

# Inhaltsverzeichnis

<b>1</b>	<b>Datenschutz made in Germany – das war mal?.....</b>	<b>1</b>
	Aleksandra Sowa	
	Literatur.....	5
<b>2</b>	<b>Dokumentationspflichten der DS-GVO als Prüfgegenstand .....</b>	<b>7</b>
	Daniela Duda	
2.1	Vorwort.....	7
2.2	Verfahrensverzeichnis nach dem BDSG .....	9
2.3	Vorabkontrolle nach dem BDSG .....	10
2.4	Meldepflicht nach dem BDSG.....	10
2.5	Verzeichnis von Verarbeitungstätigkeiten gemäß DS-GVO .....	11
2.5.1	Erleichterung für KMU? .....	11
2.5.2	Wegfall des Jedermannverzeichnisses .....	13
2.5.3	Verzeichnis des Auftragsverarbeiters.....	13
2.6	Weitere Dokumentationspflichten .....	13
2.6.1	Datenschutz-Folgenabschätzung .....	13
2.6.2	Meldepflichten .....	15
2.7	Prüffragen im Bereich der Dokumentationspflichten .....	16
2.7.1	Weitere Prüfungsansätze .....	20
2.8	Fazit .....	21
	Literatur.....	22
<b>3</b>	<b>Organisationen grundrechtskonform mit dem Standard-Datenschutzmodell gestalten .....</b>	<b>23</b>
	Martin Rost	
3.1	Einleitung.....	23
3.2	Die drei Komponenten des SDM: Ziele, Verfahren, Schutzbedarfe .....	26
3.3	Die Datenschutz-Grundverordnung und das SDM .....	30
3.4	Gewährleistungsziele.....	31
3.4.1	Die Beziehungen der Schutzziele untereinander.....	34

3.5	Schutzbedarf .....	38
3.5.1	Schutzbedarfskategorien „normal“, „hoch“, „sehr hoch“ .....	39
3.5.2	Ausgewählte Aspekte zum Schutzbedarf: Kumulierung, Angreifermodell, Konflikt SDM – IT-GS, Vertraulichkeit .....	41
3.6	Schutzmaßnahmen für hohen Schutzbedarf. ....	44
3.7	Prüfablauf mit SDM. ....	48
3.8	Das Betriebskonzept zum SDM. ....	51
3.9	An Stelle eines Fazits. ....	52
	Literatur. ....	54
<b>4</b>	<b>Shadow Audits – Ein wichtiges Instrument des Prüfers im Compliance-Zeitalter .....</b>	<b>57</b>
	Jens Carsten Laue, Alexander Geschonneck und Guido Havers	
4.1	Einleitung. ....	57
4.2	Der Begriff „Shadow Audit“ .....	59
4.2.1	Auftragsgegenstand der Abschlussprüfung .....	60
4.2.2	Der Begriff „Unregelmäßigkeit“: Definition und Erläuterung. ....	62
4.2.3	Verantwortlichkeiten für die Vermeidung und Aufklärung von Unregelmäßigkeiten .....	64
4.3	Prüferisches Vorgehen im Falle von Verstößen .....	69
4.3.1	Ablauf der Vorgehensweise durch den Prüfer .....	69
4.3.2	Forensik-Service in der Abschlussprüfung .....	71
4.4	Welche Neuerungen ergeben sich aus der Abschlussprüferreform? .....	76
4.4.1	Beachtung der Unabhängigkeitsvorschriften. ....	76
4.4.2	Erweiterte Berichtspflichten. ....	79
4.5	Schlussbemerkung .....	83
	Literatur. ....	84
<b>5</b>	<b>Das Internet der bösen Dinge. ....</b>	<b>87</b>
	Aleksandra Sowa	
	Literatur. ....	91
<b>6</b>	<b>Der IoT-Penetrationstest .....</b>	<b>93</b>
	Erlijn van Genuchten und Sebastian Schreiber	
6.1	Einführung .....	93
6.2	Was ist das Internet of Things? .....	94
6.3	Angriffsszenarien. ....	94
6.3.1	Maßnahmen .....	96
6.3.2	Konzeption. ....	96
6.4	Vor der Markteinführung .....	97
6.4.1	Analyse der Webapplikation/mobilen App .....	97
6.4.2	Analyse des Back-End. ....	99
6.4.3	Analyse der Hardware .....	101
6.4.4	Exemplarischer Projektplan. ....	102

6.5	Nach der Markteinführung .....	104
6.6	Fazit .....	105
	Literatur. ....	105
<b>7</b>	<b>IT-Sicherheitsaudits im Bereich der industriellen Produktion. ....</b>	<b>107</b>
	Mechthild Stöwer und Reiner Kraft	
7.1	Herausforderungen. ....	107
7.1.1	Konversion der Technik in Büro und Fertigung. ....	108
7.1.2	Zunehmende Anfälligkeit für IT-Risiken. ....	109
7.1.3	Besonderheiten der IT im Produktionsbereich .....	110
7.2	Standards und Normen zur IT-Sicherheit im Produktionsbereich .....	113
7.2.1	IEC 62443 .....	113
7.2.2	VDI/VDE-Richtlinie 2182. ....	115
7.2.3	ISO/IEC TR 27019 .....	115
7.2.4	NIST Empfehlungen .....	116
7.2.5	ICS Kompendium des BSI. ....	116
7.2.6	Neue IT-Grundschutz-Bausteine .....	120
7.3	Einstiegshilfen für einen systematischen Auditprozess. ....	120
7.3.1	Das Werkzeug LARS ICS des BSI .....	120
7.3.2	Checkliste des VDMA. ....	121
7.4	Fazit .....	122
	Literatur. ....	123
<b>8</b>	<b>Mensch und Maschine, oder: der Super-Revisor. ....</b>	<b>125</b>
	Aleksandra Sowa	
	Literatur. ....	130
<b>9</b>	<b>Schwarmintelligenz gegen Blackout .....</b>	<b>131</b>
	Sabine Wieland und Andreas Hartmann	
9.1	Ausgangslage in regionalen Energieverteilnetzen .....	131
9.1.1	Neue Teilnehmerstruktur .....	132
9.1.2	Anforderungen an eine Kommunikationsinfrastruktur für ein Energieverteilnetz. ....	136
9.2	Nutzung aktueller Technologien für die Sicherheit im Energieverteilnetz ...	137
9.2.1	Routing auf höchstem Niveau .....	137
9.2.2	Balance mit Schwarmintelligenz .....	139
9.2.3	Vertrauen durch Blockchain. ....	140
9.2.4	Angriffe erkennen mit dezentralem SIEM. ....	141
9.3	Ethische Grundsatzfragen .....	142
	Literatur. ....	143