

Datenschutz in Steuerberater-, Wirtschaftsprüfer- und Rechts- anwaltskanzleien

**Praxisleitfaden mit Checklisten, Übersichten
und praktischen Beispielen**

Von

Thomas Balzer

und

Erhard Buchberger

ERICH SCHMIDT VERLAG

Inhaltsverzeichnis

1. Einleitung	11
1.1 Vorwort	11
1.2 Kurzvorstellung B ² Berlin	13
1.3 Der rote Faden	14
1.4 Der grobe Ablauf	15
1.5 Vorgehensweise des Buches	15
1.6 Haftungsausschluss	16
2. Einstimmung auf die DSGVO	17
2.1 Unterschied Datenschutz und Datensicherheit	17
2.2 Was bedeutet der Datenschutz heute?	17
2.3 Unterschied BDSG und DSGVO	18
2.4 Ziele der DSGVO	19
2.5 Problematiken	19
2.6 Gesetzlicher Rahmen – weitere Gesetze	20
2.7 Wie ist der Datenschutz praxisnah anwendbar?	21
2.8 Bedeutung des Datenschutzes für Kanzleien?	22
3. Basiswissen zur DSGVO	23
3.1 Einleitung	23
3.2 Personen bezogene Daten	23
3.3 Besondere Kategorien personenbezogener Daten	23
3.4 Personenbezogene Daten in den Kanzleien	23
3.4.1 Mitarbeiter	24
3.4.2 Mandanten	24
3.4.3 Lieferanten	25
3.5 Verarbeitung personenbezogener Daten	25
3.5.1 Was ist Verarbeitung	25
3.6 Grundsätze der Verarbeitung	26
3.6.1 Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz	26
3.6.2 Zweckbindung	26
3.6.3 Datenminimierung	27
3.6.4 Richtigkeit	27
3.6.5 Speicherbegrenzung	27
3.6.6 Integrität und Vertraulichkeit	27
3.7 Rechtmäßigkeit der Verarbeitung	28
3.7.1 Personenbezogene Daten	28
3.7.2 Besondere personenbezogene Daten	28
3.8 Betroffene	29
3.8.1 Was sind Betroffene?	29
3.8.2 Rechte der Betroffenen	29

3.9	Der Verantwortliche und seine Pflichten	35
3.9.1	Wer ist Verantwortlicher?	35
3.9.2	Pflichten des Verantwortlichen	35
3.9.3	Rechenschaftspflichten	35
3.9.4	Dokumentationen	36
3.9.5	Vertragliche Verpflichtungen	50
3.9.6	Meldepflichten	53
3.10	Datenerhebung	54
3.10.1	Datenerhebung beim Betroffenen	54
3.10.2	Datenerhebung nicht beim Betroffenen	55
3.11	Datenschutzbeauftragter (DSB)	56
3.11.1	Pflichten	56
3.11.2	Qualifikationen	56
3.12	Datenschutzpanne	57
3.12.1	Was ist eine Datenschutzpanne?	57
3.12.2	Meldung einer Datenschutzpanne	57
3.12.3	Kommunikation mit der Aufsichtsbehörde	58
3.13	Geldbußen	58
3.13.1	Verstöße gegen die Bestimmungen – Teil 1	60
3.13.2	Verstöße gegen die Bestimmungen – Teil 2	60
4.	Schutz personenbezogener Daten	63
4.1	Schutzbedarfsfeststellung	63
4.2	Das Prinzip der drei Schutzebenen	67
4.2.1	Zutritt	68
4.2.2	Zugang	68
4.2.3	Zugriff	70
4.2.4	Schichtprinzip der drei Schutzebenen	70
4.2.5	Weitere Angriffsmöglichkeiten	72
4.2.6	Internet	72
4.2.7	WLAN	73
4.2.8	USB-Sticks oder externe Laufwerke	76
4.2.9	E-Mails	78
4.3	Technische und organisatorische Maßnahmen – TOM	78
4.3.1	Was sind die TOM?	78
4.3.2	Zugang, Zutritt, Zugriff	80
4.3.3	Technische Maßnahmen im Zutritt	81
4.3.4	Organisatorische Maßnahmen im Zutritt	94
4.3.5	Technische Maßnahmen im Zugang	102
4.3.6	Organisatorische Maßnahmen im Zugang	112
4.3.7	Technische Maßnahmen-»™ Zugriff	131
4.3.8	Organisatorische Maßnahmen im Zugriff	136
4.4	Trennungskontrolle	138
4.4.1	Physikalische Trennung von IT-Systemen	139
4.4.2	Mandantenfähigkeit der Software	139

4.4.3	Videüberwachung	140
4.4.4	Einsatz von Smartphones	140
4.4.5	Berechtigungskonzept	141
4.4.6	Datenbankberechtigungen	141
4.4.7	Daten auf lokalen Computern	141
4.5	Weitergabekontrolle	142
4.5.1	Dokumentation berechtigter Weitergaben	142
4.5.2	Protokollierung der Weitergaben	142
4.5.3	Berechtigungskonzept	143
4.5.4	Datenbankberechtigungen	143
4.5.5	Daten auf lokalen Computern	143
4.5.6	Verschlüsselung bei E-Mails	144
4.5.7	VN Verbindungen	145
4.5.8	Transport von Daten	145
4.5.9	Portallösungen	145
4.6	Eingabekontrolle	146
4.6.1	Protokollierung berechtigter Eingaben und Veränderungen	147
4.6.2	Berechtigungskonzept	147
4.6.3	Datenbankberechtigungen	147
4.6.4	Einsatz von Formularen	147
4.6.5	Berechtigung zum Löschen	148
4.7	Auftragskontrolle	148
4.7.1	Auftraggeber	148
4.7.2	Auftragnehmer/Auftragsverarbeiter	149
4.8	Verfügbarkeitskontrolle	149
4.8.1	Identifikation kritischer IT-Systeme	149
4.8.2	Brandschutzanlagen	149
4.8.3	Meldeanlagen für Rauch und Brand	151
4.8.4	Beschaffenheit des Serverraumes	151
4.8.5	Analyse der Serververfügbarkeit	152
4.8.6	RAID-Systeme für Server	152
4.8.7	Nutzung physikalischer/virtueller Server	154
4.8.8	Nutzung lokalbasierter oder cloudbasierter Server	155
4.8.9	Videüberwachung/Alarmanlagen	156
4.8.10	Klimatisierung	156
4.8.11	Unterbrechungsfreie Stromversorgung USV	157
4.8.12	Separate Stromkreise für Server	158
4.8.13	Datensicherungskonzept	158
4.8.14	Aufbewahrung von Datensicherungen	160
4.8.15	Kontrolle der Datensicherung	160
4.8.16	Integrität einer Datensicherung	161
4.8.17	Notfallmanagement	161
4.8.18	Identifikation von Notfällen	164

4.8.19	Risikobewertung	165
4.8.20	Maßnahmen im Umgang mit Notfällen	165
4.9	Löschkonzept	166
4.9.1	Was ist Löschen?	166
4.9.2	Erstellung des Löschkonzeptes	166
4.9.3	Multifunktionsdrucker	167
4.9.4	Definition der Prozesse	167
4.10	Umgang mit Papier	170
4.10.1	Aufbewahrung	170
4.10.2	Archivierung	170
4.10.3	Vernichtung	170
4.11	Verschlüsselung	172
4.11.1	Pseudonymisierung	172
4.11.2	Anonymisierung	172
4.11.3	Kryptografie	173
4.12	Auftragsverarbeitung – Einbindung von Dienstleistern	174
4.12.1	Identifikation der externen Dienstleister	174
4.12.2	Auftragsverhältnisse	174
4.12.3	Prüfung der Externen bezüglich der DSGVO	174
4.12.4	AV-Vertrag	175
4.12.5	Wahrnehmung der Kontrollrechte	175
4.12.6	Wiederkehrende Prüfung des Dritten	175
4.12.7	Einsatz Subunternehmer beim Dritten	176
4.12.8	Vernichtung der Daten nach Auftragsende	176
4.13	Datenschutz Management	176
4.13.1	Dokumentation des Datenschutzes	176
4.13.2	Bereitstellung für Interne und Externe	177
4.13.3	Wartung und Instandhaltung	177
5.	Prinzipieller Ablauf in der Praxis	181
5.1	Datenschutzbeauftragte(r)	181
5.1.1	Erforderlichkeit	181
5.1.2	Intern oder Extern	182
5.1.3	Benennung	183
5.1.4	Aufgaben	183
5.1.5	Qualifikation	184
5.2	Durchführen eines Datenschutzaudits	184
5.2.1	Checkliste Datenschutzaudit	184
5.2.2	Checkliste für die Vorort-Begehung	185
5.2.3	Checkliste für die TOMs	186
5.2.4	Berichtstruktur Datenschutzaudit	187
5.3	Erstellung eines Maßnahmenkataloges	188
5.3.1	Identifikation eventueller Lücken	188
5.3.2	Maßnahmenkatalog erstellen	189
5.3.3	Risikoeinschätzung	190

5.3.4	Priorisierung durchführen	190
5.3.5	Umsetzungsplan	190
5.4	Mitarbeiter	191
5.4.1	Sensibilisierung	191
5.4.2	Geheimhaltungsvereinbarung	192
5.4.3	Freigabe von Texten und Fotos	192
5.5	Externe Dienstleister	193
5.5.1	Identifikation externer Dienstleister	193
5.5.2	Bestimmung des Auftragsverhältnisses	193
5.5.3	Verträge zur Auftragsverarbeitung (AV-Verträge)	193
5.5.4	Geheimhaltungsvereinbarungen	193
5.5.5	Regelmäßige Prüfungen	194
5.6	Betroffenenrechte etablieren	194
5.6.1	Betroffenenrechte	194
5.6.2	Prozesse dokumentieren und umsetzen	194
5.7	Webseite konform gestalten	194
5.7.1	Webseite analysieren	194
5.7.2	Maßnahmen auf der Webseite	195
5.7.3	Datenschutzerklärung	195
5.7.4	Kontaktformular	195
5.8	Verschlüsselung in der Kommunikation	196
5.8.1	Kommunikation mit Mandanten	196
5.8.2	Mobile Datenträger	197
5.8.3	Messenger-Programme	198
5.8.4	Kommunikation mit öffentlichen Einrichtungen	198
5.9	Private Nutzung von Dienstgeräten	200
5.10	Videüberwachung	201
5.10.1	Videüberwachung geplant/bereits aktiv?	201
5.10.2	Checkliste Videüberwachung	201
5.10.3	Maßnahmen bei der Umsetzung	201
5.10.4	Aushang der Hinweisschilder	202
5.10.5	Information bei Anfragen Betroffener	202
5.11	Erstellung der Dokumentation	202
5.11.1	Verzeichnis der Verarbeitungstätigkeiten	202
5.11.2	Technische und organisatorische Maßnahmen	209
5.11.3	IT-Systemdokumentation	210
5.11.4	Rollen-und Verantwortlichkeiten	211
5.11.5	Zugriffberechtigungen für Daten und Systeme	211
5.11.6	Löschkonzept	212
5.11.7	Datensicherungskonzept	212
5.11.8	Infoblatt des Datenschutzes bei Auftragsbeginn	213
5.11.9	Betroffenenrechte und -prozesse	213

5.11.10	Videüberwachung	213
5.11.11	Serviceverträge mit externen Dienstleistern	213
5.12	Abschlusskontrolle	214
5.12.1	Checkliste am Ende aller Maßnahmen	214
6.	Nützliche Links	215
6.1	Gesetze	215
6.2	Ämter, Gremien, Verbände	215
6.3	Vorlagen	215
6.3.1	Verzeichnis der Verarbeitungstätigkeiten	215
6.3.2	AV-Verträge	216
6.3.3	Verpflichtung zur Verschwiegenheit	216
6.3.4	Einwilligung unverschlüsselter E-Mail-Kommunikation mit Mandanten	216
6.4	Checklisten	216
6.4.1	Fragebogen zur Umsetzung der DSGVO	216
6.4.2	Einwilligung	217
6.4.3	Datensicherheit	217
6.5	Weitere Informationen und Orientierungshilfen	217
6.5.1	Risiko für die Rechte und Freiheiten natürlicher Personen	217
6.5.2	Datenschutzfolgeabschätzung (DSFA)	217
6.5.3	Besondere Kategorien personenbezogener Daten	217
6.5.4	Drittländer	218
6.5.5	Videüberwachung	218
6.5.6	Auskunft, Löschung	218
6.5.7	Steuerberater	218
6.5.8	Datenschutzbeauftragter	218
6.5.9	Informationspflichten	219
6.5.10	Zertifizierungen	219
6.5.11	Auftragsverarbeitung	219
6.5.12	Betroffenenrechte	219
6.5.13	E-Mail und andere Internetdienste am Arbeitsplatz	219
6.5.14	Beschäftigungsdatenschutz	219
6.5.15	Maßnahmenplan	220
6.5.16	Kurzpapiere der DSK	220