

# Inhalt

<b>1</b>	<b>Einleitung</b>	1
<b>2</b>	<b>Aufbau und wesentliche Inhalte der EU-Datenschutz-Grundverordnung (EU-DSGVO)</b>	3
2.1	Anwendungsbereich der EU-DSGVO	4
2.2	Ausschlüsse aus dem Anwendungsbereich	6
2.3	Struktur der EU-DSGVO	6
2.4	Akteure im Datenschutz	7
2.5	Ziele der EU-Datenschutz-Grundverordnung	8
<b>3</b>	<b>Personenbezogene Daten und ausgewählte Inhalte der EU-Datenschutz-Grundverordnung sowie des Bundesdatenschutzgesetzes (BDSG)</b>	10
3.1	Einführung, Aufbau und Anwendungsbereich des BDSG	10
3.1.1	Rechtsgrundlagen des Bundesdatenschutzgesetzes basierend auf der Revision 2018	13
3.1.2	Nicht-öffentliche Stellen	13
3.1.3	Beschäftigte nicht-öffentlicher Stellen	14
3.2	Personenbezogene Daten	14
3.2.1	Pseudonymisierung personenbezogener Informationen	15
3.2.2	Gesundheitsbezogene personenbezogene Daten	16
3.2.3	Personenbezogene Daten von Kindern	16
3.2.4	Besondere Kategorien personenbezogener Daten	17
3.3	Wichtige Definitionen	17
3.4	Informationelle Selbstbestimmung und Rechtmäßigkeit der Verarbeitung personenbezogener Daten	19
3.5	Grundsätze des Datenschutzes	21
3.6	Informationspflichten zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten	23
3.7	Rechtmäßigkeit der Einwilligung	26
3.7.1	Wirksamkeit der Einwilligung des Betroffenen	27
3.8	Rechte der betroffenen Person	28
3.9	Auskunftsrecht des Betroffenen	29
3.10	Lösung von Daten oder Einschränkung der Verarbeitung	29
3.11	Recht auf Berichtigung	30
3.12	Recht auf Anrufung der oder des Bundesbeauftragten	30
<b>4</b>	<b>Der Datenschutzbeauftragte (DSB)</b>	31
4.1	Berufung des Datenschutzbeauftragten	31
4.1.1	Aufgaben des Verantwortlichen oder Auftragsverarbeiters	34
4.2	Stellung des Datenschutzbeauftragten im Unternehmen	36
4.3	Auswahl des Datenschutzbeauftragten	37
4.4	Aus- und Weiterbildung des Datenschutzbeauftragten	38
4.5	Aufgaben des Datenschutzbeauftragten und betriebliche Bestellung	39
4.5.1	Festlegung der Datenschutzpolitik	41
4.5.2	Jahresplan des Datenschutzbeauftragten	43

4.5.3	Datenschutzaudits .....	45
4.5.4	Audit-Reporting .....	47
4.5.5	Organisation von Gesprächsrunden zum Datenschutz .....	56
4.5.6	Überwachung und Kontrolle von Verarbeitungsverzeichnissen gemäß Art. 30 DSGVO .....	57
4.5.7	Aufstellen von Regelungen im Datenschutz .....	63
4.5.8	Umgang mit Hinweisen, Empfehlungen, Beschwerden .....	63
4.5.9	Jahresbericht des Datenschutzbeauftragten .....	65
<b>4.6</b>	<b>Haftung des betrieblichen Datenschutzbeauftragten .....</b>	<b>67</b>
<b>4.7</b>	<b>Kontrolle des betrieblichen Datenschutzes durch Aufsichtsbehörden .....</b>	<b>68</b>
<b>5</b>	<b>Technische und organisatorische Maßnahmen im Datenschutz .....</b>	<b>70</b>
5.1	Organisatorische Maßnahmen versus technische Maßnahmen .....	70
5.2	<b>14 Kontrollbereiche der technisch-organisatorischen Regelungen im Datenschutz .....</b>	<b>72</b>
5.2.1	Zugangskontrolle .....	74
5.2.2	Zugriffskontrolle .....	76
5.2.3	Transportkontrolle, Übertragungskontrolle .....	79
5.2.4	Eingabekontrolle .....	80
5.2.5	Auftragskontrolle .....	80
5.2.6	Verfügbarkeitskontrolle und Wiederherstellbarkeit .....	80
5.2.7	Trennungskontrolle .....	81
5.2.8	Speicherkontrolle .....	81
5.2.9	Benutzerkontrolle .....	82
5.2.10	Datenintegrität .....	82
5.2.11	Datenträgerkontrolle .....	82
5.2.12	Zuverlässigkeit .....	82
<b>6</b>	<b>Datenschutz-Folgenabschätzung, Risikobewertung, Schutzstufenkonzept .....</b>	<b>83</b>
6.1	Verhältnismäßigkeit des Maßnahmenkonzepts .....	83
6.2	Folgenabschätzung und Risikobewertung im Umgang mit personenbezogenen Daten .....	87
<b>7</b>	<b>Betriebliche Regelungen für den Datenschutz .....</b>	<b>93</b>
7.1	<b>Clean Desk .....</b>	<b>93</b>
7.2	<b>Private Nutzung von Telekommunikationseinrichtungen und -systemen im Unternehmen .....</b>	<b>93</b>
7.3	<b>Telefondatenerfassung .....</b>	<b>96</b>
7.4	<b>Private IT im Unternehmen .....</b>	<b>98</b>
7.5	<b>Umgang mit USB-Sticks .....</b>	<b>98</b>
7.6	<b>Nutzung betrieblicher Laptops .....</b>	<b>101</b>
7.6.1	Vereinbarung zur Nutzung betrieblicher Laptops .....	101
7.6.2	Technische und organisatorische Maßnahmen für Laptops .....	101
7.7	<b>Telefax-Umgang .....</b>	<b>105</b>
7.8	<b>Organisation des betrieblichen Postwesens .....</b>	<b>106</b>
7.9	<b>Vorgehen bei externen Anfragen (z. B. Behörden) .....</b>	<b>108</b>
7.10	<b>Einsatz von Multifunktionsgeräten .....</b>	<b>110</b>
7.11	<b>Beschaffung von Hard- und Software .....</b>	<b>112</b>

<b>7.12</b>	<b>Speicherung/Sicherung von Daten .....</b>	113
<b>7.13</b>	<b>Veröffentlichung von Bildern und Videos .....</b>	114
7.13.1	Bilder im Internet von Mitarbeitern veröffentlichen – Was ist zu beachten? .....	114
7.13.2	Gestaltung von Internetseiten .....	114
7.13.3	Ausnahmen .....	115
7.13.4	Interessensabwägung .....	115
<b>7.14</b>	<b>Einsatz von Videosystemen .....</b>	116
7.14.1	Videoüberwachung öffentlich zugänglicher Räume .....	116
7.14.2	Betriebliche Videoüberwachung .....	116
<b>7.15</b>	<b>Vernichtung, Entsorgung von Dokumenten und Datenträgern personenbezogenen Inhalts .....</b>	123
<b>7.16</b>	<b>Reisedaten von Arbeitnehmern .....</b>	124
<b>7.17</b>	<b>Fahrzeugrückgabe .....</b>	126
<b>7.18</b>	<b>Regelungen zum mobilen Arbeiten und Home-Office .....</b>	126
<b>8</b>	<b>Auftragsverarbeitung .....</b>	129
<b>8.1</b>	<b>Pflichten des Auftragsverarbeiters .....</b>	129
<b>8.2</b>	<b>Vertragliche Regelungen in der Auftragsverarbeitung .....</b>	131
<b>8.3</b>	<b>Leitfaden für einen Auftragsverarbeitungsvertrag aus datenschutzrechtlicher Sicht .....</b>	131
<b>8.4</b>	<b>Verträge mit Dienstleistern der Auftragsverarbeitung .....</b>	133
<b>8.5</b>	<b>Verfahrensanweisung zur Auftragsverarbeitung .....</b>	136
<b>9</b>	<b>Drittstaatentransfer .....</b>	139
<b>10</b>	<b>Datenschutz im Personalwesen – Bewerbungsverfahren .....</b>	142
<b>10.1</b>	<b>Verarbeitung von Beschäftigtendaten .....</b>	143
<b>10.2</b>	<b>Erhebung von Daten beim Bewerber/Beschäftigten .....</b>	147
<b>10.3</b>	<b>Führen von Personalakten .....</b>	148
<b>10.4</b>	<b>Elektronische Gehaltsabrechnung .....</b>	149
<b>10.5</b>	<b>Verpflichtung auf das Datengeheimnis .....</b>	150
<b>11</b>	<b>Vertragliche Regelungen mit Dienstleistern .....</b>	151
<b>12</b>	<b>Umgang mit Datenpannen .....</b>	155
<b>12.1</b>	<b>Anforderungen an das Vorgehen bei Datenpannen und sonstigen kritischen Ereignissen .....</b>	155
<b>12.2</b>	<b>Phishing und Spishing .....</b>	155
<b>12.3</b>	<b>Vorgehen bei Datenverlust .....</b>	165
<b>13</b>	<b>Schulungen und Unterweisungen im Datenschutz .....</b>	169
<b>13.1</b>	<b>Schulungen und Unterweisungen .....</b>	169
<b>13.2</b>	<b>Schulungs- und Unterweisungsplanung .....</b>	171
<b>14</b>	<b>Datenschutzkonzept und Datenschutzhandbuch .....</b>	173
<b>14.1</b>	<b>Datenschutzhandbuch .....</b>	173
<b>14.2</b>	<b>Wesentliche Schritte zum Aufbau eines betrieblichen Datenschutzkonzepts – eine Zusammenfassung .....</b>	174

<b>15</b>	<b>Liste der Mindestregelungen im betrieblichen Datenschutz .....</b>	175
<b>16</b>	<b>Sanktionen .....</b>	176
	<b>Anhang mit ergänzenden Vorlagen .....</b>	180