
Inhaltsverzeichnis

1	Einleitung	1
1.1	Einleitung	1
1.2	Über diesen Praxisleitfaden	3
1.3	Aufbau des Praxisleitfadens	4
2	Anforderungen an den Datenschutz	7
2.1	Bedeutung des Datenschutzes	8
2.2	Datenschutzrecht	9
2.2.1	Informationelle Selbstbestimmung	9
2.2.2	Datenschutzgrundsätze	9
2.2.3	Datenschutzgesetze	11
2.3	Auswirkungen auf die betriebliche Praxis	15
2.4	Notwendigkeit eines Datenschutzmanagementsystems	17
	Literatur	19
3	Datenschutzmanagementsysteme	21
3.1	Ein Managementsystem für den Datenschutz	22
3.1.1	Das Konzept des Managementsystems	22
3.1.2	Vorteile eines DSMS	22
3.1.3	Vermeintliche Nachteile widerlegt	26
3.2	Normungen und Gütesiegel rund um den Datenschutz	28
3.2.1	Notwendigkeit eines Datenschutznachweises	28
3.2.2	Eignung für ein Datenschutzmanagementsystem	31
3.2.3	Vorgehensweise der SAP AG	34
	Literatur	36
4	Voraussetzungen schaffen	39
4.1	Szenarien	40
4.2	Voraussetzungen	42
4.2.1	Anwendungsbereich festlegen	42
4.2.1.1	Einbeziehung der Verantwortlichen	44

4.2.1.2	Scoping	48
4.2.2	Entscheidungsvorlage für die Geschäftsleitung	58
	Literatur	59
5	Implementierung	61
5.1	PDCA-Zyklus, KVP und DSMS	62
5.1.1	PDCA	62
5.1.2	Kontinuierlicher Verbesserungsprozess (KVP)	63
5.1.3	DSMS-PDCA	64
5.2	Implementierung anhand des DSMS-PDCA	67
5.2.1	Datenschutzziele festlegen und einführen	67
5.2.1.1	Datenschutzziele definieren	68
5.2.1.2	Governance Model zur Umsetzung der Ziele	70
5.2.1.3	Datenschutz-Policy	79
5.2.2	Projektstart	86
5.2.2.1	Inhaltliche Aspekte des Projektstartes	86
5.2.2.2	Beteiligte	88
5.2.3	Risikoanalyse	92
5.2.3.1	Gestufte Vorgehensweise	92
5.2.3.2	Risikoanalyse und -behandlung	95
5.2.3.3	Prozessanalyse	112
5.2.3.4	Einbeziehung der DSMS-Akteure in die Maßnahmenplanung	116
5.2.4	Dokumentation	119
5.2.4.1	Sinn und Zweck der DSMS-Dokumentation	120
5.2.4.2	Aufbau einer DSMS-Dokumentation	121
5.2.4.3	Aspekte der DSMS-Dokumentation	123
5.2.5	Roll-out	138
5.2.5.1	Vorbereitung	138
5.2.5.2	Bekanntmachung	140
5.2.5.3	Nachbereitung	141
5.2.6	Trainings	145
5.2.6.1	Notwendigkeit einer Datenschutz-Awareness	146
5.2.6.2	Grundlegende Aspekte von Datenschutztrainings	147
5.2.6.3	Inhalte	149
5.2.6.4	Methoden	153
5.2.6.5	Weitergehende Awareness-Maßnahmen	154
5.2.7	Realisierung des DSMS	159
5.2.7.1	Einordnung in den Kontext des DSMS-PDCA	160
5.2.7.2	Kommunikation	161
5.2.7.3	Risikoüberwachung	164
5.2.7.4	Veränderungen und Vorabkontrolle	166

5.2.7.5	Überprüfung der Dienstleister	168
5.2.7.6	Datenschutzvorfälle und Anfragen von außerhalb	172
5.2.7.7	Kontrolle der Umsetzung	174
5.2.7.8	Beginn mit der kontinuierlichen Verbesserung	177
5.2.8	Audit-Planung	181
5.2.8.1	Über DSMS-Audits	182
5.2.8.2	Audit-Cycle als systematische Abfolge der Prüfkativitäten	188
5.2.8.3	Aspekte des Audit-Programms	191
5.2.9	Interne Audits	195
5.2.9.1	Vorbereitung	195
5.2.9.2	Durchführung	202
5.2.9.3	Nachbereitung	205
5.2.10	Management Review	211
5.2.10.1	Einordnung in den Kontext	211
5.2.10.2	Beteiligte	212
5.2.10.3	Eingaben und Ergebnisse	213
5.2.11	Externe Audits und Zertifizierung	217
5.2.11.1	Kunden-Audit (2nd-Party-Audit)	218
5.2.11.2	Zertifizierungs-Audit (3rd-Party-Audit)	219
5.2.12	Finale Anpassungen	223
5.2.13	Fazit zur Implementierung	224
5.2.13.1	Beteiligte	224
5.2.13.2	Agenda	225
5.3	Überführung in den Regelbetrieb	227
5.3.1	Ziele überprüfen	228
5.3.2	Jahresplan aufstellen	228
5.3.3	Risikoanalyse und Erstellung des Maßnahmenplans	229
5.3.4	Dokumentenrevision	229
5.3.5	„Re-Roll-out“	230
5.3.6	Umsetzung der Maßnahmen	230
5.3.7	Interne Audits	231
5.3.8	Management Review	231
5.3.9	Externe Audits	231
5.3.10	Fazit zum Status des DSMS	231
Literatur	233
6	Ausweitung des DSMS	235
6.1	Anpassung der Regelkreise	236
6.2	Besonderheiten der parallelen Aktivitäten	236
6.2.1	Plan-Phase	236
6.2.2	Do-Phase	238
6.2.3	Check-Phase	239
6.2.4	Act-Phase	239

7 Abschließende Bewertung	241
7.1 Das SAP-Datenschutzmanagementsystem im dritten Jahr – ein Fazit	242
7.2 Das Konzept des DSMS – eine zukunftsweisende Lösung auch für KMU ..	243
Glossar	245
Sachverzeichnis	249