2. Vorschriften und Empfehlungen

Im Folgenden werden Vorschriften und (zwingende) Empfehlungen aus gesetzlichen Anforderungen, Verordnungen und Fachgutachten sowie internationale und nationale Standards erläutert und damit verbundene Fragestellungen diskutiert. Ein Anspruch auf Vollständigkeit kann nicht abgeleitet werden, da insbesondere Branchen- und Unternehmensspezifika nicht berücksichtigt werden können. Es ist daher sinnvoll, auf weiterführende Literatur (siehe Literaturverzeichnis) zu den jeweiligen Bereichen zurückzugreifen.

2.1. Gesetze und Verordnungen in Österreich

Eine der zentralen gesetzlichen Vorgaben im Zusammenhang mit dem Informationsmanagement in Österreich stammt aus dem Jahr 1997 und wurde im Rahmen des damaligen Insolvenzänderungsgesetzes in das GmbH-Gesetz sowie in das Aktiengesetz aufgenommen. Dabei wurde die Einführung eines angemessenen Internen Kontrollsystems als ein verpflichtendes Kriterium definiert. Diese oftmals diskutierte und zugleich sehr wenig konkrete Beschreibung bildet die Grundlage einer Vielzahl von Anforderungen, insbesondere aber des Erfordernisses, Kontrollen für Risiken, die im Bereich des Informationssystems existieren, zu implementieren.

Aus abgaben- und unternehmensrechtlicher Sicht (Bundesabgabenordnung, Unternehmensgesetzbuch) wird eine vollständige, geordnete, inhaltsgleiche, urschriftgetreue und nachvollziehbare Darstellung von Geschäftsfällen und Aufzeichnungen gefordert. Insbesondere Nachweise für die Nachvollziehbarkeit und Vollständigkeit sind aufzuzeichnen bzw. Bücher sind zu führen.

2.1.1. Datenschutzgesetz 2000 (DSG); Fassung vom 7.7.2016

Das Datenschutzgesetz befasst sich mit dem Schutz vor missbräuchlicher Datenverwendung von personenbezogenen Daten, wobei zwischen personenbezogenen und sensiblen Daten zu unterscheiden ist.

Personenbezogene Daten sind nicht nur der Name, das Geburtsdatum, die Adresse bzw. die Sozialversicherungsnummer, sondern darunter fallen auch Videoaufzeichnungen, Fotos und Stimmaufnahmen von Personen sowie biometrische Daten wie etwa Fingerabdrücke, da anhand dieser die Identität bestimmt oder bestimmbar ist. Zu den sensiblen Daten zählen rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit oder z.B. Informationen zur Gesundheit.

Im Zusammenhang mit dem ISMS ist § 14 des DSG hervorzuheben. Darin wird festgehalten, dass für alle Organisationseinheiten eines Auftraggebers oder Dienstleisters, die Daten verwenden, Maßnahmen zur Gewährleistung der Datensicherheit zu

treffen sind. Unter diese fallen Zugriffsberechtigungen, Vorschriften für Mitarbeiter sowie Protokollierung. Ferner wird betroffenen Personen in §§ 27 und 28 das Recht auf Richtigstellung oder Löschung von Daten eingeräumt, das von den Unternehmen technisch und organisatorisch umzusetzen ist.

Folgende Fragestellungen ergeben sich im Zusammenhang mit dem Datenschutzgesetz:

Fragen für Prüfungsplanung und -durchführung

- Wurde eine Datenklassifizierung eingeführt, um Fragestellungen des Datenschutzgesetzes hinreichend zu adressieren?
- Wurden Maßnahmen ergriffen, die die Gewährleistung der Datensicherheit betreffen, und können diese nachvollzogen werden?
- Befasst sich im Unternehmen eine Person mit datenschutzrechtlichen Anforderungen und stellt diese sicher, dass Neuregelungen im ISMS berücksichtigt werden?

2.1.2. Arbeitsverfassungsgesetz

Im Zusammenhang mit dem ISMS ist auch das Arbeitsverfassungsgesetz zu nennen, wenngleich es nicht das erste Gesetz ist, das man üblicherweise einbeziehen würde. In diesem werden unter anderem Mindestlohn und Kündigungsschutz beschrieben, vor allem für das ISMS haben aber die darin festgelegten Rechte und Pflichten des Betriebsrates wesentliche Bedeutung. Dabei ist bei Auswertungen von mitarbeiterbezogenen Daten und Protokollen zu berücksichtigen, dass personenbezogene Daten nur für den Zweck verwendet werden dürfen, für den sie erhoben wurden. Für allgemeine Analysen ist daher eine Analyse ohne Personenbezug zu bevorzugen, da in diesem Fall keine spezifischen Anforderungen im Zusammenhang mit der Einbindung des Betriebsrats zu berücksichtigen sind.

Ansonsten sind personenbezogene Auswertungen jedenfalls sehr kritisch bzw. als unzulässig zu betrachten, wenn schutzwürdige Interessen von Personen betroffen sind (Daten-Screening von Mitarbeitern, Bildaufnahmen, Videoüberwachung etc.). Möglicherweise zulässig sind prozessabhängige Prüfungen von Geschäftsfällen und bei begründetem Verdacht.

Folgende Fragestellungen ergeben sich im Zusammenhang mit dem Arbeitsverfassungsgesetz:

Fragen für Prüfungsplanung und -durchführung

- Kennen wir die für unsere Analysen und Auswertungen relevanten Einschränkungen hinsichtlich schutzwürdiger Interessen?
- Wurde definiert, wann und in welchem Ausmaß der Betriebsrat einbezogen werden muss?

2.1.3. Telekommunikationsgesetz

Die Zielsetzung des Telekommunikationsgesetzes 2003 war neben der Regelung für Anbieter von Telekommunikationsdiensten die Sicherstellung eines chancengleichen und funktionsfähigen Wettbewerbs sowie die Sicherstellung von Integrität und Sicherheit von öffentlichen Kommunikationsnetzen. Im Zusammenhang mit dem ISMS ist hier der häufig diskutierte Bereich der Vorratsdatenspeicherung von Bedeutung. Dabei handelt es sich um die Speicherung aller Kommunikationsdaten von Telefon- und Internetnutzern über einen Zeitraum von sechs Monaten für Ermittlungsbehörden bei Verdacht, dass der Nutzer ein strafrechtlich relevantes Delikt begangen hat. In Österreich ist die Vorratsdatenspeicherung seit 1. Juli 2014 nicht mehr zulässig. Verbindungsdaten dürfen nur mehr zur Abrechnung verwendet werden.

Folgende Fragestellungen ergeben sich im Zusammenhang mit dem Telekommunikationsgesetz:

Fragen für Prüfungsplanung und -durchführung

- Hat eine Klärung stattgefunden, ob in Teilbereichen das Unternehmen Anbieter von Telekommunikationsdiensten (z.B. E-Mail) ist?
- Wie wurde sichergestellt, dass Kommunikationsdaten für existierende Telekommunikationsdienste nicht gespeichert werden?

2.1.4. Signaturgesetz

Im Rechts- und Geschäftsverkehr können Signaturverfahren mit unterschiedlichen Sicherheitsstufen und Zertifikatsklassen für die Kommunikation von Information und Daten verwendet werden. Die expliziten Anforderungen an diese Signaturverfahren wurden in Österreich im Signaturgesetz festgehalten, wobei eine sichere elektronische Signatur grundsätzlich das rechtliche Erfordernis einer eigenhändigen Unterschrift erfüllt. Durch die mittlerweile im Zusammenhang mit den abgabenrechtlichen Anforderungen adaptierten Anforderungen (siehe Umsatzsteuerrichtlinie) hat die elektronische Signatur bei elektronischen Rechnungen an Bedeutung verloren. Insbesondere im E-Mail-Verkehr, aber auch für die Sicherstellung des Manipulationsschutzes bei Kassensystemen haben Signaturen noch Relevanz.

Folgende Fragestellung ergibt sich im Zusammenhang mit dem Signaturgesetz:

Fragen für Prüfungsplanung und -durchführung

- Wurden im Unternehmen Überlegungen angestellt, Signaturen einzusetzen, und, wenn ja, entsprechen die eingesetzten Verfahren den für diesen Zweck genannten Anforderungen (z.B. eigenhändige Unterschrift, Sicherstellung der sicheren Übermittlung von Daten)?

2.1.5. Dienstnehmerhaftpflichtgesetz

Fügt ein Arbeitnehmer dem Dienstgeber bei Erbringung seiner Arbeitsleistung einen Schaden zu, so kommen die Bestimmungen des Dienstnehmerhaftpflichtgesetzes zur Anwendung. Dabei ist jedenfalls von Relevanz, dass von einer entschuldbaren Fehlleistung immer dann auszugehen ist, wenn dem Arbeitnehmer nur ein geringfügiges Versehen vorgeworfen werden kann. Bei der Bemessung des Verschuldens des Dienstnehmers ist auf folgende Umstände Bedacht zu nehmen:

- auf das Ausmaß der mit der ausgeübten Tätigkeit verbundenen Verantwortung,
- inwieweit bei der Bemessung des Entgelts ein mit der ausgeübten Tätigkeit verbundenes Wagnis berücksichtigt worden ist,
- auf den Grad der Ausbildung des Dienstnehmers,
- auf die Bedingungen, unter denen die Dienstleistung zu erbringen war, und
- ob mit der vom Dienstnehmer erbrachten Dienstleistung erfahrungsgemäß die nur schwer vermeidbare Möglichkeit oder Wahrscheinlichkeit des Eintritts eines Schadens verbunden ist.

Folgende Fragestellungen ergeben sich im Zusammenhang mit dem Dienstnehmerhaftpflichtgesetz:

Fragen für Prüfungsplanung und -durchführung

- Wurden im Unternehmen ausreichende Vorkehrungen getroffen, Mitarbeiter hinsichtlich ihrer Verantwortung im Zusammenhang mit dem ISMS zu sensibilisieren?
- Sind entsprechende Fortbildungen und Schulungen für Mitarbeiter vorgesehen, damit diese ihren Tätigkeiten qualifiziert nachkommen können?

2.1.6. Betrugsbekämpfungsgesetz 2010

Im Bereich des ISMS spielt auch das Betrugsbekämpfungsgesetz aus dem Jahr 2010 eine wesentliche Rolle. So ist eine zentrale Anforderung daraus, dass sich die Geschäftsfälle des Unternehmens in ihrer Entstehung und Abwicklung verfolgen lassen können. Vorkehrungen zur Sicherstellung dieser Nachvollziehbarkeit wie eine Protokollierung oder ein Konzept zur Authentifizierung sind zumeist im Bereich des ISMS verankert oder sind eng mit diesem verbunden.

Folgende Fragestellung ergibt sich im Zusammenhang mit dem Betrugsbekämpfungsgesetz 2010:

Fragen für Prüfungsplanung und -durchführung

- Wird aus organisatorischer und technischer Sicht die Anforderung der Nachvollziehbarkeit der Geschäftsfälle durch das ISMS adressiert bzw. wurden diese Überlegungen berücksichtigt?

2.1.7. Unternehmensrechts-Änderungsgesetz (URÄG 2008)

Eine, wenn nicht die zentrale Anforderung im Zusammenhang mit dem Risikomanagement und der Ausgestaltung des Internen Kontrollsystems in Unternehmen stammt aus dem Unternehmensrechts-Änderungsgesetz (URÄG) 2008. Durch dieses wurden die Aufgaben des Aufsichtsrates konkretisiert und sowohl die Evaluierung des Risikomanagements als auch die Überwachung des Internen Kontrollsystems als wesentliche Kernaufgabe des Aufsichtsrates bzw. des Prüfungsausschusses festgelegt.

Zu den wesentlichen Aufgaben des Prüfungsausschusses zählen:

- die Überwachung des Rechnungslegungsprozesses;
- die Überwachung der Wirksamkeit des Internen Kontrollsystems, gegebenenfalls des Internen Revisionssystems, und des Risikomanagementsystems der Gesellschaft.

Folgende Fragestellungen ergeben sich im Zusammenhang mit dem URÄG 2008:

Fragen für Prüfungsplanung und -durchführung

- Sind Risikomanagement und Internes Kontrollsystem in den für das ISMS wesentlichen Bereichen hinreichend ausgestaltet, implementiert und wirksam?
- Wie erfolgt im Unternehmen die Kommunikation in den Bereichen Risikomanagement und Internes Kontrollsystem und ist der Aufsichtsrat bzw. der Prüfungsausschuss darüber informiert?

2.1.8. KFS/DV1

Das KFS/DV1 ist ein Fachgutachten des Fachsenats für Datenverarbeitung der Kammer der Wirtschaftstreuhänder in Österreich. Darin werden die Grundsätze einer ordnungsmäßigen Buchführung zusammengefasst. Diese wurden aus den abgabenrechtlichen und unternehmensrechtlichen Bestimmungen abgeleitet. Wesentliche Themengebiete sind die Anforderungen an das Änderungsmanagement sowie die Informationssicherheit.

Folgende Fragestellungen ergeben sich im Zusammenhang mit dem KFS/DV1:

Fragen für Prüfungsplanung und -durchführung

- Welche Anwendungen werden im Unternehmen als buchungsrelevant eingestuft und müssen aus diesem Grund den Anforderungen des KFS/DV1 genügen?
- Erfüllen meine buchungsrelevanten Anwendungen und Systeme die Anforderungen des KFS/DV1?

2.2. Gesetze und Verordnungen in Deutschland

2.2.1. KontraG

Das KontraG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich) wurde im Jahr 1998 beschlossen und konkretisiert Vorschriften im Bereich des Handelsgesetzbuches und des Aktiengesetzes mit dem Ziel, sowohl Vorstand als auch Aufsichtsrat und Wirtschaftsprüfer im Zusammenhang mit dem Risikomanagement und dem Internen Kontrollsystem stärker in die Haftung zu nehmen. So müssen ein unternehmensweites Risikomanagement implementiert und Aussagen zu den Risiken in den Lagebericht des Jahresabschlusses aufgenommen werden.

Folgende Fragestellungen ergeben sich im Zusammenhang mit dem KontraG:

Fragen für Prüfungsplanung und -durchführung

- Sind Risikomanagement und Internes Kontrollsystem in den für das ISMS wesentlichen Bereichen hinreichend ausgestaltet, implementiert und wirksam?
- Wie erfolgt im Unternehmen die Kommunikation im Zusammenhang mit Risikomanagement und Internem Kontrollsystem und ist der Aufsichtsrat bzw. der Prüfungsausschuss darüber informiert?

2.2.2. Bundesdatenschutzgesetz (BDSG)

Der Zweck des Bundesdatenschutzgesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. (§ 1 (1) BDSG). Zentraler Grundsatz ist das Verbotsprinzip mit Erlaubnisvorbehalt, dies bedeutet: Die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten sind grundsätzlich verboten. Sie sind nur dann erlaubt, wenn eine klare Rechtsgrundlage gegeben ist (d.h., das Gesetz erlaubt die Datenverarbeitung in diesem Fall) oder wenn die betroffene Person ausdrücklich (meist schriftlich) ihre Zustimmung zur Erhebung, Verarbeitung und Nutzung gegeben hat (§ 4 BDSG). Ferner, und dies ist ein wesentlicher Unterschied zur österreichischen Gesetzgebung, haben öffentliche und nicht-öffentliche Stellen, die personenbezogene Daten automatisiert verarbeiten, einen Beauftragten für den Datenschutz schriftlich zu bestellen (§ 4f BDSG).

Folgende Fragestellungen ergeben sich im Zusammenhang mit dem Bundesdatenschutzgesetz:

Fragen für Prüfungsplanung und -durchführung

- Wurde eine Datenklassifizierung eingeführt, um Fragestellungen des Datenschutzgesetzes hinreichend zu adressieren?
- Wurden Maßnahmen ergriffen, welche die Gewährleistung der Datensicherheit betreffen, und können diese nachvollzogen werden?

- Befasst sich im Unternehmen eine Person mit datenschutzrechtlichen Anforderungen und stellt sicher, dass Neuregelungen im ISMS berücksichtigt werden?

2.2.3. Arbeitnehmerhaftung

Die Arbeitnehmerhaftung ist in Deutschland im Bürgerlichem Gesetzbuch (BGB) geregelt und legt eine Verpflichtung zum Schadensersatz fest (§ 280 BGB). Der Arbeitnehmer muss, da er auf Basis seines Dienstvertrages Vertragspartner ist, für den verursachten Schaden aufkommen. Da dieser aber auf Anweisung seines Arbeitgebers tätig ist und aus diesem Grund in vielen Fällen nicht oder nur zum Teil Einfluss auf seine Arbeit bzw. Tätigkeiten hat, ist seine Haftung auf eine von ihm zu vertretende Pflichtverletzung beschränkt. In § 619a BGB ist eine Beweislastumkehr festgelegt.

Folgende Fragestellungen ergeben sich im Zusammenhang mit der Arbeitnehmerhaftung:

Fragen für Prüfungsplanung und -durchführung

- Wurden im Unternehmen entsprechende Vorkehrungen getroffen, Mitarbeiter hinsichtlich ihrer Verantwortung im Zusammenhang mit dem ISMS zu sensibilisieren?
- Sind die notwendigen Fortbildungen und Schulungen für Mitarbeiter vorgesehen, damit diese ihren Tätigkeiten qualifiziert nachkommen können?

2.2.4. Telekommunikationsgesetz (TKG)

Das Telekommunikationsgesetz in Deutschland hat die Regelung eines chancengleichen und funktionsfähigen Wettbewerbs für Anbieter von Telekommunikationsdiensten sowie die Sicherstellung von Integrität und Sicherheit von öffentlichen Kommunikationsnetzen zum Zweck. Im Gegensatz zu Österreich und anderen Mitgliedstaaten der EU sieht dieses im Zusammenhang mit der Vorratsdatenspeicherung eine Speicherung von Verbindungsdaten (z.B. Rufnummer des anrufenden und angerufenen Anschlusses, Datum und Uhrzeit) über einen Zeitraum von zehn Wochen vor. Eine Speicherung der jeweiligen Funkzellen ist für vier Wochen vorgeschrieben.

Folgende Fragestellungen ergeben sich im Zusammenhang mit dem Telekommunikationsgesetz:

Fragen für Prüfungsplanung und -durchführung

- Hat eine Klärung stattgefunden, ob in Teilbereichen mein Unternehmen Anbieter von Telekommunikationsdiensten (z.B. E-Mail) ist?
- Wie wurde sichergestellt, dass Kommunikationsdaten für mögliche Telekommunikationsdienste gemäß den Anforderungen gespeichert werden bzw. im Fall von Inhaltsdaten nicht gespeichert werden?
- Wurden hinreichende Vorkehrungen getroffen, um die Daten zu schützen?

2.2.5. Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)

Die GoBD fassen grundsätzliche Regeln und Anforderungen für Aufbewahrung, Führung und Zugriff von buchungsrelevanten Daten bzw. Systemen für Deutschland zusammen. Sie wurden 2014 vom Deutschen Bundesfinanzministerium verabschiedet und haben, wenn auch nur für Deutschland, ihre verbindliche Gültigkeit. Als Nachfolger der Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS) versuchen sie insbesondere Anforderungen an eine ordnungsgemäße Buchhaltung aus den Gesetzestexten für die Buchhaltungen in elektronischer Form abzuleiten bzw. zu konkretisieren.

Folgende Fragestellungen ergeben sich im Zusammenhang mit der GoBD:

Fragen für Prüfungsplanung und -durchführung

- Welche Anwendungen werden als buchungsrelevant eingestuft und müssen aus diesem Grund den Anforderungen der GoBD genügen?
- Erfüllen buchungsrelevante Anwendungen und Systeme der Organisation die Anforderungen der GoBD?

2.2.6. IT-Sicherheitsgesetz

Im Juni 2015 wurde vom deutschen Bundestag das IT-Sicherheitsgesetz (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme) beschlossen. Dieses regelt, dass Betreiber kritischer Infrastrukturen (Unternehmen der Energie, Informationstechnik, Telekommunikation, Transport und Verkehr etc.) ein Mindestniveau an IT-Sicherheit einhalten müssen sowie IT-Sicherheitsvorfälle dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zu melden haben. Eine häufige Reaktion auf die in dem Gesetz geforderten Maßnahmen stellt die Implementierung eines ISMS dar, wenn dies auch nicht explizit im Gesetz gefordert wird.

Folgende Fragestellungen ergeben sich im Zusammenhang mit dem IT-Sicherheitsgesetz:

Fragen für Prüfungsplanung und -durchführung

- Betreibt das Unternehmen kritische Infrastrukturen und hat demzufolge die Anforderungen des IT-Sicherheitsgesetzes zu erfüllen?
- Welche Maßnahmen wurden implementiert, um die Anforderungen zu erfüllen, und genügen diese, um ein hinreichendes Niveau der Sicherheit von informationstechnischen Systemen sicherzustellen und zugleich auch „unverzügliche" Meldungen von Sicherheitsvorfällen zu ermöglichen?