Balzer • Buchberger

Datenschutz in Steuerberater-, Wirtschaftsprüfer- und Rechtsanwaltskanzleien

Praxisleitfaden mit Checklisten, Übersichten und Beispielen

ESV ERICH SCHMIDT VERLAG

ERICH
SCHMIDT
VERLAG

Datenschutz in Steuerberater-, Wirtschaftsprüfer- und Rechtsanwaltskanzleien

Praxisleitfaden mit Checklisten, Übersichten und praktischen Beispielen

Von

Thomas Balzer

und

Erhard Buchberger

ERICH SCHMIDT VERLAG

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Weitere Informationen zu diesem Titel finden Sie im Internet unter
http://ESV.info/978-3-503-18865-9

Zitiervorschlag:
Balzer/Buchberger, Praxisleitfaden zur Umsetzung der DSGVO in Steuerberater-, Wirtschaftsprüfer- und Rechtsanwaltskanzleien

ISBN 978-3-503-18865-9 (gedrucktes Werk)
ISBN 978-3-503-18866-6 (eBook)

Druck: docupoint, Barleben

Inhaltsverzeichnis

1. Einleitung 11
1.1 Vorwort 11
1.2 Kurzvorstellung B² 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 Personenbezogene 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 im 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 Videoüberwachung ... 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 VPN-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 Videoüberwachung/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 Videoüberwachung ... 201
5.10.1 Videoüberwachung geplant/bereits aktiv? ... 201
5.10.2 Checkliste Videoüberwachung ... 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 Videoüberwachung ... 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 Videoüberwachung ... 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

1. Einleitung

1.1 Vorwort

Die Europäische Datenschutzgrundverordnung – kurz EU-DSGVO oder auch DSGVO – ist für viele Unternehmen oder Unternehmer möglicherweise zunächst kein Wort, das einen ein freudiges Lächeln entlockt. So scheint es doch, als hätte der europäische Gesetzgeber wieder eine weitere Bürde geschnürt, die einem Unternehmer nur wieder weitere Aufwendungen, Maßnahmen und damit verbunden auch zusätzliche Kosten auferlegt.

Bereits vorab gab es durch das Bundesdatenschutzgesetz (BDSG) eine gesetzliche Vorgabe, die es ebenso zu beachten und umzusetzen galt und noch umzusetzen gilt. Auch hier wurden und werden bei Verstößen Bußgelder durch die Aufsichtsbehörden verhängt. Doch es wurde eben in der Vergangenheit nur sehr wenig geprüft oder gar sanktioniert. Durch die neue DSGVO ist das Thema Datenschutz wieder in den Vordergrund gerückt und verbunden mit höheren Bußgeldern definitiv wieder sichtbarer geworden.

Die Berücksichtigung der DSGVO ist nicht nur ein Vorteil für den Datenschutz an sich, der natürlichen Personen und deren zugehörige personenbezogene Daten. Ein Großteil aller erforderlichen Maßnahmen innerhalb Ihrer Kanzlei, um die DSGVO umzusetzen, sind in technischer und organisatorischer Hinsicht auch aus einer anderen Perspektive mehr als sinnvoll und können sogar gewinnbringend sein. Wie kommen wir darauf?

Wir wechseln einmal die Perspektive, weg von der DSGVO und den betroffenen Personen, deren personenbezogenen Daten Sie in ihrer Kanzlei verarbeiten, hin zu Ihnen, dem Unternehmer, dem Kanzleibesitzer. Sicher möchten Sie alle ihre Daten in der Kanzlei schützen, also über die personenbezogenen Daten zum Beispiel die ihrer Mitarbeiter und Mandanten hinaus. Der Schutz soll so angemessen sein, oder wie man so schön sagt, nach „Stand der Technik“ und mit einem machbaren und vertretbaren beziehungsweise sinnvollen organisatorischen, technischen und schließlich monetären Aufwand. Dazu zählt unter anderem der Schutz gegen unbefugten Zugriff in analoger Weise, also beispielsweise durch Einbruch oder Diebstahl, wie in digitaler Weise, also zum Beispiel über das stets verbundene Internet oder durch Schadcodes in Form von sogenannten Trojanern, die sich an E-Mails hängen.

Die wesentlichen Maßnahmen, die bei der Umsetzung der DSGVO durchgeführt werden, dienen letztendlich auch dem Schutz aller Daten des Unternehmens beziehungsweise Ihrer Kanzlei. Es überrascht uns in unserer täglichen Praxis daher nicht, wenn wir immer wieder auf Unternehmer stoßen, denen wir diese Erkenntnis nahebringen können. Das macht es vielen Unternehmern dann bereits schon zu Beginn leichter, sich mit den durch die Umsetzung der DSGVO anfallenden Aufwendungen „anzufreunden“.

Zudem können noch einige positive Seiteneffekte gleich während der Umsetzung angestoßen werden. Durch die Analyse, beziehungsweise dem sogenannten Datenschutzaudit, werden auch teils ineffiziente Prozesse oder Systeme zu Tage gefördert, welche sich historisch oder im Rauschen des alltäglichen, produktiven Wirkens, eingeschlichen haben.

Im Folgenden schauen wir dabei stets auch über den Tellerrand der DSGVO auf das gesamte Unternehmen, sowohl in technischer, organisatorischer und prozeduraler Sicht und erkennen so zusätzliche Potenziale.

Wir hoffen Ihnen mit unserem Buch die wesentlichen Informationen zur praxisnahen Umsetzung der DSGVO in einer kompakten und informativen Form an die Hand zu geben.

Wir wünschen Ihnen dabei viel Erfolg.

Ihr Thomas Balzer & Erhard Buchberger[1]

1 Foto: Der Gottwald – *https://der-gottwald.de*.

1.2 Kurzvorstellung B² Berlin

Wir, B² Berlin möchten uns Ihnen kurz vorstellen. Wir sind eine Unternehmensberatung mit folgenden Tätigkeitsschwerpunkten:

- Unternehmensberatung
- Geschäftsprozessmanagement
- Auswahlverfahren
- Projektmanagement
- Konzepterstellung
- Coaching & Schulungen
- Datenschutzbeauftragte/Datenschutzauditoren (TÜV Nord zertifiziert)

Dabei konzentrieren wir uns zudem in den letzten Jahren auf zwei neue, wichtige Themenbereiche:

DSGVO

„Europäische Datenschutzgrundverordnung".

Das Thema dieses Buches.

GoBD

„Grundsätze zur ordnungsgemäßen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff".

Dieses Thema behandelt die Frage, wie in einem Unternehmen mit steuerlich relevanten Informationen beziehungsweise Dokumenten umgegangen werden sollte. Dies wird im Rahmen einer Betriebsprüfung seit 2015 besonders für die Unternehmer wichtig.

Wir, die Geschäftsführer Dipl.-Ing. Thomas Balzer und Dipl.-Ing. Erhard Buchberger bündeln unsere Praxiserfahrungen aus über 25 Jahren unserer unterschiedlichen Beratungstätigkeit in unserem Unternehmen B² Berlin. Thomas Balzer war über 25 Jahre in einem deutschen, international agierenden Pharmakonzern tätig und durchlief dort verschiedene Abteilungen in der IT, der Logistik und Produktion und in unterschiedlichen Funktionen. Erhard Buchberger war viele Jahre als Unternehmensberater für Geschäftsprozessmanagement und Einführung von geschäftsprozessbasierten EDV-Systemen tätig.

B² Berlin ist unter anderem Partner des Steuerberaterverbandes Berlin-Brandenburg und verschiedener großer Steuerberaterkanzleien im Raum Berlin-Brandenburg. Wir referieren in verschiedenen Wirtschaftsverbänden der Industrie und des Handwerks und sind unter anderem als Dozenten an der Beuth Hochschule und der Fachhochschule des Mittelstandes in Berlin tätig.

1.3 Der rote Faden

Wenn wir uns dem Datenschutz zuwenden, stellen sich uns verschiedene grundsätzliche Fragen, die es zu berücksichtigen gilt:

- Was bedeutet der Datenschutz, die DSGVO, für meine Kanzlei?
- Wie hoch ist der Grad der aktuellen DSGVO-Konformität in meiner Kanzlei?
- Wie überprüfe ich den aktuellen Status in meiner Kanzlei?
- Brauche ich einen Datenschutzbeauftragten?
- Welche Dokumentations- beziehungsweise Informationspflichten habe ich?
- Was sind die Betroffenenrechte?
- Was ist mit der Webseite meiner Kanzlei?
- Was ist organisatorisch und/oder technisch zu tun?
- Welche Meldefristen gibt es für meine Kanzlei?
- Was wäre eine sinnvolle Reihenfolge in der Umsetzung?
- Wie integriere ich meine Mitarbeiter?
- Wie groß ist dabei der personelle und organisatorische Aufwand?
- Was wird es am Ende kosten?

Und bei diesen Fragen kommt bei uns der „rote Faden" ins Spiel. Sicher gibt es unterschiedliche Ausprägungen und Interpretationen was der „rote Faden" genau ist. Wir meinen damit eine strukturierte Vorgehensweise. Sie ermöglicht es dem Verantwortlichen, also Ihnen, dem Kanzleibesitzer, die personellen, technischen und zeitlichen Aufwände, die zugehörigen Prioritäten und die jeweiligen Umsetzungsgrade abschätzen zu können. Damit behält der Verantwortliche die gesamte Laufzeit der Umsetzung im Auge und kann so die erforderlichen Maßnahmen, zusätzlich zum operativen und produktiven Alltag, voranbringen.

In unserer langjährigen Unternehmensberatung setzen wir dabei auf die Erfahrungen und die Methoden des klassischen Projektmanagements, also der strukturierten und kontrollierten Abarbeitung mittels eines Projektplanes, mithilfe dessen alle relevanten Arbeitspakete in eine sinnvolle und machbare Reihenfolge gebracht und praxisnah abgearbeitet werden können. Alle Betroffenen haben so stets einen klaren und nachvollziehbaren Überblick über das Projekt, was ein wesentlicher Erfolgsfaktor für eine gute und erfolgreiche Umsetzung ist.

Vielleicht fragen Sie sich, was die Umsetzung der DSGVO in ihrer Kanzlei mit einem Projekt zu tun haben könnte. Nun, die Umsetzung der DSGVO in ihrer Kanzlei hat mindestens einen Projektcharakter. Die Methodik, wie in der Praxis der Projektplan genutzt wird, ist hier ebenfalls anwendbar und dient der Kanzlei beziehungsweise dem Kanzleiinhaber und den Beschäftigten als Werkzeug, quasi als „roter Faden".

1.4 Der grobe Ablauf

Folgender prinzipieller Ablauf hat sich in der Praxis bewährt.

- Zunächst das Thema DSGVO zur Chefsache erklären und starten
- Einbeziehung eines Datenschutzbeauftragen (nach Bedarf)
- Datenschutzaudit intern durchführen und
- identifizierte Lücken technisch/organisatorisch schließen:
  - Auftragsverarbeitungsverträge abschließen
  - Geheimhaltungsvereinbarungen abschließen
  - Prozesse zu den Informationspflichten etablieren
  - Prozesse zu den Betroffenenrechte etablieren
  - Dokumentationen erstellen
  - Webseite sicher machen
  - Schulung beziehungsweise Sensibilisierung der Mitarbeiter
  - Regelmäßige Überprüfungen des Status
  - etc.

1.5 Vorgehensweise des Buches

Ein Praxisleitfaden für die DSGVO. Wie sollte dieser aufgebaut sein?

Nun, nach unserer Meinung so, dass Sie, der Leser, auch am Ende prinzipiell in der Lage sind, ihre Kanzlei der DSGVO entsprechend konform zu gestalten. Wir teilen dieses Buch in folgende Kapitel:

- Kapitel 1: Einleitung
- Kapitel 2: Einstimmung auf die DSGVO
- Kapitel 3: Basiswissen zur DSGVO
- Kapitel 4: Schutz personenbezogener Daten
- Kapitel 5: Prinzipieller Ablauf in der Praxis
- Kapitel 6: Nützliche Links (Vorlagen, Formulare, Checklisten, etc.)

Kapitel 2 stimmt zunächst etwas auf die DSGVO ein.

Kapitel 3 widmet sich den Basis-Themen rund um die DSGVO aus der theoretischen Sicht, so dass sie sich einen Überblick über die wichtigsten Themen und Begriffe machen können. Es ist zudem mit Beispielen aus der Praxis versehen, um die Inhalte verständlicher zu machen.

Kapitel 4 beschäftigt sich umfangreich mit dem Thema „Schutz personenbezogener Daten". Diesem Thema haben wir deshalb ein eigenes Kapitel gegeben, da es für die spätere, praxisnahe Umsetzung von großer Bedeutung ist. Auch dieses Kapitel enthält Beispiele aus der Praxis zum besseren Verständnis.

Kapitel 5 geht dann auf die praxisnahe Umsetzung konkret ein und zeigt Ihnen einen möglichen Weg, wie Sie die DSGVO in ihrer Kanzlei umsetzen können.

Sollten Sie also mit der DSGVO bereits schon inhaltlich gut vertraut sein, könnten Sie prinzipiell auch direkt in dieses Kapitel springen und gleich loslegen. Kapitel 3 und Kapitel 4 dienen dann auch als Nachschlagewerk.

Kapitel 6 stellt Ihnen nützliche Links bereit, die auf weitere und teils tiefergehende Informationen enthalten. Hier finden Sie unter anderem Verweise auf weitere Checklisten oder Vorlagen.

1.6 Haftungsausschluss

Dieses Buch ersetzt keine individuelle Beratung. Ein Beratungsvertrag kommt durch dieses Buch nicht zustande. Alle Informationen wurden sorgfältig bearbeitet und zusammengetragen. Es wird gleichwohl – auch seitens der Autoren – keine Gewähr und somit auch keine Haftung für die Richtigkeit, Aktualität und Vollständigkeit der Inhalte und Darstellungen übernommen.

2. Einstimmung auf die DSGVO

2.1 Unterschied Datenschutz und Datensicherheit

Zunächst eine Begriffsklärung, denn oft werden beide Begriffe verwechselt oder im falschen Kontext genannt.

Datensicherheit – ein modernerer Begriff dafür ist „Informationssicherheit" – behandelt den Schutz von Daten hinsichtlich gegebener Anforderungen bezüglich deren Vertraulichkeit, Verfügbarkeit und Integrität.

Beispiele:
- die Sicherheit der Vertraulichkeit durch geeignete Ablagesysteme und der zugehörigen Berechtigungen im EDV-System
- die Sicherstellung der Verfügbarkeit durch eine schlüssige, durchgängige und valide Datensicherung

Datenschutz – mit Datenschutz wird der Schutz personenbezogener Daten vor etwaigem Missbrauch durch Dritte bezeichnet.

Das können wir uns etwa so vorstellen: Was im analogen Leben der Bodyguard für einen Menschen ist, also der Schutz des physischen Körpers des Menschen vor Dritten, ist der Datenschutz für das digitale Umfeld, also der virtuellen, digitalen Welt.

Datenschutz betrachten wir daher immer auch als digitalen „Personenschutz". Es geht also beim Datenschutz nicht primär um den Schutz der Daten, sondern um den Schutz der Person, der die Daten gehören. Ein Thema also, das uns alle betrifft und dem wir uns deshalb zuwenden und Aufmerksamkeit schenken sollten.

2.2 Was bedeutet der Datenschutz heute?

Die „digitale Welt" mit ihren facettenreichen Möglichkeiten findet sich heute in allen Bereichen des Lebens wieder, sowohl im privaten, als auch im gewerblichen Umfeld. Gerade in gewerblichen Bereichen hat die Verwendung digitaler Technik in den letzten Jahren sehr stark zugenommen und wird auch zukünftig weiter zunehmen, denn es gibt stetig neue Entwicklungen und Einsatzmöglichkeiten. Ein Geschäft ohne IT zu betreiben ist heute nahezu undenkbar.

Mit zunehmender Funktionalität beziehungsweise Programmvielfalt steigt jedoch auch weiterhin unsere Abhängigkeit von den digitalen Werkzeugen. Kaum ein Arbeitsprozess ist heute noch ohne deren Einsatz möglich und deshalb finden sie sich bei den bekannten Office-Produkten, bis hin zu komplexeren Systemen und IT-Umgebungen wieder.

So wird auch in den Kanzleien neben den klassischen Papierakten auch immer mehr IT eingesetzt. Der Trend geht immer mehr dazu über, Papier vollständig durch elektronische Dateien und Akten zu ersetzen. In vielen Kanzleien wird immer mehr digitalisiert und bestehende Papierakten werden gescannt und den digitalen Prozessen zugeführt. Einige Kanzleien haben mittlerweile vollständig auf die digitale Verarbeitung umgestellt und Papier liegt, wenn überhaupt, nur noch im Archiv. Dadurch liegen immer mehr personenbezogene Daten in elektronischer Form vor und in einer Kanzlei zudem mit sehr sensiblem Inhalt.

Der Datenschutz gewinnt so zunehmend an Bedeutung und die DSGVO hat zum Ziel, die sogenannten betroffenen Personen, also die Menschen und deren personenbezogenen Daten zu schützen. So kommen wir als Unternehmensberater auch zu der Aussage, dass Datenschutz wie ein Personenschutz ist, nur eben in einer digitalen, expandierenden Welt.

2.3 Unterschied BDSG und DSGVO

Die DSGVO für Deutschland ist am 25. Mai 2018 in Kraft getreten, genau zwei Jahre später, als sie in der EU in Kraft getreten ist. Deutschland bekam diese „Verlängerung", da es bereits schon zuvor einen sehr hohen Datenschutzstandard hatte. Diese zwei Jahre sollten nun die Möglichkeit bieten, sich mit der DSGVO vertraut zu machen und sie in Ruhe umzusetzen.

Eigentlich eine gute Sache. Doch viele hatten diesen zeitlichen Vorsprung nicht in ihren Planungen berücksichtigt oder ihm die notwendige Priorität zugestanden und damit nicht oder nur unzureichend genutzt. Das führte nun vor Anfang 2018 zu einer relativ großen Panik, als auch in der Presse, Wochen vor dem 25. Mai 2018, das Thema „Die DSGVO kommt immer näher" zunehmend publiziert wurde.

Viele handelten nun quasi in letzter Minute, was jedoch nicht immer erfolgreich war, denn die DSGVO ist ein neues Gesetz und wirft in seiner praktischen Umsetzung noch heute immer wieder Fragen zu ihrer Umsetzung auf. Wie sollte damit nun angemessen umgegangen werden?

Es gab ja zum Start keine belastbaren Urteile. Auf diese werden wir noch einige Zeit warten müssen und so stützten sich viele daher auch auf das bisherige BDSG. Einige waren damals stark verunsichert und haben dadurch fast panisch reagiert. So wurden unter anderem private und gewerbliche Webseiten, Vereinsseiten oder Online-Shops geschlossen, nur aus Angst davor, den nunmehr hohen Bußgeldern bei Nichtkonformität mit der DSGVO willkürlich ausgeliefert zu sein. Ein entsprechend wirtschaftlicher Verlust ging dabei sicher bei einigen Betroffenen mit einher.

Die DSGVO ist eine Verordnung, die unmittelbar und in allen Ländern der EU umzusetzen ist. Doch wie erwähnt, es gab schon vor der DSGVO andere Daten-

schutzgesetze. Und der Vorgänger der DSGVO war in Deutschland quasi das Bundesdatenschutzgesetz, kurz BDSG, welches 1977 in Kraft trat.

Seit der DSGVO ist es nun in BDSG alter Fassung, kurz BDSG a. F. umbenannt worden. Doch es gilt das BDSG weiterhin, jedoch in einer auf die DSGVO angepassten neuen Fassung, welches daher auch als BDSG n. F. oder BDSG-neu bezeichnet wird. Die DSGVO enthält nämlich eine Reihe von sogenannten Öffnungsklauseln, die es den einzelnen EU-Ländern gestatten, eigene Gesetze darauf aufzusetzen. Damit sind seit dem 25. Mai 2018 die DSGVO und das BSDG-neu in Deutschland umzusetzen.

Was genau alles das BDSG-neu für Deutschland zusätzlich regelt, ist nicht Inhalt dieses Buches. Doch sei eine wichtige Tatsache erwähnt. Das BDSG-neu legt für deutsche Unternehmen die Messlatte für den Umsetzungsaufwand noch etwas höher. Hier möchten wir ein Beispiel nennen:

Die DSGVO gibt zum Beispiel keine untere Grenze für die Anzahl von Personen vor, die stetig personenbezogene Daten in einem Unternehmen verarbeiten, um dann einen Datenschutzbeauftragten benennen zu müssen. Das jedoch regelt das BDSG-neu. Hier kommt die mittlerweile vielen bekannte Grenze her, nach der ab 10 Personen ein Datenschutzbeauftragter zu benennen ist.

Kommt ein interner Datenschutzbeauftragter zum Einsatz, ist er entsprechend zu qualifizieren und in seinem Wissenstand aktuell zu halten. Das könnte dann auch ein Grund für den Einsatz eines externen Datenschutzbeauftragten werden. Beides hat Vor- und Nachteile, auf die wir noch im Kapitel 3.11 näher eingehen. Doch beide Varianten verursachen in jedem Fall Kosten.

2.4 Ziele der DSGVO

Im Art. 1 DSGVO sind die Ziele definiert:

- Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.
- Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.
- Der freie Verkehr personenbezogener Daten in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden.

2.5 Problematiken

Bei der Umsetzung der DSGVO und auch dem BDSG-neu stoßen wir seit Inkrafttreten immer wieder auf Probleme bei Fragen, die sich mit einer verhältnismäßigen, praxisnahen, machbaren und sinnvollen Umsetzung beschäftigen. Die Ursache liegt im Wesentlichen an diesen Umständen:

- Keine gefestigte Interpretations- beziehungsweise Auslegungshilfen: EuGH-Rechtsprechung bezieht sich auf die außer Kraft gesetzte Richtlinie 95/46/EG
- Stellungnahmen/Orientierungshilfen des Europäischen Datenschutzausschusses müssen erst noch formuliert werden
- Kommentierungen aus der Literatur existieren nur bedingt und wenn doch, dann sind sie nicht immer in einer für Jedermann verständlichen Form verfasst.

Das bedeutet, dass:

- Unternehmen sich anfangs einer großen Rechtsunsicherheit bei der Auslegung der EU-DS GVO stellen werden müssen.
- eine unterschiedliche Auslegungspraxis in den Mitgliedstaaten durch den Europäischen Datenschutzausschuss und den EuGH noch zu nivellieren ist.

Dies ist jedoch kein Grund, die Umsetzung der DSGVO und des BDSG-neu zeitlich auszusetzen oder gar ganz oder teilweise zu verwerfen. Ebenso außer Frage steht der Sinn und Zweck beider Gesetze für die Menschen, deren Daten verarbeitet werden. Es bleibt daher in einigen Bereichen also weiterhin eine Interpretationssache, die für sein eigenes Unternehmen geeigneten Maßnahmen zu definieren, auszulegen und zu ergreifen.

In jedem Fall aber ist das Anfangen wichtig. Die Sensibilisierung mit dem Thema, die zeitnahe Abarbeitung, das Setzen eines Status Quo und das regelmäßige Aktualisieren im Thema sind wichtige Stationen. So leisten wir einen hohen und sinnvollen Beitrag, um die Menschen der gegenwärtigen und zukünftigen Generationen zu schützen, dessen personenbezogene Daten wir täglich verarbeiten oder zukünftig noch verarbeiten werden.

2.6 Gesetzlicher Rahmen – weitere Gesetze

Neben der DSGVO gibt es seit langem weitere gesetzliche Regelungen zum Datenschutz. Dazu gehören zum Beispiel:

- Auf Bundesebene das Bundesdatenschutzgesetz BDSG (BDSG-neu seit 25. Mai 2018) BDSG a. F. seit 1977 regelt den Datenschutz für die Bundesbehörden und den privaten Bereich (das heißt für alle Wirtschaftsunternehmen, Institutionen, Vereine etc. gegenüber natürlichen Personen).
- Datenschutzrechtliche Regelungen in weiteren Gesetzen, wie dem Telekommunikationsgesetz (TKG), Telemediengesetz (TMG), Fluggastdatengesetz (FlugDaG), Bürgerliches Gesetzbuch (BGB), Kunst Urheberrechtsgesetz (KUG), etc.
- Datenschutzgesetze der Länder regeln den Datenschutz in Landes- und Kommunalbehörden

– Nach der Rechtsprechung des Bundesverfassungsgerichts ein Grundrecht, dem Recht auf informationelle Selbstbestimmung. Wird im Grundgesetz zwar nicht explizit erwähnt, ist aber aufgenommen in die meisten Landesverfassungen.

2.7 Wie ist der Datenschutz praxisnah anwendbar?

Wie bereits erwähnt, gegenwärtig ist die Umsetzung immer noch auf Interpretationen und Auslegungen angewiesen. Das wird auch in der Zukunft so bleiben, auch wenn es dann mehr belastbare Aussagen, Auslegungen und Rechtsurteile geben wird. Es handelt sich eben um Gesetze und nicht um eine Norm wie sie zum Beispiel in der DIN zu finden wäre.

Doch ist dies nicht der Zweck eines Gesetzes. Vielmehr ist genau dieser Spielraum, den Gesetze geben müssen, erforderlich, um sie überhaupt flächendeckend in der Praxis umsetzbar machen zu können. Fluch und Segen zugleich? Möglicherweise. Denn glaubt man alles richtig interpretiert und dann entsprechend umgesetzt zu haben, könnte es dann doch noch sein, dass es Andere anders sehen. Im ungünstigsten Fall landet es dann vor einem Richter, der ebenfalls eine Sicht auf die Dinge hat. Wie kann man es also dann überhaupt „richtig" machen?

Eine Lösung liegt darin, dass es einen, auch für andere Personen dokumentierten und nachvollziehbaren Weg gibt, der durch den gesamten Verlauf vom Beginn bis zur Umsetzung geführt hat. Es beginnt dabei unter anderem mit der Thematisierung und der Priorisierung des Datenschutzes selbst. Dann mit der aktiven Auseinandersetzung, was an personenbezogenen Daten im Unternehmen oder im Auftrag durch Dritte verarbeitet wird und einer darauf aufgesetzten Risikoabschätzung hinsichtlich möglicher Schäden für die Betroffenen im Falle von zum Beispiel Datenpannen.

Daran anschließend folgt das Aufsetzen geeigneter Maßnahmen und Prozesse, um allen identifizierten Anforderungen mit einem machbaren, technischen (Stand der Technik) und personellen sowie organisatorischem Aufwand gerecht zu werden. Am Ende zählt immer mehr, wenn etwas zum digitalen Schutz natürlicher Personen getan wurde, als sich dem Thema nicht angemessen zugewendet oder gar abgewendet zu haben.

Eine praxisnahe Anwendung des Datenschutzes ist daher nach unserer Erfahrung immer möglich. Jede Maßnahme, die dem Schutz der Personen, also den sogenannten Betroffenen dient, ist besser als nichts. Und es bedarf auch nicht unbedingt eines großen Aufwandes, einen Grundschutz zu etablieren, denn bereits wenige technische oder organisatorische Maßnahmen können oft schon eine sichtbare Verbesserung gegenüber vorher darstellen.

2.8 Bedeutung des Datenschutzes für Kanzleien?

Steuerberater, Wirtschaftsprüfer und Rechtsanwälte sind Berufsgeheimnisträger und bereits vom Gesetz her zur Verschwiegenheit verpflichtet. Es könnte daher vielleicht hier die Meinung vertreten werden, dass damit der hier diskutierte Datenschutz für sie nur eine untergeordnete Rolle spielen könnte, da sie bereits schon höheren berufsrechtlichen Vorgaben unterworfen sind.

Bei der DSGVO ist deutlich, dass ihre Ausgestaltung von der Unternehmensrechtsform und dem Tätigkeitsprofil unabhängig ist. Jede gewerbliche Tätigkeit, welche auch personenbezogene Daten verarbeitet, führt somit automatisch zur Anwendbarkeit der DSGVO. So ist die DSGVO auch in den Kanzleien wirksam, und zwar unabhängig von der Rechtsform, der Kanzleigröße oder der Art der Mandanten.

Und ganz wichtig ist dabei, dass das Thema Datenschutz unbedingt zur „Chefsache" erklärt wird. Zum einen deshalb, da die DSGVO ein Gesetz ist, welches mit hohen Geldbußen bei Verstößen verbunden ist. Diese Tatsache unberücksichtigt lassen birgt damit ein nicht zu unterschätzendes und unkalkulierbares finanzielles Risiko für den Unternehmer. Zum anderen, weil eine konsequente, zeitnahe und lückenlose Umsetzung des Themas nur möglich wird, wenn dies auch von der Kanzleileitung angestoßen, unterstützt und (vor-)gelebt wird.