
    - wann dies erfolgte bzw.
    - Einsichtnahme in die Begründung, warum die Mitteilung nicht erfolgte. Die Begründung muss auch die Informationen enthalten, wer die Begründung wann verfasste.
- Beauftragung einer Übertragung personenbezogener Daten an einen anderen Verantwortlichen entsprechend Art. 20 Abs. 1 DS-GVO

- Beauftragung der Bereitstellung) einer Kopie der sie betreffenden personenbezogenen Daten (zur Weiterverarbeitung) in elektronischer Form für die betroffene Person entsprechend Art. 20 Abs. 1 DS-GVO
- Dokumentation des Widerspruchs einer betroffenen Person hinsichtlich der Verarbeitung dieser Person zuordenbare Daten sowie Weiterleitung des Widerspruchs zwecks Bearbeitung an die jeweils zuständige Person bzw. Abteilung.

Zu den einzelnen Funktionen müssen Auftragslisten vorhanden sein, aus denen ersichtlich wird, wann etwas beauftragt wurde, wer für die Bearbeitung zuständig ist, bis wann die Abarbeitung des Auftrags erfolgt sein soll und wie der aktuelle Bearbeitungsstatus ist. Die Auftragslisten sollten die Möglichkeit bieten, dass man nach Betroffenengruppen (Patienten, Beschäftigte, Dritte) filtern kann.

2.2 Auswertungsmöglichkeiten

Ein Datenschutz-Cockpit muss diverse Auswertungen ermöglichen, welche eine stichprobenartige Kontrolle hinsichtlich der Rechtmäßigkeit der Verarbeitung erlaubt.

Hierzu gehören insbesondere folgende Auswertungsmöglichkeiten:

- Wer hat wann aus welchen Gründen auf welche Daten zugegriffen? Z.B.
    - zu Zwecken der Abrechnung oder der Versorgung auf Patientendaten,
    - zu Zwecken der Administration von Zugriffsrechten auf Beschäftigtendaten,
    - zu Zwecken der Datenschutzkontrolle
- Wer hat welche Rechte hinsichtlich welcher Verarbeitung von welchen personenbezogenen Daten? Dies beinhaltet eine Überprüfung bezüglich
    - Welche Rechte hat welche Person?
    - Welche Rechte hat welche Rolle?
    - Welche Rollen sind welcher Person zugeordnet?
    - Wer darf auf Daten eines bestimmten Patienten zugreifen?
- Ermöglichung der stichprobenartigen Auswertung von Protokolldateien hinsichtlich Ereignissen, welche potenziell auf Datenschutzverstöße hinweisen. Hierzu **können** insbesondere gehören:
    - Mehrfache Anmeldung des Benutzers, wobei „mehrfach“ durch den Verantwortlichen festgelegt wird
    - Änderung Systemrichtlinien
    - Anmeldung außerhalb der Dienstzeit
    - Anmeldung im Subsystem außerhalb des KIS- Kontextes, aber mit KIS-Zugangsdaten
    - Anzahl Fehlanmeldungen > 3
    - Druck > 1 Dokument ohne Begründung
    - Erweitern der Benutzerberechtigung zu administrativen Rechten
    - Export > 1 Dokument ohne Begründung
    - Löschen von Dokumenten
    - Löschen von Dokumenten ohne Begründung
    - Notfallanmeldung ohne Begründung
    - Suche über mehrere Patienten
    - Suche über mehrere Patienten über Abteilungsgrenzen hinweg
    - Veränderung am Regelwerk zur Protokollierung
    - Veränderung am Regelwerk zur Protokollierung ohne Begründung
    - Zugriff auf Auditprotokoll

    - Zugriff auf Auditprotokoll ohne Begründung
    - Zugriff auf Patientendaten außerhalb des Behandlungskontextes
    - Zugriff auf VIP-Daten (bzw. entsprechend geschützte Daten) außerhalb des Behandlungskontextes
    - Zugriff mit „Super-User“-Rechten außerhalb der Arbeit an der Systemkonfiguration
- Die Ermöglichung der Überprüfung, wer wann welche Protokolldaten aus welchem Grund ausgewertet hat.
- Eine Überprüfung der Sicherheit der Verarbeitung, beinhaltend insbesondere
    - Richtlinien hinsichtlich Vergabe von Passwörtern/Passphrasen (Stichwort „Kennwortkomplexität“)
    - Vorgaben bzgl. automatischer Abmeldung bei Inaktivität
    - Suche nach inaktiven Benutzern, wobei die Zeitdauer der Inaktivität individuell einstellbar sein muss
- Suche nach Systemanwendern, die seit x Tage kein Login hatten (z. B. wegen Ausscheiden aus dem Unternehmen)

Natürlich müssen die Aktionen hinsichtlich der datenschutzrechtlichen Auswertungen protokolliert und festgehalten werden, sodass nachvollziehbar ist, wer wann aus welchen Gründen auf diese Funktionalitäten zugegriffen hat.

Neben den medizinischen IT-Systemen werden andere Systeme eingesetzt, die maßgeblich mit zu beachten sind, weil diese für einen ordnungsgemäßen Betrieb unabdingbar sind. Hierzu gehören z. B. auch Firewall-Systeme, welche eine Fernwartung ermöglichen. Auch hierfür sind entsprechende Funktionalitäten unabdingbar. Gerade im Bereich einer Firewall muss eine Funktionalität verfügbar sein, welche einen Überblick über alle verfügbaren externen Anbindungen bietet: Welcher externe Partner darf unter welchen Umständen wie in das interne Netz gelangen um was zu leisten?

2.3 Reporting

Ein Datenschutz-Cockpit muss ein Reporting, insbesondere hinsichtlich der Ergebnisse der beschriebenen Auswertungen, ermöglichen. Dabei ist zu gewährleisten, dass das Reports sowohl ausgedruckt wie auch als pdf-Datei exportiert werden können.

Um Entwicklungen darstellen zu können, sollten auch Reports von zwei Zeitpunkten miteinander verglichen und Änderungen dargestellt werden können.

2.4 Überblick Anforderungen

Anforderungen an ein Datenschutz-Cockpit

Drei Kern-Anforderungen:

- Gewährleistung Betroffenenrechte
- Auswertung
- Reporting

Gewährleistung Betroffenenrechte

- Erteilung einer Auskunft entsprechend Art. 15 Abs. 1 DS-GVO
- Erteilung einer Kopie für den Betroffenen entsprechend Art. 15 Abs. 2 DS-GVO
- Beauftragung der Überprüfung auf Richtigkeit und ggf. Korrektur fehlerhafter Daten entsprechend Art. 16 DS-GVO
- Beauftragung der Löschung personenbezogener Daten gemäß Art. 17 DS-GVO
- Beauftragung einer Einschränkung der Verarbeitung („Sperrung") der Daten entsprechend Art.18 DS-GVO
- Überprüfung, ob der in Art. 19 DS-GVO verankerten Mitteilungspflicht bei Berichtigung, Verarbeitungseinschränkung oder Löschung personenbezogener
- Beauftragung einer Übertragung personenbezogener Daten an einen anderen Verantwortlichen entsprechend Art. 20 Abs. 1 DS-GVO
- Beauftragung der Erstellung einer Kopie der Daten zur Weiterverarbeitung in elektronischer Form für die betroffene Person entsprechend Art. 20 Abs. 1 DS-GVO
- Dokumentation des Widerspruchs einer betroffenen Person hinsichtlich der Verarbeitung dieser Person zuordenbare Daten sowie Weiterleitung des Widerspruchs zwecks Bearbeitung an die jeweils zuständige Person bzw. Abteilung

Auswertungsmöglichkeiten:

- Wer hat wann aus welchen Gründen auf welche Daten zugegriffen?
- Wer hat welche Rechte hinsichtlich welcher Verarbeitung von welchen personenbezogenen Daten?
- Ermöglichung der stichprobenartigen Auswertung von Protokolldateien hinsichtlich Ereignissen, welche potentiell auf Datenschutzverstöße hinweisen. Z. B.:
  - Mehrfache Anmeldung des Benutzers
  - Änderung Systemrichtlinien
  - Anmeldung außerhalb Dienstzeit
  - Erweitern der Benutzerberechtigung zu administrativen Rechten
  - Löschen von Dokumenten
  - Löschen von Dokumenten ohne Begründung
  - Notfallanmeldung ohne Begründung
  - Suche über mehrere Patienten
  - Zugriff auf Auditprotokoll
  - Zugriff auf VIP-Daten (bzw. entsprechend geschützte Daten) außerhalb Behandlungskontext
  - Zugriff mit „Super-User"-Rechten außerhalb der Arbeit an der Systemkonfiguration
- Prüfung, wer wann welche Protokolldaten aus welchem Grund ausgewertet hat.
- Eine Überprüfung der Sicherheit der Verarbeitung
- Suche nach Systemanwendern, die seit x Tage kein Login hatten

Reporting

Ein Datenschutz-Cockpit muss ein Reporting, insbesondere hinsichtlich der Ergebnisse der beschriebenen Auswertungen, ermöglichen. Reports müssen sowohl ausgedruckt wie auch als pdf-Datei exportiert werden können.