DSGVO und Qualitätsmanagement: Herausforderungen kennen, Synergien nutzen

Die DSGVO ist in Kraft. Mit ihren hohen Bußgeldern bei Verstößen hat sie das Thema Datenschutz auf der Prioritätenliste von Unternehmen ganz nach oben katapultiert. Und doch: Noch immer arbeiten viele nicht konform. Ein Datenschutz-managementsystem hilft, die DSGVO-Anforderungen konsequent umzusetzen. Wer bereits über ein gut etabliertes Qualitätsmanagementsystem verfügt, kann Synergien nutzen und kommt schneller ans Ziel.

Seit dem 25. Mai 2018 müssen Unternehmen die Forderungen der EU-Datenschutzgrundverordnung (DSGVO) umsetzen. Diese EU-weit gültige Verordnung löst die bisherige Datenschutzrichtlinie 95/46/EG ab. Aktuell kämpfen viele deutsche Unternehmen auch jetzt noch damit, die Forderungen der DSGVO zu erfüllen, denn der Zwang zur Umsetzung hat sich durch die EU-Verordnung deutlich verschärft. Anders als bisher sind Unternehmen rechenschaftspflichtig (Art. 5 Abs. 2 DSGVO) und müssen nachweisen, dass sie die geforderten Anforderungen einhalten. Bei Verstößen drohen Bußgelder von bis zu 20 Millionen Euro beziehungsweise bis zu vier Prozent des weltweiten Jahresumsatzes.

Datenschutz mit System

Ein systematisches Datenschutzmanagement unterstützt dabei, DSGVO-konform zu arbeiten und dieses Risiko zu minimieren. Dafür gilt es zunächst, den aktuellen Umsetzungsstand im Unternehmen zu ermitteln. Das Bayerische Landesamt für Datenschutzaufsicht bietet zu diesem Zweck ein Datenschutz-Werkzeug an, mit dem Unternehmen anhand von 28 Fragen selbst einschätzen können, wie gut sie bei den wesentlichen Datenschutzanforderungen aufgestellt sind. Doch schon bei der Beantwortung dieser Fragen werden DSGVO-Neulinge schnell an ihre Grenzen stoßen.

Eine mangelhafte Kenntnis der Gesetzeslage sowie lückenhaftes Fachwissen im Datenschutz sind die wesentlichen Gründe dafür, dass die Umsetzung der DSGVO-Vorgaben vielen Unternehmen so schwerfällt. Ein Datenschutz-beauftragter muss nicht nur die gesetzlichen Vorgaben in allen Einzelheiten kennen. Er muss auch in der IT zu Hause sein – und zwar sowohl operativ, beispielsweise in der IT-gestützten Steuerung von Prozessen, als auch im Hinblick auf die IT-Sicherheit. Zudem benötigt er ausreichend organisatorische Kenntnisse, um die neuen Anforderungen flächendeckend in gelebte Praxis zu überführen. Ein solch tiefes wie breit gefächertes Fachwissen können Unternehmen mit weniger als 100 Mitarbeitern erfahrungsgemäß kaum intern aufstellen. Auch Unternehmen, die nicht gesetzlich verpflichtet sind, einen Datenschutzbeauftragten zu benennen, sind daher gut beraten, sich externe Hilfe zu holen.

Status quo prüfen

Im ersten Schritt gilt es, den Status quo zu erfassen. In welchen Prozessen tauchen personenbezogene Daten auf? Wie werden sie gespeichert und verarbeitet? Auf welcher Gesetzesgrundlage erfolgt dies? Welche Systeme sind dafür im Einsatz – sowohl elektronisch als auch klassisch in Papierform?

Unternehmen, die bereits ein Managementsystem etabliert haben, sind hier im Vorteil. Denn sie leben das Prinzip eines kontinuierlichen Verbesserungsprozesses und kennen die Vorgehensweisen bei Audits. Die DSGVO beschreibt die Pflichten der Verantwortlichen (v.a. Informationspflichten) und die Rechte der Betroffenen (z.B. auf Auskunft und Löschung). Darüber hinaus können Unternehmen mit einem funktionierenden Managementsystem die bestehenden Strukturen, Methoden und Dokumentationen für die DSGVO-Umsetzung heranziehen und Schritt für Schritt um die Datenschutzthemen erweitern. Dies reduziert den Umsetzungsaufwand deutlich.

QMS und DSGVO: Synergien nutzen

Gerade mit der ISO 9001 für Qualitätsmanagementsysteme (QMS) ergeben sich einige Synergieeffekte, die Unternehmen gezielt auf dem Weg zur DSGVO-Konformität nutzen sollten. Die in ihrem QMS bereits dokumentierten Prozesse, Abläufe und Verantwortlichkeiten etwa sind eine solide Basis, um die von der Verordnung vorgegebenen Dokumentationspflichten zu erfüllen. Denn wie das QM muss auch das Datenschutzmanagement Zuständigkeiten und Informationspflichten nachvollziehbar regeln und nachweisen. Für das erforderliche Verzeichnis aller Datenverarbeitungstätigkeiten können ebenfalls viele Informationen aus der bestehenden QMS-Dokumentation herangezogen werden. Umgekehrt gilt es allerdings auch, die bestehenden Prozesse auf ihre Datenschutzanteile zu prüfen – eine Vorgabe der DSGVO. Damit könnten in Audits Datenschutzthemen stärker als bisher zur Sprache kommen.

Eine wichtige Forderung der DSGVO ist darüber hinaus die Datenschutzfolgenabschätzung (DSFA nach Art. 35 „Data Protection Impact Assessment“). Bei ihrer Aufstellung können die im bestehenden QMS angewandten Mechanismen zur Risikoanalyse und -bewertung helfen.

Und auch im Zusammenhang mit erforderlichen Schulungen und Unterweisungen der Mitarbeiter zum gesetzeskonformen Umgang mit personenbezogenen Daten gibt es deutliche Parallelen in den Anforderungen von DSGVO und QM. Da liegt es nahe, bestehende Konzepte und Nachweisstrukturen direkt zu nutzen.

Fehlende Prozesse ergänzen

Nach der detaillierten Bestandsaufnahme und einer ersten Umsetzung von DSGVO-Forderungen – gegebenenfalls mithilfe von betrieblichen Managementsystemen – zeigt sich, an welchen Stellen in der aktuellen Prozesslandschaft noch Löcher klaffen. Alle Unternehmen müssen beispielsweise einen neuen Prozess für die Rechte der Betroffenen entwickeln und festschreiben. Das Gleiche gilt für die gesamte Informationssicherheit. Sie ist ein wesentlicher Bestandteil des Datenschutzes – auch bei Unternehmen, die kein Managementsystem für Informationssicherheit nach ISO 27001 im Einsatz haben: Die DSGVO fordert die Umsetzung technisch-organisatorischer Maßnahmen (TOMs), die Unternehmen zum Schutz von personenbezogenen Daten einführen müssen. Auf solche Sicherungsmaßnahmen geht die ISO 9001 ebenso wenig ein wie auf IT-spezifische Prozesse. Und auch die 114 Controls zur Informationssicherheit, die die ISO 27001 vorgibt und die in die gleiche Richtung zielen wie die TOMs der DSGVO, decken die Datenschutzanforderungen zu wenig ab. Best Practices werden somit erst die nächsten Monate bringen. Bislang gibt es auch keine konkreten Vorgaben seitens der Aufsichtsbehörde, wie der Status des Datenschutzes in Unternehmen künftig ermittelt werden soll.

Fazit

Auch wenn die DSGVO in ihrer praktischen Umsetzung noch Fragen offenlässt, hilft ein systematisches Vorgehen Unternehmen, ihr Risiko auf ein Minimum zu reduzieren. Gerade Organisationen mit einem bestehenden Qualitätsmanagementsystem nach ISO 9001 werden zahlreiche Parallelen bei dokumentierter Information, Prozessen, Strukturen und Verantwortlichkeiten finden – und haben damit nicht nur auf dem Weg zur DSGVO-Konformität einen entscheidenden Vorteil. Sie können auch anstehenden QM-Audits gelassener entgegensehen, bei denen seit Inkrafttreten der EU-Verordnung in Sachen Datenschutz genauer hingeschaut wird.

Mehr Informationen zur ISO 9001 finden Sie unter www.tuev-sued.de/ms/iso-9001.