DIN

Grit Reimann

Betrieblicher Datenschutz Schritt für Schritt – gemäß EU-Datenschutz-Grundverordnung

Lösungen zur praktischen Umsetzung – Textbeispiele, Musterformulare, Checklisten

2., vollständig überarbeitete und erweiterte Auflage 2018

Herausgeber:

DIN Deutsches Institut für Normung e.V.

Beuth Verlag GmbH · Berlin · Wien · Zürich

Inhalt

1 Einleitung 1

2 Aufbau und wesentliche Inhalte der EU-Datenschutz-Grundverordnung (EU-DSGVO) 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

3 Personenbezogene Daten und ausgewählte Inhalte der EU-Datenschutz-Grundverordnung sowie des Bundesdatenschutzgesetzes (BDSG) 2018 10

3.1 Einführung, Aufbau und Anwendungsbereich des BDSG 2018 10

3.1.1 Rechtsgrundlagen des neuen Bundesdatenschutzgesetzes 13

3.1.2 Nicht-öffentliche Stellen 13

3.1.3 Beschäftigte nicht-öffentlicher Stellen 13

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 25

3.7.1 Wirksamkeit der Einwilligung des Betroffenen, § 51 BDSG 25

3.8 Datengeheimnis 27

3.9 Rechte der betroffenen Person 27

3.10 Auskunftsrecht des Betroffenen 27

3.11 Löschung von Daten, § 58 BDSG 28

3.12 Rechtauf Anrufung der oder des Bundesbeauftragten 29

4 Der Datenschutzbeauftragte (DSB) 30

4.1 Berufung des Datenschutzbeauftragten 30

4.1.1 Aufgaben des Verantwortlichen oder Auftragverarbeiters 33

4.2 Stellung des Datenschutzbeauftragten im Unternehmen 35

4.3 Auswahl des Datenschutzbeauftragten 35

4.4 Aus-und Weiterbildung des Datenschutzbeauftragten 36

4.5 Aufgaben des Datenschutzbeauftragten und betriebliche Bestellung 37

4.5.1 Festlegung der Datenschutzpolitik 38

4.5.2 Jahresplan des Datenschutzbeauftragten 40

4.5.3 Datenschutzaudits 42

4.5.4 Audit-Reporting 44
4.5.5 Organisation von Gesprächsrunden zum Datenschutz 49
4.5.6 Überwachung und Kontrolle von Verarbeitungsverzeichnissen gemäß Art. 30 DSGVO/§ 70 BDSG 49
4.5.7 Aufstellen von Regelungen im Datenschutz 57
4.5.8 Umgang mit Hinweisen, Empfehlungen, Beschwerden 58
4.5.9 Jahresbericht des Datenschutzbeauftragten 60
4.6 Haftung des betrieblichen Datenschutzbeauftragten 64
4.7 Kontrolle des betrieblichen Datenschutzes durch Aufsichtsbehörden 65

5 Technische und organisatorische Maßnahmen im Datenschutz 66
5.1 Organisatorische Maßnahmen versus technische Maßnahmen 66
5.2 14 Kontrollbereiche der technisch-organisatorischen Regelungen im Datenschutz . 68
5.2.1 Zugangskontrolle 70
5.2.2 Zugriffskontrolle 72
5.2.3 Transportkontrolle, Übertragungskontrolle, Speicherkontrolle 76
5.2.4 Eingabekontrolle 77
5.2.5 Auftragskontroile 77
5.2.6 Verfügbarkeitskontrolle 77
5.2.7 Trennungskontrolle 78

6 Datenschutz-Folgeabschätzung, Risikobewertung, Schutzstufen-konzept 79
6.1 Verhältnismäßigkeit des Maßnahmenkonzepts 79
6.2 Folgeabschätzung und Risikobewertung im Umgang mit personenbezogenen Daten 81

7 Betriebliche Regelungen für den Datenschutz 86
7.1 Private Nutzung von Telekommunikationseinrichtungen und -Systemen im Unternehmen 86
7.2 Telefondatenerfassung 88
7.3 Private IT im Unternehmen 90
7.4 Umgang mit USB-Sticks 91
7.5 Nutzung betrieblicher Laptops 94
7.5.1 Vereinbarung zur Nutzung betrieblicher Laptops 94
7.5.2 Technische und organisatorische Maßnahmen für Laptops 94
7.6 Telefax-Umgang 98
7.7 Organisation des betrieblichen Postwesens 98
7.8 Vorgehen bei externen Anfragen (z.B. Behörden) 99
7.9 Einsatz von Multifunktionsgeräten 100
7.10 Beschaffung von Hard- und Software 102
7.11 Speicherung/Sicherung von Daten 103
7.12 Einsatz von Videosystemen 104
7.12.1 Videoüberwachung öffentlich zugänglicher Räume 104
7.12.2 Betriebliche Videoüberwachung 104
7.13 Vernichtung, Entsorgung von Dokumenten und Datenträgern personen-bezogenen Inhalts 109
7.14 Reisedaten von Arbeitnehmern 110

8 Auftragsverarbeitung 112
8.1 Pflichten des Auftragsverarbeiters 112
8.2 Vertragliche Regelungen in der Auftragsverarbeitung IIA
8.3 Leitfaden für einen Dienstleistungsvertrag aus datenschutzrechtlicher Sicht 114
8.4 Verträge mit Dienstleistern der Auftragsverarbeitung 116

9 Übermittlung personenbezogener Daten in Drittstaaten und internationale Organisationen 120
9.1 Datenübermittlung mit geeigneten Garantien 120
9.2 Datenübermittlung ohne geeignete Garantien 121
9.3 Sonstige Datenübermittlungen an Empfänger in Drittstaaten 121

10 Datenschutz im Personalwesen – Bewerbungsverfahren 122
10.1 Verarbeitung von Beschäftigtendaten 123
10.2 Erhebung von Daten beim Bewerber 126
10.3 Führen von Personalakten 127
10.4 Verpflichtung auf das Datengeheimnis 127

11 Vertragliche Regelungen mit Dienstleistern 130

12 Schulungen und Unterweisungen im Datenschutz 134
12.1 Schulungen 134
12.2 Unterweisungen 134
12.3 Schulungsplanung 136

13 Datenschutzkonzept und Datenschutzhandbuch 137
13.1 Datenschutzhandbuch 137
13.2 Schritte zum Aufbau eines betrieblichen Datenschutzkonzepts – eine Zusammenfassung 138

14 Liste der Mindestregelungen im betrieblichen Datenschutz 139

15 Sanktionen 140

Anhang mit ergänzenden Vorlagen 143