Einleitung

Im Jahr 2016 trat auf europäischer Ebene die Datenschutz-Grundverordnung (DSGVO) in Kraft, die ab dem 25. Mai 2018 in allen EU-Mitgliedstaaten gilt. Die DSGVO soll für ein einheitliches und modernes Datenschutzrecht sorgen.

Kurz vor dem Stichtag im Frühjahr 2018 war in den Unternehmen sowie in der Öffentlichkeit eine gewisse Panik zu beobachten. Viele sahen sich einer Herkulesaufgabe gegenüber, denn in vielen Fällen wurden die Informations-, Dokumentations- und Sorgfaltspflichten bei der Datenverarbeitung in der Vergangenheit eher stiefmütterlich behandelt. Die Bußgelder, die für bestimmte Datenschutzverstöße verhängt werden können, sind erheblich: Für besonders gravierende Verstöße beträgt der Bußgeldrahmen bis zu 20 Millionen Euro oder für Unternehmen bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes im vorangegangenen Geschäftsjahr.

2017 erschien die 1. Auflage des Werkes, das Sie nun in den Händen halten. Wir haben uns zum Ziel gesetzt, den Leserinnen und Lesern einen verlässlichen Leitfaden zum Thema *Datenschutz mit SAP* zu geben. Diese 2. Auflage geht nun über SAP S/4HANA und die SAP Business Suite weit hinaus. Denn mit der zunehmenden Verbreitung von Cloud-Lösungen stellt sich immer dringlicher die Frage, wie Datenschutz in der Cloud sichergestellt werden kann. Aus diesem Grund werden in dieser 2. Auflage Lösungen wie SAP Ariba, SAP Cloud Platform, SAP Concur und SAP SuccessFactors in ihren Datenschutzmöglichkeiten betrachtet.

Nachfolgend möchten wir Ihnen die Zielsetzung und die Inhalte des Buches vorstellen. Die meisten Leserinnen und Leser derartiger Fachbücher nutzen diese als Nachschlagwerke; wir möchten darüber hinaus auch einen »roten Faden« mitgeben, also einen Hinweis dazu, welche Abschnitte Sie lesen sollten, um sich einen umfassenden Überblick zum Datenschutz mit SAP zu verschaffen.

Ziel des Buches

Dieses Buch soll Sie in die Lage versetzen, in Ihrer SAP-Landschaft einen datenschutzkonformen Betrieb sicherstellen zu können. Dazu sind Überlegungen zur Rechtsanwendung erforderlich. Diese Überlegungen sollen keinesfalls einen anwaltlichen Rat oder eine juristische Meinung ersetzen. Vielmehr dienen unsere Ausführungen im Wesentlichen der Kontextuali-

sierung und der Begründung, warum welche Features wie genutzt werden können. Dies wären dann auch schon die ersten beiden wesentlichen Teilziele unseres Buches: eine aus der Softwareperspektive stammende Betrachtung möglicher Anwendungen des geltenden Rechts und ein Verständnis der zur Verfügung gestellten Features.

Das nächste wesentliche Teilziel ist es, Ihnen zu zeigen, wie Sie am sinnvollsten ein solches Implementierungsprojekt starten.

Insoweit ist dieses Buch ein Dreiklang aus Annahmen zu den rechtlichen Tatbeständen, technischen Funktionen und einem Vorgehensmodell. Dadurch, dass wir die rechtlichen Annahmen transparent werden lassen, haben Sie auch die Möglichkeit, zu eigenen Schlüssen zu gelangen und ein individuelles Vorgehensmodell zu entwickeln.

Aufbau des Buches

Das Buch ist in 14 Kapitel gegliedert, die wir im Folgenden zur besseren Orientierung in Form von Kurzdarstellungen zusammengefasst haben. Sie erhalten einen Überblick, was Sie in den einzelnen Kapiteln erwartet und an wen sich das betreffende Kapitel jeweils richtet bzw. für wen die Lektüre ein Muss ist.

Rechtsgrundlagen

In **Kapitel 1**, »›Maßnehmen für Maßnahmen‹: Einführung«, wenden wir uns den Rechtsgrundlagen zu, die unserer Ansicht nach für den Systembetrieb zu berücksichtigen sind. Wir empfehlen Ihnen, dieses Kapitel in jedem Fall vollständig durchzuarbeiten!

Zwar informieren wir Sie in diesem Kapitel auch über drohende Bußgelder und den räumlichen Geltungsbereich der rechtlichen Vorschriften, entsprechend unserer Zielsetzung, beschäftigen wir uns aber primär mit Prozessen, Daten und dem Systembetrieb. Zunächst klären wir die wesentlichen Grundlagen der Verarbeitung. Wir diskutieren u. a., welche Voraussetzungen unseres Erachtens erfüllt sein müssen, um überhaupt personenbezogene Daten verarbeiten zu dürfen, und welche Daten als besonders problematisch – eben als Daten besonderer Kategorien – zu behandeln sind.

Im Anschluss daran stellen wir den jeweiligen Anforderungen die technischen Umsetzungsmöglichkeiten und ihre sachlogischen Grenzen gegenüber.

Besonderes Gewicht kommt Abschnitt 1.2.12, »Angemessenheit der Maßnahmen, Dokumentation und Nachweis«, und Abschnitt 1.2.13, »Sicherheit der Verarbeitung«, zu. Hier diskutieren wir die Herausforderungen der tech-

nischen Sicherheit sowie der ständigen Dokumentation und des fortlaufenden Nachweises. Prinzipiell ist anzunehmen, dass die Aufgaben »Sicherheit« und »Nachweis der Sicherheit« zu einem endlos währenden Kontrollzirkel führen, der bei Neueinführungen oder Verfahrensänderungen mit einer Datenschutz-Folgeabschätzung beginnen muss. Diese skizzieren wir in Abschnitt 1.2.14, »Datenschutz-Folgenabschätzung«. Zu den Nachweisen gehört auch das Verzeichnis der Verarbeitungstätigkeiten, das wir in Abschnitt 1.2.15, »Verzeichnis von Verarbeitungstätigkeiten«, behandeln.

Im nachfolgenden Abschnitt 1.3, »Welche Anforderungen sind notwendigerweise technisch zu unterstützen?«, diskutieren wir, welche Anforderungen aus unserer Sicht zwingend einer technischen Umsetzung bedürfen, wie z. B. der Nachweis der Zweckbindung der Verarbeitung (Abschnitt 1.3.1, »Zweckbindung der Verarbeitung«), die Löschung von Daten, die in Deutschland traditionell im Fokus der Aufsichtsbehörden stehen (Abschnitt 1.3.3, »Datenlöschung – Datensperrung«) oder das Auskunftsrecht (Abschnitt 1.3.6, »Auskunft«).

Im nächsten Abschnitt 1.4, »Welche Anforderungen können technisch unterstützt werden?«, gehen wir auf Anforderungen ein, die zwar nicht zwingend durch eine technische Lösung zu unterstützen sind, aber durch eine technische Lösung signifikant vereinfacht werden können. Beispiele hierzu geben wir in Abschnitt 1.4.1, »Einwilligung«, und in Abschnitt 1.4.4, »Vorabauskunft«.

Personenbezogene Daten in SAP-Systemen

In **Kapitel 2**, »›Wo laufen sie denn‹: Wo Sie personenbezogene Daten finden«, weisen wir exemplarisch unterschiedliche personenbezogene Daten nach, z. B. den Kundestammsatz, den zentralen Geschäftspartner, aber auch verbundene transaktionale Daten. Ferner diskutieren wir in diesem Kapitel die Zusammenhänge zwischen Stammdaten und transaktionalen Daten.

Wenn Sie die SAP Business Suite kennen und Ihnen auch der Zusammenhang zwischen Stammdaten und transaktionalen Daten in Bezug auf den Datenschutz klar ist, können Sie dieses Kapitel überspringen.

Vorgehensweise im Projekt

In **Kapitel 3**, »›Vom ersten Schritt zum Weg zum Ziel‹: Vorgehensmodell«, entwickeln wir unseren Vorschlag zum Projektvorgehen. Wir legen die Lektüre dieses Kapitels daher all denen nahe, die sich mit den Mühen eines Einführungsprojekts auseinandersetzen müssen oder wollen.

In Abschnitt, 3.1.1, »Was bedeutet der induktive Ansatz?«, legen wir dar, warum zumindest in einem Bestandssystem die Wahrheit in den Daten liegt und somit ein Top-down-Ansatz in der Regel nicht sinnvoll ist. Wir zei-

gen, warum jedes Projekt im Bestand mit dem Sperren und Löschen beginnen sollte und es anschließend Schritt für Schritt durchgeführt werden kann, bis wir Ihnen in Abschnitt 3.1.10, »Audit, Nachweis und Dokumentation«, darlegen, wie Sie auch den Nachweispflichten Genüge tun können. Schließlich stellen wir in Abschnitt 3.2, »Wege zum Verzeichnis von Verarbeitungstätigkeiten«, dar, warum unser Bottom-up-Ansatz auch die Darstellung im Verzeichnis von Verarbeitungstätigkeiten vereinfacht.

SAP Information Lifecycle Management

In **Kapitel 4**, »›Auch das Ende muss bestimmt sein‹: Sperren und Löschen mit SAP Information Lifecycle Management«, ist für Leser gedacht, die das Sperren und Löschen auch technisch umsetzen sollen.

Zunächst stellen wir Ihnen in einer Einführung Begriffe und Zusammenhänge vor. Was wir nicht darstellen, sind Ansätze der »klassischen Archivierung«, da diese zwar möglich, aber aus unserer Sicht nicht empfehlenswert für das datenschutzbezogene Sperren und Löschen sind. In Abschnitt 4.2, »Überblick über das Sperren und Löschen mit SAP ILM«, zeigen wir Ihnen die zwingenden vorbereitenden Maßnahmen und Einstellungen, die Sie vornehmen müssen, um das vereinfachte Sperren und Löschen, basierend auf SAP ILM, einzuführen. In Abschnitt 4.3, »Vorbereitungen für das vereinfachte Sperren«, widmen wir uns der Entwicklung der betriebswirtschaftlichen Perspektive des Sperrens und Löschens. Vergessen Sie nicht, dass die Daten, über die wir sprechen, in einem komplexen betriebswirtschaftlichen Zusammenhang zu betrachten sind, aus dem sich neben der Notwendigkeit des Sperrens und Löschens auch betriebswirtschaftliche und rechtliche Notwendigkeiten der Aufbewahrung ergeben. Diese Betrachtung führen wir in Abschnitt 4.4, »Stamm- und Bewegungsdaten sperren«, für das Löschen fort. In Abschnitt 4.6, »Legal Case Management«, stellen wir das Verfahren dar, das ursprünglich für das Handling von rechtsfallverbundenen Aufbewahrungspflichten gedacht war, aber auch dazu geeignet ist, das »Recht auf Einschränkung der Verarbeitung« im Sinne des Art. 18 DSGVO zu realisieren. Schließlich gehen wir in Abschnitt 4.8, »Zeitabhängiges Sperren personenbezogener Daten in der Personaladministration (SAP ERP HCM-PA)«, auf die Besonderheiten des Sperrens in SAP ERP HCM-PA ein.

Zweck der Verarbeitung

Kapitel 5, »›Struktur ist alles‹: Verarbeitung muss auf dem Zweck basieren«, ist ein herausforderndes Kapitel, in dem dargestellt wird, wie Sie die zweckbezogene Datentrennung im System sicherstellen können. Nach einer einleitenden Betrachtung in Abschnitt 5.1, »Verantwortlicher und Zweck«, in der wir den zwingenden Zusammenhang zwischen einer juristischen Person im Sinne der DSGVO (Verantwortlicher) und dem Zweck der Verarbeitung entwickeln, stellen wir in Abschnitt 5.2, »Organisationsstrukturen (Linienorganisation)«, und Abschnitt 5.3, »Prozessorganisation«, dar, wie Linien- und Prozessorganisation im System konfiguriert sein müssen, um eine zweckbezogene Verarbeitung im Mandanten nachweisen zu können. In Abschnitt 5.4, »Linien- und Prozessorganisation definieren den Zweck«, bringen wir die beiden Dimensionen der Linie und des Prozesses schließlich zusammen.

Für Sie heißt das: Sofern Sie einen instruktiven Überblick über die Thematik erhalten oder sich in ihrer beruflichen Praxis mit Berechtigungen bzw. mit dem Sperren und Löschen beschäftigen, ist die Lektüre dieses Kapitels ein klares Muss, auch wenn die Thematik (zunächst noch) sehr abstrakt abgehandelt wird.

Data Controller Rule Framework

Kapitel 6, »›Dem Ende Struktur geben‹: Data Controller Rule Framework«, schließt thematisch an Kapitel 5 an. Beschäftigten wir uns im vorangehenden Kapitel mit systematisch herzuleitenden Modellüberlegungen, stellen wir nun konkrete Überlegungen zu den notwendigen Schritten für den »umgekehrten« Geschäftsprozess des Sperrens und Löschens an (Abschnitt 6.1, »Organisation des Löschens in Geschäftsprozessen«). Des Weiteren führen wir in die Neuentwicklung des Data Controller Rule Frameworks ein, das auf der in Kapitel 5 vorgenommenen Abstraktion basiert und das Pflegen von Regeln in SAP ILM aus der betriebswirtschaftlichen Perspektive vereinfacht. (Patentanträge zu dieser Lösung sind anhängig.)

Kapitel 6, »›Dem Ende Struktur geben‹: Data Controller Rule Framework«, ist also für die Vereinfachung des Sperren und Löschens wesentlich und insofern für alle, die sich hiermit beschäftigen, Pflichtlektüre.

Berechtigungskonzept

Kapitel 7, »›Die Struktur berechtigt‹: Auswirkungen auf das Berechtigungskonzept«, stellt die Ableitungen aus der Zwecktrennung für das Berechtigungskonzept in den Mittelpunkt. Es ist dementsprechend nur für das Berechtigungskonzept und das Audit des Berechtigungskonzepts von Relevanz bzw. für diejenigen unter Ihnen gedacht, die einen Einstieg in diese komplexe Problematik benötigen.

Wir beschäftigen uns zunächst in Abschnitt 7.1, »Benutzer und Berechtigungen – eine Einführung«, nur sehr allgemein mit dem Thema *Berechtigungen*, um dann in den beiden folgenden Abschnitten unsere Erkenntnisse aus Kapitel 5, »›Struktur ist alles‹: Verarbeitung muss auf dem Zweck basieren«, zum Thema *Zwecktrennung* auf das Berechtigungskonzept anzuwenden. In Abschnitt 7.4, »Berechtigungsrisiken«, widmen wir uns der Definition von Berechtigungsrisiken.

Information Retrieval Framework

Kapitel 8, »›Transparenz gewinnt‹: Information Retrieval Framework«, richtet sich an diejenigen von Ihnen, die sich mit Auskunft, Vorabauskunft und einer etwaigen Nutzung für das Verzeichnis von Verarbeitungstätigkeiten beschäftigen. Wir zeigen Ihnen in diesem Kapitel, wie Sie das neue Information Retrieval Framework bei der Aufgabe unterstützt, transparente Auskunft an Betroffene zu geben. Auch dieses Framework ist eine Neueinführung, für die Patentanträge seitens der Autoren anhängig sind. Nach einer allgemeinen Einführung, in der wir auch den Zusammenhang zwischen Auskunft und Vorabinformation darstellen, widmen wir uns in den folgenden Abschnitten zunächst dem Einrichten des Information Retrieval Frameworks, um dann in Abschnitt 8.6, »Beauskunftung durchführen«, die Abwicklung einer Auskunft konkret zu beschreiben.

Read Access Logging

Kapitel 9, »›Schau mal, wer da liest‹: Read Access Logging«, ist wichtig für Leser, die als besondere Form des überwachenden Schutzes eine Protokollierung rein lesender Zugriffe auf personenbezogene Daten einführen möchten. Einleitend stellen wir das Spannungsfeld, in dem sich die Leseprotokollierung zwingend bewegt, dar, um anschließend das technische Einrichten detailliert zu erläutern.

SAP Master Data Governance

Kapitel 10, »›Der Herr der Daten werden‹: SAP Master Data Governance«, ist für alle gedacht, die an dauerhaften Lösungen in Bezug auf rechtskonforme, plattformübergreifende Datenqualität interessiert sind.

Wir beschreiben in diesem Kapitel, wie Sie die zusätzliche Lösung SAP Master Data Governance nutzen können, um dauerhaft für bestimmte Daten sicherzustellen, dass diese plattformübergreifend datenschutzkonform verarbeitet werden können. Während im Standard die Korrektur der Daten möglich ist, versetzt Sie SAP Master Data Government dazu in die Lage, bestimmte wesentliche Daten dauerhaft rechtskonform zu halten.

Datenschutz in Cloud-Lösungen

In **Kapitel 11**, »›Der Kopf in den Wolken‹: Datenschutz in Cloud-Lösungen«, beschreiben wir wesentliche Besonderheiten der Cloud-Lösungen. So erläutern wir z. B. in Abschnitt 11.1.3, »Rollen und Verantwortlichkeiten«, unser Verständnis der Rollen und Verantwortlichkeiten und gehen in Abschnitt 11.2.8, »Technische und Organisatorische Maßnahmen (TOM) in den SAP-Cloud-Lösungen«, auf die Umsetzung der technisch-organisatorischen Maßnahmen in der Cloud ein.

SAP Cloud Platform

Im **Kapitel 12**, »›Lösungen, die wachsen und nicht wuchern‹: Datenschutz in der SAP Cloud Platform«, stellen wir Ihnen die Datenschutzfunktionen der SAP Cloud Platform vor, unserer nativen Cloud-Plattform für Ihre Entwicklungen, aber auch für die Entwicklungen unserer Partner. Wir stellen dar, um was es sich bei der SAP Cloud Platform handelt, wie dort entwickelt

werden kann und welche Datenschutzfunktionen aktuell zur Verfügung gestellt werden.

Ariba, Concur, SuccessFactors und Customer Experience

In **Kapitel 13**, »›In der Wolke auf Sicht steuern‹: Übersicht über die Datenschutzfunktionen in SAP-Cloud-Lösungen« beschreiben wir die Datenschutz-Features in SAP Ariba, SAP Concur, SAP SuccessFactors und SAP Customer Experience. Bei Letzterem sind besonders die SAP-Lösungen SAP Customer Data Cloud, SAP Marketing Cloud, SAP Commerce Cloud, SAP Sales Cloud und SAP Service Cloud im Vordergrund.

Kontrollsystem

Den Abschluss bildet **Kapitel 14**, »›Täglich grüßt das …‹: Schützen, Kontrollieren, Nachweisen und Kontrollen nachweisen«. Wir erwähnten bereits, dass mit der DSGVO aus unserer Sicht ein endloser Kontroll- und Nachweiskreis beginnt. Unsere zuständigen Gewährsleute aus der Entwicklung hätten dieses Kapitel gerne auf mehrere Hundert Seiten aufgeblasen. Dies wäre der Sache auch gerecht, nur nicht dem geneigten Leser, der einer Einführung bedarf. Aus der – aus unserer Sicht – relevanten Rechtsgrundlage der DSGVO entwickeln wir in diesem Kapitel nach und nach, welche Kontrollen erforderlich sind. Wir beginnen mit Abschnitt 14.1, »Kontrollrahmen und Grundlagen der Verarbeitung«, und Abschnitt 14.2, »Rechtmäßigkeit, Treu und Glauben und Transparenz«, die generell noch abstrakt gehalten sind. Anschließend fokussieren wir uns auf bestimmte Prüfgebiete der DSGOV – wie z. B. Zweckbindung oder Integrität und Vertraulichkeit. Schließlich gelangen wir in Abschnitt 14.10, »Beispiele technischer Kontrollhandlungen«, zu konkreten, aber immer noch exemplarischen Kontrollhandlungen.

Sind Sie nur an einem Überblick interessiert, empfehlen wir Ihnen lediglich die Lektüre von Abschnitt 14.1, »Kontrollrahmen und Grundlagen der Verarbeitung«, bis Abschnitt 14.9, »Abstrakte technische Kontrollhandlungen«. Abschnitt 14.10, »Beispiele technischer Kontrollhandlungen«, richtet sich hingegen an den technisch versierten Leser, der einen ersten Eindruck davon erhalten will, was in Bezug auf Kontrollen und Nachweise zu tun ist. Dabei haben wir uns bewusst knapp gehalten – denn uns ist es wichtig, dass Sie eine Vorstellung davon erhalten, was zu tun ist.

Anhang

In **Anhang A**, »Glossar«, finden Sie eine Übersicht über zentrale Begriffe der DSGVO. In **Anhang B** haben wir relevante Transaktionen und Reports sowie SAP-Hinweise zusammengestellt. **Anhang C**, »Literaturverzeichnis«, enthält Tipps für weiterführende Informationen.

Zusatzinformationen

In hervorgehobenen Informationskästen sind Inhalte zu finden, die wissenswert und hilfreich sind, aber etwas außerhalb der eigentlichen Erläuterung stehen. Damit Sie die Informationen in den Kästen sofort einordnen können, haben wir die Kästen mit Symbolen gekennzeichnet:

Kästen mit diesem Symbol geben Ihnen spezielle Empfehlungen, die Ihnen die Arbeit erleichtern können.

In Kästen, die mit diesem Symbol gekennzeichnet sind, finden Sie zusätzliche Informationen oder wichtige Inhalte, die Sie sich merken sollten.

Mit diesem Symbol haben wir Besonderheiten gekennzeichnet, die Sie beachten sollten. Es warnt Sie außerdem vor häufig gemachten Fehlern oder Problemen, die auftreten können.

Mit diesem Symbol weisen wir auf Szenarien aus der Praxis hin und erläutern, wie die Funktionen im Einzelnen eingesetzt werden.

Danksagung

Volker Lehnert

Bereits im Jahr 2011 erschien das erste Datenschutzbuch unter meiner Co-Autorschaft. 2012 übernahm ich als Product Owner zusammen mit einem Teil des Autorenteams des vorliegenden Buches die Verantwortung für den Datenschutz in der SAP Business Suite und später für SAP S/4HANA. Zahlreiche Entwicklerinnen und Entwickler haben seitdem an Datenschutzfeatures in diesen Lösungen gearbeitet, zahlreiche Kolleginnen und Kollegen, z. B. aus dem GRC-Management oder auch aus SAP Data Custodian, haben mit diesem Team die Kooperation gesucht, um den Datenschutz im Portfolio zu stärken. All diesen Kolleginnen und Kollegen wäre zu danken. Da es sich aber um Hunderte handelt, muss mein Dank allgemein bleiben.

In jedem Fall ist namentlich meiner Familie zu danken: meiner Tochter Sara Dittrich und meiner Partnerin Dr. Monika Dittrich, die schlechte Laune ertragen und mir Zeit lassen mussten, denn die 2. Auflage dieses Buches war eine schwere Geburt. Meiner Lektorin, Eva Tripp vom Rheinwerk Verlag, danke ich für ihre Geduld.

Iwona Luther

Ich danke Ihnen, liebe Leserin oder lieber Leser, für Ihr Interesse am vereinfachten Sperren und Löschen mit SAP ILM im Kontext des Datenschutzes.

Denn ohne Ihr Interesse gäbe es diese 2. Auflage unseres Buches – mit dem deutlich umfangreicheren Kapitel zu SAP ILM – nicht. Bedanken möchte ich mich auch bei Volker Lehnert. Danke, Volker, dass du mich gefragt hast, ob ich an diesem Buch mitwirken möchte. Ohne dich wäre ich nie Buchautorin geworden – und es hätte auch mein Buch »SAP Information Lifecycle Management« nicht gegeben.

Markus Röder

Mein Dank geht zuerst an das Autorenteam, hier insbesondere an Volker Lehnert, der mich als Autor für neue Kapitel in der 2. Auflage seines Buches zum Thema Cloud-Systeme ins Team holte. Außerdem gilt mein Dank vielen Kolleginnen und Kollegen bei SAP, die sich unermüdlich für den Datenschutz einsetzen. Mein Dank geht auch an das Lektorat des Rheinwerk Verlags, insbesondere an unsere Projektleiterin Eva Tripp für den tollen Support. Last but not least möchte ich mich bei meiner Familie bedanken, die mir bei der Arbeit, die sich oft in die Abendstunden erstreckte, den Rücken freihielt.

Thorsten Bruckmeier

Im Januar 2017 präsentierte ich zusammen mit Matthias Vogel eine Vision für den Datenschutz auf der SAP Cloud Platform. Die beschriebe Lösung wäre heute ohne Unterstützung vieler Kolleginnen und Kollegen bei SAP nicht verfügbar. Nun ist es möglich, in diesem Buch die fertige Lösung zu beschreiben, dafür bin ich sehr dankbar. Mein Dank geht auch an das Lektorat des Rheinwerk Verlag und insbesondere an Eva Tripp für ihre tolle Unterstützung. Zuletzt möchte ich mich bei meiner Frau und meinen vier Kindern bedanken, die es mir ermöglichten, ungestört am Buch zu arbeiten.

Björn Christoph

Es war mir ein Vergnügen, viele Jahre an der Umsetzung des komplexen Themas Datenschutz mitzuwirken, Lösungen zu erarbeiten und Ihnen die aktuellen Lösungen in dieser 2. Auflage näherbringen zu können. Mein Dank gilt insbesondere meinen geschätzten Kollegen Volker Lehnert und Carsten Pluder für die enge Zusammenarbeit in den letzten Jahren, allen Kolleginnen und Kollegen, die mich unterstützt haben, sowie unserer Lektorin, Frau Eva Tripp vom Rheinwerk Verlag

Carsten Pluder

Ich empfinde es als großes Glück, so viele Jahre schon mit so vielen tollen Kolleginnen und Kollegen am Thema Datenschutz in SAP-Systemen arbeiten zu dürfen. Dementsprechend geht mein Dank zuallererst an all die Personen bei SAP, die uns in den letzten Jahren unterstützt haben. Ich freue mich über die Möglichkeit, diese Fortschritte in der 2. Auflage dieses Buches zu beschreiben. Daher geht mein Dank sowohl an das Autorenteam als auch an den Rheinwerk Verlag und insbesondere an Eva Tripp für das wunderbare Ergebnis unserer gemeinsamen Arbeit.