FINSOZ e.V.
FACHVERBAND
INFORMATIONSTECHNOLOGIE IN SOZIALWIRTSCHAFT
UND SOZIALVERWALTUNG E.V.

IT-Compliance-Guideline für die Sozialwirtschaft

– Richtlinienpapier FINSOZ e.V. –

Status: Freigegeben

Datum: 24.09.2014

Version: 1f

Über FINSOZ e.V.

Der Fachverband FINSOZ wurde 2010 mit dem Ziel gegründet, den Nutzwert der IT in der Sozialwirtschaft zu steigern. Die derzeit etwa 150 Mitglieder repräsentieren alle drei Bereiche der Branche: Verbände und Einrichtungsträger der Sozialwirtschaft, Anbieter von IT-Lösungen sowie Hochschulen, Institute und Beratungsunternehmen. Mit dieser Zusammensetzung der Mitglieder ist der Verband einzigartig in der sozialen Landschaft Deutschlands.

FINSOZ e.V.
Mandelstraße 16, 10409 Berlin
Telefon +49 30 42084-512
Internet www.finsoz.de

Wir bedanken uns bei den Mitwirkenden der FINSOZ-Arbeitsgruppe IT-Compliance für ihr Engagement bei der Erstellung dieser Guideline:

Thomas Althammer	Althammer & Kill GmbH & Co. KG, Hannover
Dietmar Bölling	AWO Nordhessen GmbH, Kassel
Ute Doleczik	PRW Consulting GmbH, München
Michaela Grundmeier	Verein kath. Altenhilfeeinrichtungen e. V., Hamm
Klaus Küsters	Landschaftsverband Rheinland, Bedburg-Hau
Christian Lax	Alida Schmidt-Stiftung, Hamburg
Markus Lück	RZV Rechenzentrum Volmarstein GmbH, Volmarstein
Jan Medenwaldt	Redline DATA GmbH, Ahrensbök
Frank Nelles	Stephanus IT GmbH, Berlin
Berthold Thiel	AWO Bezirksverband Hessen-Süd e. V., Frankfurt
Wilfried Reiners	PRW Rechtsanwälte, München

Der besseren Lesbarkeit halber wurde auf eine geschlechterspezifische Unterscheidung der Begrifflichkeiten verzichtet. Bezeichnung wie Datenschutzbeauftragter, Sicherheitsbeauftragter, Mitarbeiter, etc. umfasst somit auch immer die weibliche Form.

Inhaltsverzeichnis

1. Präambel

Nachhaltiger Erfolg in der Sozialbranche ist kein Zufall. Er ist vielmehr das Ergebnis strategischer Planungen und Umsetzungen, verbunden mit einem jahrelangen und fortdauernden Verbesserungsprozess. In diesem Umfeld sollte auch das Thema IT-Compliance und IT-Risiko-Management (im Folgenden zusammen als „IT-Compliance" bezeichnet) als Teilbereich platziert werden. Oberstes Ziel von IT-Compliance ist somit eine nachhaltige Verbesserung und Sicherung des Erfolgs.

Das hier dargestellte Modell des sachgerechten IT-Compliance-Managements orientiert sich an den so genannten T/O/R-Principles. Die T/O/R-Principles verstehen sich als die Basis des IT-Compliance-Managements in den Dimensionen **T**echnik, **O**rganisation und **R**echt. Die optimale „T/O/R"-Zusammensetzung besteht aus dem richtigen Technikeinsatz, dem Aufbau einer angemessenen Organisation und der rechtlichen Vorsorge und Überprüfung.

2. Bedeutung von IT-Compliance in der Sozialwirtschaft

Begriffe wie „Compliance" und „Corporate Governance" haben ihren festen Platz in der öffentlichen Wahrnehmung erreicht. Börsennotierte Unternehmen haben diese Themen weitgehend schon im Griff oder arbeiten an deren Institutionalisierung. Die Diskussion um diese Begriffe hat nun auch den Mittelstand und damit die Sozialwirtschaft, die von ihrer Größenordnung vornehmlich mittelständisch orientiert ist, erreicht. Dabei herrscht Unklarheit über die praktische Bedeutung der Begriffe. Das Wort „Compliance" (englisch für „Befolgung") bedeutet die Einhaltung von Verhaltensmaßregeln, Gesetzen und Richtlinien in Betrieben und Einrichtungen. Wesentlicher Inhalt ist somit der Aufbau einer angemessenen Organisation zur Umsetzung einer optimalen Betriebsführung und -kontrolle, unter Beachtung von betrieblich oder gesetzlich vorgegebenen Regeln. Aus den allgemeinen Vorschriften - etwa zur sorgfältigen Betriebsführung - lassen sich in angemessenem Rahmen auch Regeln für die Sozialwirtschaft ableiten.

IT-Compliance ist nicht gänzlich neu. Niemand wird ernsthaft behaupten, dass die Sozialwirtschaft und ihre IT bisher nicht rechtskonform geführt wurden. Ausnahmen gab es und wird es geben, daran ändern auch neue Begriffe nichts. Dennoch hat das Recht in der IT-gestützten Welt stärkeren Einzug gehalten.

Fest steht, dass sich die IT in den letzten 20 Jahren immer mehr in die Abwicklung der Betriebsprozesse eingebracht hat. IT-Compliance bedeutet dabei zunächst, dass auch im IT-Umfeld des Betriebes, das heißt in allen Bereichen, in denen IT zur Anwendung kommt (z. B. im Bereich der E-Mail-Systeme), die rechtlichen Rahmenbedingungen (z. B. Post-/ Fernmeldegeheimnis und Datenschutz) eingehalten werden. Unter IT-gestützter Compliance wird hier die Überprüfung der Einhaltung von Compliance-Vorschriften mittels IT (in der Regel Software) verstanden (z. B. im Rahmen des Risikomanagements oder des Monitorings von Applikationen).
Alte und neue Vorschriften werden sprachlich in den folgenden Ausführungen einheitlich als IT-Compliance-Vorschriften bezeichnet.

2.1 Ist Compliance Pflicht?

In der Literatur[1] wurde schon im Jahr 2005 eine allgemeine Rechtspflicht zur Einrichtung einer Compliance-Organisation für alle Unternehmen behauptet. Dem wurde entgegnet, dass die existierenden spezialgesetzlichen Vorschriften nicht ausreichten, um daraus eine für alle Unternehmen existierende Verpflichtung zur Einrichtung einer Compliance-Organisation abzuleiten.[2]
Dies darf aber nicht zu dem Schluss führen, dass es sich hierbei um eine Diskussion über die Notwendigkeit der Compliance-Organisation handelt. Völlig unbestritten ist, dass die Einhaltung der Gesetze eine Unternehmenspflicht darstellt, für deren Verwirklichung die Unternehmensleitung zuständig ist. Hierin unterscheiden sich auch Privatwirtschaft, öffentlich oder kirchlich geführte Einrichtungen nicht.

[1] Schneider, ZIP 2003, 645.
[2] Hauschka, ZIP 2004, 877.

Die Notwendigkeit zur Einhaltung gesetzlicher Regelungen durch Unternehmen ergibt sich aus dem Grundsatz, dass Gesetze − auch durch juristische Personen − einzuhalten sind. Unternehmen und Unternehmensverantwortliche sind über die §§ 9, 30 und 130 Ordnungswidrigkeitsgesetz (OWiG) gefordert, dafür Sorge zu tragen, dass aus dem Unternehmen heraus keine Gesetzesverstöße erfolgen. Werden entsprechende Organisations- und Aufsichtsmaßnahmen nicht ergriffen, können Unternehmensleitung und auch das Unternehmen selbst zu Strafen verurteilt werden, wenn es aus dem Unternehmen zu Gesetzesverstößen gekommen ist. Macht sich somit ein Mitarbeiter des Unternehmens durch Korruption strafbar, so drohen dem Unternehmen nicht nur zivilrechtliche Klagen des Geschäftspartners, dessen Mitarbeiter bestochen wurden. Vielmehr muss auch das Unternehmen damit rechnen, dass gegen das Unternehmen oder gegen die Unternehmensleitung ein Ordnungswidrigkeitsverfahren eingeleitet wird, weil den Organisations- und Aufsichtspflichten nicht nachgekommen wurde.

Daneben regeln eine Vielzahl von gesetzlichen Vorschriften unmittelbare Pflichten und Verantwortungen des Unternehmens, die dieses einzuhalten hat und bei deren Nichteinhaltung dem Unternehmen unter Umständen empfindliche Strafzahlungen drohen (z.B. aus Kartellrechtsverstößen). Eine Pflicht zur Sicherstellung der Compliance ergibt sich somit aus der Pflicht zur Abwendung von wirtschaftlichem Schaden vom Unternehmen[3].

2.2 Ist Risikofrüherkennung Pflicht?

Die gesetzliche Verpflichtung zur Risikofrüherkennung und zur Integration eines Überwachungssystems ist für die Privatwirtschaft durch das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) im Mai 1998 eingeführt worden. Ziel des KonTraG ist es, die Corporate Governance in deutschen Unternehmen zu verbessern. Deshalb wurden mit diesem Artikelgesetz etliche Vorschriften aus dem Handels- und Gesellschaftsrecht verändert. Das KonTraG präzisiert und erweitert dabei hauptsächlich Vorschriften des HGB (Handelsgesetzbuch) und des AktG (Aktiengesetz). Mit dem

[3] http://de.wikipedia.org/wiki/Compliance_(BWL).

KonTraG wurde die Haftung von Vorstand, Aufsichtsrat und Wirtschaftsprüfern in Unternehmen erweitert.

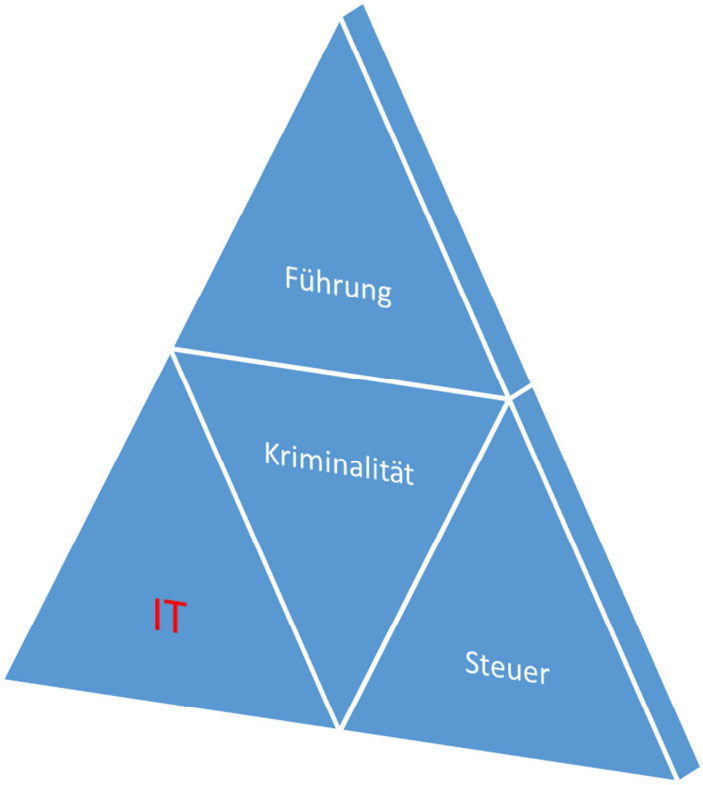
Kern des KonTraG ist eine Vorschrift, die Unternehmensleitungen dazu zwingt, ein unternehmensweites Früherkennungssystem für Risiken (Risikofrüherkennungssystem) einzuführen und zu betreiben sowie Aussagen zu Risiken und Risikostruktur des Unternehmens im Lagebericht des Jahresabschlusses der Gesellschaft zu veröffentlichen. So heißt es in § 91 AktG Abs. 2: „*Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden*“[4]. In der Gesetzesbegründung heißt es, dass für eine GmbH je nach Größe und Komplexität ihrer Struktur nichts anderes gilt. Eine konkrete Ausprägung zur Umsetzung und Beschaffenheit eines solchen Überwachungssystems hat der Gesetzgeber nicht eingebracht. Im Zweifel verstößt somit die fehlende Umsetzung eines Risikofrüherkennungssystems schon gegen das geltende Recht. Das Unternehmen erfüllt damit auch nicht die Compliance-Anforderungen.

Es liegt nahe zu glauben, dass die vorgenannten Grundsätze lediglich für die Privatwirtschaft gelten. Dies ist ein weitverbreiteter Irrtum. Sie gelten für alle, auch öffentliche und kirchliche Einrichtungen, die sich an das deutsche Recht und seine Rechtsprechung gebunden fühlen. Hintergrund ist, dass das KonTraG letztlich auf die ARAG ./. Garmenbeck Entscheidung des BGH[5] zurückgeht, in der die Grundsätze der Haftung aufgezeigt wurden.

[4] RegE KonTraG 1997 Begründung zu § 91 Abs. 2 AktG.
[5] BGH, Urteil vom 21.04.97 - II ZR 175/95.

3. Rechtliche Rahmenbedingungen von IT-Compliance

Wie bereits zuvor erwähnt, ist der Kreis der rechtlichen Rahmenbedingungen im Compliance-Umfeld umfassend. IT-Compliance ist Teil des gesamten Compliance-Bereichs und spielt in der Regel eine weitaus größere Rolle, als in der nachfolgenden Grafik dargestellt. IT-Compliance ist ein Baustein des Compliance-Gesamtpaketes und der Umfang des Compliance-Gesamtpaketes variiert je nach Einrichtung / Betrieb.



Zunächst hat ein Betrieb also einmal festzustellen, welche IT-Compliance-Vorschriften für ihn gelten. Neben den zutreffenden Gesetzen in ihren unterschiedlichsten Ausprägungen wie etwa das Telekommunikationsgesetz (TKG), das Bundesdatenschutzgesetz (BDSG), die Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU – Stichwort digitale Steuerprüfung) und den Sozialgesetzen, sind zudem die bereits existierenden Richtlinien und Handlungsempfehlungen von BSI, ISO-Standards, ITIL, COBIT, IDW PS 330 und viele andere zu beachten.

Betroffene Bereiche von IT-Compliance sind zum Beispiel die GDPdU-konforme Archivierung von Daten, die E-Mail-Archivierung oder die Einführung eines Dokumentmanagementsystems.

Die Kernaufgabe besteht in der Dokumentation und der entsprechenden Anpassung der IT-Ressourcen und der Analyse und Bewertung der entsprechenden Problem- oder Gefahrenpotentiale (auch: Risikoanalyse). Zu den Ressourcen gehören Hardware, Software, IT-Infrastruktur (Gebäude, Netzwerke), Services (z.B. Webservices) und die Rollen und Rechte der Software-Anwender. Wichtig ist hierbei, dass die Umsetzung von Compliance als ein dauerhafter Prozess und nicht als kurzfristige Maßnahme aufgefasst wird.

4. Zuständigkeit für IT-Compliance

Die Einhaltung von Compliance-Vorschriften und damit die Rechtskonformität des Betriebes ist Aufgabe der obersten Führungsebene. Zwar kann die Einhaltung der Compliance-Vorschriften delegiert werden, die Delegation erfordert allerdings ihrerseits wieder, dass die Auswahl des Compliance-Beauftragten sorgfältig erfolgt, ein regelmäßiges Reporting an die Führungsspitze und eine Kontrolle dieser Schlüsselposition durchgeführt werden.

Bei der Umsetzung von IT-Compliance-Vorschriften treten nicht selten folgende Konstellationen auf:
Fragt man einen Hersteller, wie Compliance umzusetzen ist, dann bekommt man technische Daten von Hardware, Software und Applikationen als Antwort. Fragt man einen Berater/Consultant, erhält man Ausführungen, in denen zumindest Begriffe wie Verfügbarkeit, Vertraulichkeit, Authentizität, Autorisierung, Integrität, Rechtskonformität, Zurechenbarkeit, Effektivität und Effizienz auftauchen. Fragt man den Hausjuristen, antwortet dieser mit Themen des IT-Rechts, während die IT-Leitung im Unternehmen mit

knappen Budgets meist wenig Kapazitäten für die Umsetzung von IT-Compliance-Vorgaben hat und häufig nur rudimentäre Dokumente beisteuern kann.
Doch Frustration und Ärger über die Gesetzgebung müssen nicht sein. Compliance ist Teamarbeit und nach der hier vertretenen Auffassung ist die Umsetzung von Compliance-Regelungen eine Aufgabe, mit der sich mehrere Personen inhaltlich befassen müssen. Dem IT-Compliance-Verantwortlichen sollten dabei unterschiedliche Profile zur Aufgabenerledigung beigestellt werden.

5. IT-Compliance umsetzen

Die Umsetzung von IT-Compliance beginnt mit einem ersten IT-Compliance-Projekt für einen Teilbereich. An diesem Projekt, das aus drei initialen Phasen und einer ständigen Nachkontrolle in Form von Audits besteht, sind mehrere Personen beteiligt. Hier wird empfohlen, dass sich die oberste Entscheiderebene gemeinsam mit der IT-Leitung, der Rechtsabteilung (oder einem erfahrenen IT-Anwalt), dem Datenschutzbeauftragten und gegebenenfalls den Leitern der Fachabteilungen einen Überblick verschafft und die für die eigene Einrichtung relevanten Regelungen benennt. Dann folgen die weiteren Schritte der Umsetzung und die Abbildung der spezifischen Anforderungen in konkreten

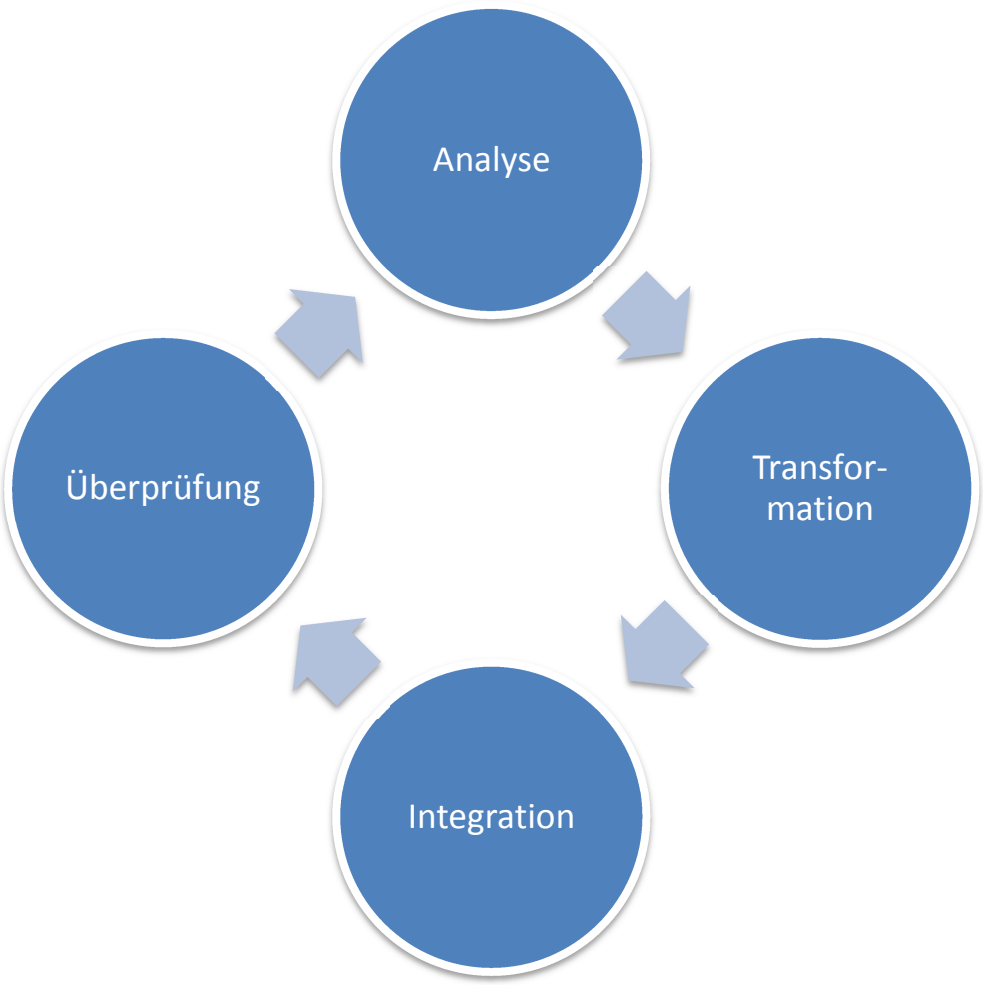
IT-Aktivitäten und regelmäßigen Audits. Der Umsetzung von IT-Compliance-Projekten werden häufig Schwachstellen-Audits sowie Security-, Strategie- und Prozessberatung oder technische Risikoanalysen vorgeschaltet. Dies dient vor allem der Klärung, welche Applikationen sich auf welchem Sicherheitsniveau befinden.

5.1 Die vier Phasen der Umsetzung

In der **ersten Phase (Analyse)** müssen zunächst die für die Einrichtung relevanten Compliance-Vorschriften ermittelt werden. Dabei zeigt die Erfahrung, dass etwa 50 % der relevanten Vorschriften für alle Betriebe der Sozialwirtschaft gleich sind, die weiteren 50 % sich aus betrieblichem Zweck, Konfession und Zugehörigkeiten bestimmen. Die rechtlichen Anforderungen an Leitungskräfte und Mitarbeiter ergeben sich entweder aus formellen Gesetzen, aus Anforderungen der Verwaltung (etwa Rundschreiben, Richtlinien) oder aber aus allgemeinen Richtlinien und Standards (wie zum Beispiel DIN und ISO). Zwar haben gerade letztere Vorschriften keinen unmittelbaren Rechtscharakter, sie können aber sehr wohl zur Auslegung und als Maßstab herangezogen werden, zum Beispiel bei der Frage des Verschuldens oder ob bestimmte IT-Infrastrukturen ein angemessenes IT-Sicherheitsniveau aufweisen.

Vergleichen wir eine soziale Einrichtung, einen Online-Computerhändler und einen Verlag, der ein Gesellschaftsmagazin verlegt. Alle drei Betriebe werden als GmbH geführt. Für alle drei Betriebe gelten z. B. die gleichen Vorschriften aus dem GmbHG, dem Steuerrecht, dem Datenschutzrecht und den allgemeinen Vorschriften wie Abgabenordnung, etc. Für die soziale Einrichtung gelten darüber hinaus gesetzliche Vorschriften aus dem Sozialrecht. Für den Online-Computerhändler ist es wichtig, dass er z. B. die Vorschriften zum Fernabsatzgesetz kennt. Für den/die Journalisten/in des Gesellschaftsmagazins wird es wichtig sein, dass bei einer Online-Kommunikation der Informantenschutz und die Pressefreiheit gewahrt werden. Daraus ergibt sich die Erkenntnis, dass IT-Compliance sich nicht aus einem immer gleichen Gesetzeskatalog zusammensetzt, sondern dass die einschlägigen Vorschriften erst in der Analyse ermittelt werden.

In der **zweiten Phase (Transformation)** müssen die relevanten Vorschriften auf IT-gestützte Prozesse übertragen werden. Am Ende erfolgt die Erstellung einer Richtlinie oder eines Rechtskatalogs, die bzw. der für alle Mitarbeiter als gültiger Kodex für gesetzmäßiges und verantwortungsbewusstes Handeln im Betrieb festgelegt wird. Damit bekennen das Unternehmen und die Mitarbeiter sich zur Rechtstreue. Dieser Schritt ist eine Herausforderung für das Compliance-Team, denn während es einige Gesetze gibt, die ihre Anforderungen an die IT recht präzise definieren (z. B. das Bundesdatenschutzgesetz in § 9 mit Anlage), sind andere Vorschriften schwieriger umsetzbar. Hierzu gehört etwa die Klärung der Frage, welches IT-Sicherheitsniveau den Anforderungen der Sorgfalt in der Sozialbranche entspricht.



In der **dritten Phase (Integration)** wird die Einhaltung der relevanten Vorschriften als geprüfte und überprüfte Selbstverständlichkeit in den Regelbetrieb überführt. Da sich

auch Gesetze und Vorschriften ändern, sollte nach einer gewissen Zeit ein **Audit (vierte Phase)** durchgeführt werden.

Die Herangehensweise zum Aufbau und Einführung der IT-Compliance ähnelt der im Qualitätsmanagement. Vieles liegt schon vor und wird im täglichen Geschäft bereits erfolgreich angewendet und umgesetzt. Kein Unternehmen arbeitet komplett „non IT-compliant". Als Einstieg in das Projekt werden also zunächst vorhandene Richtlinien, Anweisungen und Verfahren durch die Fachbereiche zusammengetragen. Die nun vorhandene Basis ist die Grundlage der zu erstellenden IT-Compliance-Richtlinie, deren Punkte im Laufe des Projektes ggf. ausgebaut, angepasst oder ergänzt werden. Die auf diesem Weg aufgedeckten Lücken und unvollständige Themenbereiche werden nun in den beschrieben 4 Phasen der Umsetzung einzeln bearbeitet.

Sind alle Punkte vervollständigt, ist das Projekt der Erstellung abgeschlossen. Bei der in der vierten Phase beschrieben Überwachung und Überprüfung der Richtlinie kann nach einem ähnlichem Prinzip ebenfalls auf Bestehendes zurückgegriffen werden, wie zum Beispiel auf Prozesse mit denen aktuell auf technische oder gesetzliche Weiterentwicklungen reagiert wird.

5.2 Was bringt der Einsatz einer Compliance-Management-Software?

Für mittelständische Unternehmen und Einrichtungen wird die einfache Umsetzung der relevanten IT-Compliance-Vorschriften im Vordergrund stehen. Zumindest für den Bereich der Risikofrüherkennung drängt sich daher die Frage auf, ob der Einsatz von Software zu empfehlen ist.

Nach den gesetzlichen Anforderungen müssen gravierende Risiken so früh erkannt werden, dass noch geeignete Maßnahmen zur Abwehr getroffen werden können. Dazu müssen die relevanten Informationen nicht nur frühzeitig vorliegen, sondern sie müssen auch aktuell und abrufbar sein. Hier bleiben nur wenige Organisationsmittel übrig, um diese Anforderungen nicht nur unter rechtlichen, sondern vor allem auch unter

betriebswirtschaftlichen Gesichtspunkten zu erfüllen.[6] Der Einsatz einer geeigneten Software ist dabei das wohl effektivste Mittel. Damit stellt sich also nicht die Frage, ob der Einsatz einer Software sinnvoll ist, sondern vielmehr welche Software im jeweiligen Fall die richtige Lösung ist. Dies lässt sich pauschal nicht im Vorhinein feststellen, für das kleinere Unternehmen kann hier schon ein clever entwickeltes Eigenprodukt ausreichen, für größere Unternehmen sind dies möglicherweise Werkzeuge, die in den Anschaffungskosten deutlich über EUR 100.000 hinausgehen.

5.3 Wie wird gestartet?

In der ersten Phase ist das Projektteam zu bestimmen, das für die IT-Compliance verantwortlich ist. Der nächste Schritt ist eine umfassende Überprüfung der IT-Infrastruktur und ihrer Prozesse. Dabei ist der T/O/R-Ansatz eine pragmatische und in der Praxis erprobte Methode. Mit ihr werden zunächst systematisch die technischen und organisatorischen Bereiche der IT aufgenommen und analysiert. Sodann werden die Möglichkeiten der Verbesserung der Planungssicherheit im Sinne einer Früherkennung der Risiken aufgezeigt und mit dem unter Kostengesichtspunkten Machbaren in Relation gesetzt. Es folgt die rechtliche Überprüfung mit dem Ziel, die relevanten Bereiche zu identifizieren und ein Konstrukt zu erreichen, bei dem die Haftungsrisiken minimiert werden.

Entscheidend für die Priorität bei der Umsetzung von Maßnahmen ist die konsolidierte Risikoanalyse, die sich aus den Einzelanalysen der Bereiche Technik, Organisation und Recht zusammensetzt. Auf diese Art wird, mit einer konsolidierten IT-Sicherheitsanalyse, der Grundstein für ein IT-Risiko-Management gelegt, worüber die Einhaltung der für die IT relevanten Compliance-Vorschriften sichergestellt wird.
In der nächsten Stufe ist zu prüfen, welche Softwaretools für die Umsetzung der definierten Anforderungen die beste Unterstützung leisten können. In der Folge werden Testbetrieb, Echtbetrieb und Auditierungen die nächsten Meilensteine markieren.

[6] Vgl. Schlaghecke S. 296 in Hauschka, Corporate Compliance (Beck Vlg.).

6. Datenschutzgesetzgebung

Ein zentraler Pfeiler im Bereich IT-Compliance stellt die einschlägige Datenschutzgesetzgebung dar. Je nach Trägerschaft (kommunal, kirchlich, anderweitig gemeinnützig sowie privatwirtschaftlich) sind hierfür unterschiedliche Gesetzesgrundlagen heranzuzuiehen. Allen ist gemein, dass es gerade für die häufig im Sozialwesen anzutreffenden Verbandsstrukturen kein Konzernprivileg gibt. Jede Gesellschaft in einem Trägerverbund ist somit als eigenständige Organisation zu betrachten und der Datenschutz ist entsprechend auch je Gesellschaft zu organisieren (z. B. mit Ernennung eines Datenschutzbeauftragten je Gesellschaft oder der Organisation von Auftragsdatenverarbeitung bei Nutzung zentraler IT-Ressourcen).

6.1 Technisch-organisatorische Maßnahmen

Trotz der gesetzlichen Unterschiede sind die Anforderungen des Bundesdatenschutzgesetzes (BDSG) in gleicher oder ähnlicher Form auch in den anderen Rahmenbedingungen (Landesdatenschutzgesetze, DSG-EKD, KDO) anzutreffen. Eine erste Orientierung bieten also die technisch-organisatorischen Maßnahmen nach § 9 BDSG. Deren Bedeutung und Relevanz wird anhand einiger Praxisbeispiele näher erläutert.

Zutrittskontrolle

„… Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren."

Konkrete Beispiele aus der Praxis:

- Serverraum und PC-Arbeitsplätze sind stets abgeschlossen, wenn niemand anwesend ist
- Zutritt ist mit Schlössern und Einbruchsschutz ausreichend gesichert
- Es existiert ein Schlüsselverzeichnis und für Gäste eine Anwesenheitskontrolle

Häufige Schwierigkeiten in der Praxis:

- Schutz öffentlicher Bereiche (Empfangstresen, etc.)?
- Zutrittskontrolle bei Heimarbeitsplätzen?

Zugangskontrolle

„… zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle)."

Konkrete Beispiele aus der Praxis:

- Die Nutzung von IT-Systemen ist durch Benutzername/Passwort und ggf. ein Hardware-Token geschützt
- Für das Anlegen, Ändern und Sperren von Benutzerkonten gibt es einen definierten Prozess nach dem 4-/6-Augen-Prinzip
- Es existieren Regelungen zur Passwortgüte (Art, Länge, Änderungshäufigkeit, …)

Häufige Schwierigkeiten in der Praxis:

- Gruppenkonten bei der Nutzung von PCs im Team (z. B. auf Wohnbereichen/in Wohngruppen stationärer Einrichtungen)
- Kein durchgängiges Berechtigungs- und Kontrollkonzept in Verbindung mit Stichprobenprüfungen auf Lücken
- Umsetzung eines einheitlichen Verzeichnisdienstes im Unternehmen mit zentraler Steuerung und Überwachung von Zugriffsrechten

Zugriffskontrolle

„… zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können."

Konkrete Beispiele aus der Praxis:

- Es existiert ein umfangreiches, möglichst durchgängiges Berechtigungskonzept, das die verschiedenen Anwendungen und IT-Systeme berücksichtigt
- Die Zugriffsrechte auf Daten und Funktionen werden nach Arbeitsaufgabe und Einsatzort differenziert vergeben (Rollenkonzept)
- Eine automatische Abmeldung oder Bildschirmschoner mit Passwortsperre verhindern, dass bei Verlassen des Arbeitsplatzes Unberechtigte auf die Systeme zugreifen können

Häufige Schwierigkeiten in der Praxis:

- Zugriffsrechte werden zu weitreichend vergeben oder bei Arbeitsplatzveränderungen nicht ausschließlich auf die neue Tätigkeit abgestellt
- Fehlende Kontrolle durch stichprobenartige Prüfungen und die Einsicht in Zugriffsprotokolle

Weitergabekontrolle

„… zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist."

Konkrete Beispiele aus der Praxis:

- Die Nutzung externer Datenträger wird weitestgehend vermieden und die Speicherung erfolgt ausschließlich in verschlüsselter bzw. geschützter Form
- Bei Fernwartung/Fernzugriff werden datenschutzkonforme Systeme eingesetzt, die Art und Umfang der Fernwartung dokumentieren und die sichere Übertragungswege garantieren

Häufige Schwierigkeiten in der Praxis:

- Fehlende Verschlüsselung und fehlende Protokollierung bei Weitergabe und Versand von Daten
- Datenexporte werden nicht erfasst/dokumentiert
- Verzicht auf Verschlüsselung von E-Mails bei Versand vertraulicher Daten; Nutzung von außereuropäischen Speicherdiensten im Internet wie Dropbox

Eingabekontrolle

„… zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind."

Konkrete Beispiele aus der Praxis:

- Für relevante IT-Systeme findet eine Protokollierung von Eingaben auf Datensatzebene und in einem Anwendungs-/Änderungsprotokoll statt

Häufige Schwierigkeiten in der Praxis:

- Fehlende Überprüfung der Protokollierung in Form von Stichproben
- Mangelnde Umsetzung von Möglichkeiten zur Eingabekontrolle in IT-Systemen

Auftragskontrolle

„… zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können."

Konkrete Beispiele aus der Praxis:

- Abschluss detaillierter Vereinbarungen zur Auftragsdatenverarbeitung nach §11 BDSG für alle relevanten Bereiche mit Personendatenbezug
- Regelmäßige Überprüfung auf Einhaltung rechtlicher und technischer Vorgaben beim Auftragsdatenverarbeiter

Häufige Schwierigkeiten in der Praxis:

- Fehlen eines Vertrages zur Auftragsdatenverarbeitung, mangelnde Auswahl des Anbieters und Unterlassung der Vorabkontrolle
- Einhaltung von Aufbewahrungs- und Löschfristen; fehlende Transparenz über Zuständigkeiten und Wechsel von Verantwortlichen oder externen Dienstleistern
- Berücksichtigung der Schweigepflichten nach § 203 StGB

Verfügbarkeitskontrolle

„… zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle).“

Konkrete Beispiele aus der Praxis:

- Brandschutzanlage und unterbrechungsfreie Stromversorgung für zentrale Systeme der IT-Umgebung
- Netzzugangskontrollen durch Firewalls und Einsatz von Virenschutzsystemen
- Umfangreiches Datensicherungskonzept inkl. organisatorischer Regelungen zur Verantwortung und Durchführung der Aufgaben

Häufige Schwierigkeiten in der Praxis:

- Serversysteme werden nicht regelmäßig auf mögliche technische Risiken hin überprüft (Test der USV, Kontrolle der Ereignisprotokolle)
- Fehlendes Notfallkonzept, so dass bei Ausfällen nicht klar geregelt ist, wer zu kontaktieren ist und was zu veranlassen ist
- Mangelnde oder unvollständige Prüfung der Datensicherung auf Wiederherstellbarkeit in regelmäßigen Abständen

Trennungsgebot

„… zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können."

Konkrete Beispiele aus der Praxis:

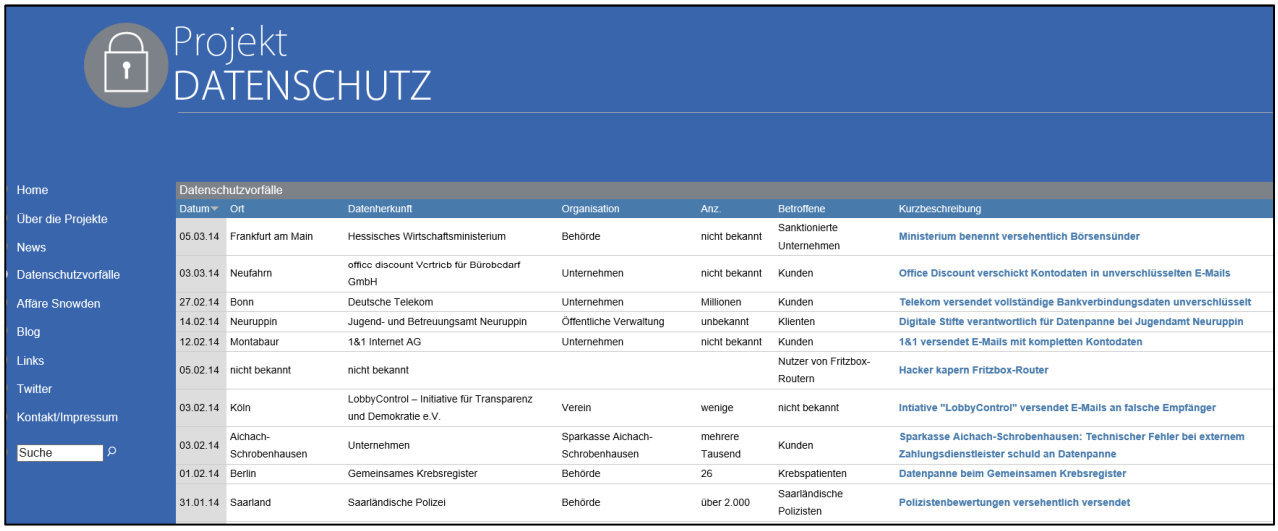
- Verwendete IT-Systeme sind mandantenfähig aufgebaut
- Das Berechtigungskonzept berücksichtigt die organisatorische Zugehörigkeit von Mitarbeitern
- Systeme für Test- und Schulungszwecke nutzen nur ausreichend pseudonymisierte oder anonymisierte Daten

Häufige Schwierigkeiten in der Praxis:

- Datenbestände von datenschutzrechtlich unabhängigen „verantwortlichen Stellen" sind nicht ausreichend voneinander getrennt, z. B. die Daten einer ausgegründeten Servicegesellschaft vom Datenbestand der Einrichtung
- Zugriffsrechte werden nicht detailliert genug vergeben und sorgen für „Datenmissbrauch", z. B. nutzt ein Anbieter von „Essen auf Rädern" die Patientendaten des Pflegedienstes einer Schwestergesellschaft für Werbezwecke (es gibt noch kein Konzernprivileg)

6.2 Umgang mit Datenpannen

Niemand wünscht sich eine Datenpanne und dennoch passieren sie in einem nicht zu unterschätzenden Umfang. Die private Website www.projekt-datenschutz.de gibt hierzu einen Überblick.



Projekt DATENSCHUTZ

Home
Über die Projekte
News
Datenschutzvorfälle
Affäre Snowden
Blog
Links
Twitter
Kontakt/Impressum
Suche

Datenschutzvorfälle

Datum	Ort	Datenherkunft	Organisation	Anz.	Betroffene	Kurzbeschreibung
05.03.14	Frankfurt am Main	Hessisches Wirtschaftsministerium	Behörde	nicht bekannt	Sanktionierte Unternehmen	Ministerium benennt versehentlich Börsensünder
03.03.14	Neufahrn	office discount Vertrieb für Bürobedarf GmbH	Unternehmen	nicht bekannt	Kunden	Office Discount verschickt Kontodaten in unverschlüsselten E-Mails
27.02.14	Bonn	Deutsche Telekom	Unternehmen	Millionen	Kunden	Telekom versendet vollständige Bankverbindungsdaten unverschlüsselt
14.02.14	Neuruppin	Jugend- und Betreuungsamt Neuruppin	Öffentliche Verwaltung	unbekannt	Klienten	Digitale Stifte verantwortlich für Datenpanne bei Jugendamt Neuruppin
12.02.14	Montabaur	1&1 Internet AG	Unternehmen	nicht bekannt	Kunden	1&1 versendet E-Mails mit kompletten Kontodaten
05.02.14	nicht bekannt	nicht bekannt			Nutzer von Fritzbox-Routern	Hacker kapern Fritzbox-Router
03.02.14	Köln	LobbyControl – Initiative für Transparenz und Demokratie e.V.	Verein	wenige	nicht bekannt	Intiative "LobbyControl" versendet E-Mails an falsche Empfänger
03.02.14	Aichach-Schrobenhausen	Unternehmen	Sparkasse Aichach-Schrobenhausen	mehrere Tausend	Kunden	Sparkasse Aichach-Schrobenhausen: Technischer Fehler bei externem Zahlungsdienstleister schuld an Datenpanne
01.02.14	Berlin	Gemeinsames Krebsregister	Behörde	26	Krebspatienten	Datenpanne beim Gemeinsamen Krebsregister
31.01.14	Saarland	Saarländische Polizei	Behörde	über 2.000	Saarländische Polizisten	Polizistenbewertungen versehentlich versendet

Aber auch das Gesetz hat an unterschiedlichen Stellen Regelungen getroffen, etwa in § 42a BDSG (Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten). Dort heisst es, „wenn festgestellt wird, dass personenbezogene Daten unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen, ist dies unverzüglich der zuständigen Aufsichtsbehörde sowie den Betroffenen mitzuteilen“.

Die Benachrichtigung des Betroffenen muss unverzüglich erfolgen, sobald angemessene Maßnahmen zur Sicherung der Daten ergriffen worden oder nicht unverzüglich erfolgt sind und die Strafverfolgung nicht mehr gefährdet wird. Die Benachrichtigung der Betroffenen muss eine Darlegung der Art der unrechtmäßigen Kenntniserlangung und Empfehlungen für Maßnahmen zur Minderung möglicher nachteiliger Folgen enthalten. Die Benachrichtigung der zuständigen Aufsichtsbehörde muss zusätzlich eine Darlegung möglicher nachteiliger Folgen der unrechtmäßigen Kenntniserlangung und der von der Stelle daraufhin ergriffenen Maßnahmen enthalten.

Soweit die Benachrichtigung der Betroffenen einen unverhältnismäßigen Aufwand erfordern würde, insbesondere aufgrund der Vielzahl der betroffenen Fälle, tritt an ihre Stelle die Information der Öffentlichkeit durch Anzeigen, die mindestens eine halbe Seite umfassen, in mindestens zwei bundesweit erscheinenden Tageszeitungen oder durch eine andere, in ihrer Wirksamkeit hinsichtlich der Information der Betroffenen gleich geeignete Maßnahme. Eine Benachrichtigung, die der Benachrichtigungspflichtige erteilt hat, darf in einem Strafverfahren oder in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen ihn oder einen in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen des Benachrichtigungspflichtigen nur mit Zustimmung des Benachrichtigungspflichtigen verwendet werden.

6.3 Kirchlicher Datenschutz (DSG-EKD und KDO-DV)

Die Kirchen als öffentlich-rechtliche Religionsgemeinschaften können innerhalb der geltenden Gesetze ihre Angelegenheiten selbstständig ordnen und verwalten. Dieses Selbstverwaltungsrecht ist im Grundgesetz und der Weimarer Verfassung garantiert und verhindert eine Beaufsichtigung und Kontrolle der Kirchen durch den Staat. Damit gilt der kirchliche Datenschutz auch für die dem Diakonischen Werk oder dem Deutschen Caritasverband angehörenden Einrichtungen, also für Krankenhäuser, Altenheime und andere Einrichtungsarten.

In der evangelischen Kirche gilt das im Jahr 1993 verkündete Datenschutzgesetz DSG-EKD, das von den Landes- bzw. Gliedkirchen mit ergänzenden Erlassen regional erweitert werden kann. Für die diakonischen Werke gelten damit die Regelungen ihrer jeweiligen Landeskirche zusammen mit dem DSG-EKD.
Die Katholische Kirche hat mit der Anordnung über den Kirchlichen Datenschutz (KDO) und die zugehörige Durchführungsanordnung (KDO-DV) einen vergleichbaren Erlass geschaffen. Dieser wurde durch alle 27 Erzbistümer und Bistümer förmlich in Kraft gesetzt. Auch in der katholischen Kirche wurden teilweise ergänzende datenschutzrechtliche Regelungen regional festgelegt.

Umfang und Geltungsbereich des Datenschutzes in kirchlichen Einrichtungen ist nicht nur von der Konfession und der jeweiligen Regionszugehörigkeit abhängig. Das evangelische Datenschutzrecht unterscheidet beispielsweise auch zwischen vier kirchlichen Stellen:

- Kirchliche Behörden
- Kirchliche Stellen (u. a. kirchliche Werke und Einrichtungen)
- Diakonisches Werk
- Sonstige Dienststellen

Es können unterschiedliche datenschutzrechtliche Regelungen Anwendung finden, je nach Abhgängigkeit und Zuordnung einer Einrichtung zu einer dieser Stellen.

Auch in der katholischen Kirche werden verschiedene Stellen unterschieden:

- Verantwortliche Stelle, die einem Bistum untersteht
- Verantwortliche Stelle, die einem Orden untersteht
- Caritas
- Kurie (Leitungs- und Verwaltungsorgane)

Hier ergeben sich durchaus Unterschiede, z. B. über das Amt und die Aufgaben des Datenschutzbeaftragten.

6.4 Schweigepflicht (§ 203 StGB)

Die ärztliche Schweigepflicht gilt nicht nur für private/gemeinnützige Organisationen, sondern im gleichen Maße auch für medizinische und soziale/pflegerische Einrichtungen der evangelischen und katholischen Kirche. So wurde die Orientierungshilfe Krankenhausinformationssysteme im Mai 2011 sowohl von den Datenschutzbeauftragten der evangelischen als auch von den Datenschutzbeauftragten der katholischen Kirche zustimmend zur Kenntnis genommen.

Es ist auch zu beachten, dass ein Tun auch in einem Nichtstun (Unterlassen) bestehen kann. Nach § 13 Abs. 1 StGB muss der Täter rechtlich dafür einzustehen haben, dass der Erfolg nicht eintritt. Dies ist der Fall, wenn der Täter eine sogenannte Garantenstellung zur Vermeidung des eingetretenen Erfolges innehat. Zu unterscheiden sind Garantenstellungen, die daraus entstehen, dass eine Person verpflichtet ist, Gefahren

von bestimmten Rechtsgütern abzuwehren (Beschützergarant) von Garantenstellungen, die daraus erwachsen, dass eine Person Gefahren, die von einer bestimmten Gefahrenquelle ausgehen, abschirmen soll (Überwachergarant). Im Bereich der Sozialwirtschaft dürfte diese Garantenstellung in vielen Fällen vorliegen.

Die Schweigepflicht entpuppt sich dabei gerade in der Zusammenarbeit mit externen IT-Dienstleistern als rechtlich schwierig zu lösender Bereich. Während die Auftrags-datenverarbeitung eine Einbindung von Hard- und Software-Lieferanten ermöglicht, werden im Rahmen einer Fernwartung sensibler personenbezogener Daten beispielsweise die Anforderungen der Schweigepflicht häufig verletzt. So sind die Forderungen des Strafgesetzbuches als ein wesentlciher Pfeiler einer IT-Compliance-Strategie besonders zu berücksichtigen.

7. Organisatorische Notwendigkeiten

Menschen, deren Leben durch eine Entscheidung berührt und verändert wird,
müssen an dem Prozess, der zu dieser Entscheidung führt,
beteiligt sein und gehört werden.
(John Naisbitt, amerikanischer Trend- und Zukunftsforscher)

Es ist erforderlich, dass das Projekt zur Umsetzung der Richtlinie zur „Chefsache" erklärt wird und volle Rückendeckung durch die Geschäftsführung erfährt. Genauso unersetzlich ist aber auch die Schaffung zahlreicher organisatorischer Voraussetzungen, um die notwendigen Rahmenbedingungen zu setzen, damit die IT-Compliance-Guideline auf einen erfolgreichen Weg gebracht werden kann. Dabei sind die im Folgenden vorgestellten Bausteine zu berücksichtigen:

- Ansprechpartner im Vorstand bzw. auf Leitungsebene
- Einbindung Datenschutzbeauftragter und Datenschutzkonzept
- Einbindung der Mitarbeitervertretung
- Einbindung IT-Sicherheitsbeauftragter (soweit vorhanden)
- Richtlinie zur IT-Nutzung
- Prozessbeschreibung für internes Kontrollsystem / Qualitätsmanagement

7.1 Ansprechpartner im Vorstand bzw. auf Leitungsebene

Eine Richtlinie zur IT-Compliance berührt die gesamte Organisation mit all ihren Mitarbeitern und Gremien. Es wird durch eine verbindliche Einführung in Arbeitsabläufe eingegriffen und gewohnte Verfahrensweisen müssen ggf. angepasst werden. Aus diesem Grund ist eine Einbeziehung aller Mitarbeiter und eine transparente Einführung eine wichtige Grundlage, um eine breite Akzeptanz und Kooperation im Unternehmen zu erreichen. Zur Umsetzung nötiger Veränderungen ist ein Projekt zur Etablierung einer solchen Richtlinie hierarchisch möglichst hoch anzugliedern und interdisziplinär zu besetzen.

Es empfiehlt sich, eine Projektorganisation aufzusetzen, die die beteiligten Gruppen einbindet, strukturiert und an deren Spitze, zum Beispiel als Vorsitzender eines Projektlenkungsausschusses, ein Mitglied auf Geschäftsführungsebene steht. Dieses Geschäftsführungsmitglied gibt die mit der IT-Compliance-Richtlinie zu erreichenden Ziele vor, legt eine eindeutige Projektleitung fest und lässt von den Projektteilnehmern einen Umsetzungsfahrplan erarbeiten.

Über Projektfortschritt und auftretende Probleme wird regelmäßig an den Projektlenkungsausschuss berichtet, so dass seitens der Geschäftsführung frühzeitig moderierend eingewirkt werden kann und notwendige Entscheidungen getroffen werden, damit sich kein Projektstillstand aufgrund nicht aufgelöster Konflikte ergibt. Die Notwendigkeit, kurzfristig nachhaltige und für alle verbindliche Entscheidungen herbeizuführen, macht deutlich, dass dies ausschließlich durch Vorstands- oder Geschäftsführungsebene sichergestellt werden kann.

7.2 Einbindung des Datenschutzbeauftragten

Ziel des Datenschutzes ist es, den Schutz personenbezogener Daten sicherzustellen, um natürliche Personen davor zu schützen, durch den Umgang mit ihren personenbezogenen Daten in ihren Persönlichkeitsrechten beeinträchtigt zu werden. Für die Einhaltung dieses Ziels ist der Datenschutzbeauftragte der Einrichtung oder ersatzweise ein bestellter Betriebsbeauftragter für den Datenschutz verantwortlich. Er trägt dafür Sorge, dass die einschlägigen Datenschutzgesetze auf Bundes-, Landes- und/oder institutioneller Ebene beachtet werden und stellt die dafür notwendigen Regelungen in einem Datenschutzkonzept dar.

Zwischen Datenschutz und IT-Compliance gibt es viele Parallelen und auch überschneidende Anforderungen, die gleiche Ziele verfolgen. Beispiele dafür sind Zutritts-, Zugangs- und Zugriffsberechtigungen, die aus Sicht beider Disziplinen auf das Notwendigste beschränkt sein sollten. Es besteht aber auch die Möglichkeit von Interessenkonflikten, wenn z.B. aus Compliance-Sicht möglichst viele Systemeingaben protokolliert werden sollen, um später beweissichernd darauf zurückgreifen zu können, während der Datenschutz

diese Protokollierungen überall dort, wo personenbezogene Daten betroffen sind, auf ein Mindestmaß reduziert wissen möchte.

Daraus ergibt sich, dass der Datenschutzbeauftragte in das Projekt IT-Compliance einzubinden ist, um die Belange des Datenschutzes ausreichend zu berücksichtigen sind. Die Regelungen eines bestehenden Datenschutzkonzeptes müssen in die einrichtungsindividuelle IT-Richtlinie einfließen und die Grundlage dieser bilden. Sollte ein ausformuliertes Datenschutzkonzept noch nicht existieren, besteht die Möglichkeit, dies als Teil der IT-Compliance-Richtlinie zu erstellen.

Grundlage für die IT-Compliance ist weiterhin, die Mitarbeitenden wirksam auf die Datenschutzbestimmung und die damit einhergehende Geheimhaltung verpflichtet zu haben. Bei der Verarbeitung personenbezogener Daten haben die Mitarbeiter/-innen für ihren Verantwortungsbereich und Arbeitsplatz die erforderlichen Vorkehrungen für die Einhaltung der Datenschutzbestimmungen zu treffen. Über die notwendigen Maßnahmen und Regelungen sind die Mitarbeitenden einzuweisen und müssen dies im Rahmen einer gesonderten Erklärung unterzeichnen.

7.3 Richtlinie zur IT-Nutzung

Ein weiteres Dokument, das als Voraussetzung zur Erstellung einer IT-Compliance-Guideline vorhanden sein muss, ist eine für alle Mitarbeitenden verbindlich anzuwendende Richtlinie zur IT-Nutzung. Diese regelt, in welcher Art und in welchem Umfang die Mitarbeiter/-innen die von der Einrichtung bereitgestellten IT-Anwendungen nutzen dürfen und welche Einschränkungen dabei zu beachten sind. Insbesondere sollte es hier Vorgaben für alle Anwendungen mit Schnittstellen in die Außenwelt geben, insbesondere zur E-Mail- und Internetnutzung, da hier der sensible Bereich der Datenweitergabe betroffen ist. Explizit zu regeln ist auch die Handhabung von mobil betriebenen Endgeräten wie Smartphones oder Notebooks sowie Zugriffe von außen auf das Netzwerk der Organisation, z. B. wenn Heimarbeitsplätze vereinbart sind.

Zu diesem Komplex gehören auch Regelungen zum Umgang mit Passwörtern und Benutzer-Kennungen oder das Verbot, selbständig IT-Anwendungen auf den bereitgestellten Arbeitsplatzgeräten zu installieren oder betriebsfremde Endgeräte im Netzwerk der Einrichtung ohne vorherige Zustimmung zu betreiben. Neben diesen organisatorischen Regelungen sollte immer der Grundsatz beachtet werden, nicht gewünschte Aktivitäten soweit wie möglich technisch durch die IT-Abteilung zu unterbinden.

7.4 Arbeitnehmer und Mitarbeitervertretung

Ein wichtiges Thema der IT-Compliance ist die Akzeptanz der aufgestellten Regelungen bei allen betroffenen Gruppen. Die größte Gruppe der Betroffenen stellen die Mitarbeitenden. Somit ist die Einbindung der Mitarbeitervertretung (MAV) in die Erarbeitung einer IT-Compliance-Richtlinie eine wichtige, vertrauensbildende und akzeptanzfördernde Maßnahme und in jedem Fall zu empfehlen.

Die Verpflichtung, inwieweit eine MAV-Einbindung geboten ist, ist von der Trägerschaft der Organisation und den dort anzuwendenden Regelungen und Vereinbarungen abhängig und kann durchaus unterschiedlich sein. In der Regel wird die Mitarbeitervertretung ein Informationsrecht haben, da das organisatorische Umfeld der von ihr vertretenen Mitarbeiter durch die Richtlinie unmittelbar beeinflusst wird. Unabhängig von einer rechtlichen Verpflichtung ist die Einbindung der MAV allein deshalb sinnvoll, um die oben beschriebene positive Wirkung auf die Akzeptanz der Belegschaft zu nutzen.

7.5 Regelungen für ein internes Kontrollsystem / Qualitätsmanagement

Ein im Rahmen des internen Qualitätsmanagement einzuführendes internes Kontrollsystem (IKS) stellt einen organisatorischen Rahmen für Änderungen an IT-Verfahren, insbesondere im Bereich des Rechnungswesens, dar. Damit soll die Verfügbarkeit der Systeme sowie die Authentizität und Integrität der Daten sichergestellt werden. Dolose Handlungen sind so zu vermeiden sowie die Grundsätze ordnungsgemäßer Buchführung (GoB/GoBS) zu gewährleisten. Es setzt sich zumeist aus hierarchisch aufgebauten Freigabemechanismen unter Berücksichtigung des 4-Augen-Prinzips und Dokumentationsvorschriften für durchgeführte Änderungen zusammen. Üblicherweise hat es den Charak-

ter einer Dienstanweisung und ist verbindlich von allen Nutzern eines IT-Verfahrens anzuwenden. Damit stellt es einen wichtigen Baustein einer IT-Compliance-Guideline dar. Sollte in einer Einrichtung kein separates IKS installiert sein, müssen die grundsätzlichen Regeln eines solchen Kontrollsystems Gegenstand der IT-Compliance-Richtlinie sein und können später als Basis für die Entwicklung eines korrespondierenden eigenständigen IKS dienen. Die organisatorischen Regelungen des IKS können durch die IT-Compliance-Richtlinie um technische Regeln ergänzt werden.

7.6 Einbindung eines IT-Sicherheitsbeauftragten (wenn vorhanden)

Das Ziel der Informationssicherheitspolitik ist es, die Verarbeitung, Aufbewahrung und Übermittlung von Informationen so zu gestalten, dass die Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit der Informationen gewährleistet wird.
Vertrauliche Informationen müssen vor unbefugter Preisgabe geschützt werden. Sie müssen vollständig und unverändert verfügbar sein und nur den dafür bestimmten Personenkreis zugänglich gemacht werden. Der Informationssicherheit kommt deshalb im Zusammenhang mit IT-Compliance eine zentrale Bedeutung zu.

Zwischen Informationssicherheit und Datenschutz gibt es zahlreiche Überschneidungen und Parallelen, aber auch deutliche Abgrenzungen. Während sich der Datenschutz um alle personenbezogenen Daten kümmert, schließt die Informationssicherheit alle schützenswerten Daten ein, also auch Betriebs- und Geschäftsgeheimnisse der eigenen Organisation oder auch von Geschäftspartnern. Aus diesen Aufgabenstellungen können durchaus konkurrierende Anforderungen erwachsen. Während der Aspekt der Informationssicherheit möglichst umfangreiche Aufzeichnungen über vorgenommene Datenerfassungen und -änderungen benötigt, sollten diese aus Sicht des Datenschutzes auf das unbedingt notwendige Maß beschränkt werden, sofern personenbezogene Daten betroffen sind. Aus diesem Grunde ist eine Aufgabentrennung bei der Wahrnehmung dieser Themenbereiche nicht nur sinnvoll, sondern erforderlich.

Um definierte Sicherheitsziele zu erreichen, ist es notwendig, alle dazu erforderlichen Maßnahmen unternehmensweit abzustimmen und funktional zu bündeln. Die getroffe-

nen Regelungen unterliegen einem stetigen Verbesserungsprozess, in dessen Rahmen sie überprüft und weiterentwickelt werden. Anpassungen sind zu dokumentieren und die zu Grunde liegenden Unterlagen immer auf aktuellem Stand zu halten.

Um diesen Anforderungen gerecht zu werden, empfiehlt sich die Benennung eines Informationssicherheitsbeauftragten, der die oben beschrieben Aufgaben wahrnimmt. Er darf nicht in Personalunion zum bestellten Datenschutzbeauftragten stehen. Er muss über die erforderlichen Fachkenntnisse verfügen und eine hohe Zuverlässigkeit besitzen. Der Informationssicherheitsbeauftragte wird bedarfsgerecht fortgebildet, um auf sich ändernde Anforderungen jederzeit angemessen reagieren zu können.
Somit kann der Informationssicherheitsbeauftragte die tragende Rolle bei der Umsetzung der IT-Compliance-Richtlinie spielen.

8. Fazit, nächste Schritte und Empfehlungen

„Man merkt nie, was schon getan wurde, man sieht immer nur, was noch zu tun bleibt."
(Maire Curie)

Dieser Ausspruch von Marie Curie umschreibt das Dilemma indem wir uns befinden, wenn wir uns mit IT-Compliance beschäftigen. Der erste Eindruck wird sein, dass sich ein weiterer Aufgabenberg auftürmt, der bearbeitet werden soll.

Dieses IT-Compliance Richtlinienpapier soll bei der Bestandsaufnahme helfen und Handlungsempfehlungen geben, um offene Punkte zielgerichtet abzuarbeiten. Das Thema IT-Compliance ist kein Modethema, sondern wird auch in der Sozialwirtschaft immer wichtiger. Informationstechnologie muss regelkonform gestaltet sein. Aus diesem Grund sind im zweiten Teil dieses Richtlinienpapiers eine Reihe von Checklisten enthalten, die bei der Beantwortung der Frage „Wie compliant ist meine Organisation?" helfen können (siehe Punkt 9.) Auf Basis dieser Arbeitshilfen wird das, was noch zu tun bleibt, für die eigene Organisation besser zu fassen sein.

Nach der ersten Bestandsaufnahme werden Sie feststellen, dass einige oder viele Themen in Ihrer Organisation bereits bearbeitet werden oder diese schon implementiert sind. Die Lücken gilt es strukturiert zu schließen. Diese Lücken können im Bereich Technik, Organisation oder Recht liegen (T/O/R- Prinzip). Es ist deshalb geboten, dass die Umsetzung der IT-Compliance-Themen auf Geschäftsführungs-/Vorstandsebene anzusiedeln ist.

Eine weitere wichtige Erkenntnis sollte sein, dass mit der Implementierung von IT-Compliance die Wertschöpfung und die Qualität der Arbeit in der Sozialwirtschaft gesteigert werden. Themenbereiche werden nicht „doppelt" bearbeitet, sondern ergänzen sich. Deutlich wird dies an den Themen Datenschutz und IT-Sicherheit. Beides sind auch Themen, die in einer IT-Compliance-Richtlinie Einzug halten bzw. die aus der IT-Compliance erwachsen können, wenn diese noch nicht als Einzelthemen in der Organisation verhaftet sind.

Wir hoffen, dass wir mit diesem Positionspapier aufzeigen konnten, dass sich dieses Projekt gut in überschaubare Einzelaufgaben darstellen lässt. So lassen sich kurzfristige Erfolge sichtbar machen. Wichtig ist in unseren Augen die Erkenntnis, dass mit einer Richtlinie zur IT-Compliance nicht die gesamte Organisation verändert wird. Das kann Mitarbeitern/Beteiligten Angst machen. In der Umsetzung sollte das Thema IT-Compliance als kontinuierlicher Verbesserungsprozess gesehen werden (Methode Kaizen), an dem die Mitarbeiter maßgeblich beteiligt sind.

Soll IT-Compliance in der Organisation mit eigenen Mitarbeitern umgesetzt werden, kann die Fortbildung der FinSoz-Akademie zum „IT-Compliance-Beauftragter der Sozialbranche“ einen hilfreichen Einstieg darstellen. Im Rahmen weiterer Akademie-Angebote und der in Planung befindlichen Zertifizierung „SECU-ZERT“ auf Basis von IT-Grunschutz-Bausteinen unterstützt FINSOZ auch bei weiteren Schritten im IT-Compliance-Umfeld.

Zuerst sind jedoch die Geschäftsführungen und Vorstände gefragt, um den Stein ins Rollen zu bringen und damit die Organisation für die Zukunft fit zu machen und weitere Potentiale zur Steigerung der Qualität und Wertschöpfung freizulegen.

9. Checklisten

Als praktische Ergänzung zu dieser IT-Compliance Guideline wurden von der FINSOZ-Arbeitsgruppe IT-Compliance Checklisten erstellt. Mit ihrer Hilfe kann der eigene Umsetzungsgrad im Bereich IT-Compliance gesteuert und überprüft werden. Für FINSOZ-Mitglieder stehen diese Checklisten kostenfrei zur Verfügung und können bei der Geschäftsstelle angefordert werden.
Für Nicht-Mitglieder wird eine Schutzgebühr von 50,– € erhoben.