KANTON AARGAU

BEAUFTRAGTE FÜR ÖFFENTLICHKEIT UND DATENSCHUTZ

18.08.2020

Untersuchungsbericht

Sensibilisierungsreview bei kantonalen Listenspitälern betreffend Datenschutz

Inhaltsverzeichnis

Zusammenfassung

Im Kanton Aargau gelegene Akutspitäler mit kantonalem Leistungsauftrag im Sinn von Art. 39 Abs. 1 lit. e KVG sind kantonale öffentliche Organe und unterstehen dem Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (IDAG; § 2 Abs. 1 i.V.m. § 3 lit. c Ziff. 2 IDAG), soweit sie in Erfüllung des Leistungsauftrags tätig sind. Die Beauftragte für Öffentlichkeit und Datenschutz (OEDB) überwacht die Anwendung der Vorschriften über den Datenschutz (§ 32 Abs. 1 lit. a IDAG). Dabei sind Prüfungen (sog. Reviews oder Audits) in verschiedener Breite und Tiefe möglich; diese richten sich nach dem Ziel des jeweiligen Audits.

Am 9. Januar 2018 beschloss der Grosse Rat des Kantons Aargau Änderungen des IDAG, die am 1. August 2018 in Kraft getreten sind. Mit diesem Beschluss wurden wichtige neue Bestimmungen erlassen, wie z.B. die Einführung der Datenschutz-Folgenabschätzung, der Vorab-Konsultation sowie der Meldepflicht bei Verletzungen der Datensicherheit. Der Regierungsrat erliess zudem in der VIDAG Ausführungsbestimmungen zur Datensicherheit und zur Auftragsdatenbearbeitung. Diese Änderungen der Gesetzgebung veranlassten die Datenschutzbeauftragte, gut ein Jahr nach Inkrafttreten der neuen Bestimmungen, bei den Akutspitälern des Kantons Aargau mit einem kantonalen Leistungsauftrag gemäss Art. 39 Abs. 1 lit. e KVG ein Sensibilisierungsreview durchzuführen. Ziel dieser Sensibilisierung war es, die Spitäler auf diese Änderungen aufmerksam zu machen und gleichzeitig festzustellen, wie weit ein aktives Management der Datensicherheit betrieben wird.

Die Spitäler sind verpflichtet, die von ihnen bearbeiteten Personendaten durch angemessene organisatorische und technische Massnahmen gegen unbefugtes Bearbeiten zu schützen. Sie müssen den Nachweis erbringen, dass sie die Datenschutzbestimmungen einhalten (§ 12 IDAG). In Konkretisierung dieser Vorschrift verlangen § 4 und § 5 der Verordnung zum IDAG, dass bestimmte Massnahmen zur Einhaltung der Schutzziele – Vertraulichkeit, Integrität, Verfügbarkeit, Zurechenbarkeit und Nachvollziehbarkeit – zu treffen und zu dokumentieren sind. Diese Massnahmen müssen sich am Schutzbedarf der Daten beziehungsweise den Gefahren für die Persönlichkeit der Patientinnen und Patienten orientieren. Sie sind regelmässig durch die Spitäler selbst auf ihre Zweck- und Verhältnismässigkeit zu überprüfen und den technischen Entwicklungen anzupassen. Das Gesetz schreibt keine Einhaltung bestimmter technischer Normen vor; die Datensicherheit muss im Ergebnis genügend im Sinn der gesetzlichen Vorgaben sein. Dies lässt sich nur durch ein ganzheitliches Datensicherheitsmanagement erreichen, das sich an den Anforderungen der ISO-Normen 27001 und, 27701 oder gleichwertigen Normen orientiert. Eine Zertifizierung wird jedoch nicht verlangt.

Festgestellt wurde, dass nur bei wenigen Spitälern ein Datenschutzmanagementsystem mit einer konsequenten Strategie der Geschäftsleitung bestand, jedoch in einigen Spitälern nach Erhalt des Fragekatalogs Verbesserungsanstrengungen unternommen wurden. Die Änderungen des IDAG waren nur selten bekannt, andere Spitäler wollten noch abwarten bis die Revision des Bundesgesetzes über den Datenschutz in Kraft ist. In Bezug auf viele Aspekte besteht noch Nachholbedarf. Die konkreten Einschätzungen sowie die dazugehörenden Massnahmen werden in Kapitel 5 näher dargelegt.

Für die Akutspitäler mit Leistungsauftrag wurden einzelne Untersuchungsberichte erstellt. Sie müssen der OEDB innerhalb von drei Monaten seit Erhalt des Untersuchungsberichts mitteilen, ob die darin genannten Massnahmen umgesetzt werden. Nach einem Jahr ist der OEDB die Umsetzung der konkreten Massnahmen zu beschreiben respektive eine bereits vorhandene Konformität der einzelnen Punkte zu bestätigen.

Abkürzungen und Begriffsdefinitionen

Audit oder Review	Ein Audit oder Review untersucht, ob Prozesse, Anforderungen und Richtlinien eines geforderten Standards erfüllt sind
Abs.	Absatz
Datensicherheit	Wird in vorliegendem Bericht synonym zu "Informationssicherheit" verwendet
DSG	Bundesgesetz über den Datenschutz vom 19. Juni 1992 (SAR 235.1, DSG)
Empfehlung	Aufsichtsmassnahmen der OEDB i.S.v. § 32 Abs. 3 IDAG
IDAG	Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen vom 24. Oktober 2006 (SAR 150.700, IDAG)
i.S.v.	im Sinne von
i.V.m.	in Verbindung mit
lit.	litera (= Buchstabe)
OEDB	Beauftragte für Öffentlichkeit und Datenschutz des Kantons Aargau
Reglement	Gesamtheit von Vorschriften, Bestimmungen, die für einen bestimmten Bereich, für bestimmte Tätigkeiten, gelten
Verbesserungsmassnahmen	Beratung durch die OEDB, indem mögliche Handlungen zur Verbesserung einer festgestellten oder möglicherweise bestehenden Datensicherheitsproblematik aufgezeigt werden
VIDAG	Verordnung zum Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen vom 26. September 2007 (SAR 150.711, VIDAG)
Video	Die Videotechnik, kurz Video genannt, umfasst die elektronischen Verfahren zur Aufnahme, Übertragung, Bearbeitung und Wiedergabe von bewegten Bildern sowie ggf. des Begleittons. Dazu gehören ferner die eingesetzten Geräte wie Videokamera, Videorekorder und Bildschirm.
DIN EN ISO/IEC 27001:2017-06	ISO/IEC - Norm Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmanagementsysteme - Anforderungen (ISO/IEC 27001:2013 einschliesslich Cor 1:2014 und Cor 2:2015); Deutsche Fassung EN ISO/IEC 27001:2017
ISO/IEC 27701:2019-08	ISO/IEC-Norm Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines

1. Rechtsgrundlagen

Gesetz vom 24. Oktober 2006 über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (IDAG), SAR 150.700

Verordnung vom 26. September 2007 zum Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (VIDAG), SAR 150.711

2. Gewährleistung der Datensicherheit

Verantwortlich für die Einhaltung der datenschutzrechtlichen Vorgaben ist dasjenige öffentliche Organ, welches die erhobenen Daten verwendet oder entsprechende Aufträge vergibt (§ 18 IDAG). Im vorliegenden Fall ist das jeweilige Spital verantwortlich für die Einhaltung der datenschutzrechtlichen Vorgaben. Diesem obliegt es, durch geeignete technische und organisatorische Massnahmen sicherzustellen, dass die bearbeiteten Personendaten angemessen geschützt sind und Datenschutzverletzungen vermieden werden. Das jeweilige Spital muss auch sicherstellen, dass die entsprechenden Kontrollen der Einhaltung der datenschutzrechtlichen Vorgaben bei den beauftragten externen Dienstleistungserbringern möglich sind.

3. Empfehlungen der OEDB

Stellt die OEDB fest, dass Vorschriften über den Datenschutz verletzt werden, kann sie dem öffentlichen Organ im Sinne einer Beratung Verbesserungsmassnahmen unterbreiten. Die OEDB kann dem öffentlichen Organ auch eine förmliche Empfehlung abgeben, wobei das öffentliche Organ zu erklären hat, ob es der Empfehlung folgen wird (§ 32 Abs. 3 IDAG). Lehnt das öffentliche Organ die Befolgung der Empfehlung ab oder entspricht es dieser nicht, kann die OEDB die Empfehlung ganz oder teilweise als Verfügung erlassen (§ 32 Abs. 4 IDAG).

4. Ziel und Zweck des Reviews, Vorgehen bei der Prüfung und Inhalt des Berichts

Der Fokus des Reviews liegt beim Vorhandensein der notwendigen Strukturen und Prozesse zur Gewährleistung der sicheren Bearbeitung von personenbezogenen Daten und dem Stand der spitalinternen Umsetzung der am 1. August 2018 in Kraft getretenen Änderungen des IDAG und der VIDAG.

Der Audit basiert auf den Antworten der Spitäler auf die im Sensibilisierungsfragebogen gestellten Fragen. Diese betrafen folgende Gebiete:

- Umsetzungsstrategie
- Datenschutz- und Informationssicherheitsrichtlinie
- Interne Kontroll- und Beratungsinstanzen
- Klinikinformationssystem
- Kontrolle der Datenzugriffe
- Datenschutzverletzungen
- Auftragnehmende
- Löschung von Personendaten
- Sicherstellung des Auskunftsrechts
- Datenaustausch

Es wurden zudem stichprobenweise Dokumente eingefordert, die in den Antworten erwähnt, diesen aber nicht beigelegt wurden.

Der Untersuchungsbericht stellt keine vertiefte Kontrolle der einzelnen Massnahmen zur Gewährleistung der Datensicherheit durch die OEDB dar.

5. Auswertung

Im Rahmen dieses Berichtes wird bei der Einschätzung nicht auf die Antworten der einzelnen Spitäler eingegangen, sondern eine Gesamteinschätzung aufgeführt. Dabei stehen Aspekte, die aus Sicht des Datenschutzes wesentlich und/oder aus Risikoüberlegungen in Bezug auf die befragten Spitäler wichtig sind, im Fokus. Die empfohlenen Massnahmen sind generell gehalten und betreffen den Aufbau eines Datenschutz-Managementsystems sowie einzelne zentrale Massnahmen der Datensicherheit, die von allen untersuchten Spitälern erreicht werden sollten. Es ist Aufgabe des jeweiligen einzelnen Spitals, selbständig und eigenverantwortlich zu prüfen, inwiefern die empfohlenen Massnahmen intern bereits wirksam umgesetzt sind sowie allfällige Handlungspflichten zu erkennen. Die Spitäler haben innert einem Jahr seit Erstattung des definitiven Untersuchungsberichts der OEDB einen entsprechenden Umsetzungsbericht respektive eine entsprechende Erklärung der datenschutzkonformen Umsetzung zukommen lassen.

Umsetzungsstrategie	
Einschätzung: Die meisten Spitäler haben angegeben, eine Strategie zu besitzen. Diese bezog sich aber generell auf den Datenschutz und nicht auf die neuen Bestimmungen des IDAG und VIDAG. Nur ein Spital hat diese respektive die EU-DSGVO Anpassungen gemacht. Einige Spitäler haben im Verlauf des Reviews begonnen, ihre Strategie zu verbessern oder besser zu dokumentieren. Ein konkretes Managementsystem fehlt aber in den meisten Fällen. Das unternehmerische Risiko wird bei allen erfasst, nicht hingegen die Gefahr für die Persönlichkeit und die Grundrechte der von einer Datenbearbeitung Betroffenen.	**Empfohlene Massnahme:** Es wird empfohlen, ein Datenschutzmanagementsystem (DSMS) aufzubauen (z.B. ISO/IEC 27001 und 27701). Ein DSMS legt fest, mit welchen Instrumenten und Methoden das Management die auf Informationssicherheit ausgerichteten Aufgaben und Aktivitäten nachvollziehbar lenkt (plant, einsetzt, durchführt, überwacht und verbessert). Zu einem Managementsystem gehören folgende grundlegende Komponenten: • Management-Prinzipien • Ressourcen • Mitarbeiter • Sicherheitsprozess • Leitlinie zur Informationssicherheit, in der die Sicherheitsziele und die Strategie zu ihrer Umsetzung dokumentiert sind • Sicherheitskonzept • Informationssicherheitsorganisation Hilfsmittel bei der Umsetzung der Datenschutzstrategie sind die Datenschutzorganisation (Regeln, Anweisungen; Prozesse, Abläufe; Strukturen) sowie ein Datenschutzkonzept (Beschreibung des Informationsverbundes, Risikobewertung mit Identifikation der zu schützenden Informationen [mit Hilfe eines Verzeichnisses der Datenbearbeitungen], Massnahmen).
Datenschutz- und Informationssicherheitsrichtlinie	
Einschätzung: Nach Ankündigung der Sensibilisierungskontrolle gingen vermehrt Beratungsanfragen bei der OEDB ein. Viele der Spitäler haben Datenschutzleitlinien im Dezember 2019 oder Januar 2020 in Kraft gesetzt. Die restlichen gaben an, über eine solche Richtlinie zu verfügen und diese im Jahre 2020	**Empfohlene Massnahme:** Erstellung einer Informationssicherheitsrichtlinie respektive Überprüfung einer bestehenden Informationssicherheitsrichtlinie, ob die Prozesse zur Information der betroffenen Personen, Durchführung der Datenschutz-Folgenabschätzung und Einleitung der Vorab-Konsultation, Feststellung und Meldung

entsprechend der Änderungen des IDAG aus dem Jahre 2018 anzupassen.	von Verletzungen der Datensicherheit und Löschung von Personendaten entsprechend den Änderungen des IDAG per 1. August 2018 implementiert wurden.
Interne Kontroll- und Beratungsinstanzen	
Einschätzung: Positiv festgehalten werden kann, dass die meisten Spitäler über eine/n Datenschutzbeauftragte/n verfügen. Aus den Beantwortungen ging aber hervor, dass es zumindest fraglich ist, ob genügend Ressourcen investiert werden und ob eine ausreichende Unabhängigkeit besteht, um eine wirksame interne Aufsicht zu gewährleisten.	**Empfohlene Massnahme:** Interne Kontroll- und Beratungsinstanzen (z.B. Datenschutzbeauftragte/r des Spitals) stellen sicher, dass die vorgegebenen Richtlinien eingehalten und gesetzeskonform eingesetzt werden. Sie minimieren dadurch das Risiko von Datenschutzverletzungen der Organisation. Diese Instanz muss neben den anderen von ihren auszuführenden Tätigkeiten genügend freie Kapazität haben, um Kontrollen durchzuführen. Die Ausstattung mit genügend Ressourcen ist deshalb von essentieller Bedeutung. Der oder die Datenschutzbeauftragte sollte über ausreichende berufliche Qualifikationen verfügen und über Fachwissen auf dem Gebiet des Datenschutzes, weisungsungebunden sein und in seiner Stellung keinem Interessenskonflikt unterliegen. Letzteres wird angenommen, wenn sich der oder die Datenschutzbeauftragte selbst kontrollieren müsste, z.B. bei Mitarbeitern der IT- oder Personalabteilung oder Mitgliedern der Geschäftsleitung. Funktion, Rolle und Kompetenzen sollten in einem Pflichtenheft geregelt werden. Zudem ist die erforderliche Ausbildung zur Fortbildung des Knowhows sicherzustellen.
Klinikinformationssystem (KIS)	
Einschätzung: Bis auf ein Spital verwenden alle Spitäler ein KIS. Die meisten verfügen über ein ISDS-Konzept. Nur wenige Spitäler berücksichtigen darin auch die Schnittstellen zu anderen Informationssystemen. Gemäss Beantwortung durch die Spitäler werden die Dokumente regelmässig aktualisiert.	**Empfohlene Massnahme:** Es sollte überprüft werden, ob der vorgesehene Prozess für die stete Aktualisierung des Datensicherheitskonzepts mit entsprechenden Rollen- und Zugriffsregelungen wirksam ist. Es ist ebenfalls zu prüfen, ob darin auch tatsächlich alle relevanten Ereignisse protokolliert und alle Schnittstellen zu anderen Anwendungen berücksichtigt werden. Ein besonderes Augenmerk ist auch auf die Prüfung der Notwendigkeit der Verschlüsselung der Personendaten zu legen, damit keine Offenbarung der Personendaten an unberechtigte externe oder interne Dritte erfolgt. Die Administrationsbereiche (technische Administration / Anwendungsadministration / Berechtigungsadministration) sind möglichst zu trennen und die jeweiligen Rollen unterschiedlichen Personen zuzuweisen.
Kontrolle der Datenzugriffe	
Einschätzung: Bei fast allen Spitälern bestehen Dokumente, die als Konzept einer Verwaltung der Datenzugriffe zu werten sind. Zudem bestehen verschiedene Sicherheitsmechanismen.	**Empfohlene Massnahme:** Überprüfung des Zugriffsverwaltungskonzepts auf Vollständigkeit. Sicherstellung einer periodischen Kontrolle der Zugriffe auf die Notwendigkeit des Zugriffs zur Aufgabenerfüllung. Nahegelegt wird auch eine systematische

	Überwachung der Login-Fehlversuche zur Gewährleistung der Datensicherheit.

Datenschutzverletzungen

Einschätzung: Die Spitäler melden keine oder eine geringe Anzahl Datenschutzverletzungen. Ein grosser Teil der Spitäler sieht einen Prozess zur Feststellung von Datenschutzverletzungen vor oder gibt an, zumindest über interne Meldepflichten zu verfügen.	**Empfohlene Massnahme:** Es sind technische und organisatorische Massnahmen zu implementieren, die sicherstellen, dass Verletzungen der Datensicherheit entdeckt und der internen Kontrollstelle (datenschutzverantwortliche Person) gemeldet werden. Die intern festgestellten Verletzungen der Datensicherheit sind daraufhin zu überprüfen, ob eine Meldepflicht gegenüber der OEDB und den betroffenen Personen besteht.

Auftragnehmende

Einschätzung: Die meisten Spitäler haben eine Übersicht über Vertragspartner, die in ihrem Auftrag Personendaten bearbeiten. Einige verfügen nicht über ein eigentliches Inventar dieser Vertragspartner, da deren Zahl überschaubar sei. In den Verträgen wird zumindest eine Geheimhaltungsvereinbarung unterzeichnet.	**Empfohlene Massnahme:** Für das Datenschutzmanagement bei Auftragsdatenbearbeitungen ist ein Inventar der Verträge, die eine Bearbeitung von Personendaten zum Gegenstand haben, anzulegen. Die Verträge sind auf die Übereinstimmung mit den Anforderungen von § 18 IDAG und § 12a VIDAG zu überprüfen und ein Kontrollsystem zu implementieren, welches die regelmässige Überprüfung der Verträge und deren Einhaltung durch die Vertragsnehmer gewährleistet.

Löschung von Personendaten

Einschätzung: Die Spitäler sehen keine Löschkonzepte vor. Teilweise wird eine Löschung auf Antrag der Betroffenen vorgesehen.	**Empfohlene Massnahmen:** Werden Personendaten zur Erfüllung der gesetzlichen Aufgabe sowie zu Sicherungs- und Beweiszwecken nicht mehr benötigt, sind sie gemäss § 21 IDAG von der verantwortlichen Behörde zu vernichten. Es ist ein Löschkonzept zu erstellen sowie sicherzustellen, dass unrichtige Personendaten berichtigt oder gelöscht werden können. Die zuständigen Stellen sind zu schulen.

Sicherstellung des Auskunftsrechts

Einschätzung: Die Spitäler sehen alle einen Prozess zwecks Auskunftserteilung der eigenen Personendaten vor; aufgrund der erteilten Antworten ist aber unklar, ob dieser Prozess den Anforderungen gemäss der nebenstehend empfohlenen Massnahme genügt.	**Empfohlene Massnahmen:** Es ist ein funktionierender Prozess im Sinne von § 23 IDAG aufzubauen und sicherzustellen, dass Betroffene auf Gesuch hin über die bearbeiteten Daten sowie Datenweitergaben an wen und wann sowie gestützt auf welchen Rechtsgrund innert der gesetzten Frist informiert werden können. Dabei kann die Erstellung eines Datenverarbeitungsverzeichnisses hilfreich sein, damit standardisierte Prozesse und Vorgehensweisen etabliert werden können.

	Es ist sicherzustellen, dass der allfällige Widerruf einer Einwilligung umgehend verarbeitet wird und die Information zu allen Stellen gelangt, die gestützt auf die (widerrufene) Einwilligung Patientendaten bearbeiten.
Datenaustausch	
Einschätzung: Die meisten Spitäler können ausweisen, mit wem Personendaten ausgetauscht werden. Die Betroffenen werden nach Angaben der Spitäler informiert und es wird bei fehlender gesetzlicher Grundlage für die Datenbekanntgabe eine Einwilligung der Betroffenen eingeholt. Die Prozesse dürften sich aber noch besser standardisieren lassen.	**Empfohlene Massnahme:** Der Datenaustausch mit Dritten sollte systematisch protokolliert werden, damit auch dem Auskunftsrecht der betroffenen Personen nachgekommen werden kann. Um einen effizienten Prozess zu gewährleisten, sollte in einem Verzeichnis der Datenbearbeitungen festgehalten werden, welche Datenbearbeitungen gestützt auf welche gesetzlichen Grundlagen erfolgen und wann eine Einwilligung benötigt wird. Es muss zudem sichergestellt werden, dass der Widerruf von Einwilligungen zu Datenbekanntgaben intern umgesetzt und soweit erforderlich auch Dritten mitgeteilt wird.

6. Gesamteinschätzung

Die Ergebnisse des Sensibilisierungsreviews ergeben einen deutlichen Handlungsbedarf bei einer Mehrheit der untersuchten Spitäler. Dieser wurde teilweise von den Spitälern bereits erkannt und in Auftrag gegeben. Es ist bei der jeweiligen Implementierung ein besonderes Augenmerk auf die Umsetzung der neuen Bestimmungen des IDAG und der VIDAG zu legen.

7. Weiteres Vorgehen

Die Spitäler wurden aufgefordert, innert drei Monaten seit Erhalt ihres Kontrollberichts schriftlich mitzuteilen, ob die vorgeschlagenen Verbesserungsmassnahmen umgesetzt werden können. Nach einem Jahr ist der OEDB schriftlich zu bestätigen, dass das jeweilige Spital die Bestimmungen des IDAG und der VIDAG einhält. Des Weiteren ist der OEDB mitzuteilen, welche Massnahmen wann und wie umgesetzt worden sind.

Sollte die OEDB nach der Mitteilung des öffentlichen Organs betreffend Umsetzung eine Verletzung von Datenschutzvorschriften feststellen, kann sie eine formelle Empfehlung abgeben. Das öffentliche Organ wird bei einer Empfehlung aufgefordert, innert 30 Tagen seit Erhalt der Empfehlung schriftlich mitzuteilen, ob der Empfehlung Folge geleistet wird. Wird die Befolgung der Empfehlung abgelehnt, kann die Mitteilung innert der gesetzten Frist mit einer Stellungnahme verbunden werden. Erfolgt innert Frist keine Antwort, wird die OEDB gestützt auf § 32 Abs. 4 IDAG die Empfehlung als Verfügung erlassen.

Gunhilt Kersten
Beauftragte