

Inhaltsverzeichnis

1	Der Datenschutzbeauftragte – Rolle und Aufgaben	11
1.1	Die Benennung des Datenschutzbeauftragten	11
1.1.1	Wie wird man eigentlich Datenschutzbeauftragter?	11
1.1.2	Wann muss ein Unternehmen einen Datenschutzbeauftragten benennen?	13
1.2	Die Rolle des Datenschutzbeauftragten – Bin ich jetzt für den Datenschutz verantwortlich?	14
1.2.1	Die Aufgaben des Datenschutzbeauftragten – Was muss ich konkret tun?	15
1.2.2	Was muss ich im Rahmen meiner Beratungs- und Unterrichtspflicht tun?	15
1.2.3	Persönliche Voraussetzungen des Datenschutzbeauftragten – Passt die Aufgabe zu mir?	17
2	Struktur und Verantwortlichkeit	20
2.1	Compliant – nur ein Modewort?	21
2.1.1	Was hat Datenschutz mit einem Compliance Management System zu tun?	21
2.1.2	CMS – Was bedeutet das für den Datenschutz in Ihrem Unternehmen?	22
2.1.3	Welche Schritte sind zu gehen?	22
2.1.4	Welche konkreten Aufgaben folgen?	23
2.2	Governance-Struktur – Auf mehrere Schultern verteilen – Unterstützer sichern	23
2.2.1	Datenschutzziele	23
2.2.2	Datenschutzleitlinie	24
2.2.3	Vorlage für eine Leitlinie	25
3	Das Verzeichnis von Verarbeitungstätigkeiten (VVT)	28
3.1	Was ist eigentlich eine „Verarbeitungstätigkeit“?	29
3.2	Muss jedes „Verarbeiten“ einzeln dokumentiert werden?	30
3.3	Die Summe der Verarbeitungstätigkeiten = das VVT	31
3.4	Beispiele für typische Verarbeitungstätigkeiten	32
3.5	Wozu braucht es ein VVT?	34
3.6	Muss jeder Betrieb ein VVT führen?	35

3.7	Erstellt man ein VVT „nur“ für die Aufsichtsbehörde?	35
3.8	Das VVT als wichtigstes Werkzeug des Datenschutzbeauftragten	36
3.9	Welche Angaben benötigt ein VVT, damit es nicht nur fürs Gesetz genügt, sondern auch für die Praxis sinnvoll ist?	37
3.10	Wie sieht so eine Dokumentation einer Verarbeitungstätigkeit ganz konkret aus?	38
3.11	Was hat es mit dem VVT für Auftragsverarbeiter auf sich?	40
4	Einbindung externer Dienstleister	42
4.1	Verschiedene „Arten“ von externen Dienstleistern	42
4.2	Wer sind die beteiligten Parteien?	45
4.3	Wann ist ein Vertrag zur Auftragsverarbeitung erforderlich?	46
4.3.1	Warum sollten bestehende Verträge mit Dienstleistern an die DS-GVO angepasst werden?	46
4.3.2	Was ist auf Seiten des Auftraggebers zu beachten?	47
4.4	Auswahl des Auftragnehmers	48
4.5	Vertragliche Regelungen der Auftragsverarbeitung – Pflichten des Auftragnehmers	48
4.5.1	Weisungen	49
4.5.2	Verpflichtung auf das Datengeheimnis	49
4.5.3	Unterauftragnehmer	49
4.5.4	Unterstützungspflichten bei Beantwortung von Anfragen	49
4.5.5	Löschung nach Vertragsbeendigung	50
4.5.6	Pflicht zur Bereitstellung von Informationen und Ermöglichung von Überprüfungen	50
4.5.7	Weitere Dokumentationspflichten des Auftragnehmers	50
4.6	Prozessbeschreibung Einbindung neuer Dienstleister	51
5	Informationspflichten und Betroffenenrechte	52
5.1	Informationspflichten	52
5.1.1	Wann ist zu informieren?	53
5.1.2	Über was ist zu informieren?	54
5.1.3	Wie ist zu informieren?	55
5.1.4	5 konkrete Umsetzungsschritte in der Praxis	57
5.2	Betroffenenrechte	57
5.2.1	Welche Rechte hat der Betroffene?	57
5.2.2	In welchem Zeitraum sind die Betroffenenrechte zu erfüllen?	61

5.2.3	Implementierung eines Prozesses zur Erfüllung der Betroffenenrechte	62
5.2.4	5 konkrete Umsetzungsschritte in der Praxis	63
6	Technische und organisatorische Maßnahmen (TOMs)	65
6.1	Was sind technische und organisatorische Maßnahmen?	66
6.2	Inhalt der technischen und organisatorischen Maßnahmen	68
6.3	Bewertung der Wirksamkeit/Auswahl geeigneter technischer und organisatorischer Maßnahmen/Risikobewertung	69
6.3.1	Stand der Technik	70
6.3.2	Implementierungskosten	70
6.3.3	Art, Umfang, Umstand und Zweck der Verarbeitung	71
6.3.4	Kann man Risiko berechnen?	72
6.4	Löschkonzept	74
6.4.1	Aufbewahrungsfristen	74
6.4.2	DIN 66398	75
6.4.3	Schritt für Schritt zum Löschkonzept	75
6.5	Datenschutzmanagement-System	76
6.5.1	Planen (Plan)	77
6.5.2	Umsetzen (Do)	78
6.5.3	Prüfen (Check)	78
6.5.4	Reagieren (Act)	78
6.5.5	Datenschutzmanagement-Software	79
6.6	Datenschutzfolgenabschätzung	79
6.6.1	Was ist eine Datenschutzfolgenabschätzung?	80
6.6.2	Wie ist eine Datenschutzfolgenabschätzung durchzuführen?	81
6.6.3	Unterstützung für die Durchführung einer Datenschutzfolgenabschätzung	86
7	Umgang mit Datenschutzverstößen	87
7.1	Was sind Datenschutzverstöße?	87
7.2	Meldung an die Aufsichtsbehörde	89
7.3	Meldung an die betroffenen Personen	90
7.4	Prozess zur Meldung von Datenschutzverstößen	91
8	Alltag als DSB – fortlaufende Maßnahmen	92
9	Arbeitshilfen	94

9.1	Benennungsurkunde für Datenschutzbeauftragte	96
9.2	Verpflichtungserklärung zur Einhaltung der datenschutzrechtlichen Anforderungen nach DS-GVO	97
9.3	DS-GVO – Compliance Planung	103
9.4	Datenschutz-Governance-Struktur	105
9.5	Festlegung der Datenschutzziele	108
9.6	Musterdatenschutzerklärung für Websitebetreiber nach den Vorgaben der DS-GVO	109
9.7	Muster zur Erhebung der Informationspflichten bei personenbezogenen Daten der Beschäftigten	112
9.8	Technische und organisatorische Maßnahmen gemäß Artikel 32 DS-GVO ..	114
9.9	Verzeichnis von Verfahrenstätigkeiten	115
10	Glossar	116
11	Literatur	120
12	Stichwortverzeichnis	122