baum · reiter & collegen
RECHTSANWÄLTE

Compliance und Datenschutz in Kliniken

„Datenschutz in der Medizin – Update 2019“, Wiesbaden, 07.05.2019

Rechtsanwalt Dr. Olaf Methner
Fachanwalt für IT-Recht und Arbeitsrecht

Wer sind wir?

- 2001: Gründung der heutigen Kanzlei baum reiter & collegen durch Prof. Dr. Julius Reiter und Dr. Olaf Methner
- Seit 2007: weiterer Partner/Namensgeber Gerhart Baum, Bundesinnenminister a.D.
- Kanzleistruktur: 4 Partner, 11 angestellte Rechtsanwälte, ca. 30 Mitarbeiter Office + juristische Hilfskräfte
- Mandanten: Kommunen, Unternehmen (Geschäftsleitungen, Betriebsräte), Verbraucher

Tätigkeitsschwerpunkte

- Compliance
  - Auszeichnung Wirtschaftswoche „Top 25 Compliance-Anwälte“
  - Öffentliche bekannte Mandate z.B. Sonderermittlung in der Telekom-Bespitzelungsaffäre und in der Datenschutzaffäre der Deutschen Bahn
  - Complianceberichte
  - Compliance- und Antikorruptionsschulungen
  - Beratung zu Hinweisgeber-Systemen; Ombudsstelle für anonyme Tippgeber
- Arbeitsrecht
- IT-Recht (Schwerpunkt Datenschutzrecht)
- Bank- und Kapitalmarktrecht
- Verfassungsrecht (z.B. erfolgreiche Verfassungsbeschwerden gegen Online-Durchsuchung und Vorratsdatenspeicherung)
- Opferschutz (Germanwings-Absturz, Loveparade-Katastrophe)
- Verbraucherschutz (VW-Abgasskandal)
- Sachverständige in Gesetzgebungsverfahren im Deutschen Bundestag

Unsere aktuelle Compliance-Erfahrung

- Beratung von Kommunen im Bereich Datenschutz/IT-Recht
- Beratung von Unternehmen/Arbeitnehmervertretern (u.a. DAX-Konzern; Rechtsschutzversicherung) bei der Einführung von Hinweisgeber-Systemen sowie anderen Themen des Compliance-Managements und Beschäftigtendatenschutzes
- Jährlicher Compliance-Bericht für ein beliehenes Unternehmen im Kfz-Bereich
- Compliance- und Antikorruptionsschulungen eines kommunalen IT-Dienstleisters
- Veröffentlichungen (u.a.):
  - Reiter, Methner u.a.: „Mit Compliance Wirtschaftskriminalität vermeiden“, Schäffer-Pöschel-Verlag 2013
  - Reiter, Methner: „Compliance“ in Jäschke (Hrsg.), „Datenschutz im Gesundheitswesen“, MVV Verlag, 2. Aufl. 2018
  - Reiter, Methner: „Rechtliche Rahmenbedingungen für CSR und Compliance“ in Kleinfeld/Martens (Hrsg.), „CSR- und Compliance-Management“, Springer Gabler Verlag 2018

Süddeutsche.de

2. April 2019, 18:46 Neue Verordnung Firmen, die den Datenschutz missachten, müssen jetzt zahlen

• Öffentliche Unternehmen müssen die neue Grundverordnung umsetzen, wie Bayerns oberster Datenschützer Thomas Petri mahnt.

• Derzeit gibt es für sie noch eine Schonfrist, doch schon bald drohen bei einem Verstoß empfindliche Geldbußen.

• Petri hat bereits einige bemerkenswerte Vorfälle in Kliniken registriert.

Von Lisa Schnell Öffentlich geführte Unternehmen wie Kliniken oder Stadtwerke müssen in absehbarer Zeit mit teils hohen Bußgeldern rechnen, wenn sie sich nicht ernsthaft bemühen, die neue Datenschutzgrundverordnung umzusetzen. Fast ein Jahr nach der Einführung warnt der Datenschutzbeauftragte der Staatsregierung Thomas Petri: "Nehmt die neuen Regeln ernst, wir machen auch ernst."

Als oberster Hüter über den Datenschutz in Bayern kann Petri seit der Einführung der DSGVO Bußgelder verhängen. Als Ordnungsbehörde ist er sogar dazu verpflichtet, wenn öffentliche Wettbewerbsunternehmen wie Kliniken dagegen verstoßen. Der Bußgeldrahmen geht bis zu 20 Millionen Euro.

Compliance in Kliniken: Schon Alltag oder „unentdecktes Terrain“?

2017: Studie „Compliance im Klinikmarkt“ von Ernst & Young

Ergebnisse:

- Nur 16,2 % der befragten Kliniken verfügten über kein Compliance-Management-System (CMS).
- 52,8 % der Kliniken haben ihr CMS beim Vorstand oder der Geschäftsführung angesiedelt. Meistens handelte es sich bei den Compliance-Beschäftigten um Ärzte oder sonstige Personen mit medizinischer Ausbildung.
- 81 % der Befragten meinten, dass das CMS Straftaten nicht verhindern konnte. Hauptdelikte: Abrechnungsbetrug (35,6 %), Arbeitsschutz/-recht und Hygiene (27,5 %), Datenschutz (12,6 %)
- Nur 16 % der Krankenhaus-Manager bekannten sich klar zu Ethik und Integrität.
- 38 % der Befragten hatten Ziele und konkrete Vorgaben fürs Compliance-Management formuliert.

Fazit: Durch CMS müssen Mitarbeiter ein schärferes Bewusstsein für Formen des Fehlverhaltens entwickeln.

III. Compliance und ihre Ziele

Compliance bedeutet Rechts- und Regelkonformität, also die Übereinstimmung des Handelns der Unternehmensleitung, der Beschäftigten und anderer im Betriebsablauf eingebundener Personen mit der Rechtsordnung, betrieblichen und sonstigen Regeln.

Welche Ziele verfolgt Compliance? Mindeststandards nach der Rechtsprechung:

- Prävention zur Vermeidung von Schäden und Sanktionen
- Unternehmensleitung und Beschäftigte sollen vor Fehlverhalten bewahrt werden, das auf Unwissenheit oder Fahrlässigkeit beruht (Frühwarnsysteme!).
- Soziale Vorteile durch harmonische Zusammenarbeit im Betrieb
- Imagegewinn
- Einhaltung von Werten
- Handlungen halten internen Kontrollen und öffentlichen Prüfungen stand.

Nicht jedes Verhalten ist gut oder sinnvoll, nur weil es die Grenzen des rechtlich Vertretbaren nicht überschreitet.

Die Compliance-relevanten Rechtsgebiete sind:

- & Arbeitsrecht
- & IT-Recht (IT-Sicherheit und Datenschutz)
- & „Healthcare Compliance“ (z.B. Arzneimittelsicherheit)
- & Strafrecht
- & Ordnungswidrigkeitenrecht
- & Steuerrecht
- & Vergaberecht (im öffentlichen Bereich)
- & Kartellrecht
- & Umweltrecht
- & Qualitätsmanagement

Was sind die Konsequenzen bei Nicht-Compliance? (1)

- Ineffektivität und Ineffizienz
- Vertrauens- und Reputationsverlust
- Staatliche Ermittlungsverfahren
- Verlust/Gefährdung von Arbeitsplätzen
- Verhängung von Strafen und Geldbußen
- Schadensersatzpflichten
- Leitungspersonen konzentrieren sich auf Verteidigungsaktivitäten und nicht auf die Kernaufgaben.

Welche sind die Konsequenzen bei Nicht-Compliance? (2)

Schadensrecht	Strafrecht	OWiG	Arbeitsrecht/ Dienstrecht	Reputationsschaden
Schadenersatz-ansprüche, §§ 630a ff., 823 ff. BGB	Betrug § 263 StGB	§ 30 OWiG (iVm. Straftat oder Ordnungswidrigkeit)	Abmahnung	Fehlerhaftes Verhalten führt nicht zwingend zu wirtschaftlichen Schäden. Jedoch können Vertrauens- und Reputationsschäden für Kliniken, Geschäftsleitungen sowie für den einzelnen Mitarbeiter gleichermaßen schwerwiegendere Folge darstellen.
	Untreue § 266 StGB	§ 130 OWiG	Kündigung	
	Datenschutzverstöße, §§ 41, 42 BDSG		Disziplinar-maßnahmen	
	Fahrlässige Körperverletzung § 229 StGB		Mitarbeiter-Regress	

Welche sind die Konsequenzen bei Nicht-Compliance? (3)

§ 30 OWiG
Haftung der juristischen Person bei Straftat oder Ordnungswidrigkeit einer Leitungsperson

§ 130 OWiG
Haftung wegen Aufsichtspflichtverletzung

Bußgeld
Bei Vorsatz: bis zu 10 Mio. EUR
Bei Fahrlässigkeit: bis zu 4 Mio. EUR
Alternativ: Gewinnabschöpfung

Bußgeld
Bei Straftat: bis zu 1 Mio. EUR
Bei Ordnungswidrigkeit: Siehe OWiG
Alternativ: Gewinnabschöpfung

Wer haftet: Unternehmen, Leitungspersonen und/oder Mitarbeiter?

	Schadens-recht	Strafrecht	OWiG	Arbeitsrecht/ Dienstrecht	Reputations-schaden
Unternehmen	x		x		x
Leitungs-personen		x	x	x	x
Sonstige Mitarbeiter		x		x	x

Ein Compliance-Management-System (CMS) besteht aus:

- & Organisationsform
- & Organisationsprinzipien
- & Compliance-Maßnahmen
- & Compliance-Überwachung
- & Compliance-Optimierungen (soweit erforderlich)

VII. Lösung: Schutz der Klinik und der Mitarbeiter durch CMS-System

Einerseits: BGH, Urteil vom 09.05.2017, Az. 1 StR 265/16

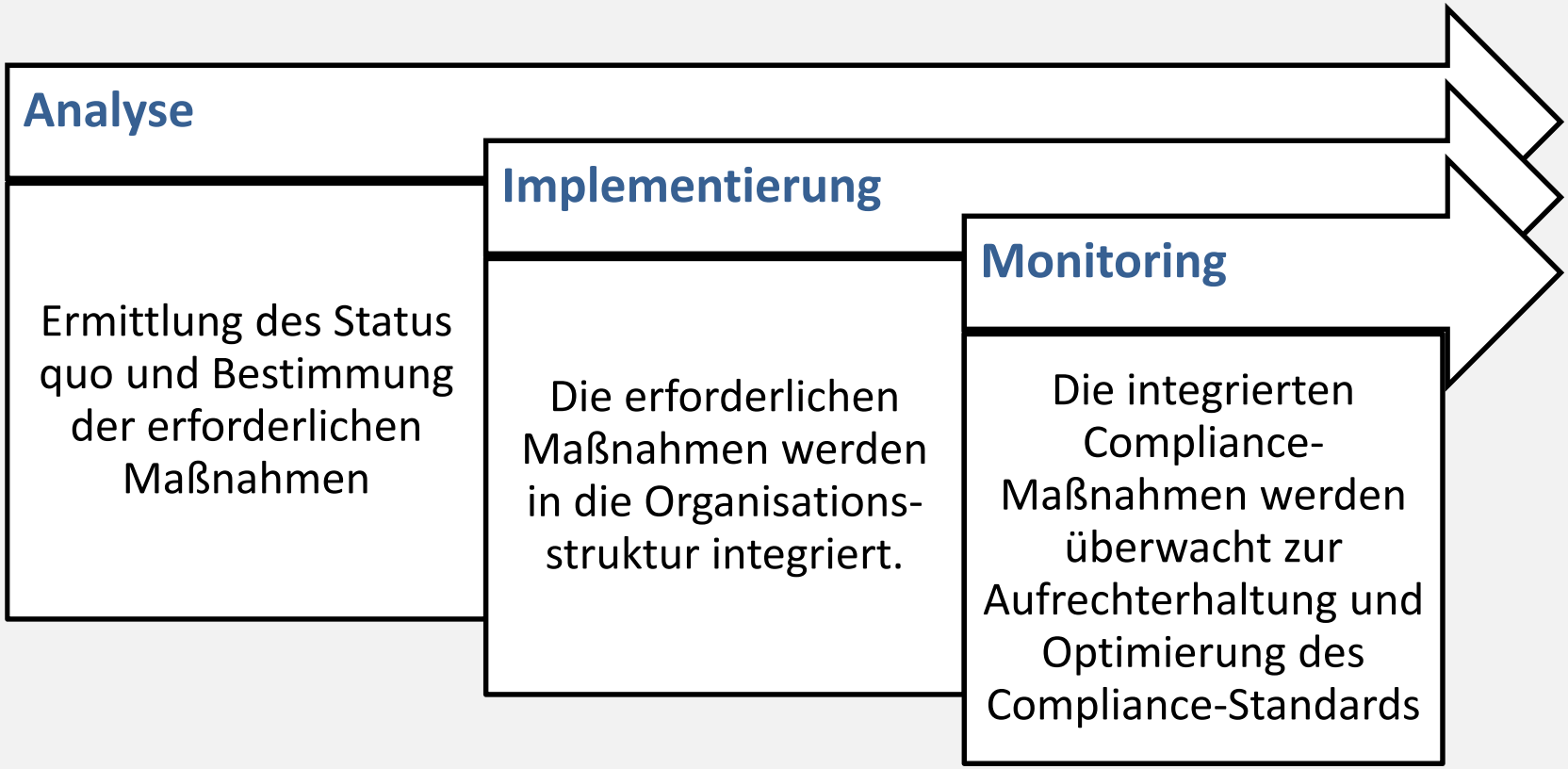
Nach § 30 OWiG können juristische Personen mit erheblichen Verbandsgeldbußen sanktioniert werden. Der BGH hat nun höchstrichterlich festgestellt, dass die Implementierung eines effektiven Compliance-Management-Systems, das auf die Vermeidung von Rechtsverstößen ausgelegt sein muss, bußgeldmindernde Wirkung haben kann.

Andererseits: LG München I, Urteil vom 10.12.2013, Az. 5 HKO 1387/10

Die Geschäftsleitung eines Unternehmens muss allgemein ein Compliance-System einrichten, damit das Unternehmen und seine Mitarbeiter keine Gesetzesverletzungen begehen. Der Verzicht auf ein solches System oder die mangelhafte Überwachung des Systems bedeuten per se eine Pflichtverletzung.

VII. Lösung: Schutz der Klinik und der Mitarbeiter durch CMS-System

Drei Schritte zum wirksamen Compliance-Management-Systems:



Zu 1: Analyse des Status quo

- Die Analyse muss sich auf sämtliche Teilrechtsordnungen erstrecken, die Gegenstand des Verwaltungshandelns sein können.
- Typische Schwachstellen finden sich in den Bereichen:
  - Personalwesen
  - IT-Wesen (IT-Sicherheit; Datenschutz)
  - Beschaffungswesen
- Die Risiken, Schwachstellen und typische Fehler sowie deren Ursache innerhalb eines Bereiches werden ermittelt und klassifiziert.
- Passende und bewährte Compliance-Maßnahmen können ausgewählt werden.

Zu 2: Mögliche Bestandteile eines Compliance-Management-Systems

Organisation

Form

- & Interne oder externe Organisation
- & Vollständig oder nur für Teilbereiche
- & Compliance als eigenständige Organisationseinheit oder Integration in bestehende Abteilung
- & Ausführung durch haupt- oder nebenamtliche Mitarbeiter

Prinzipien

- & Verantwortungsprinzip
- & Dokumentationsprinzip
- & Mehraugenprinzip
- & Fortbildungsprinzip
- & Evaluierungsprinzip
- & Sanktionsprinzip
- & Verhältnismäßigkeitsp.
- & Sonstige…

Maßnahmen

- & Maßnahmen zur Entgegenwirkung festgestellter Risiken und Schwachstellen
- & Füllung von Wissenslücken durch Beratung und Schulungen
- & Kontrollmechanismen
- & Hinweisgebersysteme
- & Aufdeckungs- und Ermittlungsmanagement
- & Reaktions- und Sanktionsmanagement
- & Notfallszenarien
- & Dokumentation: Compliance-Handbuch
- & Verantwortung: Ggf. Compliance-Officer u. Antikorruptionsbeauftragter

Schritt 1: Vorbeugung/Organisation

- Aufbau von Organisationsstrukturen
- Klarstellung von Verantwortlichkeiten (Risikoüberwachung)
- Kommunikation gegenüber Mitarbeitern (Broschüre; Intranet)
- Dienstanweisungen
- Schulungen
- Aktualisierungen/Anpassungen an Rechtslage (z.B. Datenschutz) oder technischen Fortschritt (z.B. Datensicherheit)

Schritt 2: Ermittlung

- Bei objektiven Hinweisen auf Fehlverhalten oder Gesetzesverstöße: interne Ermittlungen (z.B. Anhörungen; ggf. Computerauswertungen unter Beachtung des Beschäftigtendatenschutzes)
- Ggf. Einschaltung externer (neutraler) Ermittler
- Bestimmte Ermittlungsmethoden ausschließlich Polizei/Staatsanwaltschaft vorbehalten!

Schritt 3: Konsequenzen/Dokumentation

- Keine Ermittlung nur zur Ermittlung!
- Arbeits- und strafrechtliche Konsequenzen zumindest zu prüfen!
- Verzicht auf Sanktionen muss begründet werden.
- Ggf. Fehleranalyse und –behebung (Organisation)
- Dokumentation: Organisationsstruktur, Ermittlung, Folgen (Sanktionen oder Verzicht hierauf, Fehleranalyse und –behebung)

Compliance zur Korruptionsbekämpfung:

- Aufklärung/Schulung über „Was ist erlaubt?“ und „Was ist verboten?“
- Aufklärung über mögliche Sanktionen
- Klare (vertraglich vereinbarte) Vorgaben des Arbeitgebers
- Anzeige- und Mitteilungspflichten gegenüber dem Arbeitgeber bei Erhalt oder dem Angebot von Vergünstigungen oder Belohnungen
- Hinweisgebersysteme (siehe gleich)

Was bedeutet „Hinweisgebersysteme“?

& Alle Regelungen im Unternehmen, die im Zusammenhang mit Hinweisen und der Organisation ihrer Umsetzung stehen.

& Beispiele:

- Telefon-Hotline;
- E-Mail-Postfach;
- Online-Meldesystem;
- Ombudsleute

Wozu dienen „Hinweisgebersysteme“?

& Repression: Aufdeckung von Fehlverhalten; Verbesserung von Kontrollmechanismen

& Prävention: Wegen des erhöhten Entdeckungsrisikos wird Fehlverhalten verhindert.

Was kann Inhalt von Hinweisen sein?

- Kriminelle Handlungen: Betrug, Untreue, Diebstahl, Korruption
- Missstände im operativen Geschäft
- Sonstiges Fehlverhalten: Mobbing, Diskriminierung, Verstöße gegen Arbeitsschutz etc.

Welche Überlegungen sprechen für Hinweisgebersysteme?

- Rechtliche Gründe: Rechtssicherheit für Arbeitnehmer, die Missstände entdecken; Enthaftung für Leitungspersonen
- Risikoerkennung und –vermeidung: Ergänzung zu eigenen Kontrollen/ Reportings des Unternehmens; Ordnung und Strukturierung von Untersuchungen und Kommunikationsprozessen
- Unternehmenskultur: Wichtigkeit der Mitarbeiter; Generalprävention

VII.B.3. Konkret: Hinweisgebersysteme - Ombudsleute -

Was sind die Vorteile eines Ombudswesens?

- Ombudsleute können als eigenständige externe Ansprechpersonen oder auch als integraler Bestandteil eines Hinweisgebersystems verwendet werden.
- Ombudsleute bieten persönlichen Kontakt.
- Ombudsleute bieten persönliches Vertrauen.

Welche Anforderungen müssen Ombudsleute erfüllen?

- Integrität; Gewährleistung absoluter Vertraulichkeit und Verschwiegenheit (Rechtsanwälte: strafbewehrte Verschwiegenheitspflicht, § 43a BRAO, § 203 I Nr. 3 StGB; Aussageverweigerungsrecht, § 53 I Nr. 3 StPO)
- Rechtliche und wirtschaftliche Fachkenntnisse und Erfahrung
- Kenntnisse der Abläufe und Organisation im Unternehmen

Wie kann das Ombudswesen im Unternehmen eingeführt werden?

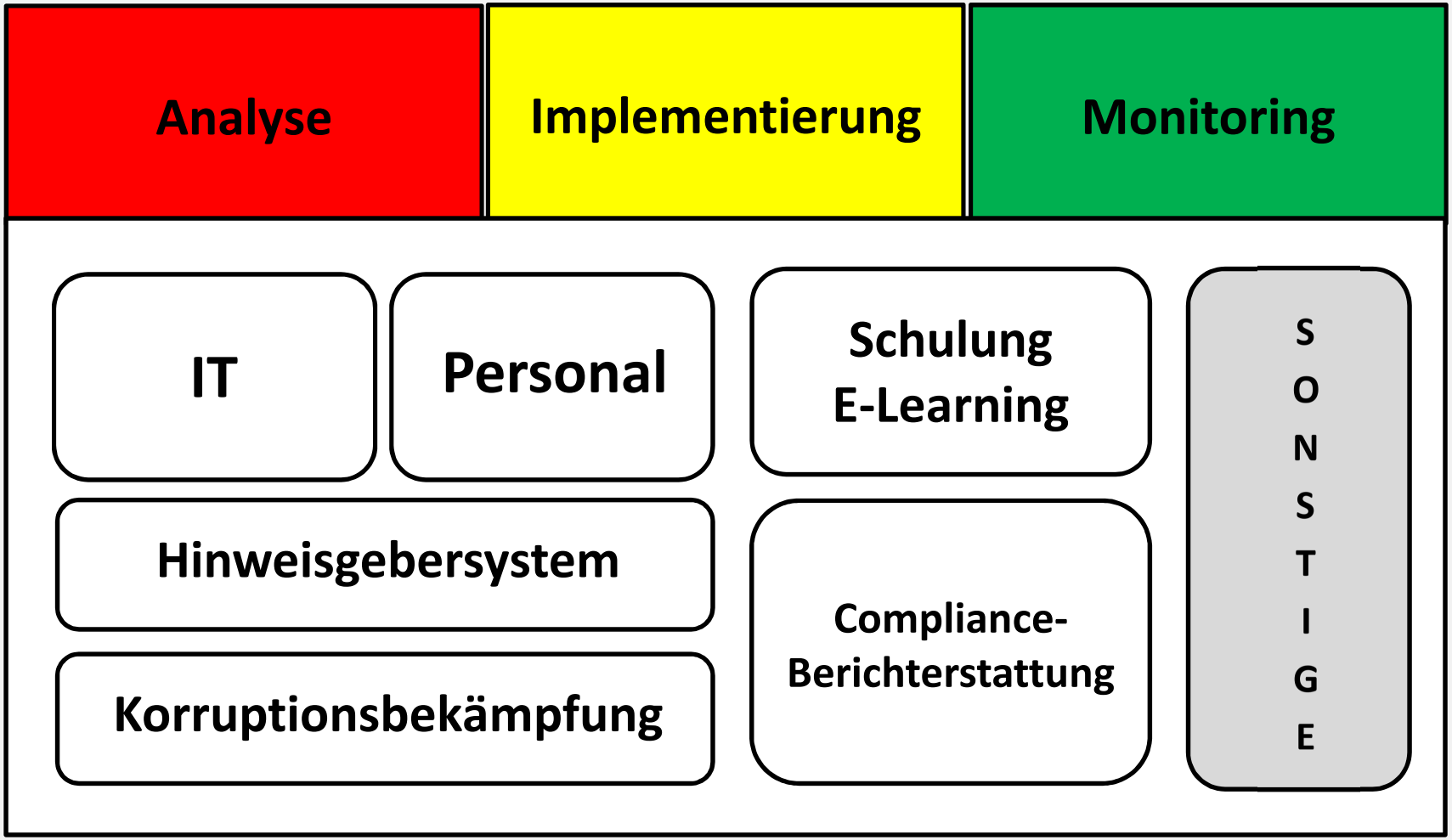
- Mitarbeiter müssen frühzeitig einbezogen und informiert werden: Die Akzeptanz und das Vertrauen der Mitarbeiter in die Integrität der Ombudsleute ist wesentlich für Erfolg und Effektivität des Ombudswesens.

- Vorbehalte gegen Hinweisgeber („Verräter“, „Denunzianten“) müssen von Anfang an verhindert werden: Das Ombudswesen kann als Förderung des gemeinschaftlichen Unternehmenszwecks zur kontinuierlichen Optimierung der Arbeitsbedingungen und Verhinderung von Fehlentwicklungen dargestellt werden.

Zu 3: „Sicherung der Sicherung“

- Durch Überwachung soll die ständige Compliance-Organisation und die Kontrolle ihrer Sicherungssysteme gewährleistet werden
- Lücken sollen aufgedeckt und geschlossen werden
- Anpassungen an neue Gegebenheiten oder neue Rechtslagen sind möglich
- Berichterstattung durch Compliance-Bericht

VIII. Was können wir für Sie tun?



baum · reiter & collegen

RECHTSANWÄLTE

Dr. Olaf Methner
Fachanwalt für IT-Recht
Fachanwalt für Arbeitsrecht
Fachanwalt für Bank- und Kapitalmarktrecht

Benrather Schlossallee 101 • 40593 Düsseldorf
Tel.: 02 11 - 836 805 70 • Fax: 02 11 - 836 805 70
E-Mail: kanzlei@baum-reiter.de • Web: www.baum-reiter.de