



Digitale Prozesse stehen häufig im Konflikt mit IT-Sicherheit und Datenschutz. Nicht, wenn man es von Beginn an gemeinsam betrachtet.

Dr. Uwe Günther
Experte für Digitalisierung und IT-Management

COMPLIANCE MANAGEMENT BEI DER DIGITALISIERUNG VON GESCHÄFTS-PROZESSEN

Digitale Geschäftsprozesse eröffnen weitreichende Möglichkeiten, bestehende Prozesse zu beschleunigen und sicherer zu gestalten. Wir zeigen Ihnen, wie Sie Risiken in den Bereichen Informationssicherheit und Datenschutz in Ihr Compliance Management System integrieren und somit Haftungsrisiken minimieren.

In erster Linie bestehen die Ziele bei der Digitalisierung von Geschäftsprozessen darin, bisherige Abläufe zu automatisieren und damit effizienter und/oder effektiver zu gestalten. Häufig wird dabei vernachlässigt, die Maßnahmen zur Einhaltung der gesetzlichen und sonstigen regulatorischen Anforderungen (Compliance) parallel weiterzuentwickeln. Außerdem können sich durch den Einsatz neuer Technologien auch neue bzw. andere Risiken ergeben.

Was ist das Problem?

Die zunehmende Komplexität und Anzahl von Transaktionen digitaler Geschäftsprozesse machen es sowohl für Unternehmen als auch für Externe (beispielsweise Geldgeber, Versicherungen oder die Finanzverwaltung) schwierig, Abläufe nachzuvollziehen und zu verstehen. Vollständig digitalisierte Geschäftsprozesse zeichnen sich unter anderem durch einen hohen Automatisierungsgrad ohne manuelle Eingriffe aus. Dies bedeutet in der Regel auch, dass Risiken durch automatisierte (und somit ggf. schwer nachvollziehbare) Kontrollen zu behandeln sind. An dieser Stelle ist es wichtig, dass interne Kontrollsysteme als wesentlichen Bestandteil eines Compliance Management Systems entsprechend anzupassen und um neue Technologien zu erweitern. Wie neue Technologien auch das IKS eines Unternehmens beeinflussen können, haben wir in unserem vorherigen

Beitrag gezeigt.

Eine zusätzliche Komplexität ergibt sich aus der Zusammenarbeit und den gegebenenfalls entgegenstehenden Zielen der Prozessbeteiligten: Die Prozesseigner sind daran interessiert, Ziele wie beispielsweise die schnellere Bearbeitung von Bestellungen zu realisieren. Andere Beteiligte, wie beispielsweise die Beauftragten für Informationssicherheit oder Datenschutz, hingegen müssen aus Unternehmenssicht die Einhaltung der entsprechenden gesetzlichen Vorgaben gewährleisten. Die Einhaltung dieser Vorgaben geht jedoch in der Regel mit einem erhöhten Aufwand innerhalb des zu modernisierenden Prozesses einher. Die Ziele der Prozesseigner und die der Verantwortlichen für Informationssicherheit oder Datenschutz sind selten von Anfang an deckungsgleich.

Für die Verantwortlichen besteht die Herausforderung bei der Digitalisierung von Geschäftsprozessen insbesondere darin, die Nachvollziehbarkeit für alle internen und externen Adressaten zu gewährleisten. Dies bildet die Grundlage für die angemessene Berücksichtigung sämtlicher regulatorischer Anforderungen im Rahmen eines Compliance-Management-Systems.

Informationssicherheit

Informationssicherheit hat den Schutz von Informationen (unabhängig davon, ob elektronisch oder auf Papier gespeichert) zum Ziel. Das Unternehmen stellt sich dabei die Frage, wie Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationen sichergestellt werden können.

Nur wenn die Unternehmensleitung beim Thema Informationssicherheit mit gutem Beispiel vorangeht und die Mitarbeiter verinnerlicht haben, dass neben den fachlichen Anforderungen auch nichtfachliche



Themen der Informationssicherheit wichtig für den Unternehmenserfolg sind, kann ein Unternehmen seine Prozesse rechtskonform ausgestalten. Schließlich trägt jeder (Mit-)Verantwortung für die Informationssicherheit.

Bei der Digitalisierung von Geschäftsprozessen können Sie dieses Risikobewusstsein gewinnbringend nutzen: Während des gesamten Lebenszyklus ist Informationssicherheit in die Geschäftsprozesse zu integrieren. Wenn die Projektbeteiligten mit Hilfe des Informationssicherheitsbeauftragten bereits in der Planungsphase wesentliche Risiken für die Informationssicherheit erkennen und behandeln können, erspart dies ein aufwändiges Nachbessern im Produktivbetrieb.

Datenschutz

Datenschutz soll den Einzelnen davor schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

Ein Datenschutzbeauftragter hat dafür Sorge zu tragen, dass die Datenschutzbestimmungen eingehalten werden. Er ist für den Aufbau einer angemessenen Datenschutzorganisation zuständig und berät und unterstützt bei Fragen zum Thema Datenschutz innerhalb des Unternehmens. Genau wie beim Thema Informationssicherheit sind auch beim Datenschutz das Risikobewusstsein sämtlicher Beteiligten und die enge Einbindung des Datenschutzbeauftragten elementare Bausteine zur Rechtskonformität. Bei der Auswahl geeigneter technischer und organisatorischer Maßnahmen sollten die Synergien, die sich aus der großen Schnittmenge zwischen Datensicherheit im Datenschutz und Informationssicherheit ergeben, genutzt werden. Viele Maßnahmen stellen ebenfalls eine Kontrolle im IKS eines Unternehmens

dar und sollten entsprechend dokumentiert werden.

Praktische Umsetzung

Häufig zeigt sich, dass es durchaus gemeinsame Interessen von Prozesseignern und den Verantwortlichen für Informationssicherheit bzw. Datenschutz gibt: Ein Verlust von Kundendaten beispielsweise bedeutet für das Unternehmen einen Vertrauens- und Reputationsverlust, welcher sich in verringerten Umsatzerlösen für die Prozesseigner bemerkbar machen kann.

Ziel bei der Digitalisierung von Geschäftsprozessen sollte es also sein, Gemeinsamkeiten der fachlichen und nichtfachlichen Prozesse herauszuarbeiten und eine enge Kommunikation der Beteiligten über den gesamten Lebenszyklus der Prozesse sicherzustellen. Dies stellt man sicher, wenn man Datenschutz und Informationssicherheit als integralen Bestandteil eines Compliance Management Systems betrachtet und operativ lebt. Nur dann können Unternehmen es schaffen, einerseits die Digitalisierung für die Optimierung ihrer Prozesse zu nutzen und andererseits keine neuen Risiken durch Veränderungen ihrer Prozesse eingehen zu müssen.

Wenn es Ihnen gelungen ist, alle Mitarbeiter ihres Unternehmens für die Themen Informationssicherheit und Datenschutz zu sensibilisieren, haben Sie die Grundlage für eine rechtskonforme Digitalisierung gelegt. Dennoch sind formelle Anforderungen wie eine nachvollziehbare Dokumentation unter anderem aufgrund von Buchführungspflichten unverzichtbar. Von der Zusammenarbeit fachlicher und nichtfachlicher Prozessverantwortlicher können Sie aber auch in diesem Zusammenhang profitieren: Organisieren Sie Ihre Dokumentation prozessorientiert. Beschreiben Sie die Prozesse in einem zentralen Dokument (z. B. Verfahrensdokumentation, Qualitätsmanagementhandbuch, Risikomanagement). Aggregieren Sie die Ergebnisse einzelner Kontrollmaßnahmen Ihres IKS ebenfalls in einem Dokument und verknüpfen oder „verlinken“ nun die beiden Dokumente und

ergänzen Sie diese mit Ausführungen zu Informationssicherheit und Datenschutz. Damit vermeiden Sie, separate Dokumente für die einzelnen Compliance-Felder vorhalten zu müssen, die jeweils individuell zu aktualisieren sind. ●

FAZIT

Eine rechtssichere Digitalisierung von Geschäftsprozessen setzt die Zusammenarbeit aller Beteiligten voraus. Die Sensibilisierung von Mitarbeitern für die Themen Informationssicherheit und Datenschutz trägt dazu bei, das Risikobewusstsein zu stärken und Risiken frühzeitig zu erkennen. Eine prozessorientierte Dokumentation, die sämtliche Anforderungen an die Rechtskonformität der zu digitalisierenden Prozesse betrachtet, erleichtert die Nachvollziehbarkeit für interne und externe Adressaten. Gerne unterstützen wir Sie bei diesen Vorhaben.



Christoph Dessel
christoph.dessel@curacon.de



Dr. Uwe Günther
uwe.guenther@curacon.de

CORONA-BEDINGTE PRÄMIE FÜR BESCHÄFTIGTE – § 150a SGB XI

Die Corona-bedingte Sonderzahlung, welche zwischen 100 und 1.000 Euro beträgt, können Beschäftigte beanspruchen, die im Bemessungszeitraum vom 1. März bis 31. Oktober 2020 für mindestens 3 Monate in einer oder mehreren nach § 72 SGB XI zugelassenen Pflegeeinrichtungen in der Pflege tatsächlich tätig waren.

Melde- und Auszahlungsverfahren

Der GKV-Spitzenverband hat für die Meldung und die Auszahlung der Prämie Verfahrensregelungen festgelegt (Prämien-Festlegungen Teil 1 und Teil 2): Hiernach erhalten die Pflegeeinrichtungen und Arbeitgeber von den Pflegekassen Vorauszahlungen spätestens zum 15. Juli und 15. Dezember 2020 ausgezahlt, wenn die benötigten Beträge bis zum 19. Juni 2020 (Pflegeeinrichtungen)/29. Juni 2020 (Arbeitgeber) und 15. November 2020 gemeldet worden sind. Die Meldung erfolgt über ein elektronisches Verfahren. Nachgemeldete Beträge werden spätestens zum 15. März 2021 ausgezahlt. Die Pflegeeinrichtungen und Arbeitgeber müssen die Beschäftigten über deren Anspruch auf Zahlung der Prämie unverzüglich nach Inkrafttreten der Festlegungen informieren. Die Prämien müssen unverzüglich nach Erhalt der Vorauszahlung ausgezahlt werden. Spätestens muss eine Auszahlung mit der nächstmöglichen regelmäßigen Entgeltauszahlung erfolgen.

Anzeige- und Nachweisverfahren

Zum 15. Februar 2021 müssen der Pflegekasse in Textform die Höhe und der Zeitpunkt der erfolgten Auszahlung der Prämien angezeigt werden. Zur Überprüfung der Auszahlungen kann die Pflegekasse zum Nachweis der tatsächlichen Auszahlung die Vorlage pseudonymisierter Entgeltabrechnungen verlangen.

Wurde ein zu niedriger Betrag ausgezahlt, kann die Pflegeversicherung den Differenzbetrag zurückfordern. Wurde hingegen ein höherer Betrag ausgezahlt, kann mit Ausnahme einer Nachmeldung bis zum 15. November 2020 bzw. 15. Februar 2021

keine weitere Nachzahlung beansprucht werden. Erfolgt die verpflichtende Mitteilung nicht innerhalb der Frist, hat die zuständige Pflegekasse die ausgezahlten Beträge zurückzuverlangen. Die Prämie kann durch die Länder oder die zugelassenen Pflegeeinrichtungen aufgestockt werden. Die Länder regeln dazu das Verfahren selbst oder übernehmen die Regelungen des GKV-Spitzenverbands. ●

FAZIT

Um den bestehenden Anspruch der Beschäftigten gegenüber den Pflegeeinrichtungen und Arbeitgebern auf Auszahlung der Prämie erfüllen zu können, ist es wichtig, die in den Festlegungen des GKV vorgegebenen Fristen- und Verfahrensregelungen zur Meldung der Beträge dringend einzuhalten, damit die an die Beschäftigten verpflichtend auszahlenden Prämien tatsächlich ausgezahlt und nachfolgend deren Auszahlung in dem nachgeschalteten Nachweisverfahren belegt werden können.



Sibylle Scheer
sibylle.scheer@curacon-recht.de



Kai Tybussek
kai.tybussek@curacon-recht.de