

Auf einen Blick

1	»Maßnahmen für Maßnahmen«: Einführung	31
2	»Wo laufen sie denn«: Wo Sie personenbezogene Daten finden	99
3	»Vom ersten Schritt zum Weg zum Ziel«: Vorgehensmodell	127
4	»Auch das Ende muss bestimmt sein«: Sperren und Löschen mit SAP Information Lifecycle Management	153
5	»Struktur ist alles«: Verarbeitung muss auf dem Zweck basieren	253
6	»Dem Ende Struktur geben«: Data Controller Rule Framework	273
7	»Die Struktur berechtigt«: Auswirkungen auf das Berechtigungskonzept	299
8	»Transparenz gewinnt«: Information Retrieval Framework	315
9	»Schau mal, wer da liest«: Read Access Logging	355
10	»Der Herr der Daten werden«: SAP Master Data Governance	389
11	»Der Kopf in den Wolken«: Datenschutz in Cloud-Lösungen	405
12	»Lösungen, die wachsen und nicht wuchern«: Datenschutz in der SAP Cloud Platform	435
13	»In der Wolke auf Sicht steuern«: Übersicht über die Datenschutzfunktionen in SAP-Cloud-Lösungen	477
14	»Täglich grüßt das ...«: Schützen, Kontrollieren, Nachweisen und Kontrollen nachweisen	599

Inhalt

Geleitwort	19
Einleitung	21

1 »Maßnahmen für Maßnahmen«: Einführung 31

1.1 Die DSGVO fiel nicht vom Himmel	32
1.2 Was bedeutet die DSGVO für Sie?	33
1.2.1 Begriffliche und sachliche Grundlagen	34
1.2.2 Einschränkung durch speziellere Regelungen	39
1.2.3 Grundlagen der Verarbeitung	40
1.2.4 Daten besonderer Kategorien	42
1.2.5 Rechtfertigende Tatbestände zur Verarbeitung	44
1.2.6 Die Besonderheiten der Einwilligung als rechtfertigender Tatbestand zur Verarbeitung	44
1.2.7 Transparenzgebot	49
1.2.8 Richtigkeit der Daten	54
1.2.9 Recht auf Vergessenwerden	54
1.2.10 Datenübertragbarkeit (Portability)	57
1.2.11 Widerspruch, automatisierte Entscheidungen und Profiling	58
1.2.12 Angemessenheit der Maßnahmen, Dokumentation und Nachweis	59
1.2.13 Sicherheit der Verarbeitung	60
1.2.14 Datenschutz-Folgenabschätzung	65
1.2.15 Verzeichnis von Verarbeitungstätigkeiten	66
1.3 Welche Anforderungen sind notwendigerweise technisch zu unterstützen?	67
1.3.1 Zweckbindung der Verarbeitung	67
1.3.2 Datenrichtigkeit – Korrektur	69
1.3.3 Datenlöschung – Datensperrung	70
1.3.4 Technisch-organisatorische Maßnahmen (TOM)	73
1.3.5 Rechenschaftspflichten – Auditierbarkeit	82
1.3.6 Auskunft	85

1.4 Welche Anforderungen können technisch unterstützt werden?	88
1.4.1 Einwilligung	88
1.4.2 Datenminimierung	88
1.4.3 Datenrichtigkeit – Datenmanagement	90
1.4.4 Vorabauskunft	90
1.4.5 Verzeichnis von Verarbeitungstätigkeiten	91
1.4.6 Rechenschaftspflichten – Compliance Management	92
1.5 Auftragsverarbeitung	95
1.6 Zusammenfassung	97
2 »Wo laufen sie denn«: Wo Sie personenbezogene Daten finden	99
<hr/>	
2.1 SAP Business Suite und SAP S/4HANA	100
2.2 Stammdaten – Bewegungsdaten	100
2.3 Personenbezogene Daten in SAP ERP und SAP S/4HANA	102
2.3.1 Geschäftspartner	102
2.3.2 Unmittelbar personenbezogene Datensätze in Financials	103
2.3.3 Weitere personenbezogene Datensätze in FI	109
2.3.4 Mitarbeiterdaten in FI	110
2.3.5 Benutzerdaten in FI	110
2.3.6 Unmittelbar personenbezogene Datensätze in CO	111
2.3.7 Mittelbar personenbezogene Datensätze in CO	112
2.3.8 Reporting-Tools in CO und kundeneigenes Reporting	114
2.3.9 Benutzerdaten in CO	115
2.3.10 Unmittelbar personenbezogene Daten in SD	115
2.4 Personenbezogene Daten in SAP ERP Human Capital Management	117
2.4.1 Arten personenbezogener Daten in SAP ERP HCM	117
2.4.2 Benutzerdaten in SAP ERP HCM	121
2.5 Personenbezogene Daten in SAP Customer Relationship Management	121
2.5.1 Geschäftspartner als Stammdaten	121
2.5.2 Bewegungsdaten von Geschäftspartnern	124

2.5.3 Datenaustausch mit anderen SAP-Systemen	124
2.5.4 Auswertungsmöglichkeiten von Geschäftspartnern im Marketing	125
2.6 Zusammenfassung	125
3 »Vom ersten Schritt zum Weg zum Ziel«: Vorgehensmodell	127
<hr/>	
3.1 Übersicht zur Vorgehensweise	127
3.1.1 Was bedeutet der induktive Ansatz?	130
3.1.2 Sperren und Löschen personenbezogener Daten als Startpunkt	131
3.1.3 Trennung nach Zweckbestimmungen	134
3.1.4 Zwecktrennung und Berechtigungen	136
3.1.5 Auskunft an den Betroffenen	137
3.1.6 Protokollierung	138
3.1.7 Sicherheit in der Datenübertragung	139
3.1.8 Technische Sicherheit	140
3.1.9 Datenübertragbarkeit	141
3.1.10 Audit, Nachweis und Dokumentation	142
3.1.11 Ergebnis unseres Vorgehensmodells	145
3.1.12 Was bedeutet der deduktive Ansatz	146
3.2 Wege zum Verzeichnis von Verarbeitungstätigkeiten	148
3.2.1 Induktiver Ansatz versus deduktiver Ansatz	148
3.2.2 Wo treffen sich die beiden Ansätze?	150
3.3 Zusammenfassung	151
4 »Auch das Ende muss bestimmt sein«: Sperren und Löschen mit SAP Information Lifecycle Management	153
<hr/>	
4.1 Einführung	154
4.2 Überblick über das Sperren und Löschen mit SAP ILM	160
4.3 Vorbereitungen für das vereinfachte Sperren	164

4.3.1	Vorbereitungen für das Sperren von Stammdaten in Transaktion SPRO	165
4.3.2	Vorbereitungen für das Sperren von Bewegungsdaten in Transaktion SPRO	171
4.3.3	Vorbereitungen für das Sperren von Stammdaten in SAP ILM	172
4.3.4	Vorbereitungen für das Sperren von Bewegungsdaten in SAP ILM	177
4.3.5	Vorbereitungen für das Sperren und Löschen von Stammdaten – die Anwendungsregelvarianten	180
4.3.6	Vorbereitungen für das Archivieren von Stamm- und Bewegungsdaten	184
4.3.7	Vorbereitungen aus der Sicht vom abhängigen und zentralen Stammdatensystem	186
4.4	Stamm- und Bewegungsdaten sperren	190
4.4.1	Bewegungsdaten im Geschäftsprozess sperren	190
4.4.2	Gesperrte Bewegungsdaten im Geschäftsprozess anzeigen	191
4.4.3	Stammdaten im Geschäftsprozess sperren	194
4.4.4	Lokaler EoP-Check (Zwischenprüfung ohne Setzen des Sperrkennzeichens)	203
4.4.5	Gesperrte Stammdaten im Geschäftsprozess anzeigen	203
4.4.6	Stammdaten im Geschäftsprozess entsperren	206
4.5	Datenvernichtung	209
4.5.1	Wege der Datenvernichtung	209
4.5.2	Vernichtung aus der Datenbank per Archivierungsobjekt	211
4.5.3	Vernichtung aus der Datenbank per Datenvernichtungsobjekt	212
4.5.4	Archivdateien aus der zertifizierten ILM-Ablage	216
4.6	Legal Case Management	226
4.6.1	Übersicht und Anzeige vorhandener Rechtsfälle	227
4.6.2	Das Konzept der BOR-Objekttypen und ihre Verbindung zu ILM-Objekten	227
4.6.3	Rechtsfall anlegen oder ändern	228
4.6.4	Rechtsfallbedingte Sperren setzen	234
4.6.5	Extraktion von Datenobjekten mit Legal Hold	237
4.6.6	Rechtsfall abschließen oder löschen	239

4.7	ILM-Benachrichtigungen	240
4.7.1	Löschen verteilter Daten	240
4.7.2	Sperren und Löschen von personenbezogenen Daten	242
4.7.3	Funktionen und Konfiguration der ILM-Benachrichtigungen	244
4.8	Zeitabhängiges Sperren personenbezogener Daten in der Personaladministration (SAP ERP HCM-PA)	250
4.9	Zusammenfassung	251
5	»Struktur ist alles«: Verarbeitung muss auf dem Zweck basieren	253
5.1	Verantwortlicher und Zweck	253
5.2	Organisationsstrukturen (Linienorganisation)	257
5.2.1	Wichtige Organisationsstrukturen	258
5.2.2	Was, wenn die Strukturen anders eingerichtet wurden?	262
5.3	Prozessorganisation	263
5.3.1	Betriebswirtschaftliche Objekte in SD	266
5.3.2	Zweckattribute in der Kundenauftragsabwicklung	270
5.4	Linien- und Prozessorganisation definieren den Zweck	270
5.5	Zusammenfassung	272
6	»Dem Ende Struktur geben«: Data Controller Rule Framework	273
6.1	Organisation des Löschens in Geschäftsprozessen	274
6.2	Funktionen und Konfiguration des Data Controller Rule Frameworks	278
6.2.1	Das Data Controller Rule Framework konfigurieren	280
6.2.2	Regeln im Data Controller Rule Framework pflegen	288
6.3	Zusammenfassung	297

7	»Die Struktur berechtigt«: Auswirkungen auf das Berechtigungskonzept	299
7.1	Benutzer und Berechtigungen – eine Einführung	299
7.1.1	Benutzer	299
7.1.2	Berechtigungen – Berechtigungsfelder und Berechtigungsobjekte	301
7.2	Organisationsebenen neu denken	305
7.3	Prozessattribute identifizieren	308
7.4	Berechtigungsrisiken	309
7.5	Zusammenfassung	314
8	»Transparenz gewinnt«: Information Retrieval Framework	315
8.1	Transparenz – Auskunft und Vorabinformation	316
8.2	Neuerungen im Information Retrieval Framework	317
8.3	Setup des Information Retrieval Frameworks	319
8.3.1	Business Function aktivieren	319
8.3.2	Systemstatus festlegen	320
8.3.3	Berechtigungen zuweisen	321
8.3.4	Automatisierte Datenvernichtung einrichten	321
8.3.5	ILM-Objekte im Kontext des Information Retrieval Frameworks	322
8.3.6	Modellierungsverhalten aktivieren	323
8.4	Ein Datenmodell erzeugen	324
8.4.1	Ablauf des Modellierungsprozess	324
8.4.2	Initiales Datenmodell generieren	325
8.4.3	Beispieldaten erzeugen	328
8.4.4	Datum zur Beauskunftung auswählen	328
8.4.5	BAdI-Implementierungen erstellen	329
8.4.6	BAdI-Methoden implementieren	330
8.5	Datenmodell testen	335
8.5.1	Zweckbestimmungen manuell anlegen	335
8.5.2	Testsuche von Daten	339
8.6	Beauskunftung durchführen	344

8.6.1	Zweckbestimmungen definieren	344
8.6.2	Datenbeschaffung starten	345
8.6.3	Datenabfragen verwalten	346
8.7	Komplexere Feldverknüpfungen	349
8.8	Datenmodell im Browser anzeigen	350
8.9	Bestehende Datenmodelle übernehmen	352
8.10	Zusammenfassung	353
9	»Schau mal, wer da liest«: Read Access Logging	355
9.1	Anforderungen an eine Leseprotokollierung	355
9.2	Verfügbarkeit und Funktionsumfang von Read Access Logging	357
9.3	Setup und Pflege	358
9.3.1	Funktionsweise	358
9.3.2	Berechtigungen	359
9.3.3	Aktivierung	359
9.4	Festlegen von Zweckbestimmung und Protokolldomänen	361
9.4.1	Zweckbestimmung	361
9.4.2	Protokolldomänen	362
9.5	Aufzeichnungen für UI-Kanäle	364
9.6	Konfigurationen	368
9.7	Auswertung von Protokollen	373
9.7.1	Manuelle Auswertung	373
9.7.2	Automatisierte Suche in Read-Access-Logging-Protokollen	376
9.8	Konfigurationen für Remote-API-Kanäle	377
9.8.1	Konfiguration für den Remote-Function-Call-Kanal	377
9.8.2	Konfiguration für Analytics	379
9.9	Bedingungen	381
9.10	Transportmechanismen	386
9.11	Import und Export	386
9.12	Zusammenfassung	387

10 »Der Herr der Daten werden«: SAP Master Data Governance	389
10.1 Transparenz erzielen	389
10.2 Die Szenarien der Stammdatenpflege	390
10.3 Central Governance in SAP Master Data Governance	391
10.4 Konsolidierung in SAP Master Data Governance	393
10.5 Kombination der Szenarien	396
10.6 Sensible Daten mit SAP Master Data Governance bearbeiten	396
10.7 Organisatorische Trennung	398
10.8 Datenqualitätssicherung mit Services	400
10.8.1 Die verschiedenen Services	400
10.8.2 Proxy-Anbieter	402
10.9 Zusammenfassung	403
11 »Der Kopf in den Wolken«: Datenschutz in Cloud-Lösungen	405
11.1 Datenschutz aus Sicht der Cloud – eine Einführung	405
11.1.1 Merkmale von Cloud-Lösungen	406
11.1.2 Datenschutz und Datensicherheit	409
11.1.3 Rollen und Verantwortlichkeiten	410
11.2 Datenschutzservices und -prozesse für die SAP-Cloud-Lösungen	412
11.2.1 Datenschutzbeauftragter und Datenschutzorganisation	412
11.2.2 Rechte der betroffenen Person	413
11.2.3 Meldung einer Datenschutzverletzung	413
11.2.4 Transparenz	414
11.2.5 Rechenschaftspflicht	416
11.2.6 Weitere Auftragsverarbeiter	422
11.2.7 Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen	423
11.2.8 Technische und Organisatorische Maßnahmen (TOM) in den SAP-Cloud-Lösungen	424
11.2.9 Risikomanagement	433
11.2.10 Laufende Konformität	433
11.3 Zusammenfassung	433

12 »Lösungen, die wachsen und nicht wuchern«: Datenschutz in der SAP Cloud Platform	435
12.1 Was ist SAP Cloud Platform?	435
12.1.1 Standard-Services von SAP Cloud Platform finden und mieten	436
12.1.2 Datenschutzfunktionen und Dokumentation der SAP Cloud Platform	439
12.1.3 Die TOM der SAP Cloud Platform	439
12.2 Datenschutzfunktionen von SAP Subscription Billing	443
12.2.1 Einführung	443
12.2.2 SAP Cloud Platform Personal Data Manager: Auskunft-Tool für personenbezogene Daten	447
12.2.3 Personenbezogenen Daten mit dem SAP Cloud Platform Data Retention Manager löschen	454
12.2.4 Die Auditlog-Funktion der SAP Cloud Platform	459
12.3 Datenschutzfunktionen der SAP Cloud Platform für kundeneigene Cloud-Anwendungen	461
12.3.1 Datenschutzfunktionen von SAP Master Data Integration	462
12.3.2 Den SAP Cloud Platform Data Retention Manager installieren und konfigurieren	466
12.3.3 Retention-Regeln des SAP Cloud Platform Data Retention Managers konfigurieren	469
12.3.4 Den SAP Cloud Platform Data Retention Manager nutzen	474
13 »In der Wolke auf Sicht steuern«: Übersicht über die Datenschutzfunktionen in SAP-Cloud-Lösungen	477
13.1 Einführung	477
13.2 Datenschutz in SAP Ariba	480
13.2.1 Überblick über SAP Ariba	480
13.2.2 Personenbezogene Daten in SAP Ariba	481
13.2.3 Datenschutzfunktionen in SAP Ariba	482

13.3 Datenschutz in SAP Concur	500
13.3.1 Überblick über SAP Concur	500
13.3.2 Personenbezogene Daten in SAP Concur	500
13.3.3 Datenschutzfunktionen in SAP Concur	501
13.4 Datenschutzfunktionen in SAP SuccessFactors	521
13.4.1 Überblick über SAP SuccessFactors	521
13.4.2 Personenbezogene Daten in SAP SuccessFactors	522
13.4.3 Datenschutzfunktionen in SAP SuccessFactors	524
13.5 Datenschutzfunktionen in SAP Customer Experience	553
13.5.1 Überblick über SAP Customer Experience	553
13.5.2 Datenschutzfunktionen von SAP Customer Data Cloud	555
13.5.3 Datenschutzfunktionen von SAP Marketing Cloud	578
13.5.4 Datenschutzfunktionen von SAP Commerce Cloud	583
13.5.5 Datenschutzfunktionen von SAP Sales Cloud und SAP Service Cloud	589
13.6 Zusammenfassung	597
14 »Täglich grüßt das ...«: Schützen, Kontrollieren, Nachweisen und Kontrollen nachweisen	599
14.1 Kontrollrahmen und Grundlagen der Verarbeitung	600
14.2 Rechtmäßigkeit, Treu und Glauben und Transparenz	601
14.2.1 Folgerungen aus Art. 5 Abs. 1 Buchst. a	601
14.2.2 Kontrollmöglichkeiten für Art. 5 Abs. 1 Buchst. a	602
14.3 Zweckbindung	603
14.3.1 Folgerungen aus Art. 5 Abs. 1 Buchst. b	604
14.3.2 Kontrollmöglichkeiten für Art. 5 Abs. 1 Buchst. b	605
14.4 Datenminimierung	606
14.4.1 Folgerungen aus Art. 5 Abs. 1 Buchst. c	607
14.4.2 Kontrollmöglichkeiten nach Art. 5 Abs. 1 Buchst. c	609
14.5 Richtigkeit	610
14.5.1 Folgerungen aus Art. 5 Abs. 1 Buchst. d	610
14.5.2 Kontrollmöglichkeiten für Art. 5 Abs. 1 Buchst. d	611
14.6 Speicherbegrenzung	612

14.6.1 Folgerungen aus Art. 5 Abs. 1 Buchst. e	613
14.6.2 Kontrollmöglichkeiten für Art. 5 Abs. 1 Buchst. e	614
14.7 Integrität und Vertraulichkeit	614
14.7.1 Folgerungen aus Art. 5 Abs. 1 Buchst. f	615
14.7.2 Kontrollmöglichkeiten für Art. 5 Abs. 1. Buchst. f	616
14.8 Rechenschaftspflicht	623
14.9 Abstrakte technische Kontrollhandlungen	625
14.10 Beispiele technischer Kontrollhandlungen	627
14.10.1 Kontrollbedarf 1: Information Retrieval Framework	628
14.10.2 Kontrollbedarf 2: Data Controller Rule Framework	629
14.10.3 Kontrollbedarf 3: Attributierung	629
14.10.4 Kontrollbedarf 4: Schnittstellenkontrollen	630
14.10.5 Kontrollbedarf 5: Verwendungsnachweise	631
14.10.6 Kontrollbedarf 6: Authentifizierung	633
14.10.7 Kontrollbedarf 7: Minimalprinzip im Berechtigungskonzept	634
14.10.8 Kontrollbedarf 8: Speicherkontrolle	635
14.10.9 Kontrollbedarf 9: Zugriffskontrolle	635
14.10.10 Kontrollbedarf 10: Übermittlungskontrolle	636
14.10.11 Kontrollbedarf 11: Transportkontrolle	637
14.10.12 Kontrollbedarf 12: Verschlüsselung	637
14.10.13 Kontrollbedarf 13: Entpersonalisierung	637
14.10.14 Kontrollbedarf 14: Datensperrung	638
14.10.15 Kontrollbedarf 15: Datenlöschung	644
14.10.16 Kontrollbedarf 16: Dublettenprüfung	645
14.10.17 Kontrollbedarf 17: Stammdatenmanagement	645
14.10.18 Kontrollbedarf 18: Scoring-Werte	646
14.10.19 Kontrollbedarf 19: Patch-Management	646
14.10.20 Kontrollbedarf 20: Transportwesen	646
14.10.21 Kontrollbedarf 21: Code-Review	647
14.10.22 Kontrollbedarf 22: Umfang der Verarbeitung	647
14.10.23 Kontrollbedarf 23: Änderbarkeit von System und Konfiguration	648
14.10.24 Kontrollbedarf 24: Protokollierung von Programmänderungen	649
14.10.25 Kontrollbedarf 25: Tabellenänderungen	649
14.10.26 Kontrollbedarf 26: Belegprotokollierung	650
14.10.27 Kontrollbedarf 27: Verhaltensprotokollierung	651
14.10.28 Kontrollbedarf 28: Ereignisprotokollierung	653
14.10.29 Kontrollbedarf 29: Benutzerkonzept	654

14.10.30	Kontrollbedarf 30: Kennwortregeln	655
14.10.31	Kontrollbedarf 31: Standardbenutzer	656
14.10.32	Kontrollbedarf 32: Benutzeradministration	657
14.10.33	Kontrollbedarf 33: Transparente Berechtigungsrisiken	658
14.10.34	Kontrollbedarf 34: Backup und Disaster Recovery	658
14.11	Zusammenfassung	658

Anhang

A	Glossar	663
B	Relevante Transaktionen, relevante Reports, Hinweise	669
C	Literaturverzeichnis	675
D	Die Autoren	679

Index	683
-------------	-----