

## **Inhaltsverzeichnis**

<b>A. Einleitung .....</b>	<b>1</b>
<b>B. Die Auftragsverarbeitung im Sozialrecht .....</b>	<b>5</b>
I. Die Auftragsverarbeitung und ihre Abgrenzung zum Outsourcing .....	5
II. Vorteile der Auftragsverarbeitung .....	7
1. FAVORISIERUNG DER AUFTRAGSVERARBEITUNG IM SOZIALRECHT .....	7
2. WIRTSCHAFTLICHE HINTERGRÜNDE .....	10
3. LEISTUNGSSTEIGERUNG UND NUTZUNG VON AKTUELLEN KNOW-HOW .....	12
III. Nachteile der Auftragsverarbeitung .....	13
1. RISIKEN FÜR DEN BETROFFENEN .....	13
2. WIRTSCHAFTLICHE RISIKEN UND QUALITÄTSEINBUßEN .....	19
3. WISSENSVERLUST UND SCHNITTSTELLENMANAGEMENT .....	19
4. GESETZLICHE EINSCHRÄNKUNGEN .....	20
IV. Erscheinungsformen und Vertragsphasen der Auftragsverarbeitung .....	22
1. Typische Erscheinungsformen der Auftragsverarbeitung im Sozialrecht .....	22
2. Abgrenzung der Auftragsverarbeitung im Sozialrecht .....	23
3. Vertragsphasen der Auftragsverarbeitung .....	24
V. Rechtliche Regelungen für die Auftragsverarbeitung .....	28
1. Unionsrechtliche Vorgaben .....	28
a) Die Regelungen bis zum 24.05.2018 - Die Richtlinie 95/46/EG .....	28
b) Regelungen ab dem 25.05.2018 - Die Datenschutz-Grundverordnung .....	31
aa) Aufbau und Systematik der Datenschutz-Grundverordnung .....	31
bb) Ausgestaltung der Datenschutz-Grundverordnung in nationales Recht .....	33

c) Auftragsverarbeitung nach der Datenschutz-Grundverordnung .....	35
aa) Einführung.....	35
bb) Anforderungen der Datenschutz-Grundverordnung zur Auftragsverarbeitung.....	42
cc) Verantwortlichkeiten.....	43
2. Nationale Vorgaben zur Auftragsverarbeitung .....	44
a) Verhältnis der nationalen Regelungen zur Datenschutz-Grundverordnung .....	44
b) Bundesdatenschutzgesetz in der Fassung bis zum 24.05.2018.....	44
c) Sozialgesetzbuch Zehntes Buch (SGB X) in der Fassung bis zum 24.05.2018.....	46
d) Abgrenzungen zur Funktionsübertragung nach dem BDSG a. F./ SGB X a. F. bis zum 24.05.2018.....	49
e) Sozialgesetzbuch Zehntes Buch (SGB X) mit Wirkung ab dem 25.05.2018 .....	53
f) Regelungen im Sozialgesetzbuch Fünftes Buch (SGB V) Abgrenzungen zur Auftragsverarbeitung.....	54
g) Verweisvorschriften im Sozialgesetzbuch .....	54
3. Gesetzlich geregelte Aufgabenübertragung innerhalb des Sozialgesetzbuches.....	55
VI. Abgrenzung zur Übermittlung von Sozialdaten .....	56
VII. Abgrenzung zum Auftrag nach § 88 SGB X .....	58
VIII. Abgrenzung zur gemeinsamen Verantwortung nach Art. 26 DSGVO ...	60
<b>C. Exkurs: Der Sozialdatenschutz, die Bestimmung der Datenkategorien und deren Sensibilität.....</b>	<b>63</b>
I. Einführung.....	63
II. Das Recht auf informationelle Selbstbestimmung .....	63
III. Das Sozialgeheimnis .....	66

<b>IV. Klassifikation der Sozialdaten .....</b>	<b>71</b>
1. Begriff der Sozialdaten .....	71
a) Einführung .....	71
b) Persönlicher Bezug .....	72
c) Fachlicher Bezug .....	73
d) Abgrenzungen zu personenbezogenen Daten bei den Leistungsträgern .....	74
2. Betriebs- und Geschäftsgeheimnisse .....	75
3. Abgrenzung des Sozialgeheimnis zum Datengeheimnis .....	76
4. Abgrenzung des Sozialgeheimnis zum Verwaltungsverfahrensgesetz .....	78
<b>V. Besonders sensible Daten nach Art. 9 DSGVO und deren Umgang im Sozialrecht .....</b>	<b>80</b>
<b>VI. Bestimmung des Schutzbedarfes der Sozialdaten .....</b>	<b>81</b>
<b>VII. Die Datenschutz-Folgenabschätzung .....</b>	<b>86</b>
<b>D. Anforderungen an die Auftragsvergabe und zur Kontrolle des Auftragsverarbeiters .....</b>	<b>89</b>
I. Vorgaben aus der Datenschutz-Grundverordnung .....	89
II. Vorgaben aus Art. 28 DSGVO i. V. m. § 80 SGB X .....	90
III. Auftragsverarbeitung nach § 80 SGB X ab dem 25.05.2018 .....	98
1. Die Anforderungen an die Auftragsvergabe .....	98
2. Anforderungen an die Vertragsinhalte aus der Rechtslage vor dem 25.05.2018 im Zusammenspiel mit den Regelungen der DSGVO ....	106
3. Die Verwendung von Musterverträgen .....	119
4. Die Verwendung von Standardvertragsklauseln .....	121
5. Bedeutung und Umsetzung der technischen und organisatorischen Maßnahmen .....	122

6. Kriterien und Voraussetzungen für die Auswahl des Auftragsverarbeiters durch den Verantwortlichen .....	129
7. Haftung des Auftragsverarbeiters .....	131
IV. Weisungen des Verantwortlichen nach Art. 29 DSGVO .....	133
V. Vorgaben aus dem IT-Sicherheitsgesetz .....	134
VI. Die Begriffe des Überzeugens und des Überwachens .....	140
1. Allgemeines und Rechtsentwicklung .....	140
2. Bestimmung des Begriffes Überwachen .....	143
a) Der Begriff der „Überwachung“ in der DSGVO .....	143
b) Die Überwachung als staatliche Schutzpflicht .....	143
3. Der Begriff des „Überwachen“ in anderen Rechtsgebieten .....	144
a) Überwachen im Strafrecht .....	144
b) Das Umweltrecht .....	145
aa) Allgemeines .....	145
bb) Das Überwachen im Umweltrecht .....	146
cc) Das Störfallrecht .....	147
dd) Das Bundesimmissionsschutzgesetz .....	149
ee) Das Kreislaufwirtschafts- und Abfallrecht .....	150
ff) Zwischenergebnis zum Umweltrecht .....	151
c) Das Überwachen im Aktiengesetz .....	151
d) Das Überwachen im Arbeitsrecht .....	153
aa) Das Betriebsverfassungsgesetz .....	153
bb) Das Arbeitsschutzgesetz .....	154
cc) Zwischenergebnis zum Arbeitsrecht .....	155
4. Zusammenfassung der Rechtsvergleiche .....	156
VII. Möglichkeiten und Nachweise der effektiven Kontrolle des Auftragsverarbeiters durch den Verantwortlichen .....	157
1. Allgemeines .....	157
2. Möglichkeiten und Arten der Kontrolle .....	158

3.	Kontrolle des Auftragnehmers durch den Verantwortlichen .....	161
a)	Allgemeines .....	161
b)	Zuständigkeiten innerhalb der verantwortlichen Stelle .....	161
c)	Arten der Kontrolle .....	163
aa)	Einführung .....	163
bb)	Dokumentenkontrolle .....	164
cc)	Vor-Ort-Kontrolle durch den Verantwortlichen .....	164
dd)	Kontrolle des Auftragsverarbeiters durch externe Prüfer .....	167
ee)	Automatisierte Dokumenten- und Protokollkontrolle .....	169
d)	Umfang der Kontrolle .....	169
e)	Sonderfälle der Kontrolle .....	170
aa)	Fernwartung .....	170
bb)	Telearbeit von Mitarbeitern des Auftragsverarbeiters .....	173
4.	Nachweiserbringung durch den Auftragsverarbeiter .....	173
a)	Allgemeines .....	173
b)	Nachweis durch Zertifizierung, Audit und Verhaltensregeln .....	174
aa)	Unterschiede und Abgrenzungen zwischen Zertifizierung, Audit und Verhaltensregeln .....	174
bb)	Vorteile für den Verantwortlichen .....	177
cc)	Anforderungen an eine Zertifizierung .....	180
c)	Prüfung durch andere Auftraggeber .....	181
d)	Selbsttestat des Auftragsverarbeiters .....	183
5.	Managementsysteme für Datenschutz und Informationssicherheit ...	185
a)	Managementsysteme im Allgemeinen .....	185
b)	Datenschutzmanagementsysteme .....	186
c)	Informationssicherheitsmanagementsysteme .....	187
6.	Vergleich anerkannter Standards .....	189
a)	Allgemeines .....	189
b)	Zertifizierung nach ISO 27001 .....	190
c)	Umsetzung von BSI IT-Grundschutz .....	191
d)	Information Technology Infrastructure Library .....	194

e)	Common Criteria .....	195
f)	COBIT.....	195
g)	Datenschutzstandard DS-BvD-GDD-01 .....	196
h)	DIN EN ISO 9001 .....	197
i)	Datenschutzaudit nach § 78c SGB X a. F.....	197
j)	Audits in anderen Rechtsgebieten am Beispiel des Umweltschutz-audits .....	197
k)	Darstellung und Ablauf der Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz .....	199
aa)	Allgemeines .....	199
bb)	Ablauf des Audits .....	200
cc)	Kriterien der Zertifizierung.....	201
dd)	Audittypen .....	202
ee)	Aufgaben des BSI bei der Zertifizierung .....	203
ff)	Inhalte des Auditberichtes.....	203
VIII. Die Bestellung von Betriebsbeauftragten .....		204
1.	Allgemeines .....	204
2.	Der betriebliche Datenschutzbeauftragte .....	205
3.	Der Informationssicherheitsbeauftragte.....	207
IX. Prüfungen durch die Aufsichtsbehörde.....		209
1.	Allgemeines .....	209
2.	Zuständigkeiten der Datenschutzaufsicht .....	209
3.	Zuständigkeiten der Fach- und Rechtsaufsichten der Leistungsträger .....	212
4.	Informationspflichten gegenüber der Aufsichtsbehörde .....	214
5.	Ablauf einer Kontrolle durch die Aufsichtsbehörde .....	215
6.	Rechtsmittel der Aufsichtsbehörde .....	217
7.	Zwischenergebnis.....	218

X. Kontrollmöglichkeiten des Betroffenen .....	218
1. Auskunftsrechte des Betroffenen .....	218
2. Geltendmachung von Schadensersatzansprüchen durch den Betroffenen .....	221
3. Verzeichnis der Verarbeitungstätigkeiten .....	223
4. Zwischenergebnis.....	225
XI. Zeitpunkte der Prüfung des Auftragsverarbeiters .....	225
1. Rechtslage bis zum 24.05.2018 .....	225
2. Rechtslage seit dem 25.05.2018 .....	226
XII. Dokumentation der Kontrolle durch den Verantwortlichen .....	229
1. Rechtslage bis zum 24.05.2018 .....	229
2. Rechtslage seit dem 25.05.2018 .....	229
XIII. Tabellarische Gegenüberstellung der Kontrollmöglichkeiten .....	233
<b>E. Zusammenfassung der wesentlichen Ergebnisse dieser Arbeit.....</b>	<b>237</b>
<b>Literaturverzeichnis.....</b>	<b>243</b>