

Datenschutz & IT-Sicherheit

Umsetzungsanleitung und -prüfung
für Kreditinstitute in der Praxis

Herausgegeben von

Michael Berndt

Mit Beiträgen von

Andreas Kolb · Michael Borchert

Björn Toemmler

ERICH SCHMIDT VERLAG

Bibliografische Information der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen
Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über
dnb.ddb.de abrufbar.

Weitere Informationen zu diesem Titel finden Sie im Internet unter
[ESV.info/978 3 503 11094 0](http://ESV.info/978_3_503_11094_0)

Lizenzausgabe des Werkes
„Datenschutz & IT-Sicherheit“
Mit freundlicher Genehmigung
© Finanz Colloquium Heidelberg, Heidelberg, 2008

Alle Rechte an dieser Ausgabe vorbehalten
© Erich Schmidt Verlag GmbH & Co., Berlin 2008
www.ESV.info

ISSN 1866-4520
ISBN 978 3 503 11094 0

Gesamtherstellung: Infolog GmbH, Obrigheim

Inhaltsübersicht

Abschnitt 1:	Interne Überwachung der automatisierten Verarbeitung personenbezogener Daten (<i>Toemmler</i>)	1
Abschnitt 2:	Technische und organisatorische Maßnahmen zur Einhaltung besonderer Vorgaben für Datenschutz/ -sicherheit (<i>Kolb</i>)	53
Abschnitt 3:	Umsetzung, Prüfung und Beurteilung des internen IT-Sicherheitsmanagements (<i>Borchert</i>)	159
Anhang		229

Inhaltsverzeichnis

Abschnitt 1: Interne Überwachung der automatisierten Verarbeitung personenbezogener Daten	1
I. Personalwirtschaftliche Beurteilung der Aufgaben des Datenschutzbeauftragten (DSB)	3
1. Wesentlicher Bestandteil des Internen Kontrollsystems	3
1.1. Fundstellen	3
1.2. Wesentlicher Inhalt	3
1.3. Checkliste	5
1.4. Praktikerhinweise	5
2. Zur Rolle als Datenschutzbeschwerdestelle in § 4f Bundesdatenschutzgesetz (BDSG)	6
2.1. Fundstellen	6
2.2. Wesentlicher Inhalt	6
2.3. Checkliste	8
2.4. Praktikerhinweise	9
3. Positionierung gegenüber Geschäftsleitung und Mitarbeitern	9
3.1. Fundstellen	9
3.2. Wesentlicher Inhalt	9
3.3. Checkliste	11
3.4. Praktikerhinweise	12
II. Bewertung der Voraussetzungen für die erforderliche Fachkunde des DSB	12
1. Mitgestaltung an datenschutzrelevanten Regelwerken	12
1.1. Fundstellen	12
1.2. Wesentlicher Inhalt	12
1.3. Checkliste	13
2. Informations- und kommunikationstechnische Kenntnisse	14
2.1. Fundstellen	14
2.2. Wesentlicher Inhalt	14
2.3. Checkliste	15
2.4. Praktikerhinweise	15
3. Kenntnisse über datenschutzrelevante Geschäftsprozesse	16

3.1.	Fundstellen	16
3.2.	Wesentlicher Inhalt	16
3.3.	Checkliste	17
3.4.	Praktikerhinweise	17
III.	Kontrollhandlungen zur ordnungsgemäßen Anwendung der DV-Programme	18
1.	Datenverarbeitung in einem externen Rechenzentrum	18
1.1.	Fundstellen	18
1.2.	Wesentlicher Inhalt	18
1.3.	Checkliste	21
1.4.	Praktikerhinweise	22
2.	Institutsinterne Datenverarbeitungsanlage	23
2.1.	Fundstellen	23
2.2.	Wesentlicher Inhalt	23
2.3.	Checkliste	23
2.4.	Praktikerhinweise	24
3.	Standardsoftwareprogramme auf dem PC	24
3.1.	Fundstellen	24
3.2.	Wesentlicher Inhalt	24
3.3.	Checkliste	25
3.4.	Praktikerhinweise	26
IV.	Geschäftsbereichsspezifische Schulung und Unterweisung der Mitarbeiter	26
1.	Einholung einer Verpflichtungserklärung	26
1.1.	Fundstellen	26
1.2.	Wesentlicher Inhalt	26
1.3.	Checkliste	28
1.4.	Praktikerhinweise	28
2.	Datenschutzspezifische Regelungen im Intranet	29
2.1.	Fundstellen	29
2.2.	Wesentlicher Inhalt	29
2.3.	Checkliste	31
2.4.	Praktikerhinweise	32
3.	Datenschutzrichtlinien in Ergänzung zu Arbeitsanweisungen	32

3.1.	Fundstellen	32
3.2.	Wesentlicher Inhalt	32
3.3.	Checkliste	33
3.4.	Praktikerhinweise	34
V.	Prüfung der Zulässigkeitsvoraussetzungen bei der Erhebung, Speicherung, Veränderung und Übermittlung von Daten	34
1.	Fundstellen	34
2.	Wesentlicher Inhalt	34
3.	Checkliste	36
VI.	Überwachung der Löschung bzw. Sperrung personenbezogener Daten	37
1.	Fundstellen	37
2.	Wesentlicher Inhalt	37
3.	Checkliste	38
4.	Praktikerhinweise	39
VII.	Benachrichtigung des Betroffenen	40
1.	Fundstellen	40
2.	Wesentlicher Inhalt	40
3.	Checkliste	41
4.	Praktikerhinweise	42
VIII.	Regelungen zur Auskunftserteilung an den Betroffenen	42
1.	Fundstellen	42
2.	Wesentlicher Inhalt	43
3.	Checkliste	44
4.	Praktikerhinweise	44
IX.	Erstellung und Führung eines internen Verfahrensverzeichnis	45
1.	Fundstellen	45
2.	Wesentlicher Inhalt	45
3.	Checkliste	46
4.	Praktikerhinweise	46

X.	Anlässe für die Vorabkontrolle	47
	1. Fundstellen	47
	2. Wesentlicher Inhalt	47
	3. Checkliste	48
	4. Praktikerhinweise	48
XI.	Bewertung von Akquisitionsdateien infolge (k)einer Speicherung (mehr) von Angaben über Nichtkunden	49
	1. Fundstellen	49
	2. Wesentlicher Inhalt	49
	3. Checkliste	50
	4. Praktikerhinweise	51
Abschnitt 2: Technische und organisatorische Maßnahmen zur Einhaltung besonderer Vorgaben für Datenschutz/ -sicherheit		53
I.	Besondere Maßnahmen zur Zutrittskontrolle	58
	1. Festlegung der Zutrittsberechtigung zu Hardware Komponenten	58
	1.1. Einleitung	58
	1.2. Wesentliche Anforderungen	58
	1.3. Checkliste	59
	1.4. Risiken	68
	1.5. Praktische Empfehlungen	68
	2. Zutrittsregelungen für bestimmte Personengruppen und für Ausnahmesituationen	69
	2.1. Einführung	69
	2.2. Wesentliche Anforderungen	69
	2.3. Checkliste	70
	2.4. Risiken	73
	2.5. Praktische Empfehlungen	73
	3. Einsatz von Zufallsuntersuchungen	75
	3.1. Einführung	75
	3.2. Wesentliche Anforderungen	75

3.3.	Checkliste	76
3.4.	Risiken	78
3.5.	Praktische Empfehlungen	78
II.	Benutzerkontrolle der Datenverarbeitungssysteme	79
1.	Überwachung der Zugangsberechtigungen	79
1.1.	Einführung	79
1.2.	Wesentliche Anforderungen	79
1.3.	Checkliste	80
1.4.	Risiken	89
1.5.	Praktische Empfehlungen	89
2.	Passwort-Identifikation des Benutzers	90
2.1.	Einführung	90
2.2.	Wesentliche Anforderungen	90
2.3.	Checkliste	91
2.4.	Risiken	97
2.5.	Praktische Empfehlungen	97
III.	Maßnahmen zur Zugriffskontrolle	98
1.	Beschränkung des Zugriffs auf den erforderlichen Umfang (Need-To-Know-Prinzip)	98
1.1.	Einführung	98
1.2.	Wesentliche Anforderungen	99
1.3.	Checkliste	100
1.4.	Risiken	105
1.5.	Praktische Empfehlungen	106
2.	Laufende Aktualisierung der Zugriffsberechtigungen	106
2.1.	Einführung	106
2.2.	Wesentliche Anforderungen	107
2.3.	Checkliste	107
2.4.	Risiken	109
2.5.	Praktische Empfehlungen	109
3.	Protokollierung der Zugriffe und Auditierung von Benutzerrechtezuweisungen	110
3.1.	Einführung	110
3.2.	Wesentliche Anforderungen	110
3.3.	Checkliste	112

3.4.	Risiken	115
3.5.	Praktische Empfehlungen	115
4.	Abgrenzung der dem Betriebsprüfer vorzulegenden steuerlich relevanten Daten	116
4.1.	Einführung	116
4.2.	Wesentliche Anforderungen	117
4.3.	Checkliste	118
4.4.	Risiken	120
4.5.	Praktische Empfehlungen	120
IV.	Weitergabekontrolle personenbezogener Daten	121
1.	Klassifizierung der Datenträger nach Schutzbedarf	121
1.1.	Einführung	121
1.2.	Wesentliche Anforderungen	121
1.3.	Checkliste	122
1.4.	Risiken	124
1.5.	Praktische Empfehlungen	124
2.	Richtlinien für die Durchführung von Transfers	124
2.1.	Einführung	124
2.2.	Wesentliche Anforderungen	125
2.3.	Checkliste	126
2.4.	Risiken	129
2.5.	Praktische Empfehlungen	130
3.	Überprüfung der Identität der Empfänger	130
3.1.	Einführung	130
3.2.	Wesentliche Anforderungen	130
3.3.	Checkliste	131
3.4.	Risiken	133
3.5.	Praktische Empfehlungen	133
V.	Kontrollen bei der Auftragsdatenverarbeitung	133
1.	Vorgaben für eine zweckmäßige Betriebsorganisation	133
1.1.	Einführung	133
1.2.	Wesentliche Anforderungen	134
1.3.	Checkliste	135
1.4.	Risiken	139
1.5.	Praktische Empfehlungen	139

2.	Verbindliche Festlegung sämtlicher Arbeitsabläufe	140
2.1.	Einführung	140
2.2.	Wesentliche Anforderungen	140
2.3.	Checkliste	141
2.4.	Risiken	143
2.5.	Praktische Empfehlungen	143
3.	Überwachung der Einhaltung von Arbeitsanweisungen	143
3.1.	Einführung	143
3.2.	Wesentliche Anforderungen	144
3.3.	Checkliste	146
3.4.	Risiken	148
3.5.	Praktische Empfehlungen	148
VI.	Verfügbarkeitskontrolle	150
1.	Einführung	150
2.	Wesentliche Anforderungen	150
3.	Checkliste	151
4.	Risiken	156
5.	Praktische Empfehlungen	156
Abschnitt 3: Umsetzung, Prüfung und Beurteilung des internen IT-Sicherheitsmanagements		159
I.	Zielstellung und Aufbau dieses Abschnittes	161
II.	Prüfungsumfeld	162
1.	Bedeutung	162
2.	Zwischenfazit	164
3.	Checkliste	165
III.	Prüfung und Beurteilung von IT-Umfeld und -Organisation	166
1.	Strategienpyramide	166
2.	IT-Organisation	169
3.	Abgleich der Geschäftsprozesse mit Organisationsrichtlinien und Prozessbeschreibungen	175
3.1.	Prüfungsvorgehen	175
3.2.	Checkliste	176

4. Funktionstrennung mittels Kompetenzregelungen und Bearbeitungsvermerke	178
4.1. Beachtenswerte Aspekte	178
4.2. Checkliste	179
5. Prüfung des Unsicherheitsfaktors Mensch (Anwendungsfehler, Manipulation)	180
5.1. Problemskizzierung	180
5.2. Checkliste	182
6. Ad hoc-Prüfung von Teilen des IKS durch Mitarbeiter unterschiedlicher Bereiche	183
6.1. Nur eine Aufgabe der Revision?	183
6.2. Checkliste	184
IV. Überprüfung und Beurteilung infrastruktureller IT-Risiken	184
1. Risikenaufnahme	184
1.1. Prüfungshandlungen	184
1.2. Zwischenfazit	186
1.3. Checkliste	186
2. Schutzfunktionen an Schnittstelle zwischen IT-Infrastruktur und Internet	187
2.1. Ausgangslage	187
2.2. Zwischenfazit	189
2.3. Checkliste	190
3. Beschränkung der Zugriffsrechte	191
3.1. Grundsätzliches	191
3.2. Checkliste	192
4. Prüfung und Beurteilung des IT-Notfallkonzepts	193
4.1. Grundsätzliche Anforderungen an eine IT-Notfallkonzeption	193
4.2. Zwischenfazit	195
4.3. Checkliste	195
5. Sicherung der IT-Infrastruktur durch projektbegleitende Prüfungen	196
5.1. Zielsetzung	196
5.2. Checkliste	197

V.	Prozessbegleitung und Prüfung bei Entwicklung und Einsatz von IT-Anwendungen	197
1.	Organisatorische Rahmenbedingungen	197
1.1.	Einführung	197
1.2.	Checkliste	199
2.	Standardisierte Verfahren zur Veränderung der IT-Anwendungen/ IT-Systeme	200
2.1.	Change-Management als zentraler Ansatzpunkt	200
2.2.	Checkliste	203
3.	Festlegung der Kriterien für Zeitpunkt, Art und Umfang von Prüfungshandlungen	205
3.1.	Festlegung des Rahmens der Begleitung/Prüfung	205
3.2.	Checkliste	208
4.	Prüfung der Programmentwicklung, Verfahren zur Bewertung und Auswahl von (zu erwerbenden) Programmen	209
4.1.	Idealtypischer Ablauf	209
4.2.	Checkliste	213
5.	Information der Geschäftsleitung bei schwerwiegenden Bedenken gegen den Programmeinsatz	216
5.1.	Ziel der Projekt-/Prozessbegleitung	216
5.2.	Checkliste	217
VI.	Auslagerung von IT-Systemen sowie IT-gestützten betrieblichen Funktionen	217
1.	Rahmenbedingungen	217
1.1.	Einführung	217
1.2.	Checkliste	220
2.	Integration der Kontroll- und Steuerungskreisläufe des Outsourcingnehmers in das IT-Sicherheitsmanagement des Outsourcinggebers	221
2.1.	Integration von outgesourcten Bereichen	221
2.2.	Checkliste	224
3.	(Teil-)Outsourcing der besonders unternehmenskritischen IT-Sicherheit	224
3.1.	IT-Sicherheitsmanagement outsourcen?	224

3.2. Checkliste	225
4. Technisch-organisatorische Anforderungen unter Datenschutz- und Datensicherheitsaspekten	225
4.1. Grundsätze	225
4.2. Checkliste	227
Anhang	229
Anhang I: Best-Practice-Lösung zum Schutz vor Abfluss vertraulicher Informationen: fideAS® file enterprise	231
Anhang II: Pentamino	234