ESV ERICH SCHMIDT VERLAG

Handbuch Datenschutz und IT-Sicherheit

Herausgegeben von
Dr. Uwe Schläger und Jan-Christoph Thode

Unter Mitarbeit von
Dr. Christian Borchers, Conrad S. Conrad, Michael Cyl, Dr. Sebastian Ertel, Annika Freund, Clemens Grünwald, Jennifer Jähn, Dr. Irene Karper, Jan-Roman Kitzinger, Dr. Martin Klein-Hennig, Martin Kolodziej, Dr. Bettina Kraft, Dr. Sönke Maseberg, Dr. Britta Mester, Lars Meyer, Dr. Sanela Hodžić , Lea Paschke, Jan Peplow, Olaf Rossow, Jan Schirrmacher, Dr. Uwe Schläger, Felix Schmidt, Markus Schönmann, Stefan R. Seiter, Daniel Stolper, Oliver Stutz, Jan-Christoph Thode, Sven Venzke-Caprarese, Ralf von Rahden

ERICH SCHMIDT VERLAG

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Weitere Informationen zu diesem Titel finden Sie unter
ESV.info/978 3 503 17727 1

Gedrucktes Werk: ISBN 978 3 503 17727 1
eBook: ISBN 978 3 503 17728 8

Dieses Papier erfüllt die Frankfurter Forderungen der Deutschen Nationalbibliothek und der Gesellschaft für das Buch bezüglich der Alterungsbeständigkeit und entspricht sowohl den strengen Bestimmungen der US Norm Ansi/Niso Z 39.48-1992 als auch der ISO-Norm 9706.

Satz: schwarz auf weiß, Herrig & Schimschok, Berlin
Druck und Bindung: Hubert & Co., Göttingen

Vorwort

Am 25. Mai 2018 ersetzt die EU-Datenschutz-Grundverordnung das bisherige Bundesdatenschutzgesetz. Nach jahrelanger Diskussion wird damit europäisches Datenschutzrecht endlich harmonisiert, sehr zum Vorteil international tätiger Unternehmen, aber auch zum Vorteil kleinerer Online-Shops, die sich bislang innerhalb der EU nach den jeweils geltenden nationalen Datenschutzvorschriften richten mussten.

Trotz der Harmonisierung kommen auf Unternehmen neue Herausforderungen zu: Neben erweiterten Informations-, Rechenschafts- und Meldepflichten gilt es, für Verfahren mit hohen Risiken für die Persönlichkeitsrechte der Betroffenen eine Datenschutz-Folgenabschätzung durchzuführen. Auftragsverarbeiter müssen künftig ebenso wie Verantwortliche ein Verzeichnis von Verarbeitungstätigkeiten führen. Auch die Eignung technischer und organisatorischer Sicherheitsmaßnahmen muss künftig regelmäßig überprüft und dokumentiert werden. Ganz zu schweigen von den deutlich erweiterten und erhöhten Bußgeldern, die künftig von Datenschutz-Aufsichtsbehörden verhängt werden können.

Die mit der Datenschutz-Grundverordnung verbunden Neuerungen sollten für Unternehmen, die sich bislang konform zum Bundesdatenschutzgesetz aufgestellt haben, kein besonderes Problem darstellen. Wer bislang seine datenschutzrechtlichen Hausaufgaben erledigt hat, kann auf bestehenden Datenschutzstrukturen aufbauen, muss diese allerdings an einigen Stellen anpassen und gegebenenfalls erweitern. Unternehmen mit gravierenden Datenschutzdefiziten, die in der Vergangenheit eher darauf vertraut haben, nicht negativ aufzufallen, drohen allerdings nunmehr drastische Bußgelder.

Und hier setzt unser neues Datenschutz-Handbuch an: Wir, dies sind erfahrene Beraterinnen und Berater der datenschutz nord Gruppe, die seit Jahren in den Bereichen Datenschutz und Informationssicherheit als Consultant tätig sind, haben für Sie ein Datenschutz-Handbuch erstellt, das zum einen auf die neuen gesetzlichen Regelungen der Datenschutz-Grundverordnung im Detail eingeht. Zum anderen stellen wir Ihnen Best-Practice-Ansätze vor, wie den neuen gesetzlichen Vorgaben am besten entsprochen werden kann.

Das vorliegende Datenschutz-Handbuch richtet sich an betriebliche Datenschutzbeauftragte, IT-Administratoren, Unternehmensleitungen, Betriebs- oder Personalräte, aber auch an datenschutzinteressierte Beschäftigte und Kunden, die sich entweder einen Überblick über die neuen gesetzlichen Regelungen verschaffen wollen oder praxisgerechte Vorschläge zur Umsetzung der Datenschutz-Grundverordnung nachlesen möchten.

Das Datenschutz-Handbuch gliedert sich im Wesentlichen in zwei Hauptteile: Die Kapitel A bis F sind datenschutzrechtlich geprägte Kapitel, während die Kapitel G

bis J sicherheitstechnische Aspekte in den Vordergrund stellen. Nachdem wir in Kapitel A zunächst auf die neuen datenschutzrechtlichen Grundlagen eingehen, stellen wir in Kapitel B vor, wie ein betriebliches Datenschutz-Management umgesetzt werden sollte. In Kapitel C steht die gesetzeskonforme Verarbeitung von Beschäftigtendaten im Vordergrund, in Kapitel D die gesetzeskonforme Verarbeitung von Kundendaten. Kapitel E beschäftigt sich mit der Verarbeitung personenbezogener Daten im Internet, in sozialen Netzwerken und in unternehmenseigenen Intranets. Kapitel F stellt dar, in welchem Umfang Videosysteme nach der neuen Datenschutz-Grundverordnung betrieben werden können.

Der zweite Hauptteil des Handbuches beginnt in Kapitel G mit einer Darstellung der rechtlichen Grundlagen der IT-Sicherheit. In Kapitel H werden die Eckpfeiler eines Informationssicherheits-Managements beschrieben. Kapitel I stellt geeignete technisch-organisatorische Maßnahmen vor, und zwar übergreifende Maßnahmen, Infrastrukturmaßnahmen, Maßnahmen seitens der IT-Systeme, Netzwerkmaßnahmen und Maßnahmen auf Anwendungsebene. Und schließlich wird in Kapitel J beschrieben, in welcher Form Penetrationstest zur Evaluierung einer angemessenen IT-Sicherheit durchgeführt werden können.

Trotz der zahlreichen Verweise auf andere Kapitel dieses Buches sind sämtliche Hauptkapitel in sich abgeschlossen und können separat ohne Kenntnis der anderen Kapitel als Erkenntnisquelle dienen.

In diesem Sinne wünschen wir Ihnen als Herausgeber dieses Datenschutz-Handbuchs viel Spaß beim Lesen und Nachschlagen.

Bremen und Berlin, im Januar 2018

Uwe Schläger und
Jan-Christoph Thode

Inhaltsverzeichnis

Teil J