

IT-Compliance (haben Sie einen IT-Compliancebeauftragten?)

Eine immer wichtiger werdende Aufgabe von Unternehmen ist die Einhaltung der Regeln und der Gesetzeskonformität (Compliance).

In zunehmenden Maßen werden auch Geschäftsprozesse in Unternehmen digital abgebildet. Kontrollen seitens des Staats, wie z.B. durch den Zoll oder das Finanzamt aber auch durch Gerichte, Wirtschaftsprüfer usw. haben dazu geführt, dass nun auch die IT erkannt hat, dass heute und künftig alle elektronische Prozessabläufe ohne Lücken nachgewiesen werden müssen.

Beispiele für Unternehmer und IT-Verantwortliche

- Geschäftliche E-Mails fallen unter den Begriff des Handelsbriefes und müssen nach gesetzlichen Vorgaben z.B. jederzeit verfügbar und unveränderbar vorgehalten werden.
- Der Vorsteuerabzug aus elektronisch übersandten Rechnungen ist unter Einhaltung der gesetzlichen Vorgaben und durch den Einsatz entsprechender Verfahren erlaubt.
- Auch wenn der bisherige Signaturzwang rückwirkend zum 1.7.2011 weggefallen ist, so muss trotzdem jede elektronisch übersandte Rechnung gesetzlich konform archiviert werden.
- Im Rahmen des Datenschutzes sind die Verantwortlichen gesetzlich verpflichtet, die Vertraulichkeit und Integrität von Geschäftspartner- oder Mitarbeiterdaten zu schützen.
- Ein Verstoß im Rahmen der Auftragsdatenverarbeitung nach dem Bundesdatenschutzgesetz z.B. beim Outsourcing kann ein Bußgeld bis zu 50.000 Euro und höher nach sich ziehen.
- Die Entkräftung von Mobbingvorwürfen in arbeitsgerichtlichen Verfahren durch Vorlage des lückenlosen E-Mailverkehrs ist unter Umständen, ohne Nachweis des gesetzlich konformen Umgangs mit dem Medium E-Mail, schwierig oder gar nicht möglich.

Angesichts dieser Regelflut müssen die Anbieter von Hard- und Software die notwendigen Fähigkeiten der angebotenen Produkte und Services im Bereich Compliance unter Beweis stellen. Unternehmen haben schon längst erkannt, dass der richtige Umgang mit dem Thema Compliance in jeden Anforderungskatalog gehört. Aber auch Vorstände und Geschäftsführer werden sich immer häufiger ihrer eigenen Haftungsrisiken bewusst und kümmern sich vermehrt um die IT-Sicherheit, die einen nicht unerheblichen Beitrag für die IT-Compliance leistet.

Beispiele für Gesetze und Vorgaben

- GDPdUZ - Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen für den Zuständigkeitsbereich der Zollverwaltung
- Verordnungen zum Außenhandelsrecht, im Bereich der Chemie (REACH) oder Regelungen im Finanzwesen (MiFID)
- GDPdU - Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen bzw. die sogenannte "Digitale Betriebsprüfung"
- Gesetze zum Datenschutz von Bund und Länder
- Gesetze im Bereich der Telekommunikation (erweitert um Vorgaben z.B. zur Vorratsdatenspeicherung)
- KonTrag - Gesetz zur Kontrolle und Transparenz im Unternehmensbereich