Greenpaper

MULTI-COMPLIANCE-MANAGEMENT IM GESUNDHEITSWESEN

DATA SYSTEMS GmbH

Consulting is our business!

Sicherheit ist Teamarbeit!

Von Tasja Jaschinski und Andreas Jochen Holtmann

März 2021

Lage und Motivation

Die derzeitige besondere Lage stellt das deutsche Gesundheitssystem vor besondere Herausforderungen. Ambulante Pflege, stationäre Aufnahme sowie die Notfallversorgung sind am Limit. Oder darüber hinaus. Eine Dimension, die während der Pandemie verstärkt betrachtet werden muss, ist die digitale Kommunikation zwischen den Beteiligten. Gesundheitsämter verlangen von infizierten Personen, täglich ihren Gesundheitsstatus digital aufzunehmen und zu übermitteln.

Ein guter Ansatz, aber viel zu spät. Die Digitalisierung hätte bereits vor Monaten beziehungsweise Jahren im Gesundheitswesen verstärkt Einzug halten müssen. An diesem Versäumnis sind nicht allein die Bundesregierung sowie die beteiligten Behörden Schuld. Vielmehr ist es ein strukturelles Problem, dass sich seit Jahren durch das Gesundheitswesen und andere Branchen zieht. Doch spätestens seit der derzeitigen pandemischen Lage wird ein Grundproblem der Gesellschaft immer deutlicher sichtbar:

Viele reden von Digitalisierung, den Vorteilen und Chancen – aber die Umsetzung in der Praxis sieht anders aus. Gut die Hälfte der Krankenhäuser sieht die Gewährleistung der IT-Sicherheit als eine Herausforderung für die fortschreitende Digitalisierung an [1, S.6]. Zu diesem Schluss kommt auch die Bundeskanzlerin.

„Digitalisierung und Informations-Sicherheit gehören zusammen“, wird Frau Dr. Merkel als Bundeskanzlerin auf der Home-Page des Bundesamts für Sicherheit in der Informationstechnik (BSI) zitiert [2]. Von Datenschutz ist hier allerdings nicht die Rede.

Die Bundesregierung versucht seit längerer Zeit, unter anderem im Gesundheitswesen, die Digitalisierung und damit die verbundene notwendige Informationssicherheit voranzutreiben. Dies ist insbesondere bei Digitalisierungsprojekten im Krankenhausumfeld von besonderer Bedeutung.

Sichtbar wird dies unter anderem durch die Verabschiedung des Gesetzes zum Schutz elektronischer Patientendaten [3] in der Telematikinfrastruktur oder durch die Bereitstellung von Fördergeldern, wie zum Beispiel im Rahmen des Krankenhauszukunftsfonds (KHZF) [4]. In den Förderungstatbeständen dieses Fonds werden Datenschutz und Informationssicherheit jedoch beide als wesentliche Aspekte aufgeführt, die bei Digitalisierungsprojekten im Krankenhaus-Umfeld berücksichtigt werden müssen.

In vielen Organisationen sind die Felder Datenschutz und Informationssicherheit noch strikt voneinander getrennt. Auch, wenn Datenschutz und Informationssicherheit sich im Fokus der Betrachtung unterscheiden, sind viele Maßnahmen zur Absicherung deckungsgleich. Dies erfordert ein Umdenken der Beteiligten auf allen Ebenen. Ein kooperativer Ansatz, bei dem gemeinsame Prozesse als Stärke und nicht die permanente Fokussierung auf Unterschiede als Errungenschaft gefeiert wird, bringt Organisationen dem Ziel eines Multi-Compliance-Managements in einem integrierten Managementsystem ein großes Stück näher.

„If you think, compliance is expensive – try non-compliance!”

Das Zitat von Paul McNulty, ehemaliger stellvertretender Generalstaatsanwalt der Vereinigten Staaten von Amerika, drückt deutlich aus, dass eine Nicht-Berücksichtigung von gesetzlichen und regulatorischen Anforderungen zu gravierenden Folgen für Organisationen führen kann.

Werden zum Beispiel die Anforderungen des Datenschutzes nicht gemäß Datenschutz-Grundverordnung (DSGVO) umgesetzt, müssen Organisationen mit, teilweise sehr hohen, Bußgeldern rechnen.

Ein Imageverlust hat im Vergleich zu Firmen in der freien Wirtschaft nicht dieselben Auswirkungen, da Menschen bei Behandlungsbedarf aufgrund von mangelnden Leistungsalternativen trotzdem in ein Krankenhaus gehen müssen. Da Datenschutzverstöße mit Bußgeldfolge jedoch mit hoher Sicherheit in der Presse diskutiert werden, könnte dies zu einer Kürzung von Förder- und Forschungsgeldern führen.

Nicht behobene Schwachstellen können in der Folge eine Gefahr für Leib und Leben darstellen. Auch wenn der Sicherheitsvorfall in der Uniklinik Düsseldorf gemäß den Ermittlungsergebnissen der Strafverfolgungsbehörden nicht ursächlich für den Tod einer Patientin war [9], ist der mögliche Zusammenhang nachhaltig in das öffentliche Bewusstsein gerückt.

Die DSGVO verändert die Risiko-Sicht bezüglich Folgeschäden dahingehend, dass sie Organisationen zwingt mögliche Schäden aus Sicht der Betroffenen zu identifizieren und zu bewerten, nicht wie „klassisch“ aus Sicht der Organisation heraus. Darauf aufbauend müssen Organisationen entsprechende Maßnahmen definieren und umsetzen, um die Eintrittswahrscheinlichkeit zu minimieren.

Aufgrund der großen Schnittmenge der Maßnahmen zum Datenschutz und zur Informationssicherheit ist es zielführend eine gemeinsame Risikobetrachtung und -bewertung durchzuführen.

Von Datenschutz und Informationssicherheit

Aber wie weit liegen die Felder *Datenschutz* und *Informationssicherheit* tatsächlich auseinander? Nachstehend wird das Vorgehen im Datenschutz und in der Informationssicherheit beschrieben. Hierzu werden die Vorgehensweisen am Beispiel des Standard-

Datenschutzmodells[1] (SDM) sowie der IT-Grundschutz-Methodik gemäß BSI-Standard 200-2 als Referenzmodelle herangezogen.

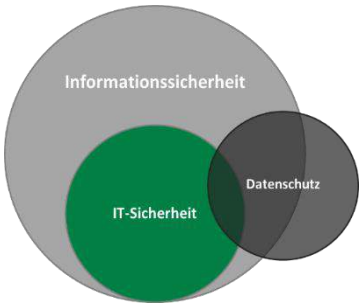
Gemäß Art. 30 DSGVO muss ein Verzeichnis über alle Verfahren geführt werden, in welchen personenbezogene Daten verarbeitet werden. Der Fokus der DSGVO liegt gemäß Art. 4 Nr.1 DSGVO auf den Daten, „die sich auf eine identifizierte oder identifizierbare natürliche Person“ (genannt „betroffene Person“) beziehen. Mithilfe von Risikostufen im Rahmen der Datenschutz-Folgenabschätzung (DSFA) kann die Kritikalität der zu verarbeitenden personenbezogenen Daten bestimmt werden. Im Rahmen der DSFA können gezielt Maßnahmen definiert werden, die das gefundene Risiko minimieren. Mithilfe des SDM und dessen Bausteine können die rechtlichen Anforderungen der DSGVO zu technischen und organisatorischen Maßnahmen (TOMs) überführt werden.

In der IT-Grundschutz-Methodik gemäß BSI-Standard 200-2 werden im Rahmen der Strukturanalyse Geschäftsprozesse und dazugehörige Informationen erfasst. Basierend auf den erfassten Informationen wird der Schutzbedarf für die Zielobjekte/Assets festgestellt. Relevante Bausteine und damit verbundene Anforderungen werden modelliert und der aktuelle Umsetzungsstand im IT-Grundschutz-Check ermittelt. Die Ermittlung und Behebung von Risiken findet in der Risikoanalyse statt. Bei der Definition und Realisierung von Maßnahmen können die Umsetzungshilfen des BSI herangezogen werden.

Generell gilt, dass der Datenschutz den Fokus auf personenbezogene Daten legt, wohingegen die Informationssicherheit aus Organisationssicht betrachtet wird.

Sicherheit ist Teamarbeit

Um Organisationen dem Ziel des Multi-Compliance-Managements näher zu bringen, gilt es nun einen kooperativen Ansatz, bei dem gemeinsame Prozesse als Stärke und nicht die permanente Fokussierung auf Unterschiede als Errungenschaft gefeiert werden, zu wählen.



Überlappung von Informationssicherheit, Datenschutz und IT-Sicherheit

Diesem Umstand trägt auch der IT-Grundschutz des BSI mit dem seit 2017 etablierten IT-Grundschutz-Kompendium Rechnung. Im Gegensatz zu früheren Versionen des BSI IT-Grundschutz wird erstmals eine direkte Berücksichtigung einer Methode für das Erreichen einer einheitlichen Datenschutz-Beratungs- und Prüfpraxis, dem SDM, gefordert.

Grundsätzlich finden sich die nachstehenden Teilaspekte in einem Managementsystem:

- Erheben von Anforderungen
- Definition des Betrachtungsraums
- Definition von Zielen
- Definition von Messkriterien
- Erstellung eines Werteverzeichnisses
- Ermittlung der Kritikalität und des damit verbundenen Schutzbedarfs
- Definition von Maßnahmen zur Absicherung im Normalbetrieb
- Vorbereitung auf besondere Situationen
- Definition von Vorgehensweisen außerhalb des Normalbetriebs
- Überprüfung der Wirksamkeit von Maßnahmen
- Identifikation von Korrektur- und Vorsorge-Maßnahmen
- Überprüfung der Wirksamkeit des Managementsystems anhand des Grads der Zielerreichung

Beispiele aus der Praxis

Grundlage der Absicherung von Organisationen ist die vollständige und korrekte Führung eines *Werteverzeichnisses.* Hierin müssen Organisationen neben materiellen Werten auch immaterielle Werte, wie zum Beispiel Prozesse und geistiges Eigentum, erfasst werden.

Der Datenschutz verlangt, Verfahren, in denen personenbezogene Daten verarbeitet werden, in einem „Verzeichnis von Verarbeitungstätigkeiten“ zu dokumentieren. In der Informationssicherheit werden Geschäftsprozesse sowie die dabei genutzten Informationen zusammengetragen. Das Verfahrensverzeichnis kann auch als Startpunkt für die Erfassung der Geschäftsprozesse gemäß BSI IT-Grundschutz dienen [5, S.80f.] Bei kritischen Infrastrukturen steht die „kritische Dienstleistung“ (kDL) im Vordergrund. Dies kann, wie in den nachfolgenden Tabellen im Rahmen der Strukturanalyse direkt mit aufgenommen werden.

Die zu erhebenden Informationen weisen daher einen hohen Grad an Überschneidung bei den verschiedenen Feldern auf. Ebenso sind im Rahmen der Erfassung der Geschäftsprozesse in der Informationssicherheit Rechtsgrundlagen eine sinnvolle Erweiterung und ein Anknüpfpunkt für beispielsweise das Datenschutzrecht. Über die Aufnahme von Verfügbarkeitszeiträumen kann der

[1] Das SDM wurde durch das Unabhängige Landeszentrum für Datenschutz (ULD) Schleswig-Holstein entwickelt.

Bezug zum Business Continuity Management (BCM) hergestellt werden.

Die nachstehenden Tabellen zeigen, wie die unterschiedlichen Themenbereiche hinsichtlich der (Geschäfts-) Prozesse und Informationen in Tabellenform zusammengefasst werden können.

ID	Bezeichnung	Zweck	Prozesstyp	kDL	Rechtliche Grundlagen der Verarbeitung	Prozess-Eigner	Prozess-kontrollierende Stelle	Verarbeitete Informationen	Verfügbarkeits-zeiträume

Tabelle 1: (Geschäfts-) Prozess-Tabelle

ID	Bezeichnung	Zweck	Personenbezogene Daten	Rechtliche Grundlagen der Verarbeitung	Informations-Eigner	Verarbeitete Informationen	Verfügbarkeits-zeiträume

Tabelle 2: Informations-Tabelle

Im nächsten Schritt muss die Bedeutung der Werte für die Organisation ermittelt werden. Hieraus leitet sich der Schutzbedarf ab. Die Einstufung des Schutzbedarfs erfolgt gemäß BSI-Standard 200-2 über sechs Schadensszenarien. Das Schadensszenario „Beeinträchtigung des informationellen Selbstbestimmungsrechts“ bezieht sich auf personenbezogene Daten. Die Kritikalität der zu verarbeitenden personenbezogenen Daten kann im Rahmen einer DSFA bestimmt werden. In den Beispieldokumenten des Bayrischen Landesbeauftragten für den Datenschutz zur DSFA werden drei Risikostufen festgelegt: geringes Risiko, Risiko und hohes Risiko [6, S.12]. Diese drei Risikostufen können im IT-Grundschutz den Schutzbedarfen normal, hoch und sehr hoch zugewiesen werden und somit die beiden Felder verknüpft werden. Sind mehr Risikostufen in der DSFA definiert, muss eine Zuordnung auf die drei Schutzbedarfe erfolgen.

Um ein angemessenes Sicherheitsniveau zu etablieren und aufrecht zu erhalten, muss eine Vielzahl von Maßnahmen umgesetzt werden. Ohne hierbei auf vorhandene, praxisbewährte „Good-Practice-Referenzen“ zurückzugreifen gestalten sich die Identifikation und Ausgestaltung von Maßnahmen sehr aufwändig. Vorgefertigte, themenorientierte Bausteine existieren sowohl im Datenschutz (im Rahmen des SDM) als auch in der Informationssicherheit (im Rahmen des IT-Grundschutzes). Auch hier ist die Menge an sich überschneidenden Themen und Anforderungen nicht zu vernachlässigen. Mithilfe eines „Mappings“ können Gemeinsamkeiten nach der Modellierung zugeordnet werden und bereits umgesetzte Anforderungen den beiden Feldern direkt zugeordnet und als erledigt betrachtet werden. Unterschiede zwischen den Datenschutz und Informationssicherheit werden hier erkennbar und können dediziert bearbeitet werden. Da in der DSFA ein risikobasierter Ansatz gewählt wird, bietet sich hier ein Zusammenschluss mit der Risikoanalyse gemäß BSI-Standard 200-3 an. Die Überführung der SDM-Bausteine in TOMs kann unter Berücksichtigung der Umsetzungshilfen des IT-Grundschutzes eine ganzheitliche Übersicht über umzusetzende Maßnahmen schaffen. Individuelle Branchen haben hierzu Anforderungen in „Branchenspezifischen Sicherheitsstandards“ (B3S) beschrieben. Speziell für Krankenhäuser existiert der B3S „Gesundheitsversorgung im Krankenhaus“.

Strukturanalyse und Schutzbedarfsfeststellung sind über den Datenschutz und die Informationssicherheit hinaus auch im Gesamtkontext des Risikomanagements von Bedeutung.

Doch nicht nur zum Aufbau von Datenschutz- und Informationssicherheitsmanagementsystemen sind die zuvor genannten Prozessschritte notwendig. So kann beispielsweise die Strukturanalyse mit der Erfassung der Geschäftsprozesse im Rahmen des BCM den Ausgangspunkt für die Business Impact Analyse (BIA) darstellen [7, S.19]. Die Risikoanalyse gemäß BSI-Standard 200-3 kann auch als Grundlage für die BCM-Risikoanalyse, die im neuen BSI-Standard 200-4[2] eingeführt wird, genutzt werden. Hierbei wird der Fokus auf die kritischen Geschäftsprozesse aus der BIA gelegt. Auch bei einer §8a BSIG-Prüfung für KRITIS-Betreiber sollte das Sicherheitskonzept, inklusive Strukturanalyse und Risikoanalyse, für die Dokumentenprüfung vorliegen [8, S.10].

Mangelnde Abdeckung dieser Felder kann zu schwerwiegenden Folgen für die Organisation führen.

Vergangenheitsbewältigung und Zukunftsgestaltung

Eines der zentralen Probleme der Digitalisierung ist der damit verbundene Aufwand, sowohl finanziell als auch organisatorisch [1, S.6]. Hieran sind Informationssicherheit und Datenschutz historisch nicht ganz unbeteiligt – bereits lange vor der Digitalisierung.

[2] Der BSI-Standard 200-4 liegt aktuell nur als Community Draft vor.

Unterstützung kann hier der KHZF leisten, der die Modernisierung von Krankenhäusern in Deutschland vorantreiben soll. Maßnahmen in diesem Kontext werden durch das Krankenhauszukunftsgesetz (KHZG) gefördert. Das Fördervolumen von bis zu 4,3 Milliarden € kann gemäß §19 KHZG unter anderem, aber nicht ausschließlich, in die Förderung der nachfolgenden Tatbestände investiert werden:

- Patientenportale
- elektronische Dokumentation von Pflege- und Behandlungsleistungen
- digitales Medikationsmanagement
- Leistungsabstimmung und Cloud-Computing Systeme
- Beschaffung, Errichtung, Erweiterung oder Entwicklung informationstechnischer, kommunikationstechnischer und robotikbasierter Anlagen, Systeme oder Verfahren und telemedizinische Netzwerke
- IT-Sicherheit sowie
- Anpassung von Patientenzimmern an die besonderen Behandlungsformen im Fall einer Epidemie

Vor allem der letzte Punkt hat während des letzten Jahres an Bedeutung gewonnen.

Die zuvor aufgezählten Themenbereiche zeigen auf, dass im Rahmen des KHZF nicht ausschließlich Wert auf das Vorantreiben der Digitalisierung gelegt wird. Er kann auch als Vehikel für Vergangenheitsbewältigung benutzt werden, was bei den förderbaren Themenbereichen dann zu besseren Digitalisierung führt. Auch die Tatsache, dass Informationssicherheit als integraler Bestandteil vorgeschrieben wird und mindestens 15% der geförderten Projektsumme darstellen muss, weist darauf hin, dass durch den KHZF auch der Grundstein der Digitalisierung verfestigt werden kann.

Über den Tellerrand hinaus

Viele Verantwortliche sind von den Dauerbrennern Datenschutz und Informationssicherheit genervt. „Lassen Sie mich doch mit diesen Themen in Ruhe!“ ist ein Satz, der immer wieder in Gesprächen mit den Leitungsebenen im Gesundheitswesen fällt. Allerdings ist das, entgegen der Erwartungen, genau das Ziel. Es soll Ruhe in den Themen herrschen. Aber bitte auch zielführend!

Nicht nur vor dem Hintergrund, dass Verstöße gegen geltende Gesetze sehr schnell teuer für die Organisation werden können, sondern auch aus strategischen Überlegungen heraus ist es notwendig, sich mit den Feldern Datenschutz und Informationssicherheit auseinanderzusetzen. Eine angemessene Abdeckung beider Felder ist zwingende Voraussetzung für eine erfolgreiche Digitalisierung. Dies zeigt erneut die Notwendigkeit eines Multi-Compliance-Ansatzes auf – ganz nach dem Ansatz: „Sicherheit ist Teamarbeit“.

Dadurch sollten Folgen von Risiken als Chance zur nachhaltigen Verbesserung verstanden werden. Mithilfe des KHZF kann sich jetzt Unterstützung gesichert werden. Bis 31. Dezember 2021 können Länder Fördermittel beim Bundesamt für Soziale Sicherung beantragen. Projekte müssen bis zum 31. Dezember 2024 abgeschlossen sein. Die beste Zeit zum Handeln ist jetzt!

Wie aktuelle Geschehnisse, wie beispielsweise der Vorfall der Uniklinik Düsseldorf, zeigen, ist es nun wichtig relevante Beteiligte an einen Tisch zu bringen. Die Motivation und Strategie hinter dem Handeln müssen transparent für die Beteiligten gemacht werden, um anschließend zu planen und umzusetzen. Denn:

„Es ist nicht genug zu Wissen –
man muss auch anwenden.

Es ist nicht genug zu Wollen –
man muss auch tun!“ [10]

Über die Autoren

Tasja Jaschinski
Tasja Jaschinski ist Senior Information Security Consultant bei der DS DATA SYSTEMS GmbH. Ihre Schwerpunkte liegen im BSI IT-Grundschutz sowie im Bereich kritischer Infrastrukturen.

Andreas Jochen Holtmann
Andreas Jochen Holtmann ist Senior Information Security Consultant bei der DS DATA SYSTEMS GmbH. Seine Schwerpunkte liegen im BSI IT-Grundschutz, ISO/IEC 27001, im Bereich kritischer Infrastrukturen sowie im Datenschutz.

Über DS DATA SYSTEMS GmbH

Die DS DATA SYSTEMS GmbH ist seit 1994 ein europaweit tätiges, unabhängiges und inhabergeführtes Beratungsunternehmen. Wir sind ein Anbieter spezialisierter Beratungs- und Prüfungsleistungen in den auf Informationssicherheit und Datenschutz fokussierten Bereichen Governance, Compliance und Security. Unsere Tätigkeiten liegen in der Schnittmenge von Wirtschaftsprüfung, Organisationsberatung und Complianceberatung. Spezialisierte Projekt- und Expertenteams unterstützen Kundinnen und Kunden aus dem Gesundheitswesen, der Industrie, Dienstleistung, Finanzdienstleistung, Handel sowie der öffentlichen Verwaltung. Die Stärke der DS DATA SYSTEMS GmbH liegt in der Kombination aus fundiertem Know-how sowie praxiserfahrenen Beratern.

info@datasystems.de https://www.datasystems.de/

Literaturverzeichnis

[1] **Deutsches Krankenhausinstitut e.V., BDO Ag Wirtschaftsprüfungsgesellschaft (2019):** Das digitale Krankenhaus, https://www.dki.de/sites/default/files/2019-11/2019-09%20Studie%20BDO%20und%20DKI_Das%20Digitale%20Krankenhaus_final.pdf, Abruf: 10.03.2021

[2] **Bundesamt für Sicherheit in der Informationstechnik (o.D.):** Homepage, https://www.bsi.bund.de/, Abruf: 10.03.2021

[3] **Bundesgesundheitsministerium (2020):** Kabinett beschließt Patientendaten-Schutz-Gesetz, https://www.bundesgesundheitsministerium.de/pdsg.html, Abruf: 10.03.2021

[4] **Bundesregierung (2020):** Investitionsprogramm für Krankenhäuser, https://www.bundesregierung.de/breg-de/aktuelles/krankenhauszukunftsgesetz-1781744, Abruf: 10.03.2021

[5] **Bundesamt für Sicherheit in der Informationstechnik (2017):** BSI-Standard 200-2, IT-Grundschutz-Methodik, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_2.pdf;jsessionid=906FCD9481E8B46DAAB8BA654CCB1DFB.internet462?__blob=publicationFile&v=2, Abruf: 10.03.2021

[6] **Der Bayrische Landesbeauftragte für den Datenschutz (2019):** Datenschutz-Folgenabschätzung, Methodik und Fallstudie, https://www.datenschutz-bayern.de/technik/orient/oh_dsfa_beispiel.pdf, Abruf: 10.03.2021

[7] **Bundesamt für Sicherheit in der Informationstechnik (2021):** BSI-Standard 200-4, Business Continuity Management, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_4_CD.pdf?__blob=publicationFile&v=3, Abruf: 10.03.2021

[8] **Bundesamt für Sicherheit in der Informationstechnik (2020):** Orientierungshilfe zu Nachweisen gemäß §8a Absatz 3 BSIG, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Kritis/Orientierungshilfe_8a_3_v11.pdf?__blob=publicationFile&v=4, Abruf: 10.03.2021

[9] **WDR (2020):** Hackerangriff auf Düsseldorfer Uniklinik: Ermittlungen wegen fahrlässiger Tötung eingestellt, https://www1.wdr.de/nachrichten/rheinland/duesseldorf-uniklinik-hackerangriff-ermittlungen-fahrlaessige-toetung-100.html, Abruf: 10.03.2021

[10] **Goethe (o.D.):** Maximen und Reflexionen. Aphorismen und Aufzeichnungen. Nach den Handschriften des Goethe- und Schiller-Archivs hg. von Max Hecker, 1907. Aus: Wilhelm Meisters Wanderjahre