Datenschutz-Management

Kein Grund für Torschlusspanik

Sanktionen von bis zu 20 Millionen Euro oder vier Prozent des weltweiten Vorjahresumsatzes: Das sind Zahlen, die jede Geschäftsleitung erblassen lassen. Dabei gibt es für Panik nicht den geringsten Anlass, ist die DSGVO doch wenig mehr als eine Kopie des BDSG: Kaum eine Bestimmung, die (zumindest in Deutschland) nicht bereits heute gilt. Neu sind die erweiterten Dokumentationspflichten – und diese Aufgabe lässt sich mit einem systematischen Management zügig in den Griff bekommen.

Von Fabian Ebner, Michael Knopp und Jörg Völker, Secorvo Security Consulting GmbH

„Alles neu macht der Mai", heißt es am 25. Mai diesen Jahres, wenn die europäische Datenschutz-Grundverordnung (DSGVO) in Kraft tritt. Das bedeutet nicht nur ein neues Recht und ein neues Bundesdatenschutzgesetz (BDSG), sondern auch viel Unsicherheit bei allen Unternehmen.

Vor allem in kleineren und mittleren Betrieben, die sich keine eigene Datenschutzabteilung leisten können (oder wollen), wird bei Datenschutzthemen häufig eher Einzelfall-bezogen und demnach wenig strukturiert reagiert statt systematisch und vorausschauend agiert. Das führt dann zu verteilten Ablagen, dezentralisierter Informationsaufbereitung und bei Einzelpersonen konzentriertem Wissen. Für eine transparente Darstellung des Datenschutzes ist diese Vorgehensweise wenig geeignet. Sie birgt bereits in sich das Risiko von Sanktionen wegen mangelnder Datenschutzumsetzung. Wurzel allen Übels sind oft zu wenige Ressourcen und ungeeignete Hilfsmittel, was sich symptomatisch in der Überforderung mancher Datenschützer widerspiegelt.

Unter solchen Gegebenheiten lässt sich ein systematischer Überblick über den Umsetzungsstand der Datenschutz-Anforderungen, sei es aus altem oder neuem Recht, nur schwer gewinnen.

Tatsächlich sind die Unterschiede in den Anforderungen der DSGVO zum bisherigen BDSG nicht so groß, wie die derzeitige öffentliche Diskussion glauben machen kann. Ein paar Aspekte müssen jedoch auch die Unternehmen beachten, die die Anforderungen des (noch geltenden) BDSG systematisch umgesetzt haben.

Jenseits der bereits heute bestehenden Datenschutzanforderungen bringt die DSGVO vor allem einen intensiveren Dokumentationsbedarf, ein Mehr an Transparenz- und Informationspflichten gegenüber den Betroffenen und den Aufsichtsbehörden und einen starken Umsetzungsanreiz in Form von deutlich erhöhten Bußgeldern.

Um die vor allem aus Art. 5 Abs. 2 DSGVO resultierende Nachweisbarkeit der Datenschutzumsetzung zu erreichen, sind insbesondere zwei Bereiche zu dokumentieren:

- die konkrete Verarbeitung der Daten in einzelnen Verfahren und
- die Umsetzung von datenschutzbezogenen Prozessen (vor allem die Einbindung des betrieblichen Datenschutzbeauftragten durch Verfahrensmeldungen, die Meldung von Datenschutzvorfällen, der Abschluss von Verträgen zur Auftragsverarbeitung, die Umsetzung von Informations- und Auskunftspflichten, die Gestaltung von Informationsflüssen und ein Berichtswesen).

Die Verarbeitungstätigkeiten werden durch ein umfassendes Verfahrensverzeichnis erfasst, die Umsetzung des Datenschutzes ist Teil der geforderten Prozessdokumentation.

Was hilft?

In der Informationssicherheit wird zur Bewältigung ähnlicher Probleme auf die Verwendung von Informationssicherheitsmanagementsystemen (ISMS) gesetzt. Für die Informationssicherheit haben sich bereits zwei Standards etabliert (ISO/IEC 27001:2013 und IT-Grundschutz auf Basis von ISO 27001). Entsprechende, ähnlich etablierte Standards stehen für den Datenschutz noch aus. Dennoch empfiehlt sich der Aufbau eines an diesen Standards orientierten Datenschutzmanagementsystems.

Ein solches Managementsystem hilft bei der Strukturierung

von Prozessen und der durchgängigen Dokumentation sowie bei der Herstellung von Nachvollziehbarkeit und Nachweisbarkeit der Datenschutzumsetzung. Es unterstützt weiterhin bei der Standardisierung von Vorgängen, der bedarfsgerechten Bereitstellung von Informationen, beispielsweise zu Prozessen, und stellt eine zu jeder Zeit mögliche Prüfbarkeit der Datenschutzumsetzung sicher.

Worauf sollte man achten?

Bei der Auswahl eines Datenschutzmanagementsystems (DSMS) sollte man auf folgende Eigenschaften achten:

_____ Je nach Unternehmensgröße und Komplexität der Datenverarbeitung ist nicht unbedingt das komplexeste und umfangreichste am Markt verfügbare System das geeignete. Gerade für betriebliche Datenschutzbeauftragte, die sich nicht lange einarbeiten können, ist das KISS-Prinzip („Keep it smart and simple“) zu empfehlen.

_____ Obwohl die Schutzgegenstände divergieren – die Informationssicherheit betrachtet das Unternehmensrisiko, die Datenschutzbewertung gilt dem Betroffenenrisiko – sind eine enge Verzahnung und die Nutzung von Synergie-Effekten zwischen dem Datenschutzmanagement und dem Informationssicherheitsmanagement sehr hilfreich. Beispielsweise kann die gleiche Methodik für die Datenschutz-Folgenabschätzung und für die Risikoanalyse in der Informationssicherheit genutzt werden. So müssen sich Mitarbeiter im Unternehmen nicht in zwei unterschiedlichen Systemen oder Methodiken zurechtfinden und die Risikobewertungen sind unmittelbar vergleichbar.

_____ Die einfache Integration bereits bestehender Informationen in das Managementsystem kann ebenfalls entscheidend den Aufwand zur Implementierung eines solchen Systems reduzieren. Damit sollte auch den unvermeidlichen Medienbrüchen (E-Mails, Telefonnotizen, Papier- und digitale Dokumente) ein Ende bereitet werden.

_____ Gleichzeitig sollte ein DSMS die nötige Flexibilität mitbringen, um mit wenig Aufwand an die Bedürfnisse des Unternehmens und an bestehende Prozessabläufe angepasst werden zu können. Das gleiche gilt natürlich für zukünftige Änderungen der Datenschutzanforderungen.

_____ Schließlich sollte ein DSMS dabei helfen, die alltäglichen Aufgaben der/des Datenschutzbeauftragten zu organisieren und zu bewältigen.

Mit einem derart geeigneten Managementsystem ist es durchaus möglich, den neuen Anforderungen der DSGVO effizient und mit überschaubarem Aufwand gerecht zu werden. Doch auch mit dieser Unterstützung braucht es nach wie vor die Bereitschaft, sich mit dem Thema Datenschutz im Unternehmen eingehend zu befassen, und den erforderlichen Umsetzungswillen.