Nutzenpotenziale regulatorischer Anforderungen zur Geschäftsoptimierung im Rahmen der digitalen Transformation

Michael Kranawetter, National Security Officer
Microsoft Deutschland GmbH

Neufassung Juni 2017

Microsoft

ISG
imagine your future

Rechtsanwalt Prof. Dr. Josef Scherer ist seit 1996 Professor für Unternehmensrecht (*Compliance*), insbesondere Risiko- und Krisenmanagement, Sanierungs- und Insolvenzrecht an der Technischen Hochschule Deggendorf. Zuvor arbeitete er als Staatsanwalt an diversen Landgerichten und als Richter am Landgericht in einer Zivilkammer.

Neben seiner Tätigkeit als Seniorpartner der Kanzlei Prof. Dr. Scherer, Dr. Rieger & Partner erstellt er wissenschaftliche Rechtsgutachten und agiert als Richter in Schiedsgerichtsverfahren. Von 2001 bis 2015 arbeitete er auch als Insolvenzverwalter in verschiedenen Amtsgerichtsbezirken.

Prof. Dr. Scherer fungiert in diversen Unternehmen als *Compliance*-Ombudsmann sowie externer Compliance-Beauftragter und ist gesuchter Referent bei Managementschulungen in namhaften Unternehmen sowie im Weiterbildungsprogramm des Senders ARD-alpha.

In Kooperation mit dem TÜV konzipierte er als Studiengangsleiter und Referent den akkreditierten berufsbegleitenden Masterstudiengang Risikomanagement und *Compliance-management* an der Technischen Hochschule Deggendorf und ist als externer Gutachter bei der (System-)Akkreditierung von Weiterbildungsstudiengängen tätig.

Seit 2012 leitet er als Vorstand des Direktoriums das Internationale Institut für *Governance, Management, Risk-* und *Compliancemanagement* der Technischen Hochschule Deggendorf als Kompetenzzentrum.

Außerdem ist er seit 2015 Mitglied des Beirates des Frankfurter Instituts für Risikomanagement und Regulierung (FIRM, www.firm.fm) und seit 2016 Mitglied des DIN-Normenausschusses Dienstleistungen (Arbeitsausschuss Personalmanagement NA 159-01-19AA) zur Erarbeitung von ISO/DIN-Standards im Personalmanagement.

Seine Forschungs- und Tätigkeitsschwerpunkte liegen auf den Gebieten Managerhaftung, *Governance-*, Risiko- und *Compliancemanagement* (GRC) sowie Vertrags-, Produkthaftungs-, Sanierungs- und Insolvenzrecht.

Zahlreiche Publikationen auf den Gebieten Managerrisiko, *Governance-*, Risiko-, Chancen- und *Compliancemanagement*, Vertragsmanagement, Arbeitsrecht und Personalmanagement, Insolvenzrecht und Sanierung, Gläubigermanagement, Produkthaftungsrecht.

Digitalisierung, Industrie 4.0 und Prozess-/*Workflow*-Management

1. Was haben *Compliance*-Berufsbilder gemeinsam?

Meine ehemaligen Berufe als Staatsanwalt und Richter und meine jetzigen beruflichen Tätigkeiten als Rechtsanwalt in Wirtschafts-(Straf-)Sachen, *Compliance*-Ombudsmann, externer *Compliance* Officer oder Berater im Bereich *Governance, Risk* und *Compliance (GRC)* haben mehrere gemeinsame Nenner: Alle Funktionen kümmern sich prophylaktisch um pflichtgemäßes Verhalten von Unternehmen, Managern und Mitarbeitern oder reaktiv um

Compliance-Verstöße. Daraus erwächst auch das gemeinsame Bedürfnis nach Diskretion, Datenschutz, Schutz von Informationen also schlichtweg: *Compliance*. In den letzten Jahren wurde von mir aufgrund der zunehmenden Datenflut und Digitalisierung sowie moderner Kommunikationstechniken auch in diesen sehr sensiblen Themenbereichen vermehrt auf *Cloud*-Lösungen gesetzt, um sowohl die Datenmengen steuern als auch die erforderliche Vertraulichkeit gewährleisten zu können.

2. Unternehmen, Manager und Mitarbeiter stoßen auf neue Herausforderungen bei ihrer täglichen Arbeit

Häufig wird der Unternehmensalltag noch durch E-Mails, Excel-Tabellen und mit MS-Office bestritten. Die Prozesse sind oft nicht dokumentiert oder nicht aktuell beziehungsweise nicht nachverfolgbar. Bei Prozessanpassungen müssen teure IT-Spezialisten erst mal die Zeit finden, um die Unternehmen zu unterstützen. E-Mails werden nach Gießkannenprinzip an alle verteilt, sodass jeder in einer E-Mail-Flut versinkt. Sofern Prozesse existieren, sind diese nicht ausreichend mit *Governance*-, *Risk*- oder *Compliance*-Komponenten angereichert.

Ideal wäre es, wenn die Abteilungen im Unternehmen auch ohne teure IT-Spezialisten ihre Prozesse jederzeit selbst aktualisieren könnten. Die Prozesse würden nicht nur dokumentiert, sondern so ausgestaltet, dass – ähnlich wie bei einer Bestellung bei Amazon – die Mitarbeiter geführt durch einen *Human-Workflow* – das Richtige richtig machen müssten. E-Mails würden nur an die tatsächlich zuständigen Adressaten verteilt, und alle Informationen, auch *Compliance*-Regelungen in Richtlinien, würden bei den jeweiligen Prozessschritten bereitgestellt. Automatisch würde auch die Dokumentation und Auswertung der Erfüllung von *Compliance*-Anforderungen oder auch von Prozessdurchlaufzeiten erfolgen. Mit *Workflow*-Management würde der Mensch und Mitarbeiter durch den Prozess geführt und damit zur Zeit- und Systemtreue angehalten.

Mit anderen Worten: Der Mensch und Mitarbeiter, der gerade wegen menschlicher Schwächen auch fehleranfällig ist, würde bei standardisierten Abläufen Fehler nur noch machen können, wenn er bewusst die Prozessvorgaben technisch überwindet und auch Kontrollen in arglistiger Weise ausschaltet.

Die als *Workflows* abgebildeten Prozessabläufe könnten mit allen sonstigen Systemen und Programmen der bereits vorhandenen IT-Landschaft verbunden werden, wie zum Beispiel SAP, Warenwirtschaftssystemen oder Dokumentenmanagementsystemen. Jeder Prozessbeteiligte wüsste, was er wann und wie und wo zu tun hat.

Auch die sogenannten „Überwachungsfunktionen"[1] (*lines of defense*) wüssten neben den Prozessbeteiligten stets, wo der Prozess gerade läuft oder eben auch sich verzögert. So wäre eine Information in Echtzeit möglich und ersparte zahlreiche Nachforschungen, Telefonate oder Meetings. Gerade die „*Compliance*" würde durch eine stets aktuelle Einbindung von Komponenten zur Erfüllung der Anforderungen aus Gesetzen, Rechtsprechung, internen verbindlichen Regeln oder Richtlinien (wie zum Beispiel Zuwendungs- oder Datenschutzrichtlinien) sowie dem anerkannten Stand von Wissenschaft und Praxis und unter Umständen auch Industriestandards (wie ISO oder COSO – Committee of Sponsoring Organizations of the Treadway Commission etc.) sichergestellt.

Wenn die Aufgaben nicht ordnungsgemäß erfüllt werden, gäbe es keine Krisentelefonate oder Anfälle von Vorgesetzten mehr, sondern eine automatisierte, effektive und effiziente Eskalation zur Behebung der Schwachstelle.

Prozessoptimierungen und Anpassungen würden nicht mehr nach Bauchgefühl, sondern auf der Basis von echten und aktuellen Prozesskennzahlen höchst effizient und effektiv durchgeführt. Über eine der Realität entsprechende Prozesskostenrechnung könnte sowohl der Input

[1] Vgl. *Scherer*, „Die Welt(en) der Überwacher", FIRM Jahrbuch 2017, S. 79-81.

des jeweiligen Prozessschrittes als auch der Output in Zahlungsströmen dargestellt werden. Das wäre die Basis für eine Wertbeitragsberechnung nach gelebten Prozessen.[2]

Das alles ist längst Realität und „Anerkannter Stand von Wissenschaft und Praxis" bei *Good-practice*-Unternehmen!

Unternehmen bzw. ihre Organe (Aufsichtsrat, Vorstand/Geschäftsführer, Gesellschafter) sind, falls sie selbst nicht pflichtwidrig und haftungsauslösend agieren möchten (§§ 93, 107 AktG, 43 GmbHG, 347 HGB), gehalten, sich an diesen „Anerkannten Stand von Wissenschaft und Praxis" zu halten.[3]

Deshalb sollten sie ihre Prozesse dokumentieren, mit Komponenten aus *Governance*, *Risk* und *Compliance* angemessen anreichern und digitalisieren. Sodann jedoch ergeben sich neue Anforderungen: kontinuierliche Gewährleistung der erforderlichen Aktualisierung der enorm gewachsenen Datenmengen, deren Verfügbarkeit und Sicherheit (Datensicherheit, Schutz vor *Cybercrime* und vieles mehr). Da sie dies selbst in der Regel nicht mehr sicherstellen können, sind sie mittelbar gezwungen, auf entsprechend spezialisierte Leistungsanbieter zu delegieren: z. B. auf Anbieter von *Cloud*-Lösungen.

3. Wieso müssen *Cloud*-Anbieter eine besondere Affinität zu *Compliance* haben?

Aufgrund des Verwaltens sensibler Daten in vielfältiger Natur müssen *Cloud*-Anbieter selbst absolut *compliant* sein. Unter anderem auch gerade, weil sie als externe Dienstleister der strengen Kontrolle und Überwachung ihrer Auftraggeber unterliegen: Dies ist ein Ausfluss der „rechtssicheren Delegation": Der Unternehmer kann nur rechtssicher seiner Organisationsverantwortung entsprechen, wenn er bei Delegation die Externen auch unter *Compliance*-Aspekten sorgfältig auswählt, sie instruiert und kontrolliert. Im Bereich des *Supplier Screening* helfen dem Delegierenden entsprechende Zertifizierungen – auch zur 4.0-Fähigkeit – des externen (IT-)Dienstleisters als Nachweise.[4]

Ein weiterer Punkt, der die besondere Affinität von *Cloud*-Anbietern zu *Compliance* begründet, besteht darin, dass – wie oben dargestellt – die diversen unternehmerischen Aktivitäten vermehrt als *Workflows* digitalisiert und in *Clouds* vorgehalten werden. *Cloud*-Anbieter in der Rolle als Unterstützer der Unternehmen im Bereich der Prozessdigitalisierung sollten auch Hilfestellung bei der Anreicherung der Unternehmensprozesse mit Komponenten aus *Governance*, *Risk* und *Compliance* und Umwandlung in *Workflows* geben können, damit die von ihnen vorgehaltenen und verwalteten digitalisierten Prozesse auch den Anforderungen diverser Regulierungen und *„interested parties"* entsprechen. Dadurch entstünde für den *Cloud*-Anbieter ein Alleinstellungsmerkmal in der Zusammenarbeit mit den Kunden und für Kunde und Anbieter eine Win-win-Situation.

„Es gibt noch viel zu tun … fangt schon mal an!"[5]

Prof. Dr. Josef Scherer

Professor für Unternehmensrecht (*Compliance*)
an der Technischen Hochschule Deggendorf

[2] Vgl. *Ludacka*, Workflow-Management, in: *Scherer/Fruth*, Integriertes Compliance-Managementsystem mit GRC, 2. Auflage, 2017, Punkt 1.2.5.

[3] Vgl. *Scherer/Fruth*, Geschäftsführer-Compliance, 2009; *Scherer/Fruth*, Governance-Management, Band 1, 2014, und Band 2, 2015; *Scherer/Fruth*, Der Einfluss von Standards, Technikklauseln und des „Anerkannten Standes von Wissenschaft und Praxis" auf Organhaftung und Corporate Governance, Corporate Compliance Zeitschrift, 2015, S. 9-17.

[4] Vgl. *Scherer*, Business Partner Screening – Überwachungspflichten bei Delegation von Aufgaben auf Externe, in: *Scherer/Fruth*, Integriertes Personal-Managementsystem mit GRC, 2017, Anlage 3.

[5] Vgl. *Scherer/Fruth*, Integriertes „GRC-Kombi-Managementsystem on demand", 2017, und *Scherer*, Thesenpapier zu digitaler Transformation (Digitalisierung), Industrie 4.0, „digital workflow management" und integriertem Managementsystem unter dem Aspekt von Governance, Risk und Compliance (GRC), 2017.