VA Notfallmanagement Datenschutz in Kliniken

Übersicht

Diese VA dient der internen Unterstützung der Datenschutzbeauftragten und -koordinierenden (DSB/DSK) in medizinischen Einrichtungen wie Kliniken und Krankenhäusern, speziell bei der rechtskonformen Umsetzung der Datenschutz-Rahmenbedingungen.

Ziel und Zweck

Die Verfahrensanweisung hat das Ziel, die Abläufe und allgemeinen Regelungen zum Datenschutz in strukturierten Prozessen und Verfahren transparent umzusetzen und gut verständlich darzustellen. Ziel dieser Beschreibung ist die Vereinheitlichung der Abläufe und die Sicherstellung der Vollständigkeit und Qualität.

Anwendungsbereich

Diese Anweisung gilt bei Datenschutzvorfällen (Datenpannen) im Kontext der Datenschutz-Grundverordnung (DSGVO).

Der Anwendungsbereich ist unabhängig von den Standorten der Einheiten und ist definiert für alle Bereiche, in denen personenbezogene Daten erfasst, verarbeitet, übertragen und gespeichert werden.

Verantwortung

Verantwortlich für die einzelnen Segmente des Verfahrens sind dazu beauftragte Personen, insbesondere:

- Datenschutzbeauftragte (DSB) und Datenschutzkoordinierende (DSK)
- Externe Dienstleistende, soweit rechtlich geregelt

Die individuellen Verantwortungsbereiche sind in Protokollen, falls vorgesehen, zu dokumentieren.

Prozesse

Datenschutzvorfälle werden nach ihrer Auswirkung klassifiziert:

- Datenpannen mit einer großen Menge von sensiblen Patient*innendaten (ab 1.000)
- Datenpannen mit einer geringen Menge von sensiblen Patient*innendaten (50 1.000 Datensätze)
- Datenpannen mit wenigen sensiblen Patient*innendaten (ein bis 50 Patienten)

Kommt es zu einer Datenpanne, ist zu klären, ob, wann und wie Datenpannen nach der DSGVO (Art. 33 und 34) den zuständigen Aufsichtsbehörden zu melden und die Betroffenen zu benachrichtigen sind.
Umfasst von der Meldepflicht sind unterschiedslos alle Verantwortlichen nach Art. 4 Abs. 5 DSGVO.

Datenpannen umfassen folgende Verletzungssituationen personenbezogener Daten:

- Vernichtung: alle Formen der Datenlöschung, die Daten unwiederbringlich machen, gleich ob rechtlich unzulässig oder unbeabsichtigt
- Verlust: unvorhergesehenes Verlorengehen von Daten, gleich ob temporär oder dauerhaft
- Veränderung: inhaltliches Umgestalten von Daten, Daten erhalten neuen Informationsgehalt
- unbefugte Offenlegung / Weitergabe: Dritter erhält Daten, Weitergabe nicht durch Einwilligung oder Rechtsvorschrift gedeckt
- unbefugter Zugang: Oder aber auch keine oder fehlerhafte Berechtigungskonzepte können schon dazu führen, da tatsächliche Kenntnisnahme nicht erforderlich ist

Die Verordnung (DSGVO) enthält eine abgestufte Melde- und Benachrichtigungs-pflicht:

Die Betroffenen müssen – im Gegensatz zur Aufsichtsbehörde – erst dann benachrichtigt werden, wenn durch die Schutzverletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen besteht.

Um die Meldepflicht gegenüber der Aufsichtsbehörde auszulösen, reicht ein „normales“ Risiko, das keiner besonderen Qualifizierung bedarf.

<u>Inhalt der Meldung an die Aufsichtsbehörde</u>

Hat die Risikoprognose ergeben, dass ein Risiko besteht, stellt sich die Frage nach Inhalt und Form der Meldung und Benachrichtigung. Die Meldung gegenüber der Aufsichtsbehörde muss dabei die folgenden Punkte umfassen:

- Beschreibung der Art der Verletzung (z.B. Datenverlust)
- Kategorien von Betroffenen (z.B. Mitarbeitende, Kund*innen) (ungefähre) Anzahl der Betroffenen, Kategorien von Datensätzen und ungefähre Anzahl der betroffenen Datensätze (z.B. Datensätze von 351 Kund*innen und 26 Mitarbeitenden betroffen, darunter Anzahl x besonders schützenswerte Daten)
- Name und Kontaktdaten der/des DSB oder sonstige Anlaufstelle
- Beschreibung der wahrscheinlichen Folgen der Schutzverletzung (z.B. finanzielle Nachteile durch unbefugte Offenlegung von Bank- und Kreditkartendaten)
- Beschreibung ergriffener und vorgeschlagener Maßnahmen, um die Schutzverletzung zu „beheben“ und um mögliche Folgen abzumildern
- Welche Maßnahmen wurden bereits ergriffen, zur Reduzierung welches Risikos und welcher Schutzverletzung? Beispiel: Zur Reduzierung physischer Schäden durch den nicht avisierten Datenverlust der Patientenakten wurde

ein Datenwiederherstellungsverfahren angewandt, wodurch die Daten zur Prozentzahl x wiederhergestellt werden konnten.
- Welche Maßnahmen wurden – etwa aus zeitlichen Gründen – noch nicht ergriffen, können aber das Risiko weiter reduzieren?

Form der Meldung

Eine besondere Form ist nicht vorgesehen. Gerade in dringenden Fällen bietet sich aber vorab eine telefonische Kontaktaufnahme mit der Aufsichtsbehörde an. Eine ausführliche Meldung, z.B. per Brief oder per Fax, folgt dann nach dem Gespräch.

Fristen

Die (Erst-)Meldung an die Aufsichtsbehörde muss unverzüglich, aber grundsätzlich innerhalb von 72 Stunden erfolgen. Diese Frist beginnt mit der Feststellung. Dabei ist ein etwaiges „Kennenmüssen“ zu beachten. Hier ist ein Untätigbleiben besonders risikoreich. Die zeitliche Frist gilt auch für Folgemeldungen, wenn neue Informationen bekannt geworden sind. Überschreitet eine verantwortliche Person die 72 Stunden, muss sie das begründen. Dabei helfen z.B. besondere Umstände des Einzelfalls, etwa ein professioneller Hackerangriff. Je länger die Frist überschritten ist, desto ausführlicher sollte die Begründung sein. Insofern geht Schnelligkeit vor Vollständigkeit und Richtigkeit.

Benachrichtigung von Betroffenen

Den Betroffenen ist anders als der Aufsichtsbehörde kein umfassendes Bild von der Schutzverletzung zu geben. Die Benachrichtigung muss lediglich die Art der Schutzverletzung, den Namen und die Kontaktdaten der/des Datenschutzbeauftragten oder einer anderen Anlaufstelle, eine Beschreibung der wahrscheinlichen Folgen sowie eine Beschreibung bereits ergriffener und zu empfehlender „Selbstschutzmaßnahmen“ enthalten.

Korrekte Dokumentation

Die Benachrichtigung muss in klarer und einfacher Sprache erfolgen, also nicht im rechtlichen Fachjargon. Ebenso muss sie so übersichtlich sein, dass sich der Inhalt direkt zur Kenntnis nehmen lässt. Die Benachrichtigung darf sich daher nur auf Informationen beziehen, die die Schutzverletzung betreffen, und keine Werbung oder ähnliche sachfremde Bezüge beinhalten.

Ausnahmen von der Benachrichtigungspflicht

Die Verantwortlichen müssen die Betroffenen in zwei Ausnahmefällen nicht benachrichtigen (Art. 34 Abs. 3 DSGVO):

- wenn sie schon im Vorfeld geeignete Sicherheitsvorkehrungen getroffen haben, die den unbefugten Zugang zu den Daten ausschließen. Dazu gehört z.B. Verschlüsselung.
- wenn sie im Nachgang Maßnahmen ergreifen, die nach aller Wahrscheinlichkeit sicherstellen, dass das (hohe) Risiko für die Betroffenen nicht mehr besteht. Hiermit sind Maßnahmen gemeint, die das Risiko

nachträglich minimieren, wie eine Wiederherstellung gelöschter Daten oder eine Fernlöschung von verlorenen Speichermedien.

Nach der Implementierung derartiger Maßnahmen, die die Pflicht entfallen lassen (können), ist zwingend eine Bewertung des etwaigen Restrisikos vorzunehmen. Nur wenn die Maßnahmen das Risiko so weit reduzieren, dass es unter die „Schwelle“ der Meldung und / oder Benachrichtigung fällt, können sich die Verantwortlichen auf die Ausnahme berufen.

Öffentliche Benachrichtigung

Bei einem unverhältnismäßigen Aufwand können die Verantwortlichen von einer Individualbenachrichtigung von Betroffenen als Regelfall absehen und sie durch eine öffentliche Benachrichtigung/Bekanntmachung ersetzen.
Von einem solchen unverhältnismäßigen Aufwand ist etwa auszugehen, wenn keine oder nur veraltete Kontaktdaten zur individuellen Benachrichtigung vorhanden sind und aktuelle erst ermittelt werden müssten, oder dann, wenn sich die Anzahl der Betroffenen (100 oder 10.000) nicht sicher eingrenzen lässt.
Bei einer öffentlichen Benachrichtigung ist die „gleiche Wirksamkeit“ im Vergleich zur Individualbenachrichtigung z.B. per Brief oder E-Mail wichtig. Die öffentliche Benachrichtigung kann – je nach Möglichkeit der Kenntnisnahme der Betroffenen – auch über das Internet erfolgen.

Dokumentationspflicht

Die Verordnung sieht bei Schutzverletzungen eine neue Dokumentationspflicht vor. Sie dient nicht nur der Aufsichtsbehörde zur Prüfung, sondern auch der Verantwortlichen selbst. Sie müssen alle Fakten, die im Zusammenhang mit der Schutzverletzung stehen, ihre Auswirkungen und die Abhilfemaßnahmen dokumentieren. Die Dokumentationspflicht lehnt sich an den Inhalt der Meldepflicht aus Art. 33 DSGVO an, kann jedoch auch mehr Informationen umfassen. So kann es erforderlich sein, z.B. – sofern bekannt – die Ursache der Schutzverletzung oder möglicherweise involvierte (externe) Personen zu dokumentieren.

Mitgeltende Dokumente:

- Bundesdatenschutzgesetz (BDSG) in der aktuellen Fassung (neu)
- Datenschutz-Grundverordnung (DSGVO) in der aktuellen Fassung
- DKG-Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus (B3S)
- §§ 135 ff. SGB V QM Richtlinie des GBA (GBA-RI)
- § 75c SGB V IT-Sicherheit in Krankenhäusern
- Datenschutzbestimmungen der Trägerschaften (z.B. Bestimmungen der RKD und EKD)