

Inhalt

Seite

1	Einleitung	1
2	Personenbezogene Daten und ausgewählte Inhalte des Bundesdatenschutzgesetzes (BDSG)	3
2.1	Historie	3
2.2	Personenbezogene Daten	3
2.3	Informationelle Selbstbestimmung	4
2.4	Rechtsgrundlagen	5
2.5	Nicht-öffentliche Stellen	5
2.6	Beschäftigte nicht-öffentlicher Stellen	5
2.7	Erhebung, Verarbeitung und Nutzung personenbezogener Daten	6
2.8	Wirksamkeit der Einwilligung des Betroffenen	6
2.9	Benachrichtigung des Betroffenen	7
2.10	Verantwortliche Stelle	8
2.11	Auskunftsrecht des Betroffenen	8
2.12	Lösung von Daten	9
3	Der Datenschutzbeauftragte (DSB)	11
3.1	Berufung des Datenschutzbeauftragten	11
3.2	Stellung des Datenschutzbeauftragten im Unternehmen	13
3.3	Auswahl des Datenschutzbeauftragten	13
3.4	Aus- und Weiterbildung des Datenschutzbeauftragten	13
3.5	Aufgaben des Datenschutzbeauftragten und betriebliche Bestellung	14
3.5.1	Aufgaben der verantwortlichen Stelle als Grundlage für die Tätigkeit des Datenschutzbeauftragten	15
3.5.2	Festlegung der Datenschutzpolitik	16
3.5.3	Jahresplan des Datenschutzbeauftragten	18
3.5.4	Datenschutzaudits	19
3.5.5	Audit-Reporting	21
3.5.6	Organisation von Gesprächsrunden zum Datenschutz	26
3.5.7	Überwachung und Kontrolle von Verfahrensverzeichnissen	26
3.5.8	Aufstellen von Regelungen im Datenschutz	35
3.5.9	Umgang mit Hinweisen, Empfehlungen, Beschwerden	35
3.5.10	Jahresbericht des Datenschutzbeauftragten	37
3.6	Zugriff auf Datenbestände durch den Datenschutzbeauftragten	41
3.7	Haftung des betrieblichen Datenschutzbeauftragten	41
3.8	Aufgaben der Aufsichtsbehörde	42
4	Technische und organisatorische Maßnahmen im Datenschutz	43
4.1	Organisatorische Maßnahmen versus technische Maßnahmen	43
4.2	Acht Kontrollbereiche der technisch-organisatorischen Regelungen im Datenschutz	43
4.2.1	Zutrittskontrolle	44
4.2.2	Zugangskontrolle	45
4.2.3	Zugriffskontrolle	46
4.2.4	Weitergabekontrolle	49
4.2.5	Eingabekontrolle	49
4.2.6	Auftragskontrolle	49
4.2.7	Verfügbarkeitskontrolle	50
4.2.8	Trennungskontrolle	50

5	Risikobewertung und Schutzstufenkonzept	53
5.1	Verhältnismäßigkeit des Maßnahmenkonzepts	53
5.2	Risikobewertung im Umgang mit personenbezogenen Daten	53
6	Betriebliche Regelungen für den Datenschutz	57
6.1	Private Nutzung von Telekommunikationseinrichtungen und -systemen im Unternehmen	57
6.2	Telefondatenerfassung	59
6.3	Private IT im Unternehmen	61
6.4	Umgang mit USB-Sticks	62
6.5	Nutzung betrieblicher Laptops	64
6.5.1	Vereinbarung zur Nutzung betrieblicher Laptops	64
6.5.2	Technische und organisatorische Maßnahmen für Laptops	65
6.6	Telefax-Umgang	66
6.7	Organisation des betrieblichen Postwesens	66
6.8	Vorgehen bei externen Anfragen (z. B. Behörden)	67
6.9	Einsatz von Multifunktionsgeräten	68
6.10	Beschaffung von Hard- und Software	70
6.11	Speicherung/Sicherung von Daten	71
6.12	Einsatz von Videosystemen	72
6.13	Vernichtung, Entsorgung von Dokumenten und Datenträgern personenbezogenen Inhalts	75
6.14	Reisedaten von Arbeitnehmern	76
7	Auftragsdatenverarbeitung und Funktionsübertragung	79
7.1	Auftragsdatenverarbeitung	79
7.2	Funktionsübertragung	80
7.3	Übermittlung personenbezogener Daten	81
7.4	Meldepflichten und Vorabkontrolle	81
8	Datenschutz im Personalwesen	83
8.1	Bewerbungsverfahren	83
8.2	Erhebung von Daten beim Bewerber	85
8.3	Personalfragebögen zur Einstellung von Mitarbeitern	85
8.4	Drogentests bei Einstellung von Mitarbeitern	86
8.5	Führen von Personalakten	86
8.6	Weitergabe von Personaldaten an Dritte	86
8.7	Übermittlung von Sozialdaten	87
8.8	Zeiterfassungssysteme und datenschutzrechtliche Anforderungen	88
9	Vertragliche Regelungen mit Dienstleistern	91
9.1	Auftragsdatenverarbeitung	91
9.2	Leitfaden für einen Dienstleistungsvertrag aus datenschutzrechtlicher Sicht	91
9.3	Verträge mit Dienstleistern der Auftragsdatenverarbeitung	92
9.4	Sonstige Verträge mit Dienstleistern aus datenschutzrechtlicher Sicht	95
10	Schulungen und Unterweisungen im Datenschutz	101
10.1	Schulungen	101
10.2	Unterweisungen	101
10.3	Schulungsplanung	103
10.4	Verpflichtung auf das Datengeheimnis	103

11	Datenschutzkonzept und Datenschutzhandbuch	105
11.1	Datenschutzhandbuch	105
11.2	Zehn Schritte zum Aufbau eines betrieblichen Datenschutzkonzepts – eine Zusammenfassung	105
11.3	Liste der Mindestregelungen im betrieblichen Datenschutz	106
12	Die neue EU-Datenschutz-Grundverordnung – Ein Ausblick	107
12.1	Benennung des Datenschutzbeauftragten	107
12.2	Stellung des Datenschutzbeauftragten im Unternehmen	108
12.3	Aufgaben und Funktion des Datenschutzbeauftragten	109