

# Inhaltsverzeichnis

<b>1</b>	<b>Der Datenschutzbeauftragte – Rolle und Aufgaben</b>	11
1.1	<b>Die Benennung des Datenschutzbeauftragten</b>	11
1.1.1	Wie wird man eigentlich Datenschutzbeauftragter?	11
1.1.2	Wann muss ein Unternehmen einen Datenschutzbeauftragten benennen?	13
1.2	<b>Die Rolle des Datenschutzbeauftragten – Bin ich jetzt für den Datenschutz verantwortlich?</b>	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
<b>2</b>	<b>Struktur und Verantwortlichkeit</b>	20
2.1	<b>Compliant – nur ein Modewort?</b>	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	<b>Governance-Struktur – Auf mehrere Schultern verteilen – Unterstützer sichern</b>	23
2.2.1	Datenschutzziele	23
2.2.2	Datenschutzleitlinie	24
2.2.3	Vorlage für eine Leitlinie	25
<b>3</b>	<b>Das Verzeichnis von Verarbeitungstätigkeiten (VVT)</b>	28
3.1	<b>Was ist eigentlich eine „Verarbeitungstätigkeit“?</b>	29
3.2	<b>Muss jedes „Verarbeiten“ einzeln dokumentiert werden?</b>	30
3.3	<b>Die Summe der Verarbeitungstätigkeiten = das VVT</b>	31
3.4	<b>Beispiele für typische Verarbeitungstätigkeiten</b>	32
3.5	<b>Wozu braucht es ein VVT?</b>	34
3.6	<b>Muss jeder Betrieb ein VVT führen?</b>	35

3.7	<b>Erstellt man ein VVT „nur“ für die Aufsichtsbehörde?</b>	35
3.8	<b>Das VVT als wichtigstes Werkzeug des Datenschutzbeauftragten</b>	36
3.9	<b>Welche Angaben benötigt ein VVT, damit es nicht nur fürs Gesetz genügt, sondern auch für die Praxis sinnvoll ist?</b>	37
3.10	<b>Wie sieht so eine Dokumentation einer Verarbeitungstätigkeit ganz konkret aus?</b>	38
3.11	<b>Was hat es mit dem VVT für Auftragsverarbeiter auf sich?</b>	40
<b>4</b>	<b>Einbindung externer Dienstleister</b>	42
4.1	<b>Verschiedene „Arten“ von externen Dienstleistern</b>	42
4.2	<b>Wer sind die beteiligten Parteien?</b>	45
4.3	<b>Wann ist ein Vertrag zur Auftragsverarbeitung erforderlich?</b>	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	<b>Auswahl des Auftragnehmers</b>	48
4.5	<b>Vertragliche Regelungen der Auftragsverarbeitung – Pflichten des Auftragnehmers</b>	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	<b>Prozessbeschreibung Einbindung neuer Dienstleister</b>	51
<b>5</b>	<b>Informationspflichten und Betroffenenrechte</b>	52
5.1	<b>Informationspflichten</b>	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	<b>Betroffenenrechte</b>	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
<b>6</b>	<b>Technische und organisatorische Maßnahmen (TOMs)</b> .....	<b>65</b>
<b>6.1</b>	<b>Was sind technische und organisatorische Maßnahmen?</b> .....	<b>66</b>
<b>6.2</b>	<b>Inhalt der technischen und organisatorischen Maßnahmen</b> .....	<b>68</b>
<b>6.3</b>	<b>Bewertung der Wirksamkeit/Auswahl geeigneter technischer und organisatorischer Maßnahmen/Risikobewertung</b> .....	<b>69</b>
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
<b>6.4</b>	<b>Löschkonzept</b> .....	<b>74</b>
6.4.1	Aufbewahrungsfristen .....	74
6.4.2	DIN 66398 .....	75
6.4.3	Schritt für Schritt zum Löschkonzept .....	75
<b>6.5</b>	<b>Datenschutzmanagement-System</b> .....	<b>76</b>
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
<b>6.6</b>	<b>Datenschutzfolgenabschätzung</b> .....	<b>79</b>
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
<b>7</b>	<b>Umgang mit Datenschutzverstößen</b> .....	<b>87</b>
<b>7.1</b>	<b>Was sind Datenschutzverstöße?</b> .....	<b>87</b>
<b>7.2</b>	<b>Meldung an die Aufsichtsbehörde</b> .....	<b>89</b>
<b>7.3</b>	<b>Meldung an die betroffenen Personen</b> .....	<b>90</b>
<b>7.4</b>	<b>Prozess zur Meldung von Datenschutzverstößen</b> .....	<b>91</b>
<b>8</b>	<b>Alltag als DSB – fortlaufende Maßnahmen</b> .....	<b>92</b>
<b>9</b>	<b>Arbeitshilfen</b> .....	<b>94</b>

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