Wie Unternehmen ein integriertes Managementsystem implementieren können, um die Anforderungen der DSGVO umzusetzen

Integriertes Managementsystem zur DSGVO-Umsetzung

Mit dem Inkrafttreten der Datenschutzgrundverordnung (DSGVO) am 25. Mai ergaben sich zahlreiche Veränderungen für Unternehmen. Um alle Anforderungen zu erfüllen und kontinuierlich zu überprüfen, sollte ein Datenschutzmanagementsystem (DSMS) implementiert und gelebt werden. Für Unternehmen, die bereits Managementsysteme eingeführt haben, empfiehlt sich die Integration eines DSMS in das bestehende System.

Von Igor Gensa, ANMATHO AG

Die DSGVO stellt viele Unternehmen, auch nach ihrem Inkrafttreten, vor große Herausforderungen. Um die zahlreichen Anforderungen zu erfüllen sowie den Rechenschafts- und Nachweispflichten des neuen Datenschutzrechts gerecht zu werden, bedarf es eines strategischen Gesamtkonzepts. Darüber hinaus muss ein risikobasiertes Verfahren definiert werden, das die Umsetzung sowie die Dokumentation und Kontrolle der technischen und organisatorischen Maßnahmen sicherstellt. Dementsprechend bleibt vielen Unternehmen und Organisationen nichts anderes übrig, als ein Datenschutzmanagementsystem (DSMS) zu implementieren.

Wer sollte ein DSMS einführen?

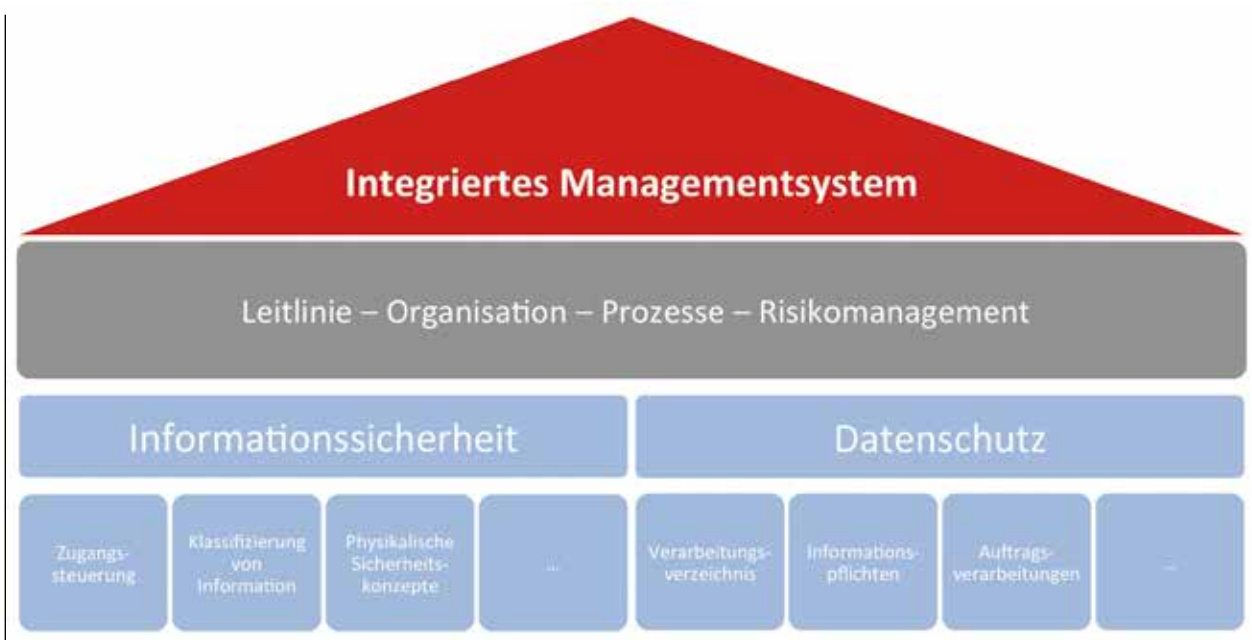
Besonders Unternehmen mit sehr hohen Anforderungen an den Datenschutz, zum Beispiel Krankenhäuser, Versicherungen, Banken oder Telekommunikationsanbieter, müssen ein besonderes Augenmerk auf die Einhaltung der DSGVO legen, um Datenschutzverletzungen und mögliche Sanktionen zu verhindern. Hier bietet ein DSMS als strategisches Gesamtkonzept Abhilfe und gewährleistet eine kontinuierliche Kontrolle und somit einen Verbesserungsprozess. Weiterhin bietet sich die Einführung eines DSMS für Unternehmen mit fest definierten und gelebten Prozessen an.

Bei der Umsetzung des DSMS empfiehlt es sich, auf bereits implementierte Managementsysteme zurückzugreifen und das DSMS darin zu integrieren. Die Integration mit allen damit einhergehenden datenschutzrelevanten Prozessen ist beispielsweise in ein Qualitätsmanagement nach ISO 9001, in das Business-Continuity-Management-System nach ISO 22301 oder in ein Energiemanagementsystem nach ISO 50001 möglich. Auch lässt es sich in ein Informationssicherheits-Managementsystem (ISMS) nach BSI IT-Grundschutz einbetten.

Best Practice mit ISO 27001

In der Vergangenheit wurden Informationssicherheit und Datenschutz oftmals separat mit nur sehr wenigen Überschneidungen betrachtet. Heute werden die meisten Geschäftsprozesse digitalisiert und ermöglichen es, Prozesse effizienter zu gestalten – das birgt jedoch auch hohe Risiken. Um diese zu minimieren und vor dem Hintergrund der DSGVO empfiehlt es sich daher, Informationssicherheit und Datenschutz gemeinsam zu betrachten. Dies ermöglicht ein integriertes Managementsystem. Vor allem bietet sich hier die Integration des Datenschutzes in ein ISMS nach ISO 27001 an. Unter Berücksichtigung der Anforderungen der DSGVO sowie anderer ISO-Normen, wie der ISO 29000 und ISO 29151, lässt sich so ein Managementsystem schaffen, das Informationssicherheit und Datenschutz gleichermaßen gewährleistet. Ein zertifiziertes ISMS nach ISO 27001 beinhaltet alle Maßnahmen, um auch die Anforderungen des Datenschutzes sowie die dazugehören technischen und organisatorischen Maßnahmen nach aktuellem Stand der Technik umzusetzen.

Bei der Integration des DSMS in ein ISMS sollte man darauf achten, möglichst viele Synergien zu nutzen. Das wird durch die Erweiterung von bestehenden Dokumenten und Prozessen ermöglicht und schafft zum einen eine durchgehende Strukturierung und zum anderen eine größere Akzeptanz durch den Wiedererken-



Aufbau eines integrierten Management-systems

nungswert. So sollte beispielsweise die bestehende Leitlinie, in der sich die Geschäftsführung zur Informationssicherheit und zum Datenschutz verpflichtet, um die Schutzziele und Prinzipien der DSGVO erweitert werden.

Beim Risikomanagement lassen sich ebenfalls Synergieeffekte nutzen, indem die Risikomethodik um die Betrachtung der Risiken für betroffene Personen und eine Datenschutz-Folgenabschätzung erweitert wird. Die für das Risikomanagement verantwortlichen Mitarbeiter müssen somit keine neue Methodik anwenden. Darüber hinaus können Risiken miteinander verglichen werden. Weitere Prozesse, wie interne Audits oder das Management-Review, kann man ebenfalls um die Anforderungen der DSGVO erweitern, sodass ein kontinuierlicher Verbesserungsprozess gewährleistet ist.

Für die Umsetzung von technischen und organisatorischen Maßnahmen eignen sich die Annex A Controls der ISO 27001. Jedoch sollten Unternehmen prüfen, ob und wie die bestehenden Maßnahmen erweitert oder geändert werden müssen, um den Datenschutzanforderungen zu genügen.

Vorteile durch Datenschutzintegration

Die Integration eines DSMS ermöglicht es, die Anforderungen der DSGVO mit bestehenden Prozessen aus dem ISMS zusammenzuführen. Beispielsweise lassen sich die Controls A.16 „Incident-Management“ um die Meldeprozesse bei Datenschutzverletzungen erweitern. Weiterhin lassen sich die Effektivität und der Ressourcen-Bedarf optimal anhand von Kennzahlen überprüfen. Ferner wird dem Datenschutzbeauftragten ermöglicht, seine Tätigkeit strukturell und nach bewährten Abläufen auszuführen. Analog zum Informationssicherheitsbeauftragten wird der Datenschutzbeauftragte ebenfalls zum Managementsystembeauftragten und somit Teil eines Managementteams. Das stärkt die Rolle des Datenschutzbeauftragten und ermöglicht die Steigerung der Akzeptanz für Datenschutz im Unternehmen. Dieser Aspekt kann zu einer positiven Awareness rund um das Thema Informationssicherheit und Datenschutz führen. Eine Kontrolle durch Aufsichtsbehörden oder durch Auftraggeber muss also nicht mehr gefürchtet werden.

Wettbewerbsvorteil integriertes Managementsystem

Nicht zu unterschätzen ist außer den genannten Vorteilen vor allem, dass die Umsetzung des Datenschutzes in einem intergrierten Managementsystem (verstärkt durch eine ISO 27001-Zertifizierung) als Qualitätsmerkmal beworben werden kann. Während Datenpannen und -skandale immer mehr zunehmen, können Unternehmen mit einem DSMS eine kontinuierliche Überprüfung und Verbesserung gewährleisten. Das lässt sich durchaus werbewirksam vermarkten und ist ein Vorteil bei großen Kunden oder bei öffentlichen Ausschreibungen. ■