avedos GRC Podcast

7. Folge | Anforderungen an eine Compliance-Management Software

mit Astrid Meyer-Krumenacker (Rechtsanwältin, Managerin, Compliance Expertin und passionierte Problemlöserin, in Folge **AMK**) und Claudia Howe (GRC Competence Lead bei avedos, in Folge **CH**)

Wien, am 26.02.2020

Disclaimer

The content of this document has been compiled with meticulous care and to the best of our knowledge. However, we cannot assume any liability for the up-to-dateness, completeness or accuracy of any of the pages.

Even where not explicitly mentioned in writing, all general references to persons refer equally to males and females.

Version 2.4, February 2018

CH: Hallo und herzlich Willkommen zum Podcast der avedos. Mein Name ist Claudia Howe und ich freue mich sehr, dass sich heute Frau Astrid Meyer-Krumenacker Zeit für mich nimmt. Vielleicht fassen Sie für unsere Zuhörer einmal kurz zusammen womit Sie sich so beschäftigen und was die Schwerpunkte Ihrer Erfahrungen sind.

AMK: Grüß Gott Frau Howe. Ich freue mich, dass wir uns heute in München treffen können. Ich bin Rechtsanwältin, Compliance-Expertin, passionierte Problemlöserin und unterstütze Unternehmen mit juristischem Risikomanagement bei der Einführung von Compliance-Management Systemen, um ihren unternehmerischen Erfolg zu sichern und im internationalen Business mitzuspielen. In der Compliance-Beratung analysiere ich Compliance- und Rechtsrisiken. Zusammen mit dem jeweiligen Unternehmen, reduziere ich diese durch geeignete präventive Compliance-Maßnahmen, wie z.B.: Schulungen, Prozessoptimierungen und maßgeschneiderte Vertragsstandards. Die juristischen Schwachstellen in Unternehmen werden so frühzeitig erkannt und behoben. Der persönliche und unternehmerische Erfolg, sowie das Geschäftswachstum werden auf diese Weise abgesichert.

CH: Das klingt ja sehr interessant. Ich kenne aus meiner Erfahrung, dass unter dem Stichwort Compliance ganz viele verschiedene Interpretationen und Auslegungen in Unternehmen herrschen. Ich möchte jetzt ganz gerne die Gelegenheit nutzen und Sie nach Ihrer Definition von Compliance fragen.

AMK: Compliance in Unternehmen besteht aus sehr vielen Bausteinen. Das sind z.B.: die einschlägig bekannten Themen wie Einladungen, Geschenke, Korruption im Allgemeinen, Geldwäsche, die Steuer-Compliance und Kartellrecht. Aber auch Themen wie Schwarzarbeit, Scheinselbstständigkeit, Datenschutz und das allgemeine Gleichbehandlungsgesetz. Das ist mit Sicherheit nicht vollständig, sondern sind nur ein paar Beispiele.

CH: Das glaub ich auch. Heute wollen wir uns ja vor allem über das Thema „Bedarf von Funktionalität einer Software" in Bezug auf Compliance-Management unterhalten. Dazu haben wir uns bereits ausgetauscht. Wir waren uns hier bei manchen grundlegenden Dingen, wie der Flexibilität der Software, Revisionssicherheit und Nachvollziehbarkeit schon sehr einig. Die erste Frage wäre jetzt: Können Sie beschreiben für welche Unternehmensprozesse man typischerweise eine Compliance-Management Software benötigt und wie diese Prozesse in Unternehmen identifiziert werden können?

AMK: Durch ein Compliance-Management System soll sichergestellt werden, dass in Unternehmen externe und interne Regeln eingehalten werden. Grundlage eines jeden effizienten Compliance-Management Systems ist eine Risikoanalyse. Hier wird festgestellt in welchen Unternehmensbereichen das Risiko besteht, dass externe Regeln (Gesetze und Verordnungen) oder interne Regeln (Verhaltenskodex) aus welchen Gründen auch immer nicht eingehalten werden, oder die Gefahr besteht, dass dem so ist. Das Ergebnis der Risikoanalyse ist dann in der Regel, dass eine solche Gefahr nicht nur in den administrativen, sondern auch in den operativen Prozessen besteht. Compliance ist kein Thema der Verwaltung allein, sondern des gesamten Unternehmens. Zusammengefasst kann man sagen, dass nach der Compliance-Risikoanalyse bekannt ist, bei welchen Prozessen Handlungsbedarf besteht. Das kann von Unternehmen zu Unternehmen sehr unterschiedlich sein und muss auch regelmäßig aktualisiert werden. Die DSGVO war beispielsweise 2017 noch kein Thema, ist aber spätestens seit Mai 2018 hochbrisant. Seitdem muss unter anderem im Customer-Relation-Management genau darauf geachtet werden, welche Kundendaten gespeichert werden. Klassische Unternehmensprozesse für eine Compliance Software sind die Finanzprozesse, Einkaufs- und Vertriebsprozesse, aber auch jene Prozesse in denen Freelancer beauftragt werden und alle anderen Prozesse, bei denen direkt oder indirekt Geld fließt. Das umfasst auch Personalprozesse.

CH: Jetzt muss ich bei Ihren Ausführungen gleich an eine Ihrer anderen Thesen denken: nämlich, dass ein Compliance-Management System auch eine präventive Funktion hat. Eine Software soll gerade diese Eigenschaft unterstützen. Können Sie hier für unsere Zuhörer noch etwas näher darauf eingehen?

AMK: Das Ziel eines Compliance-Management Systems ist die Vermeidung von Störfällen und damit die Sicherung der Reputation und des geschäftlichen Erfolges. Für Software, die zur Unterstützung eines Compliance-Management Systems eingesetzt wird, bedeutet das, dass sie in allen kritischen Prozessen eingesetzt werden können muss. Ganz wesentlich ist, dass Risiken und Abweichungen vom Prozess, die zu Störfällen führen können, eindeutig im Prozess aufgezeigt werden, es aber beispielsweise auch eine Nachricht ins Mailsystem gibt, um eine zeitnahe Reaktion zu ermöglichen. Für das Aufzeigen der Risiken und/oder Abweichung der Norm haben sich farbliche Kennzeichnungen in Verbindung mit einem Ausrufezeichen bewährt. Die Meldung des Risikos oder Störfalls muss dem Anwender umgehend ins Auge springen. Es sollte auch möglich sein, Risiken in verschiedene Stufen einzuteilen und ab einer gewissen Stufe, abhängig von der Risikobereitschaft des einzelnen Unternehmens, das Risiko gleichzeitig mit dem Aufzeigen automatisch zu eskalieren. Genauso wichtig wie das Aufzeigen, sind aber die Nachverfolgung der zu ergreifenden Aktionen, sowie deren gerichtsfeste Dokumentation. Werden im Vorfeld definierte Aktionen nicht, oder nicht im definierten Zeitrahmen ergriffen, muss auch hier wieder eine automatische Eskalation erfolgen. Soweit dazu, was eine gute Compliance Software leisten muss, wenn es mal nicht compliant verläuft. Aber auch im sogenannten Idealfall, wenn alle Aktionen in den jeweiligen Prozessen compliant ablaufen, ist die Software gefordert. Der Idealfall ist ebenfalls gerichtsfest zu dokumentieren um sich gegebenenfalls exkulpieren zu können. Es sollte außerdem möglich sein, mit der Software ein Reporting, nicht nur der Störfälle und Abweichungen, sondern auch der normalen Bestellungen und Verkäufe etc. zu erstellen. Auf diese Weise kann man feststellen, ob eventuell Verträge mit Geschäftspartnern in kritischen Ländern abgeschlossen werden, die bisher noch nicht im Fokus waren. Oder ob vielleicht neue Produkte gekauft oder verkauft werden, die vielleicht aus zollrechtlichen Gründen kritisch sind, zum Beispiel Dual-Used Produkte. Ein solches Reporting orientiert sich idealerweise an der Compliance-Risiko-Analyse und bildet die Grundlage für ein solides Monitoring. Ziel des Monitorings ist, bei Abweichungen von festgelegten Vorgaben Alarm zu schlagen und gegebenenfalls geeignete Maßnahmen, z.B. Schulungen der Mitarbeiter, oder Anpassungen des Prozesses vorzunehmen. Dafür braucht man die richtigen Informationen aus dem Reporting.

CH: Sie sprechen jetzt schon sehr praxisnah und nah an typischen Anforderungen an eine Software. Können Sie nochmal besonders hervorheben, welche Anforderungen konkret Sie aus Ihrer Arbeit sehen und welche davon Ihnen besonders am Herzen liegen?

AMK: Die Anwendung der Software muss einfach sein und idealerweise dem Anwender Arbeit und Zeit ersparen. Sie muss also den Prozess insgesamt einfacher machen. Das erhöht die Akzeptanz und reduziert Umgehungsmaßnahmen der Mitarbeiter. Das Dashboard sollte übersichtlich gestaltet sein. Hier gibt es oft sehr unterschiedliche Vorstellungen zwischen Software-Entwicklern und Anwendern mit kaufmännischem oder juristischem Hintergrund. Besonders wichtig ist, dass der Anwender beim Störfall, diesen sofort als solchen erkennt und mitgeteilt bekommt was zu tun ist. Störfälle kommen in der Regel nicht so oft vor. Wenn der Anwender in einem solchen Fall eine kleine Hilfestellung bekommt, erhöht das die Effizienz des Compliance-Management Systems. Hilfreich ist auch, wenn die verschiedenen bereits ergriffenen Aktionen im Rahmen eines Störfalles in übersichtlicher Form mit einem Mausklick abgerufen werden können. Kurz gesagt: die Software muss unterstützend, benutzerfreundlich und gleichzeitig überwachend funktionieren.

CH: Auch in meiner Berater-Vergangenheit lag der Schwerpunkt oft auf den Compliance-Risiken. Die hatten Sie ja auch zum Beginn schon erwähnt. Wenn wir uns den typischen Regelkreis näher ansehen und von den Risiken weitergehen: worauf kommt es Ihnen denn beim Monitoring an? Man identifiziert und bewertet Compliance-Risiken, und dann erfolgen Maßnahmen zum Monitoring. Was sehen Sie an Schwerpunkten oder Unterstützungsmöglichkeiten durch die Software?

AMK: Beim Monitoring wird unter anderem überprüft ob die definierten Maßnahmen zur Reduzierung der Risiken umgesetzt werden und wirksam sind. Im Idealfall erhält man hier die Bestätigung, dass die richtigen Maßnahmen umgesetzt wurden und die Risiken dadurch reduziert sind. Im anderen Fall erkennt man durch das Monitoring, dass die definierten Maßnahmen nicht greifen und den gewünschten Erfolg nicht

erzielen. Mit diesen Informationen kann man die Maßnahmen optimieren oder neue Maßnahmen definieren. Die Software muss also diese Informationen liefern und aufzeigen, wenn identifizierte Risiken nicht reduziert werden. Werden definierte Maßnahmen zur Risiko-Reduzierung umgangen oder nicht beachtet, muss dies in der Software ebenfalls aufgezeigt werden. Das Monitoring ist ein sehr wichtiger Baustein im Compliance-Management System. Mit dem Monitoring lässt sich einerseits bestätigen, dass man alles richtig gemacht hat oder dass es noch Optimierungsbedarf gibt.

CH: Der letzte Punkt ist in der Regel ja das Thema Berichterstattung. Gerade mit diesem Thema haben wir uns bei avedos auch sehr intensiv auseinandergesetzt in der letzten Zeit. Liebe Zuhörer, hier möchte ich nochmal auf die Artikel und Blogbeiträge verweisen und auch auf den Podcast, den es dazu gibt. Wenn wir jetzt nochmal das Compliance-Management System ansehen – gibt es in diesem Rahmen besondere Anforderungen? Vielleicht können Sie noch darauf eingehen, welche Möglichkeit Sie bezüglich einer einheitlichen Berichterstattung sehen (auch über verschiedene GRC Disziplinen hinweg).

AMK: Naja bei beiden geht es um die Überwachung und Reduzierung von Risiken. Beim Compliance-Management System um Risiken die aus der Nichtbeachtung von Gesetzen und Regeln entstehen. Beim „allgemeinen" Risikomanagement geht es in der Regel um finanzielle Risiken. Es liegt also in der Natur der Sache, dass es beim Reporting viele Gemeinsamkeiten gibt. Bei einem Compliance-Reporting gibt es einmal das regelmäßige Reporting, zu vorab definierten Zeitpunkten und da Ad hoc-Reporting bei einem gravierenden Störfall. Ein gut funktionierendes Reporting ist Voraussetzung dafür, dass zeitnah auf Störfälle angemessen reagiert werden kann. Hier sehe ich ebenfalls eine Gemeinsamkeit mit den anderen GRC Disziplinen. In der Praxis hat es sich bewährt, die regelmäßigen Berichte aus den verschiedenen GRC Bereichen in einen Report zusammen zu fassen. Wobei die Software so flexibel sein sollte, dass Compliance Themen angemessen und verständlich dargestellt werden können. Denn nicht jedes Compliance Thema, das ins Reporting gehört, kann ausschließlich durch Zahlen dargestellt werden. Beispielsweise drohende Gesetzesänderungen, wie im Jahr 2018 die DSGVO, demnächst die EU Whistleblowing-Richtlinie oder auch der Reputationsverlust aufgrund eines Störfalles. Letzterer kann in der Regel auch nicht genau beziffert werden. Bei gravierenden Compliance-Störfällen ist ein umgehendes Reporting notwendig, dass in der Regel andere oder zusätzliche Adressaten hat als das Regel-Reporting.

CH: Vielen Dank Frau Meyer-Krumenacker. Das waren sehr interessante Einblicke. Wir sind jetzt auch schon am Ende angekommen und ich möchte mich für Ihre Zeit bedanken. Liebe Zuhörer, auch an Sie ein herzliches Dankeschön fürs Einschalten. Ich wünsche Ihnen eine gute Zeit und bis Bald beim nächsten Podcast.

AMK: Ich bedanke mich auch für das Gespräch.

Alle Informationen zu unserem Podcast finden sie auf unserer Website unter

www.avedos.com/news/webinare-podcast/.