Datenschutz durch Prozessmanagement

Johann Bizer

Die Überschrift „Datenschutz durch Prozessmanagement“ fasst eine neue Entwicklung des Datenschutzes zu einem neuen Paradigma einer modernen Datenschutzpolitik zusammen.

■ „Datenschutz durch Prozessmanagement“ versteht sich als eine Ergänzung der bisherigen Paradigmen:

- Datenschutz durch Recht,
- Datenschutz durch Technik und
- Datenschutz durch Wettbewerb.

„Datenschutz durch Prozessmanagement“ ist für einen erfolgreichen Datenschutz in Betrieb und Verwaltung von erheblicher *strategischer Bedeutung*. Es geht um die Umsetzung der Anforderungen des Datenschutzes in die Prozesse der für die Verarbeitung personenbezogener Daten verantwortlichen Stelle. Der Datenschutz soll wirtschaftlich werden, indem er in die Aufbau und Ablauforganisation der Organisationen integriert wird („Prozessmanagement“).

Datenschutz als Managementaufgabe

Besonders deutlich wird diese Erweiterung der Datenschutzpolicy, wenn die Erfüllung der Anforderungen des Datenschutzes im modernen Managementdeutsch als Aufgabe von Compliance und Riskmanagement der Leitung der Organisation verstanden wird.

Compliance

Compliance thematisiert die Erfüllung der Anforderungen aus Gesetzen, Verträgen und Anordnungen durch eine Organisation. Zu befolgen sind die *externen gesetzlichen Anforderungen* bspw. vom Steuerrecht über das Baurecht bis zum Arbeits-, Gesundheits- sowie Datenschutzrecht.

Zu erfüllen sind von einer Organisation aber auch *vertragliche Anforderungen* bspw. über die Qualität von Produkten und Dienstleistungen. Dies ist von unmittelbarer Relevanz bei der Herstellung von Soft- und Hardwareprodukten, aber auch der Erbringung von Dienstleistungen bspw. im Wege einer Auftragsdatenverarbeitung.

Compliance ist auch ein Thema der verantwortlichen Leitung einer Organisation. Werden externe Anforderungen von der Organisation nicht erfüllt, so liegt die Verantwortung in erster Linie beim Management bzw. der Behördenleitung. Entsprechendes gilt für die Erfüllung von *internen Anforderungen*: Eine Geschäftsführung, die für ihre Organisation die Orientierung an einer technischen Norm angeordnet hat, belegt ein signifikantes Führungsveragen, wenn diese nicht befolgt wird.

Compliance bedeutet als Managementaufgabe, eine Organisation der Zuständigkeiten und Abläufe und damit ein Prozessmanagement, das eine Erfüllung der externen und internen Anforderungen einschließlich des Datenschutzes gewährleistet.

Riskmanagement

Auch das Riskmanagement ist eine Aufgabe des Managements. Nicht erst seit dem KontraG, liegt es in der Verantwortung von Geschäftsführung und Vorständen dafür zu sorgen, dass durch eine angemessene Organisation der Aufgaben und Abläufe („Prozessmanagement“) für das Unternehmen keine Schäden entstehen.

Erforderlich ist eine an die Erfordernisse des Unternehmens angepasste Risikovorsorge. Dies bedeutet bspw. für eine von der Informationstechnik abhängige Organisation, dass sie ein *funktionierendes Sicherheits- und Datenschutzmanagement* installiert, das zur Risikominimierung auf Vorfälle umgehend reagiert und proaktiv eine ausreichende Vorsorge schafft. Seine Aufgabe ist der Schutz der Unternehmenswerte, zu denen Betriebs- und Geschäftsgeheimnisse sowie die personenbezogenen Daten der Beschäftigten und der Kunden gehören.

Riskmanagement als Führungs- und Managementaufgabe bedeutet für die Verantwortlichen, dass sie für ein funktionierendes Datenschutz- und Sicherheitsmanagement sorgen müssen.

Datenschutz- und Sicherheitsmanagement

Die Einrichtung eines funktionierenden Datenschutz- und Sicherheitsmanagement ist ein zentraler Baustein der Policy „Datenschutz durch Prozessmanagement“. Sie wird durch eine Entwicklung begünstigt, die Daten- und IT-Sicherheit nicht nur auf die Formulierung und Implementierung von Maßnahmen zu beschränken, sondern ihre Wirksamkeit durch eine entsprechende Aufbau- und Ablauforganisation zu verstärken und damit dynamisch auf neue Herausforderungen einzustellen („Prozessmanagement“).

Anschauliches Beispiel für diese Entwicklung ist, die Ergänzung und Erweiterung des IT-Grundschutzes des BSI um Anforderungen an das Sicherheitsmanagement. Eine Entwicklung, die nicht nur prozessorientierte Managementsysteme wie BS7799 oder ITIL aufnimmt, sondern auch die Wiederaufnahme der Arbeiten durch die Datenschutzbeauftragten an einem „Baustein Datenschutz“ als Annex zum IT-Grundschutz des BSI begünstigt hat.

Ein Datenschutz- und Sicherheitsmanagement muss zwei unterschiedliche Aufgaben erfüllen: Die Aufgabe des *Sicherheitsmanagements* ist operativ, um die Einhaltung und Anpassung der Sicherheitsmaßnahmen durch reaktive und proaktive Maßnahmen zu gewährleisten. Mit der Integration von Datensicherheit und IT-Sicherheit schließt das Sicherheitsmanagement die „technische Flanke“ des Datenschutzes.

Das *Datenschutzmanagement* hat mit dem betrieblichen Datenschutzbeauftragten eine kontrollierende Aufgabe, die sich bei entsprechender Qualifikation auch auf die Mechanismen der Datensicherheit erstreckt. Das Datenschutzmanagement erfüllt aber auch die proaktive Aufgabe, die Datenschutzkonformität der technischen Einrichtungen und Produkte bspw. in Form einer Vorabkontrolle, einer Auditierung oder einer entsprechenden Beratung zu prüfen und abzunehmen.