DATENSCHUTZ-COMPLIANCE NACH DER DS-GVO

Kranig, Sachs, Gierschmann

Kranig, Sachs, Gierschmann
Datenschutz-Compliance nach der DS-GVO
Handlungshilfe für Verantwortliche inklusive Prüffragen für Aufsichtsbehörden
Bundesanzeiger Verlag
1. Auflage 2017
230 Seiten
ISBN-13: 978-3846207604
44,00 Euro

Das Werk bietet Hilfestellungen und Vorgabemuster für die Datenschutzorganisation und richtet sich explizit an Verantwortliche der Datenverarbeitung. Das Autorenteam setzt sich aus dem Präsidenten des Bayerischen Landesamtes für Datenschutzaufsicht (BayLDA), dem Leiter des Referats Technischer Datenschutz und IT-Sicherheit des BayLDA und einem auf Datenschutzmanagement spezialisiertem Unternehmensberater zusammen. Diese Mischung aus Jurist, Dipl.-Informatiker und Diplom-Wirtschaftsingenieur betrachtet die DS-GVO aus Compliance-Sicht.
Explizite Zielgruppe des Werkes sind die Verantwortlichen, die über Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheiden. Auftragsverarbeiter sind nicht konkret adressiert, werden aber auch nicht abgehalten, sich mit diesen Sichtweisen zu befassen.

Das Werk umfasst drei Teile: Einführung in die DS-GVO, Sicherstellung der Datenschutz-Compliance und Überwachung der Datenschutz-Compliance. Im ersten Teil wird deutlich hervorgehoben, dass die Unternehmensleitung die Verantwortung für eine regelkonforme Umsetzung der rechtlichen Anforderungen bei der Verarbeitung personenbezogener Daten trägt. Ein Umstand, der erst jetzt durch die Datenschutz-Grundverordnung und deren Sanktionsmöglichkeiten allen Managementebenen eines Unternehmens bewusst zu werden scheint. Die dabei wesentlichen Datenschutzprozesse der datenschutzkonformen Datenverarbeitung, der Sicherstellung der Betroffenenrechte und die Handhabung von Datenschutzverletzungen werden dabei als Teil der Ablauforganisation dargestellt. Die Aufbauorganisation mit den Datenschutzstrukturen über Datenschutzziele, Datenschutz-Governance-Struktur sowie der Datenschutzleitlinie bildet den weiteren Schwerpunkt des übersichtsartigen ersten Teils.

Im zweiten Teil finden sich dann detaillierte Ausführungen zu den Datenschutzprozessen der Ablauforganisation wieder. Unterstützt von vielen grafischen Abbildungen werden anschaulich die Organisationabläufe der einzelnen rechtlichen Anforderungen erläutert. Neben dem Datenschutz-Risikomanagement umfasst dies die Datenschutzdokumentation, die Sensibilisierung zum Datenschutz, die Thematik des Datenschutzaudits / bzw. der Datenschutzzertifizierung sowie das Datenschutz-Managementsystem. Ein dabei immer wieder eingeforderter Prozessschritt ist der PDCA-Zyklus (plan-do-check-act), der in vielen Organisationsstrukturen bereits z.B. bei der Informationssicherheit implementiert ist.

Die Ausführungen zum Risikomanagement beinhalten eine detaillierte Darstellung der Anforderungen an einen risikobasierten Ansatz und an einen Risikomanagementprozess. Die Matrix zur Risikobewertung folgt den Festlegungen in der ISO 29134 und wird durch anschauliche grafische Abbildungen gut nachvollziehbar vermittelt. Hinsichtlich der Umsetzung einer Datenschutz-Folgenabschätzung werden die Schritte zur Risikoidentifikation, der Risikoanalyse und der Risikoevaluation erläutert, bevor dann die Ausführungen zu den Risikobehandlungsoptionen folgen. Auch den in der DS-GVO gestiegenen Dokumentations- und Nachweispflichten (vgl. Art. 5 Abs. 2) wird durch tabellarische Aufliste der Dokumentationsanforderungen und grafischen Darstellungen Rechnung getragen.

Im abschließenden dritten Teil werden die Befugnisse der Aufsichtsbehörden dargelegt, bevor durch mehreren Prüffragen zu den einzelnen Maßnahmen eine Selbstprüfung ermöglicht wird.

Das Buch ist uneingeschränkt empfehlenswert, fasst es doch in überschaubarem Umfang die wichtigsten prozessualen Anforderungen an die Umsetzung der DS-GVO zusammen. Die vielen grafischen Darstellungen erleichtern die Komplexität der Zusammenhänge zu erfassen. Auch wenn sich das Buch explizit nur an den für die Datenverarbeitung Verantwortlichen richtet, hilft es auch dem Datenschutzbeauftragten, den Verantwortlichen effektiv zu beraten.

Rezension von Rudi Kramer,
Stellv. Vorstandsvorsitzender des BvD