

---

# Inhaltsverzeichnis

Vorwort StB Mag. Klaus Hübner, Präsident der Kammer der Steuerberater und Wirtschaftsprüfer .....	V
Vorwort des Herausgebers .....	VII
Autorenverzeichnis .....	XVII
Abkürzungsverzeichnis .....	XXI
Literaturverzeichnis .....	XXV
<b>1. Einleitung .....</b>	<b>1</b>
<b>2. Stakeholder .....</b>	<b>5</b>
2.1. Relevante Stakeholder .....	5
2.1.1. Klienten .....	5
2.1.2. Mitarbeiter des Klienten .....	6
2.1.3. Mitarbeiter der Kanzlei .....	6
2.1.4. Interessenvertreter – Kammer der Steuerberater und Wirtschaftsprüfer (KSW) .....	6
2.1.5. Mitbewerber .....	7
2.1.6. Gesetzgeber .....	7
2.1.7. Aufsichtsbehörden .....	8
2.1.8. Partner und Gesellschafter .....	8
2.2. Analyse der Stakeholder .....	9
2.2.1. Klienten .....	10
2.2.2. Mitarbeiter des Klienten .....	10
2.2.3. Mitarbeiter der Kanzlei .....	10
2.2.4. Interessenvertreter – Kammer der Steuerberater und Wirtschaftsprüfer (KSW) .....	10
2.2.5. Mitbewerber .....	10
2.2.6. Gesetzgeber .....	11
2.2.7. Aufsichtsbehörden .....	11
2.2.8. Partner und Gesellschafter .....	11
<b>3. Gesetzliche Grundlagen und Compliance .....</b>	<b>13</b>
3.1. Gesetzesmaterien zum Informationsschutz .....	13
3.1.1. Einleitung .....	13
3.1.2. Datenschutzrecht .....	13
3.1.2.1. Allgemeines .....	13
3.1.2.2. Datenschutz im Home-Office .....	15
3.1.3. Aufbewahrungspflichten .....	16
3.1.3.1. Berufspflichten .....	16
3.1.3.2. Hausdurchsuchungen .....	17
3.1.3.3. Geldwäsche- und Terrorismusfinanzierungsprävention .....	18
3.1.3.4. Bundesabgabenordnung .....	18
3.1.3.5. Unternehmensgesetzbuch und Grundsätze ordnungsgemäßer Buchführung .....	19
3.1.3.6. Sonstige Aufbewahrungsfristen .....	19



4.1.3.	Basiswerkzeuge des Informationssicherheitsmanagements .....	50
4.1.3.1.	Richtlinien .....	50
4.1.3.2.	Informationssicherheitspolitik .....	50
4.1.3.3.	Rollen und Gremien .....	50
4.1.3.4.	Methodik des Risikomanagements .....	51
4.1.3.5.	Schulungen .....	53
4.1.3.6.	Audit .....	54
4.1.3.7.	Asset Management .....	54
4.1.3.8.	Physische Sicherheit .....	55
4.1.3.9.	Zugriffskontrolle .....	55
4.1.3.10.	Notfallmanagement .....	55
<b>5.</b>	<b>Die DSGVO und die praktische Anwendung in der Wirtschaftstreuhandkanzlei .....</b>	<b>59</b>
5.1.	DSGVO-Umsetzung .....	59
5.1.1.	Unmittelbare Geltung der DSGVO .....	59
5.1.2.	Nationale Umsetzung .....	61
5.1.3.	Die DSGVO und mögliche Angriffsflächen der Kanzlei .....	62
5.1.3.1.	Datenschutzbehörde .....	62
5.1.3.2.	Mitarbeiter .....	64
5.1.3.3.	Interessenvertretungen .....	64
5.1.3.4.	Klienten .....	65
5.1.3.5.	Sonstige involvierte Geschäftspartner bzw Interessenten .....	66
5.1.3.6.	Mitbewerb .....	66
5.1.4.	E-Privacy-Verordnung .....	66
5.2.	Rechtmäßigkeit der Datenverarbeitung in der Steuerberatungskanzlei .....	67
5.2.1.	Allgemeines .....	67
5.2.2.	Die Rechtsgrundlagen .....	68
5.2.2.1.	Die Verarbeitung von „normalen/schlichten“ personenbezogenen Daten .....	68
5.2.2.1.1.	Einwilligung der betroffenen Person .....	68
5.2.2.1.2.	Vertragserfüllung / vorvertragliches Verhältnis (Vertragsanbahnung) mit der betroffenen Person .....	69
5.2.2.1.3.	Rechtliche (gesetzliche) Verpflichtung .....	70
5.2.2.1.4.	Lebenswichtige Interessen .....	71
5.2.2.1.5.	Öffentliche Aufgaben / Ausübung öffentlicher Gewalt .....	71
5.2.2.1.6.	Berechtigte Interessen .....	72
5.2.2.2.	Daten besonderer Kategorien .....	74
5.2.2.3.	Daten über strafrechtliche Verurteilungen und Straftaten (Strafregisterbescheinigungen) .....	75
5.2.3.	Exkurs: Marketingmaßnahmen und Rechtmäßigkeit .....	76
5.2.3.1.	Allgemeines .....	76
5.2.3.2.	Marketingmaßnahmen per Post .....	76
5.2.3.3.	Marketingmaßnahmen per E-Mail oder sonstige elektronische Medien .....	77
5.2.3.4.	Elektronische Marketingmaßnahmen bei Bestandskunden .....	77

5.3. Rechte der Klienten .....	79
5.3.1. Einleitung .....	79
5.3.2. Informationspflichten des Steuerberaters .....	79
5.3.3. Auskunftspflicht des Steuerberaters .....	80
5.3.4. Meldepflichten bei Verletzungen .....	81
5.3.5. Pflicht zur Datenübertragung .....	82
5.3.6. Pflichten betreffend Auftragsverarbeiter .....	82
5.3.7. Rechte der Datenschutzbehörde und Rechtsdurchsetzung .....	83
5.4. Steuerberater und Auftragsverarbeitung .....	84
5.4.1. Allgemeines zum arbeitsteiligen Verarbeiten von Daten .....	84
5.4.2. Notwendigkeit der Abgrenzung .....	85
5.4.3. Abgrenzungskriterien: Wann ist ein Verarbeiter Auftragsverarbeiter im Sinne der DSGVO? .....	86
5.4.4. Beispiele .....	88
5.4.5. Fernwartungszugriff und Prüfung oder Wartung von IT-Systemen als Auftragsverarbeitung .....	90
5.4.6. Zusammenarbeit in der eigenen Kanzlei bzw mit verbundenen Unternehmen – gemeinsame Verantwortlichkeit .....	91
5.4.7. Ist der Steuerberater „Auftragsverarbeiter“ seines Klienten? .....	93
5.4.8. Konstellationen der berufstypenübergreifenden Zusammenarbeit? .....	96
5.5. Notwendige Prozesse im Unternehmen .....	96
5.5.1. Data Breach – Datenpanne .....	97
5.5.2. Prozesse zur Wahrung der Betroffenenrechte .....	99
5.5.2.1. Grundsätzliche Rahmenbedingungen für Prozesse zur Wahrung der Betroffenenrechte .....	99
5.5.2.2. Auskunftsprozess .....	100
5.5.2.3. Löschprozess .....	102
5.5.2.4. Berichtigungsprozess .....	103
5.5.2.5. Widerspruchsprozess .....	105
5.5.2.6. Einschränkungsprozess .....	107
5.5.2.7. Datenübertragungsprozess .....	108
5.5.2.8. Datenschutz-Folgenabschätzung .....	109
5.5.3. Wiederkehrende Prozesse .....	110
5.5.3.1. Erstellung und Aktualisierung des Verzeichnisses von Verarbeitungstätigkeiten .....	110
5.5.3.2. Prüfung des Frist- oder Zweckablaufes .....	111
5.5.3.3. Audits .....	112
5.5.4. Zusammenfassung .....	112
5.5.4.1. Level 1 .....	112
5.5.4.2. Level 2 .....	112
5.6. Organisatorische und personelle Zuständigkeit im Datenschutz .....	113
5.6.1. Organisation .....	113
5.6.2. Datenschutzbeauftragter .....	114
5.6.2.1. Benennung eines Datenschutzbeauftragten in der Kanzlei .....	114
5.6.2.2. Aufgaben des Datenschutzbeauftragten .....	115

5.6.2.3.	Stellung des Datenschutzbeauftragten .....	115
5.6.2.4.	Externer oder Interner Datenschutzbeauftragter .....	116
5.6.3.	Datenschutzkoordinator .....	117
5.6.4.	Zusammenfassung .....	117
5.6.4.1.	Level 1 .....	117
5.6.4.2.	Level 2 .....	117
5.7.	Eigene Mitarbeiter im Unternehmen .....	118
5.7.1.	Relevante Bestimmungen (DSGVO, DSGVO, AVRAG, usw) .....	118
5.7.2.	Relevante Personen im Beschäftigungsverhältnis .....	123
5.7.3.	Notwendige Dokumentation .....	124
5.7.3.1.	Datenschutzerklärung .....	124
5.7.3.2.	Verpflichtungserklärung .....	126
5.7.4.	Schulungsmaßnahmen für Mitarbeiter .....	128
5.7.5.	Ausgewählte Praxisbeispiele in einer Kanzlei .....	130
5.7.6.	Schlussfolgerungen und Empfehlungen .....	132
<b>6.</b>	<b>Technische und organisatorische Maßnahmen .....</b>	<b>135</b>
6.1.	Verschwiegenheitsverpflichtung und die drei Schutzziele .....	135
6.1.1.	Vertraulichkeit .....	135
6.1.2.	Integrität .....	136
6.1.3.	Verfügbarkeit .....	136
6.2.	TOMs in der Praxis .....	137
6.2.1.	Zutritts- und Zugriffskontrolle .....	137
6.2.1.1.	Gebäudeschutz .....	138
6.2.1.1.1.	Mechanisches Schließsystem .....	138
6.2.1.1.2.	Elektronisches Schließsystem .....	138
6.2.1.1.3.	Schutz der Hardware .....	139
6.2.1.2.	Netzwerk und externer Zugriff .....	141
6.2.1.3.	Netzwerksegmentierung .....	143
6.2.1.3.1.	Segmentierung und Netzwerkplan .....	143
6.2.1.3.2.	Firewall und Routing .....	144
6.2.1.4.	Home-Office und Remote-Zugänge .....	145
6.2.1.5.	Berechtigungs- und Rollenkonzept .....	146
6.2.1.5.1.	Rollenkonzept .....	146
6.2.1.5.2.	Sonderberechtigungen und Freigabe .....	146
6.2.1.5.3.	Kontrolle der Berechtigungen .....	147
6.2.1.6.	Komplexe Passwörter und der sichere Umgang .....	148
6.2.1.6.1.	Passwort .....	148
6.2.1.6.2.	Biometrische Merkmale .....	150
6.2.1.6.3.	Zwei- oder Multi-Faktor-Authentifizierung .....	150
6.2.1.6.4.	Umgang mit Authentifizierungsmerkmalen .....	150
6.2.1.7.	Lokale Administratoren .....	151
6.2.1.8.	Videoüberwachung .....	152
6.2.2.	Geräteverwaltung .....	154
6.2.2.1.	Geräteverwaltung – Asset-Management .....	154
6.2.2.2.	Mobile-Device-Management .....	155

6.2.3.	Software- und Netzwerkmaßnahmen .....	156
6.2.3.1.	Patch- und Updatemanagement .....	156
6.2.3.2.	Verschlüsselung .....	157
6.2.3.3.	Verfügbarkeit – Backup und Restore .....	160
6.2.3.3.1.	Backup-Frequenz .....	161
6.2.3.3.2.	Aufbewahrungsort von Backups .....	161
6.2.3.3.3.	Aufbewahrungsdauer .....	162
6.2.3.3.4.	Wiederherstellungstests .....	162
6.2.3.4.	Archivierung .....	162
6.2.3.5.	Sicherheit der Daten in der Cloud .....	164
6.2.3.6.	Virenschutz .....	165
6.2.3.7.	Angriffserkennung und Alarmierung .....	166
6.2.4.	Regelungen zum sicheren Umgang mit Daten .....	168
6.2.4.1.	Sicherheits- und Endbenutzerrichtlinie .....	168
6.2.4.2.	Schulung und Sensibilisierung .....	170
6.2.4.2.1.	Gründe für die Sensibilisierung von Mitarbeitern .....	171
6.2.4.2.2.	Inhalte der Sensibilisierungsmaßnahmen .....	171
6.2.4.2.3.	Art und Weise .....	172
6.2.4.3.	Sichere Vernichtung .....	173
6.2.4.3.1.	Löschen digitaler Daten .....	174
6.2.4.3.2.	Vernichtung analoger Dokumente .....	174
6.2.4.4.	Umgang mit Daten und Geräten .....	175
6.2.4.4.1.	Umgang mit Daten .....	175
6.2.4.4.2.	Umgang mit Geräten .....	176
6.2.5.	Umgang mit Dritten .....	178
6.2.5.1.	Generelle Übermittlung von Daten .....	178
6.2.5.2.	Auftragsverarbeiter .....	178
6.2.5.3.	Sub-Auftragnehmer .....	179
6.2.5.4.	Besucherregelungen .....	179
6.2.6.	Notfallmanagement .....	180
6.2.6.1.	Risikoanalyse .....	181
6.2.6.2.	Notfallvorsorge .....	181
6.2.6.3.	Umgang mit Notfällen .....	182
6.2.6.3.1.	Wiederherstellung des normalen Betriebes .....	182
6.2.6.3.2.	Ursachenforschung .....	182
6.2.6.4.	Data-Breach-Management .....	182
6.2.6.4.1.	Wann ist eine Datenschutzverletzung zu melden .....	183
6.2.6.4.2.	Inhalte einer Datenschutzverletzung .....	183
6.2.7.	Betroffenenrechte .....	183
6.2.7.1.	Planung des Umgangs .....	184
6.2.7.2.	Export in maschinenlesbares Format .....	184
6.2.7.3.	Dokumentation .....	185



## Inhaltsverzeichnis

---

8.2.3. CEO Fraud .....	239
8.2.4. Passwortsicherheit .....	239
8.2.5. Insider .....	240
8.3. Cyberkriminalität – ein aktuelles Lagebild .....	241
8.4. Erkennung und Vermeidung .....	242
8.5. Vermeidung von Cybercrime .....	242
8.6. Nachbearbeitung von Vorfällen .....	244
8.7. Zukunft Digitalisierung .....	245
8.8. Digitalisierung im Rechnungswesen .....	247
<b>Stichwortverzeichnis .....</b>	<b>249</b>