Klotz, Michael

Working Paper

Datenschutz in KMU: Lehren für die IT-Compliance

SIMAT Arbeitspapiere, No. 01-09-001

Provided in Cooperation with:
Hochschule Stralsund, Stralsund Information Management Team (SIMAT)

Suggested Citation: Klotz, Michael (2009) : Datenschutz in KMU: Lehren für die IT-Compliance, SIMAT Arbeitspapiere, No. 01-09-001, Fachhochschule Stralsund, Stralsund Information Management Team (SIMAT), Stralsund, https://nbn-resolving.de/urn:nbn:de:0226-simat01090013

This Version is available at:
https://hdl.handle.net/10419/60090

SIMAT Arbeitspapiere
Herausgeber: Prof. Dr. Michael Klotz

SIMAT AP 01-09-001

Datenschutz in KMU – Lehren für die IT-Compliance

Prof. Dr. Michael Klotz

Fachhochschule Stralsund
SIMAT Stralsund Information Management Team

Januar 2009

ISSN 1868-064X

Klotz, Michael: Datenschutz in KMU - Lehren für die IT-Compliance. In: SIMAT Arbeitspapiere. Hrsg. von Michael Klotz. Stralsund: FH Stralsund, SIMAT Stralsund Information Management Team, 2009 (SIMAT AP, 1 (2009), 1), ISSN 1868-064X

URN der Deutschen Nationalbibliothek: urn:nbn:de:0226-simat01090013

Impressum

Fachhochschule Stralsund
SIMAT Stralsund Information Management Team
Zur Schwedenschanze 15
18435 Stralsund
www.fh-stralsund.de
www.simat.fh-stralsund.de

Herausgeber

Prof. Dr. Michael Klotz
Fachbereich Wirtschaft
Zur Schwedenschanze 15
18435 Stralsund
E-Mail: michael.klotz@fh-stralsund.de

Autor

Prof. Dr. Michael Klotz lehrt und forscht am Fachbereich Wirtschaft der FH Stralsund auf den Gebieten der Unternehmensorganisation und des Informationsmanagements. Er ist u. a. Wissenschaftlicher Leiter des SIMAT, regionaler Ansprechpartner der gfo Gesellschaft für Organisation e.V., wissenschaftlicher Beirat der ISACA und Mitherausgeber der Zeitschrift „IT-Governance“.

Datenschutz in KMU – Lehren für die IT-Compliance

Prof. Dr. Michael Klotz[1]

Zusammenfassung: IT-Compliance als Teilbereich der IT-Governance erlangt derzeit wachsende Bedeutung. Dass die Forderung nach Gesetzestreue trivial erscheint, offenbar jedoch nicht ist, belegen allein schon die in 2008 bekannt gewordenen Compliance-Verstöße. Diesbezüglich wird die Befolgung der Vorschriften des BDSG in KMU exemplarisch herangezogen. Auf dieser Basis diskutiert dieses Arbeitspapier verschiedene begriffliche und konzeptionelle Aspekte der IT-Compliance. Hierzu werden die ethischen Prinzipien der Deontologie und des Konsequentialismus genutzt. Im Ergebnis zeigen sich grundlegende theoretische Klärungen, die für den Handlungsbereich sowohl der IT-Compliance als auch des IT-Risikomanagements sowie für die Praxis des Datenschutzes nutzbar gemacht werden können.

Gliederung

Schlüsselwörter: BDSG – Corporate Governance – Datenschutz – Deontologie – KMU – Konsequentialismus – IT-Compliance – IT-Governance – Risikomanagement

JEL-Klassifikation: K39, L22, M21

[1] Prof. Dr. Michael Klotz, FH Stralsund, Fachbereich Wirtschaft, Zur Schwedenschanze 15, 18435 Stralsund, michael.klotz@fh-stralsund.de

Prolog

Pausengespräch[2] zwischen dem Autor (A) und dem Geschäftsführer (G) eines mittelständischen Unternehmens während einer regionalen Datenschutzkonferenz (im Laufe des Gesprächs hatte sich bereits herausgestellt, dass in dem Unternehmen mehr als neun Mitarbeiterinnen und Mitarbeiter mit der Verarbeitung personenbezogener Daten befasst sind).

A: Sie sind also der Datenschutzbeauftragte Ihres Unternehmens?

G: Nein, ich bin der Geschäftsführer.

A: Aber Sie haben in Ihrem Unternehmen einen Datenschutzbeauftragten?

G: Äh, nein.

A: Dann nehmen Sie als Geschäftsführer die Funktion des Datenschutzbeauftragten wahr?

G: Nein, eigentlich machen wir da kaum was.

A: Aber wir haben ja gerade gehört, dass da auch für mittelständische Unternehmen zahlreiche Verpflichtungen bestehen.

G: Ja schon, aber der Aufwand erscheint mir viel zu hoch. Dagegen scheint das Risiko ja eher gering zu sein.

A: Sie meinen die möglichen Bußgelder und Strafen?

G: Ja.

A: Dann betrachten Sie ja eigentlich den Datenschutz aus der Sicht eines Risikomanagers, der Risiken und den Aufwand für risikoreduzierende Maßnahmen gegeneinander abwägt.

G: Ja, schon.

A: Dann müssen Sie sich überlegen, was die Datenschutzmaßnahmen kosten und wie Sie damit Ihre Risiken minimieren können.

G: Ja, aber viel Zeit möchte ich dafür nicht verwenden – aber ein bisschen was müssen wir da schon noch machen.

[2] Das Gespräch wurde rekonstruiert anhand von Notizen, die unmittelbar im Anschluss an das Gespräch angefertigt wurden.

1. Einleitung

Hintergrund

Das Konzept der „IT-Governance“ hat ausgehend von den Arbeiten von WEILL in den letzten Jahren in der Fachdiskussion eine starke Verbreitung gefunden[3]. Steuerungsstrukturen für die Entwicklung, die Beschaffung und den Betrieb von Informationstechnologie (IT) sind nicht nur aus Effektivitäts- und Effizienzerwägungen, sondern auch vor dem Hintergrund einer zunehmenden, teilweise als Überregulierung empfundenen Dichte gesetzlicher Regelungen (allen voran SOX, KonTraG und demnächst BilMoG[4]) erforderlich. Neben den sich auf Entscheidungs- und Kontrollstrukturen beziehenden Governance-Vorgaben sieht sich die IT eines Unternehmens (sowohl als Technik als auch als Unternehmensfunktion) zahlreichen weiteren Anforderungen gesetzlicher und sonstiger Art gegenüber. Die Einhaltung derselben sicherzustellen ist Aufgabe der IT-Compliance.

Theoriedefizit

Wie immer bei neuen Konzepten, zumal wenn sie von der Praxis aufgegriffen und verbreitet werden (in diesem Falle vor allem von Software-, Beratungs- und Wirtschaftsprüfungsunternehmen), besteht Unsicherheit darüber, welche Bedeutung ihnen zukommt, welche neuen (oder alten) Handlungsbedarf sie adressieren und inwieweit sie insofern Aufmerksamkeit oder gar Maßnahmen erfordern. Aus wissenschaftlicher Sicht lässt sich ein Theoriedefizit ausmachen, das sich grundlegend auf die notwendige begriffliche Klärung richtet[5] – und in der Folge dann auf konzeptionelle, methodische und instrumentelle Fragen. In dieser Hinsicht soll mit diesem Arbeitspapier

---

[3] Vgl. z. B. *Weill/Woodham 2002*; *Meyer/Zarnekow/Kolbe 2003*; *Weill/Ross 2004*, *Fröschle/Strahringer 2006*; *Johannsen/Goeken 2007*.

[4] SOX = Sarbanes Oxley Act, KonTraG = Gesetz zur Kontrolle und Transparenz im Aufsichtsbereich, BilMoG = Bilanzrichtlinienmodernisierungsgesetz.

[5] Compliance wird auf sehr unterschiedliche Regelwerke bezogen. Einigkeit besteht hinsichtlich der gesetzlichen Vorgaben. Aber schon Rechtsverordnungen, Rechtsprechung und Verwaltungsvorschriften, die zu den rechtlichen Regelwerken hinzuzurechnen sind, werden häufig nicht genannt. Stattdessen wird vielfach der Begriff „Regularien“ verwendet, dessen Bedeutung und Umfang i.d.R. nicht ausgeführt wird. Dort, wo nicht nur rechtliche Vorgaben berücksichtigt werden, wird Compliance auch auf Normen und Standards bezogen (wobei mitunter nur der englische Standard-Begriff verwendet wird und hierdurch die Abgrenzung zu Normen unklar bleibt). Auch in der Einbeziehung von Verträgen gibt es unterschiedliche Begriffsfassungen, die zudem häufig nur einige wenige Beispiele für compliance-relevante Regelwerke nennen, ohne den Compliance-Begriff an sich definitorisch zu fassen versuchen.

ein Beitrag geleistet werden, der die fundamentalen, handlungsleitenden Prinzipien der „IT-Compliance“ thematisiert.

2. IT-Compliance

IT-Governance

In Anlehnung an verschiedene Definitionsangebote soll unter IT-Governance die Gesamtheit der Strukturen und Mechanismen zur Organisation und Steuerung der IT eines Unternehmens mit dem Ziel der konsequenten Ausrichtung der IT an der Unternehmensstrategie und den Geschäftserfordernissen der Fachabteilungen verstanden werden[6]. Verantwortlich für IT-Governance zeichnet die Unternehmensleitung, die nunmehr die schon seit langem geforderte Meinungsführerschaft in Bezug auf die effektive und effiziente Nutzung der IT eines Unternehmens übernehmen muss. Dieses Verständnis umfasst den Fokus der grundlegenden Definition von WEILL und WOODHAM, die die Festlegung von Entscheidungs- und Verantwortungsstrukturen hinsichtlich der Nutzung der IT in den Mittelpunkt stellen[7]. Zudem ist eine Anlehnung an den Begriff der „Corporate Governance“ gegeben, der entsprechend der Definition des DCGK (Deutscher Corporate Governance Kodex) auf das Führungssystem zur Leitung und Überwachung eines Unternehmens abstellt[8]. Insofern stellt IT-Governance einen IT-spezifischen Teilbereich der Corporate Governance eines Unternehmens dar. Hierdurch übernimmt sie auch die wesentlichen Themen der Corporate Governance, insbesondere die Einrichtung eines Risikomanagementsystems sowie den Fokus auf die Compliance, d. h. die Einhaltung der Vorgaben des rechtlichen Rahmens.

Wachsende Bedeutung der IT-Governance

In Folge der Diskussionen um die IT-Governance erlangt auch die IT-Compliance derzeit wachsende Beachtung[9]. IT-Compliance prägt sich in der Existenz spezifischer informations- und kommunikationstechnischer Einrichtungen sowie von Systemdokumentationen, Richtlinien, Kontrollergebnissen oder Notfallplänen, der konkreten Nutzung von Information und Gerätschaften u. v. a. m. aus. Diese materiellen Objekte und sichtbaren Hand-

---

[6] Vgl. z. B. *Bitkom 2006*, S. 35; *Meyer/Zarnekow/Kolbe 2003*, S. 445.

[7] Vgl. *Weill/Woodham 2002*, S. 1.

[8] Vgl. *DCGK 2007*, Präambel.

[9] Siehe beispielsweise *Hildebrand/Meinhardt 2008*, aber auch das Schwerpunktthema „IT-Compliance und -Governance“ der „Wirtschaftsinformatik“ 5/2008.

lungen machen jedoch nicht die Bedeutung des Begriffs der IT-Compliance aus, sondern dieser bezeichnet vielmehr einen immateriellen Zustand. Ob dieser Zustand in Bezug auf einen bestimmten institutionellen Geltungsbereich zu einem bestimmten Zeitpunkt vorliegt, ist eine Frage, die sich nicht hinweisend durch Bezugnahme auf die genannten Phänomene beantworten lässt. Die Antwort besteht vielmehr in einer interpretativen Bewertung als Folge einer Prüfung, ob die Ausprägung der IT des Unternehmens in ihren technischen, organisatorischen und personellen Dimensionen bestimmten, relevanten Vorgaben entspricht.[10]

Definition IT-Governance

IT-Compliance bezeichnet somit einen Zustand, in dem alle für die IT des Unternehmens relevanten bzw. als relevant akzeptierten internen und externen Regelwerke[11] nachweislich eingehalten werden. Durch die Fülle von Rechtsnormen und sonstigen Regelwerken, verbunden mit der heutigen fast durchgängigen IT-Unterstützung des gesamten Betriebsablaufes sind Compliance-Anforderungen nicht mehr "nur"“ auf steuerliche oder datenschutzrechtliche Belange begrenzt. Vielmehr geht es darum, dass die gesamte geschäftliche Tätigkeit eines Unternehmens compliant mit gesetzlichen Regelungen sein muss.

IT-Compliance-management

Um die diversen Transparenz-, Prozess-, Nachweis- und Kontrollanforderungen zu erfüllen, sind Maßnahmen zu ergreifen, die letztlich Auswirkungen bis auf jeden einzelnen Arbeitsplatz haben. Hierbei gilt es vor allem die Compliance-Anforderungen der verschiedenen Regelwerke aufeinander abzustimmen. Insofern stellt die

- Identifizierung der compliance-relevanten Regelwerke

den ersten Aufgabenbereich eines IT-Compliancemanagements dar, vgl. Abbildung 1. Daran schließen sich an:

- die Ableitung der einzuhaltenden, ggf. auch inkonsistenten Compliance-Anforderungen;

[10] Neben „Entsprechung“ werden auch die Begriffe der Übereinstimmung, Einhaltung, Befolgung oder Konformität verwendet.

[11] Nach der hier vertretenen weiten Auffassung sind dies: a) rechtliche Vorgaben, d. h. Gesetze und Rechtsverordnungen, Rechtsprechung sowie Verwaltungsvorschriften; b) Verträge; unternehmensinterne Regelwerke, z. B. Richtlinien und Verfahrensanweisungen, d) unternehmensexterne Regelwerke, vor allem Standards und Normen.

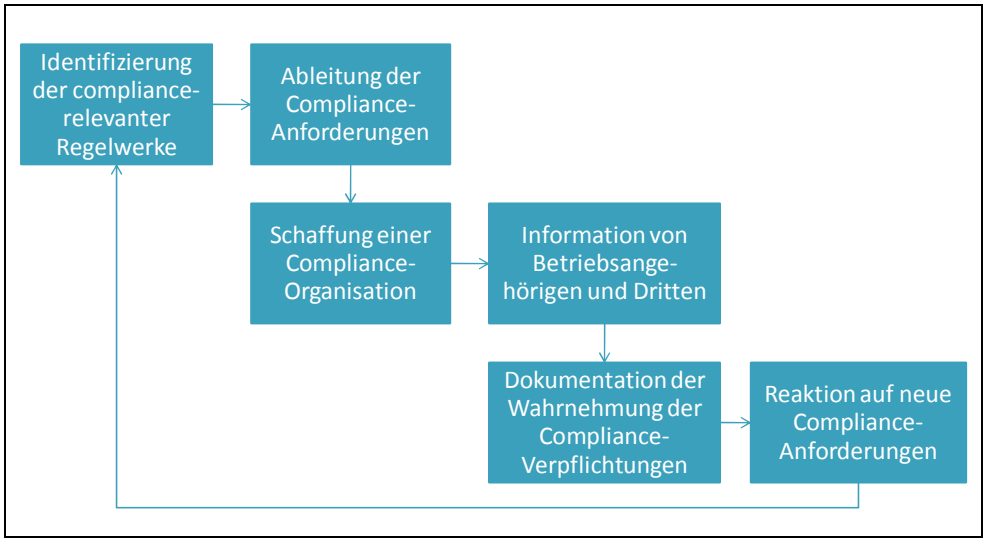


Abbildung 1
Aufgaben-bereiche des IT-Compliance-managements

- die Schaffung einer Compliance-Organisation von Prozessen, Verfahrensregelungen, Delegationen und (möglichst weitgehend automatisierten) Kontrollen zur Überwachung der Einhaltung aller Anforderungen der IT-Compliance;
- die Information aller in irgend einer Form im Hinblick auf die bestehenden Verpflichtungen handelnden Betriebsangehörigen und ggf. entsprechend eingesetzter Dritter über die einzuhaltenden Regelungen;
- die Dokumentation sowohl der Information als auch der Organisation und insbesondere deren Überwachung;
- die Reaktion auf neue Entwicklungen der Anforderungen, z. B. innerhalb der aktuellen Rechtsprechung oder erkannte interne Compliance-Schwachstellen[12].

3. Datenschutz in der KMU-Praxis

BDSG

Der Umgang mit personenbezogenen Daten wird für Unternehmen als nicht-öffentliche Stellen durch das Bundesdatenschutzgesetz (BDSG) [13] geregelt.

[12] Nach *Klotz 2007*, S. 17.

[13] Das BDSG eignet sich für die hier angestellten Überlegungen besonders gut, da es seit längerer Zeit besteht und durch die Medien und die Arbeit der Landesdatenschutzbeauftragten immer wieder in den Blickpunkt der Öffentlichkeit gerät – und derzeit auch steht. Es enthält klare Vorgaben mit IT-Bezug sowie in „Anlage zu § 9 Satz 1“ einen ausdrück-

Zu dem zuletzt im August 2006 novellierten Gesetz liegt eine umfangreiche Literatur vor, von der pragmatischen Einführung bis hin zum spezialisierten juristischen Kommentar[14]. Für Unternehmen ergeben sich aus den Regelungen des BDSG verschiedenste Verpflichtungen hinsichtlich der Datenvermeidung und -sparsamkeit, der Zulässigkeit der Erhebung, Verarbeitung und Weitergabe personenbezogener Daten, der Meldung der Verarbeitung personenbezogener Daten, der Einrichtung der Stelle eines Datenschutzbeauftragten, der Verpflichtung des Personals auf das Datengeheimnis und vor allem der Rechte der Betroffenen (d. h. Mitarbeiter, Kunden und Lieferanten eines Unternehmens).

Umsetzung des BDSG in KMU

Die Verpflichtungen zum Datenschutz sind klar geregelt, und seitens der Datenschutzbehörden steht ein umfangreiches Informationsangebot bereit, um auch kleinen und mittelständischen Unternehmen (KMU) eine effektive und effiziente Erfüllung der gesetzlichen Vorgaben zu ermöglichen. Zudem besteht durch die Beauftragung eines externen Datenschutzbeauftragten die Möglichkeit, sich die ggf. fehlende Expertise ins Haus zu holen. Trotzdem berichten Studien, aber auch die Landesbeauftragten für Datenschutz kontinuierlich über die mangelhafte Umsetzung der Vorgaben des BDSG in KMU, aber auch in größeren Unternehmen[15]. Einen detaillierten Einblick in diese Situation gibt eine Studie des Datenschutzbeauftragten für Mecklenburg-Vorpommern. Dieser hatte im Jahr 2007 eine repräsentative Befragung durchgeführt, um einen fundierten Überblick über den Stand der Umsetzung des BDSG in den Unternehmen Mecklenburg-Vorpommerns zu erhalten. Aufgrund der Wirtschaftsstruktur dieses Bundeslandes lassen sich nahezu

---

lich zu ergreifenden Maßnahmenkatalog – anders als in anderen Gesetzen, die den konkreten Weg der Befolgung einer gesetzlichen Vorgabe oftmals offenlassen. Der Stand der Compliance-Umsetzung, aber auch Motive und Probleme treten in Bezug auf das BDSG somit deutlicher zu Tage als bei anderen Gesetzen.

[14] Vgl. z. B. *Gola/Schomerus/Klug 2007*, *Witt 2007*.

[15] So hat eine Studie der UIMCert gezeigt, dass nur ca. 60% der befragten KMU, die zur Bestellung eines Datenschutzbeauftragten verpflichtet waren, dieser Vorgabe auch gefolgt sind (nach *DuD 2008)*. In *Neumann 2007* finden sich die auch im Folgenden weiter ausgeführten Ergebnisse einer Studie für KMU in Mecklenburg-Vorpommern, die die mangelhafte Umsetzung noch deutlicher aufzeigen. Doch auch in größeren Unternehmen sind Beanstandungen zu verzeichnen. Beispielsweise reklamiert der Berliner Beauftragte für Datenschutz und Informationsfreiheit in Berliner Banken Mängel bei der Umsetzung datenschutzrechtlicher Vorgaben *BlnBDI 2007*, S. 57-60.

alle an der Studie teilnehmenden Unternehmen als KMU einstufen. Im Einzelnen zeigten sich folgende Ergebnisse[16]:

- In 28% der Unternehmen findet ausdrücklich keine Verpflichtung der Mitarbeiterinnen und Mitarbeiter auf das Datengeheimnis statt. Weitere 11% der Unternehmen machten hierzu keine Angabe.
- In 23,7% der Unternehmen findet keine Kontrolle der BDSG-Vorschriften statt.
- In 46,4% der Unternehmen wurden bisher keine Datenschutzschulungen durchgeführt. Weitere 13,1% machten hierzu keine Angabe.
- In 71,4% der Unternehmen wurden bisher keine Verfahrensverzeichnisse erstellt, 11,9% machten hierzu keine Angabe.
- 33% der Unternehmen sind ihrer Pflicht zur Bestellung eines Datenschutzbeauftragten bisher nicht nachgekommen.
- In 38% der Unternehmen ist der Datenschutzbeauftragte nicht der Unternehmensleitung unterstellt.
- Von 40% derjenigen Unternehmen, die einen Datenschutzbeauftragten bestellt haben, wurde die Schriftformerfordernis der Bestellung nicht eingehalten.

Gründe für Non-Compliance

Diese Ergebnisse zeigen eine beträchtliche, in Teilbereichen sogar überwiegende Non-Compliance von KMU in Bezug auf die datenschutzrechtlichen Verpflichtungen des BDSG. Wie ist dies zu erklären? Auch hierzu gibt die Studie Auskunft. Die Ergebnisse auf die Frage, wie die Geschäftsführung das Thema Datenschutz generell einschätzt, sind in Tabelle 1 enthalten.

Offenbar lässt sich die mangelnde Beachtung des BDSG in den untersuchten KMU damit erklären, dass Vorteile der Gesetzeskonformität für viele der Unternehmen nicht existent oder nicht deutlich sind, so dass der Datenschutz auch nur von ca. der Hälfte der Unternehmen als sinnvoll bezeichnet wird. Hinzu kommt, dass diejenigen Unternehmen, die dem Datenschutz eine Sinnhaftigkeit zuerkennen, dies überwiegend aus einem formalen Grund tun, nämlich der Vermeidung von Strafen, Bußgeldern und Schadensersatz. Auch der hohe Anteil an Unternehmen, die keine Angabe ge-

[16] Nach *Neumann 2007*.

macht haben, deutet auf Orientierungslosigkeit, mangelndes Problembewusstsein, schlichte Unkenntnis o. ä. hin.

Tabelle 1
Datenschutz ...

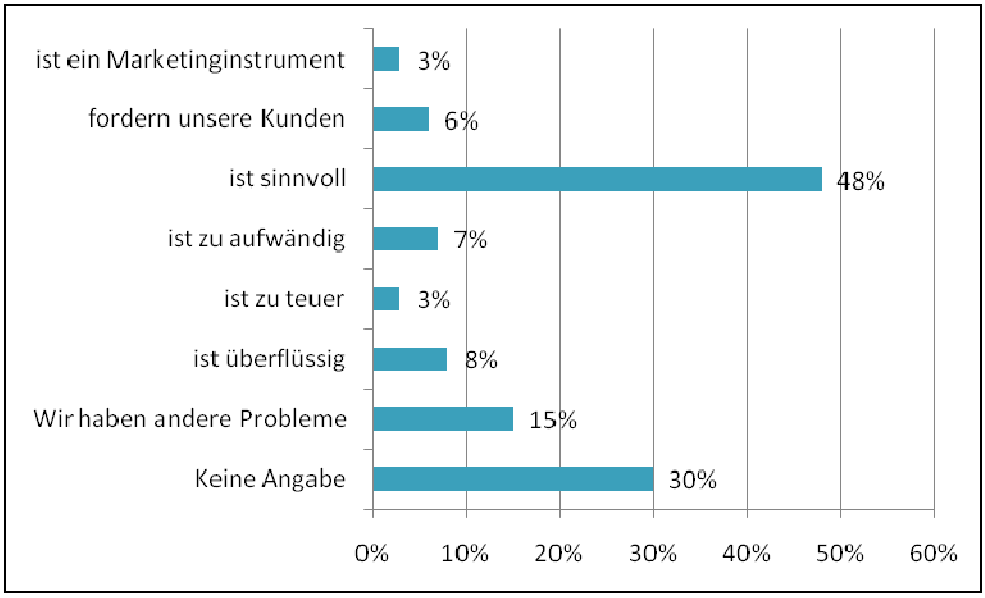
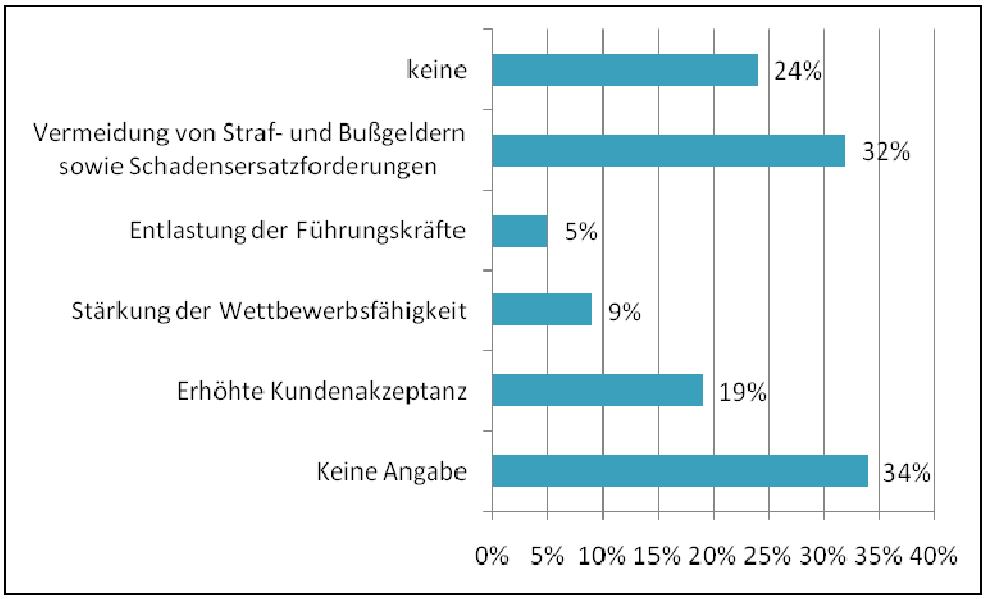


Tabelle 2 enthält die Einschätzung der Vorteile, die mit der Einhaltung der datenschutzrechtlichen Bestimmungen verbunden sind.[17]

Tabelle 2
Vorteile durch Datenschutz



[17] Bei beiden Fragestellungen waren Mehrfachantworten möglich; nach *Neumann 2007*, S. 55f.

Immerhin ein Viertel der antwortenden Unternehmen verbindet keine Vorteile mit Datenschutz. Weitere 34% machten hierzu keine Angabe, so dass insgesamt fast 60% die Befolgung der datenschutzrechtlichen Vorgaben für sich nicht mit Vorteilen verbinden. Auf der anderen Seite sehen nur knapp ein Viertel der Unternehmen positive Vorteile, die nicht nur als Schutz vor potenziellen Nachteilen zu verstehen sind, sondern bspw. auch marktseitig von Nutzen sind. Was für Folgerungen sind aus diesen Resultaten für die IT-Compliance als Handlungsbereich zu ziehen?

4. Diskussion der Folgerungen für die IT-Compliance

4.1. Konsequentialistische Erklärung der Compliance-Praxis

Konsequentialistische Handlungsbegründung

Sowohl die Studienergebnisse als auch das eingangs angeführte Pausengespräch lassen die Vermutung aufkommen, dass die meisten KMU-Verantwortlichen die Gesetzeseinhaltung davon abhängig machen, welcher Nutzen und Aufwand mit der Umsetzung des BDSG verbunden ist. Die Entscheidung für eine bestimmte Handlung danach auszurichten, welche Nutzen/Aufwand-Relation aus dieser Handlung folgt, bedeutet, die bewusst herbeigeführten oder in Kauf genommenen Folgen einer Handlung als Entscheidungskriterium für das Ausführen der Handlung heranzuziehen. Eine derartige teleologische Position gilt als konsequentialistische Handlungsbegründung, nach der die „Richtigkeit einer Handlung ausschließlich anhand ihres Zieles, und das sind in diesem Fall die Folgen, bestimmt wird“.[18] Diese Folgen müssen von Handelnden vorhergesehen und beabsichtigt sowie aus Sicht des Entscheidungsträgers für diesen natürlich auch vorteilhaft sein.

Vermeidung von Nachteilen

Eine konsequentialistisch begründete Umsetzung des BDSG richtet ihr Augenmerk also auf die Folgen dieser Umsetzung, s. Abbildung 2. Diese Folgen bestehen im Falle der geforderten Gesetzeskonformität zuerst einmal im Vermeiden von Nachteilen, die aus fehlender oder mangelhafter Compliance resultieren können, d. h. Freiheitsstrafen, Buß- oder Zwangsgelder,

[18] *Ricken 1983* S. 216. Im Rahmen seiner ethischen Überlegungen kommt es RICKEN auf die moralische Rechtfertigung an. Für die Argumentation in diesem Beitrag wird das konsequentialistische Begründungsprinzip zur Erklärung einer spezifischen Entscheidungssituation verwendet, es erfolgt jedoch keine ethische Reflektion der Entscheidung bzw. des aus ihr resultierenden Handelns.

Schadensersatz, Vertragsstrafen, Umsatzausfälle, Imageschäden oder Wettbewerbsnachteile.

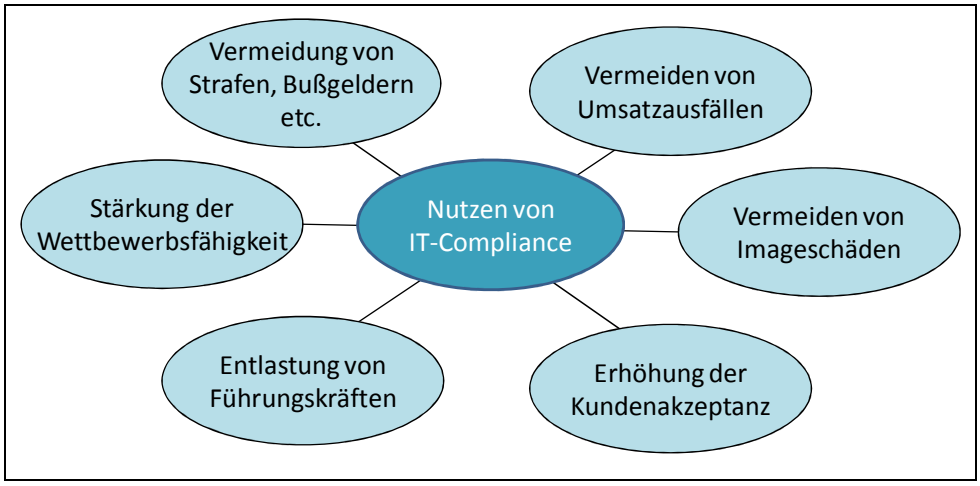


Abbildung 2
Folgen von IT-Compliance

Vorteile von Compliance

Tabelle 2 nennt aber auch Folgen, die nicht nur eine Vermeidung von Nachteilen darstellen: die Entlastung von Führungskräften, eine Stärkung der Wettbewerbsfähigkeit oder eine erhöhte Kundenakzeptanz. Die beiden letzteren Folgen können dann realisiert werden, wenn sich ein Unternehmen hinsichtlich der Gesetzesbefolgung positiv von seiner Konkurrenz abhebt und dies auch entsprechend in den Markt, vor allem gegenüber seinen Kunden kommuniziert.

Compliance-Risiken

Wird die Vermeidung von Bußgeldern, Strafen etc. als wichtigste Folge und Vorteil von IT-Compliancemaßnahmen betrachtet, führt dies dazu, IT-Compliance-Risiken für das Unternehmen bzw. die Unternehmensleitung in den Mittelpunkt der Betrachtung zu stellen. Es werden also IT-Risiken fokussiert, „die dadurch entstehen, dass die IT nicht wie geplant funktioniert, schlecht organisiert ist, nicht wie erforderlich betrieben und genutzt wird, unzureichend verfügbar oder ungenügend gesichert ist, manipuliert oder missbraucht werden kann etc., so dass hierdurch gesetzliche Auflagen (potenziell) nicht oder nur mangelhaft erfüllt werden“[19]. Ob und in welchem Ausmaß derartige Compliance-Risiken vorliegen, muss eine Risikoanalyse zeigen. Diese wird sowohl die relevanten Gesetze als auch die aktuelle Gesetzesbefolgung im Unternehmen zum Gegenstand haben.

[19] *Klotz/Dorn 2008*, S. 6f., vgl. *Hauschka 2007*, S. 3.

Risikoakzeptanz als vorherrschende Einstellung

Nun werden aber bereits Inhalt und Umfang der Risikoanalyse von den sich abzeichnenden Folgen abhängen. Wenn bspw. von vornherein nur geringfügige Strafen drohen, ist es nicht sinnvoll, diesem Risiko ein hohes Maß an Aufmerksamkeit zu widmen. Dementsprechend würden dann auch keine oder kaum Maßnahmen ergriffen, um ein rechtskonformes Handeln sicherzustellen. Ein ähnliches Ergebnis kann entstehen, wenn ein Risiko aufgrund einer bestehenden Risikoabsicherung (bspw. im Rahmen einer Versicherung) oder aufgrund einer geringen Wahrscheinlichkeit, dass ein Gesetzesverstoß verfolgt wird (gemäß der Redensart „Wo kein Kläger, da kein Richter"), keine weitergehende Beachtung findet[20]. Zumindest die Geringfügigkeit drohender Strafen sowie die bisher geringe Wahrscheinlichkeit der Ahndung dürften im Falle der mangelhaften Umsetzung des BDSG gegeben sein. Beides führt dazu, dass im Falle der Umsetzung des BDSG in KMU eine ausgeprägte Risikoakzeptanz, also das willentliche Missachten der Gesetzesnormen, anzutreffen ist.

4.2. Deontologische Charakterisierung der IT-Compliance

Relevanz deontologischer Prinzipien

Im Gegensatz zur konsequentialistischen Position steht die Auffassung, dass Gesetze zu befolgen sind, weil sie eben allgemein verbindliche Vorgaben für die Mitglieder einer Gesellschaft darstellen. Hiernach ist es die Pflicht des Einzelnen, den gesetzlichen Anforderungen nachzukommen. Die Einhaltung von Gesetzen bewirkt die notwendige Rechtssicherheit innerhalb einer Gesellschaft und realisiert die mit dem Gesetz intendierten Werte. Diese axiologische Begründung besteht für das BDSG in der Wahrung des Persönlichkeitsrechts auf informationelle Selbstbestimmung. Dass in der zitierten Studie bei der Frage nach den Vorteilen des Datenschutzes kein einziger „deontologischer Vorteil" (z. B. Gesetzestreue oder konkreter die Wahrung des informationellen Selbstbestimmungsrechts von Mitarbeitern, Kunden und Lieferanten) abgefragt wurde, kann zwar als Indiz dafür genommen werden, dass eine deontologische Position eher selten vertreten wird; trotzdem sollte aber nicht a priori davon ausgegangen werden, dass

[20] Dass sich Unternehmen in der Tat auf eine eher seltene Verfolgung von Verstößen gegen das BDSG „verlassen" können, zeigen die geringen Zahlen eingeleiteter Ordnungswidrigkeitsverfahren durch die Landesdatenschutzbeauftragten. So berichtet bspw. der Bremer Landesbeauftragte für Datenschutz und Informationsfreiheit von jeweils nur einem gegen Privatunternehmen eingeleiteten Verfahren in den beiden Jahren 2006 und 2007 (siehe *BrLfDI 2006*, S. 130; *BrLfDI 2007*, S. 165.

deontologische Prinzipien keinerlei Rolle bei der Entscheidungsfindung spielen.

Deontologische Handlungsbegründung

Nach einer deontologischen Handlungsbegründung sind somit diejenigen Kriterien maßgebend, die einer Handlung zugrunde liegen, nicht die Folgen der Handlung. Die Begründung für die Richtigkeit einer Entscheidung und einer entsprechenden Handlung liegt in der Entscheidung bzw. Handlung selbst, ungeachtet der jeweiligen Folgen. Eine deontologisch begründete Handlungsweise büßt sogar „auch in solchen Fällen nichts von ihrer Verbindlichkeit ein, in denen die Konsequenzen ihrer Befolgung in irgendeinem Sinne schlechter sind als die ihrer Nichtbefolgung“[21]. Für die Umsetzung des BDSG (aber auch anderer Gesetze) würde dies bedeuten, dass gesetzliche Vorgaben in Bezug auf den Datenschutz umzusetzen sind, auch ohne dass sich hieraus als vorteilhaft empfundene Folgen für das Unternehmen ergeben. In ökonomischer Hinsicht bedeutet dies, dass vor allem der Arbeitsaufwand und die mit der Umsetzung verbundenen Kosten akzeptiert und entsprechende finanzielle Mittel auch ohne eine positive Wirtschaftlichkeitsberechnung bereitgestellt werden.

Compliance-Anforderungen als deontische Modalaussagen

Wenn das Hauptziel der IT-Compliance in der Einhaltung gesetzlicher Vorgaben bestehen soll, ist sie im Kern deontologisch ausgerichtet. Dies zeigt sich auch darin, dass die aus einem Gesetzestext als normativer Basis resultierenden Compliance-Anforderungen als deontische Modalaussagen reformuliert werden können. Am Beispiel des BDSG lässt sich dies für die deontischen Modalitäten „geboten“, „verboten“ und „freigestellt“ wie folgt exemplarisch zeigen.

a) Deontische Modalität: „Es ist geboten, dass *p*.“

Regelung des BDSG:	„Öffentliche und nicht-öffentliche Stellen, die personenbezogene Daten automatisiert verarbeiten, haben einen Beauftragten für den Datenschutz schriftlich zu bestellen.“ (§ 4f Abs. 1, Satz 1)
Deontische Reformulierung:	„Es ist geboten, dass öffentliche und nicht-öffentliche Stellen, die personenbezogene Daten automatisiert verarbeiten, einen Beauftragten für den Datenschutz schriftlich bestellen.“

[21] *Birnbacher/Hoerster 1975*, S. 230.

b) Deontische Modalität: „Es ist freigestellt, dass *p*."

Regelung des BDSG: „Zur Verbesserung des Datenschutzes und der Datensicherheit können Anbieter von Datenverarbeitungssystemen und -programmen und datenverarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen." (§ 9a Satz 1)

Deontische Reformulierung: „Es ist freigestellt, dass zur Verbesserung des Datenschutzes und der Datensicherheit Anbieter von Datenverarbeitungssystemen und -programmen und datenverarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen."

c) Deontische Modalität: „Es ist verboten, dass *p*."

Regelung des BDSG: „Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis)." (§ 5 Satz 1)

Deontische Reformulierung: „Es ist verboten, dass die bei der Datenverarbeitung beschäftigten Personen personenbezogene Daten unbefugt erheben, verarbeiten oder nutzen (Datengeheimnis)."

Konfliktsituation

Wenn die Praxis der IT-Compliance konsequentialistisch handelt, das grundlegende Selbstverständnis der IT-Compliance jedoch deontologisch ausgerichtet ist, entsteht potenziell eine Konfliktsituation, die in der Praxis des IT-Compliancemanagements zu bewältigen ist.

4.3. Deontologisch-konsequentialistische Konfliktsituation

Beispiel: Bestellung eines Datenschutzbeauftragten

Die Darstellung der Konfliktsituation soll anhand der oben angeführten, von vielen KMU versäumten Bestellung eines Datenschutzbeauftragten erfolgen. Diese ist in § 4f BDSG (Beauftragter für den Datenschutz) geregelt.

Hiernach ist in Unternehmen ein Datenschutzbeauftragter zu bestellen, wenn mindestens zehn Arbeitnehmer wenigstens vorübergehend mit automatisierter Datenerhebung, -verarbeitung oder -nutzung beschäftigt sind (§ 4f Abs. 1 Satz 3 BDSG)[22].

Deontologische Sicht

Aus deontologischer Sicht handelt es sich bei dieser Regelung des BDSG um ein Gebot, das es unbedingt zu erfüllen gilt. Insofern ist zuerst zu prüfen, ob die Grenze von zehn Arbeitnehmern erreicht und damit die Stelle eines Datenschutzbeauftragten einzurichten ist. Sodann sind Maßnahmen zu planen und zu ergreifen, um alle gesetzlichen Vorgaben in Zusammenhang mit der Bestellung eines Datenschutzbeauftragten zu erfüllen.

Konsequentialistische Sicht

Aus konsequentialistischer Sicht stellt sich die Situation anders da. Das Wissen um die gesetzliche Vorgabe wird ebenfalls zu der Prüfung führen, ob die Bestellung eines Datenschutzbeauftragten erforderlich ist. Wenn dies der Fall ist, wird das mit dem potenziellen Gesetzesverstoß verbundene Compliance-Risiko betrachtet, dessen Höhe sich rechnerisch nach dem potenziellen Schaden multipliziert mit der Wahrscheinlichkeit des Schadenseintritts bemisst. In diesem Falle kommen prinzipiell in Frage:

- ein Bußgeld bis zu einer Höhe von 25.000,- € gem. § 43 Abs. 3 BDSG,
- ein Imageschaden, sollte der Fall an die Öffentlichkeit gelangen; hieraus evtl. resultierende
- Umsatzausfälle, wenn bisherige Kunden verloren gehen, und
- Wettbewerbsnachteile, wenn die Neukundenakquisition für die Zukunft nachhaltig beeinträchtigt wird.

Das Ergebnis dieser Analyse wird eine Abwägung zwischen Aufwand und Nutzen sein, d. h. eine Beurteilung, in welcher Relation die Kosten für Compliance-Maßnahmen zu einer erreichten Reduzierung der identifizierten und bewerteten Risiken stehen. Hierbei erfolgt eine Orientierung an unternehmensspezifischen Risikopräferenzen, bspw. unter Befolgung des

[22] In den Sätzen 1 und 5 des § 4f Abs. 1 sind weitere Fälle geregelt, die sich auf Unternehmen beziehen, die personenbezogene Daten geschäftsmäßig verarbeiten bzw. bei denen noch eine nichtautomatisierte Datenerhebung, -verarbeitung oder -nutzung vorliegt. Für die überwiegende Anzahl der KMU trifft jedoch die Regelung in § 4f Abs. 1 Satz 3 zu.

ALARP-Prinzips[23]. Im Beispiel kann dies zu der bewussten Entscheidung führen, dass kein Datenschutzbeauftragter bestellt wird, da weder das potenzielle Schadensausmaß noch die Eintrittswahrscheinlichkeit als hoch, schon gar nicht als bestandsgefährdend, eingestuft werden. Letzteres ließe sich vor allem damit begründen, dass lediglich ein Bußgeld drohe, wobei die Verfolgung durch die Aufsichtsbehörde als eher unwahrscheinlich anzusehen sei.

Struktur der Konfliktsituation

Der grundsätzliche Konflikt zwischen einer konsequentialistischen und einer deontologischen Sichtweise liegt somit dann vor, wenn eine Risikoabwägung mit dem Ergebnis der Akzeptanz bestimmter Compliance-Risiken dazu führt, dass gesetzliche Vorgaben gänzlich – oder zumindest teilweise – bewusst missachtet werden. Für die Vermittlung zwischen einer deontologischen und einer konsequentialistischen Position wird es in diesen Fällen entscheidend sein, wie die monetär nur schwer bewertbaren Folgen von Gesetzesverstößen in die Überlegungen einbezogen werden. Hierzu ist es erforderlich, Veränderungen im Umfeld einzubeziehen, und zwar nicht nur gesetzliche Änderungen (bspw. die Erhöhung von Strafgebühren), sondern auch die Entwicklung der öffentlichen Wahrnehmung. Eine gesteigerte öffentliche Aufmerksamkeit, auch und gerade im Hinblick auf den Datenschutz (vor allem vor dem Hintergrund der jüngsten Datenschutzverstöße in Fällen wie Lidl, Deutsche Telekom oder T-Mobile), kann dazu führen, dass intensiver nach potenziellen Regelverstößen gesucht wird und in der Folge angezeigt werden. Dies führt dazu, dass sich bei einem sensibilisierten Bewusstsein der Öffentlichkeit der Schaden von Non-Compliance erhöhen kann, wenn ein Unternehmen bei seinen bestehenden oder potenziellen Kunden, aber auch Mitarbeitern an Ansehen verliert – ein Gesichtspunkt, der in zunehmend auch international umkämpften Absatz- und Arbeitsmärkten tendenziell an Bedeutung gewinnt.

Lösungsmöglichkeit

Der beschriebene Konflikt muss jedoch nicht immer eintreten. Es bestehen vielmehr verschiedene Lösungsmöglichkeiten.

… bei relevanten IT-Risiken

So wird eine Auflösung des Konfliktes immer dann möglich sein, wenn Compliance-Risiken in ihrem Schadensausmaß und/oder in ihrer Schadenseintrittswahrscheinlichkeit als inakzeptabel hoch oder gar bestandsgefähr-

[23] ALARP = „As Low As Reasonably Practicable“. Hiernach wird ein Risiko akzeptiert, wenn die Kosten seiner Minimierung höher liegen als der erwartete, monetär bewertete Schaden bei Eintritt des Risikos.

dend bewertet werden. In diesen Fällen ergibt die Nutzenabwägung, dass es hinsichtlich der Risikobewertung vernünftig ist, der Vorgaben der Gesetzesnorm zu folgen, d. h. die Befolgung der Gesetze bedeutet gleichzeitig die Minimierung von Risiken. Dies dürfte bspw. für die in der dem BDSG beigefügten „Anlage (zu § 9 Satz 1)“ geforderten Zutritts-, Zugangs- und Zugriffskontrollen etc. im Hinblick auf personenbezogene Daten gelten. Die zur Einführung derartiger Kontrollen erforderlichen Maßnahmen sind gewöhnlich Bestandteil von IT-Sicherheitskonzepten, mit deren Umsetzung IT-Risiken auf ein akzeptables Maß reduziert werden.

…durch Vorgabe des konsequentialistischen Kalküls

Eine weitere Konfliktlösung ist in § 9 Satz 2 BDSG selbst enthalten. Hiernach sind die zu ergreifenden technischen und organisatorischen Maßnahmen nur dann gefordert, „wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht“. Dies entspricht dem konsequentialistischen Kalkül, denn die Angemessenheit ergibt sich ja gerade aus der Gegenüberstellung von Risikoausmaß und Aufwandshöhe der risikoreduzierenden Maßnahme. In diesem Fall erlaubt also die gesetzliche Regelung eine konsequentialistische Auslegung der Compliance-Vorgabe.

…durch Vorrang der axiologischen Begründung

Auch für die (wohl eher seltenen) Fälle, in denen Nutzen und Aufwand von Compliance-Maßnahmen als gleichgewichtig beurteilt werden, wird sich der Konflikt auflösen lassen. In diesen Fällen ist der Realisierung der Durchführung der Compliance-Maßnahmen (und damit der deontologischen Position) mit dem Hinweis auf die axiologische Begründung der Gesetzesnormen der Vorzug zu geben.

5. Fazit

Erfolg von Compliance

Die Anwendung beider ethischen Prinzipien der Deontologie und des Konsequentialismus erweist sich als sinnvolles Unterfangen, um die handlungsleitende Wertbasis der IT-Compliance zu diskutieren. Das Beispiel des Datenschutzes in KMU zeigt, dass es eben nicht ausreicht, die Gesetzesbefolgung an sich als (deontologisch) selbstverständlich zu postulieren. (IT-) Als Lehre zeit sich, dass Compliance nur dann erfolgreich umgesetzt werden kann, wenn auch die Gründe für Non-Compliance verstanden und als (konsequentialistisch) sinnhaltig akzeptiert werden. Gefordert ist somit eine abgestimmte Anwendung deontologischer und konsequentialistischer Prinzipien. Dies ist möglich, denn – wie gezeigt wurde – schließen sich deonto-

logische und konsequentialistische Betrachtung nicht notwendig gegenseitig aus.

Praxisrelevanz

Für die IT-Praxis ist diese Diskussion schon deswegen von Bedeutung, da sich beide Prinzipien in einem IT-Compliancemanagement auf der einen und einem IT-Risikomanagement auf der anderen Seite materialisieren. Somit bestehen für eine notwendige Zusammenarbeit potenziell Verständnis- und Verständigungsschwierigkeiten, denn vermutlich werden die mit den jeweiligen Aufgaben des Risiko- und Compliancemanagements Beauftragten tendenziell auch (eher) konsequentialistisch bzw. (eher) deontologisch agieren. Hieraus resultieren Herausforderungen für die Unternehmensleitung in Bezug auf die grundlegende Orientierung der beiden Bereiche, bspw. mittels entsprechender Richtlinien, und für die IT-Organisation hinsichtlich der Festlegung der jeweiligen Verantwortungsbereiche, der Schnittstellen sowie des organisatorischen Rahmens für die Zusammenarbeit.

Zurückführbarkeit der IT-Compliance auf IT-Risikomanagement

Auf der anderen Seite konnte durch die Gegenüberstellung der anhand der beiden ethischen Prinzipien der Deontologie und des Konsequentialismus jeweils unterschiedlich fundierten Bereiche der IT-Compliance und des IT-Risikomanagements gezeigt werden, dass IT-Compliance (in weiten Teilen) nicht auf IT-Risikomanagement zurückgeführt werden kann. IT-Compliance befasst sich auch mit denjenigen Compliance-Risiken, die konsequentialistisch nicht ins Gewicht fallen. Diese Erkenntnis sollte dazu dienen, eine institutionelle, aber auch methodische und instrumentelle Integration der IT-Compliance in das IT-Risikomanagement in Frage zu stellen.

Ein Nebeneffekt der hier angestellten Überlegungen ist die Charakterisierung der Complianceanforderung als deontischer Modalaussage. Aus dieser definitorischen Klärung eröffnen sich Möglichkeiten für eine formale Spezifikation von Compliance-Anforderungen. Hierfür werden zunehmend spezialisierte Policy-Sprachen genutzt[24]. Allerdings besteht, vor allem aus Anwendersicht, eine systematische Lücke zwischen der Interpretation der meist textuell vorliegenden Regelwerke und der formalen Spezifizierung mittels einer Policy-Sprache. Die systematische Darstellung der Compliance-Anforderungen als deontische Modalaussagen fördert eine schrittweise Formalisierung der in den Regelwerken enthaltenen Vorgaben und ist somit ein erster Schritt zum Schließen der genannten Lücke.

[24] Vgl. z. B. *Sackmann/Kähmer 2008*, S. 368ff.

Literaturangaben

Birnbacher/Hoerster 1975: Birnbacher, D.; Hoerster, N. (Hrsg.): Texte zur Ethik, München 1975.

Bitkom 2006: Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.; DIN Deutsches Institut der Normung e.V. Normenausschuss Informationstechnik (Hrsg.): Kompass der IT-Sicherheitsstandards – Leitfaden und Nachschlagewerk, Berlin 2006, verfügbar unter: http://www.bitkom.org/files/documents/Kompass_der_IT_28.06.06.pdf, Abruf am 04.01.2009.

BlnBDI 2007: Berliner Beauftragte für Datenschutz und Informationsfreiheit: Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit zum 31. Dezember 2007, verfügbar unter: http://www.datenschutz-berlin.de/content/veroeffentlichungen/jahresberichte, Abruf am 04.01.2009.

BrLfDI 2006: Landesbeauftragter für Datenschutz und Informationsfreiheit: 29. Jahresbericht des Landesbeauftragten für Datenschutz, Bremen, verfügbar unter: http://www.datenschutz-bremen.de/jahresberichte.php, Abruf am 04.01.2009.

BrLfDI 2007: Landesbeauftragter für Datenschutz und Informationsfreiheit: 30. Jahresbericht des Landesbeauftragten für Datenschutz, Bremen, verfügbar unter: http://www.datenschutz-bremen.de/jahresberichte.php, Abruf am 04.01.2009.

DCGK 2007: Deutscher Corporate Governance Kodex, Fassung vom 14.06.2007, verfügbar unter: http://www.corporate-governance-code.de/ger/download/D_Kodex%202007_final.pdf; Abruf am 04.01.2009.

DuD 2008: DuD Report: Aufsichtsbehörden machen ernst mit Datenschutz! In: Datenschutz und Datensicherheit, Jg. 32 (2008), Nr. 1, S. 74.

Fröschle/Strahringer 2006: Fröschle, H.-P.; Strahringer, S. (Hrsg.): IT-Governance, HMD Praxis der Wirtschaftsinformatik, Jg. 43 (2006), Nr. 250.

Gola/Schomerus/Klug 2007: Gola, P.; Schomerus, R.; Klug, C.: Bundesdatenschutzgesetz (BDSG): Kommentar, Beck Juristischer Verlag, 9., überarb. u. erg. Aufl. 2007.

Hauschka 2007: Hauschka, C. E.: Einführung. In: Ch. E. Hauschka (Hrsg.), Corporate Compliance – Handbuch der Haftungsvermeidung im Unternehmen, München 2007, S. 2-25

Hildebrand/Meinhardt 2008: Hildebrand, K.; Meinhardt, S. (Hrsg.): Compliance & Risk Management, HMD Praxis der Wirtschaftsinformatik, Jg. 45 (2008), Nr. 263.

Johannsen/Goeken 2007: Johannsen, W.; Goeken, M.: Referenzmodelle für IT-Governance – Strategische Effektivität und Effizienz mit COBIT, ITIL & Co., Heidelberg 2007.

Klotz 2007: Klotz, M.: IT-Compliance – auf den Kern reduziert. In: IT-Governance, Jg. 1 (2007), Nr. 1, S. 14-18.

Klotz/Dorn 2008: Klotz, M.; Dorn, D.-W., IT-Compliance – Begriff, Umfang und relevante Regelwerke. In: HMD Praxis der Wirtschaftsinformatik, Jg. 45 (2008), Nr. 263, S. 5-14.

Meyer/Zarnekow/Kolbe 2003: Meyer, M.; Zarnekow, R.; Kolbe, L. M.: IT-Governance – Begriff, Status quo und Bedeutung. In: Wirtschaftsinformatik, Jg. 45 (2003), Nr. 6, S. 445-448.

Neumann 2007: Neumann, K.: Projektbericht – Grunddatenerhebung betrieblicher Datenschutz in Mecklenburg-Vorpommern 2007, verfügbar unter: http://www.datenschutz-mv.de/navi/dschutz/grunddaten.html, Abruf am 04.01.2009.

Ricken 1983: Ricken, F.: Allgemeine Ethik, 3., erw. und überarb. Aufl., Stuttgart u. a. 1983.

Sackmann/Kähmer 2008: Sackmann, S.; Kähmer, M.: ExPDT – A Policy-based Approach for Automating Compliance. In: Wirtschaftsinformatik, Jg. 50 (2008), Nr. 5, S. 366-374.

Weill/Woodham 2004: Weill, P.; Woodham, J. W.: Don't Just Lead, Govern: Implementing Effective IT Governance, CISR Working Paper No. 326, MIT, Center for Information Systems Research, 2004, verfügbar unter: http://web.mit.edu/cisr/working%20papers/cisrwp349.pdf, Abruf am 04.01.2009.

Weill/Ross 2004: Weill, P.; Ross, J. W.: IT Governance: How Top Performers Manage IT - Decision Rights for Superior Results, Boston 2004.

Witt 2007: Witt, C.: Datenschutz kompakt und verständlich: Eine praxisorientierte Einführung, Wiesbaden 2007.

Das Stralsund Information Management Team (SIMAT)

Das von Prof. Dr. Michael Klotz geleitete „Stralsund Information Management Team“ (SIMAT) ist am Fachbereich Wirtschaft der FH Stralsund angesiedelt. Es bündelt akademische Lehre und Forschung, Weiterbildungsangebote und Projekte im Themenbereich des betrieblichen Informationsmanagements. Informationsmanagement richtet sich auf die effektive und effiziente Nutzung der informationellen Ressourcen eines Unternehmens. Diese Zielsetzung wird heute von verschiedenen spezialisierten Fachrichtungen in der Informatik, der Wirtschaftsinformatik und der Betriebswirtschaftslehre verfolgt. Das SIMAT arbeitet insofern interdisziplinär, wobei die inhaltlichen Schwerpunkte in Kompetenzzentren (Competence Center) fokussiert werden. Im Rahmen des RD&D-Ansatzes (Research, Development and Demonstration) dienen Labore, die mit aktuellen Tools des Informationsmanagements ausgestattet sind, sowohl der fachlichen Arbeit als auch zu Demonstrationszwecken. Eine intensive Kooperation mit ausgewiesenen Expertinnen und Experten sowie mit privatwirtschaftlichen Unternehmen und die Mitarbeit in anwendungsnahen Fachorganisationen gewährleisten eine praxis- und lösungsorientierte Vorgehensweise. Die Zusammenarbeit mit Lehrstühlen anderer Hochschulen, wissenschaftlichen Einrichtungen und eine umfangreiche Publikationstätigkeit stellen sicher, dass sich das SIMAT am State-of-the-Art des Informationsmanagements orientiert und diesen mitprägt. Auf diese Weise sind die Mitarbeiterinnen und Mitarbeiter des SIMAT in der Lage, anspruchsvolle Konzepte und Lösungen zu konzipieren und zu realisieren.

Das SIMAT versteht sich als Mittler zwischen akademischer Forschung und Lehre auf der einen, und der Wirtschaftspraxis auf der anderen Seite. Diese Transferaufgabe, verankert im Landeshochschulgesetz Mecklenburg-Vorpommerns, bildet den Schwerpunkt der Arbeit des SIMAT. Forschung und Lehre werden nicht als Selbstzweck begriffen, sondern führen zu handlungsrelevanten, innovativen Konzepten und Lösungen, die in die Unternehmenspraxis transferiert werden. Die berufliche Weiterbildung bildet hierbei ein wesentliches Element.

Die anwendungsnahe Forschung am SIMAT ist auf eine ökonomische Verwertung hin orientiert. Es sollen Innovationen entwickelt und in Kooperation mit anderen wissenschaftlichen Einrichtungen, Fach-Institutionen und Unternehmen in eine nachhaltige und profitable Praxis umgesetzt werden. Hierzu werden eigene F&E-Projekte auf dem Gebiet des Informationsmanagements und Innovationsprojekte mit Partnern durchgeführt. Zudem hat sich das SIMAT auf die betriebswirtschaftliche Begleitberatung bei IT-nahen Technologieprojekten spezialisiert. Studierenden und wissenschaftlichen Mitarbeiterinnen und Mitarbeitern wird die Möglichkeit eröffnet, an

der Lösung praktischer Problemstellungen zu arbeiten und sich so optimal auf das spätere Berufsleben vorzubereiten.

Die studentischen Mitarbeiterinnen und Mitarbeiter erhalten im SIMAT Einblick in die Arbeitsmethodik sowohl auf wissenschaftlichem als auch auf wirtschaftlichem Gebiet. Aus den Projekten des SIMAT entstehen zahlreiche Abschlussarbeiten, die den Studierenden der FH Stralsund offen stehen. Das SIMAT bietet zudem eine berufliche Perspektive für Studierende, die sich als wissenschaftliche Mitarbeiter in der anwendungsnahen Forschung qualifizieren wollen.

Das SIMAT beteiligt sich zudem an der Diskussion der wissenschaftlichen Gemeinschaft. Hierzu werden regelmäßig Arbeitspapiere veröffentlicht, die den Stand der Arbeit des SIMAT in die Öffentlichkeit tragen und zur Diskussion anregen sollen. Das SIMAT lädt zudem andere Wissenschaftler, aber auch Referenten aus der Praxis als Vortragende ein. Auf diese Weise lernen die SIMAT-Mitarbeiterinnen und -Mitarbeiter sowie andere interessierte Studierende aktuelle Forschungsergebnisse und praktische Fragestellungen aus erster Hand kennen. Erkenntnisse aus diesen Aktivitäten sowie aus den verschiedenen F&E-Projekten werden systematisch in die Lehre überführt, so dass alle Studierenden von der Forschungsarbeit des SIMAT profitieren können.

Zum Zwecke des ökonomischen Transfers verfolgt das SIMAT den RD&D-Ansatz (Research, Development and Demonstration). Hierzu wird ein Labor als Demonstrationsbereich unterhalten, das einerseits als Testbed, andererseits als Showroom dient.

- Testbed: Im Rahmen des Testbed werden Produkte und Lösungen von Kooperationspartnern des SIMAT in den Bereichen des Informations-, Projekt- und Prozessmanagements betrieben. Auf dieser technischen Grundlage werden im Rahmen von Projekten durch das SIMAT-Team prototypische Lösungen erarbeitet.
- Showroom: Im Showroom werden die erarbeiteten Lösungen und komplexe Nutzungen der verfügbaren Technologie einem Auditorium präsentiert. Hierbei werden sowohl prototypische als auch praktisch erprobte Realisierungen gezeigt.

Kontakt

FH Stralsund • SIMAT • Zur Schwedenschanze 15 • 18435 Stralsund
Ansprechpartner: Prof. Dr. Michael Klotz (Wissenschaftlicher Leiter)
☎ +49 (0)3831 45-6946
✉ michael.klotz@fh-stralsund.de

Verzeichnis der SIMAT-Arbeitspapiere

AP	Datum	Autor	Titel
01-09-001	01.2009	M. Klotz	Datenschutz in KMU – Lehren für die IT-Compliance