

Datenschutzgesetze

Datenschutzgesetze

Die Möglichkeit von Nachverfolgung und Auffinden wichtiger Daten ist für die Erfüllung gesetzlicher Auflagen wie der folgenden entscheidend:

Gramm-Leach-Bliley Act (GLBA), 1999

Aufgrund des GLBA sind Finanzinstitute dazu verpflichtet, administrative, technische und physische Werkzeuge zum Schutz der Integrität und der Vertraulichkeit von Kundendaten bereitzustellen. Die Unternehmen müssen auch die Verfügbarkeit von finanziellen Informationen sowie Geschäftskontinuität sicherstellen. Verstöße können unter anderem mit Bußgeldern von bis zu einer Million US Dollar geahndet werden.

Sarbanes-Oxley Act (SOX), 2002

SOX wurde als unmittelbare Antwort auf Firmenskandale von Unternehmen wie Enron und WorldCom beschlossen. Die Vorschriften gewährleisten die Integrität der Informationen und Finanzdaten der Unternehmen und beschäftigen sich mit Grundsätzen der Unternehmensführung. SOX betrifft US-börsennotierte Unternehmen, kann sich jedoch global auf deren Führungskräfte, Vorstände und Wirtschaftsprüfer auswirken, indem diese persönlich für die Richtigkeit und Pflege von Finanzinformationen zur Verantwortung gezogen werden. Erhebliche Strafen und Geldbußen können angewendet werden, auch Haftstrafen.

Health Insurance Portability and Accountability Act (HIPAA), 1996

HIPAA wurde zur Sicherung der Gesundheitsversorgung von Arbeitern und deren Familien im Falle von Wechsel oder Verlust des Arbeitsplatzes beschlossen. Ein Abschnitt daraus (Title II) fordert die Schaffung von Standards für elektronischen Patientenakten, für Verwaltungs- und Finanzdaten und für den Schutz und die Sicherheit medizinischer Daten. HIPAA kann Auswirkungen auf jede Organisation haben, die direkt oder indirekt im Gesundheitswesen tätig ist. Die Auswirkungen können sich sogar auf Unternehmen erstrecken, die Dienstleistungen für das Gesundheitswesen erbringen, z. B. Anbieter von Informationssystemen. Auch wenn HIPAA keine Maßnahmen zur Einhaltung von Compliance-Anforderungen festlegt, können Fehler beim angemessenen Schutz von Informationen im Sinne von HIPAA Bußgelder in Höhe von bis zu 250.000 US Dollar und Freiheitsstrafen von bis zu 10 Jahren nach sich ziehen.

Laufende oder geplante Audits sind erforderlich, um die Richtigkeit und Verfügbarkeit der Informationen zu bestätigen, entsprechend den Anforderungen der oben genannten Regelwerke. Systeme werden häufig getestet, um sicherzustellen, dass sie die relevanten Informationen fristgerecht bereitstellen können. Die Aufbewahrungsfrist für Finanzdaten im Gesundheitswesen kann zudem bis zu sieben Jahre betragen, während es für die Daten, die im Gesundheitssektor genutzt werden, eine Aufbewahrungsfrist von über 20 Jahren geben kann. Entscheidend ist, dass diese Informationen jederzeit ohne weiteres zugänglich sein müssen, wobei sich deren Inhalte über einen erheblichen Zeitraum erstrecken können.

In Australien verlangt das Datenschutzgesetz 'Privacy Act, 2001' unter Paragraf 4 - Aufbewahrung und Sicherheit personenbezogener Daten - vom 'Halter' der Datensätze, dass die in ihnen enthaltenen Angaben gegen Verlust, unberechtigten Zugriff und Nutzung, Veränderung, Offenlegung und jede andere Form des Missbrauchs geschützt werden, indem angemessene Maßnahmen zur Gefahrenabwehr getroffen werden, die im Einflussbereich des Verantwortlichen liegen. Bei Nichteinhaltung wird der Verantwortliche persönlich haftbar gemacht und muss mit strafrechtlichen Konsequenzen rechnen.

Fast jedes Land, in dem Recall tätig ist, hat nunmehr eine Form der Gesetzgebung eingeführt, um sicherzustellen, dass vertrauliche Informationen geschützt werden. Normalerweise gründen die Gesetze auf Finanzbasis und werden durch Währungs- oder Finanzbehörden auf den Weg gebracht. Für die Europäische Union finden Sie Referenzmaterial in der 'Markets in Financial Instruments Directive' (MiFID), für Großbritannien im 'Data Protection Act' und im 'Freedom of Information Act'.

* Quelle: B&L Associates, „Compliance through Proper Tape Management“