Inhaltsverzeichnis

Vorwort V

Inhaltsverzeichnis VII

Einleitung 1

§ 1. Anwendbarkeit des revDSG und der DSGVO 3
I. Welches Recht ist auf mein Unternehmen anwendbar? 3
II. Was ist der aktuelle Stand der Gesetzesrevision in der Schweiz? 3
III. Inwiefern ist mein Unternehmen von der Gesetzesrevision in der Schweiz betroffen? 4
1. Persönlicher Anwendungsbereich des revDSG 4
2. Sachlicher Anwendungsbereich des revDSG 5
a) Was sind Personendaten bzw. personenbezogene Daten? 5
b) Was ist das Bearbeiten bzw. Verarbeiten von Personendaten? 7
3. Räumlicher Anwendungsbereich des revDSG 7
4. Wann muss mein Unternehmen das kantonale Datenschutzrecht oder die strengeren Anforderungen für Bundesorgane beachten? 8
5. Was bedeutet eine Aufgabenauslagerung für «mein Unternehmen»? 9
IV. Ist meine Unternehmung von der Datenschutz-Grundverordnung der EU (DSGVO) betroffen? 9
1. Persönlicher und sachlicher Anwendungsbereich der DSGVO 10
2. Räumlicher Anwendungsbereich der DSGVO 10
a) Mein Unternehmen befindet sich in der Grenzregion zu einem EU-Land. Unter den Angestellten befinden sich deshalb Personen aus der EU (Grenzgängerinnen). Muss ich für diese Personen die DSGVO beachten? 14
b) Ist meine Unternehmung von der Datenschutz-Grundverordnung der EU (DSGVO) auch dann betroffen, wenn ich nur als Auftragsverarbeiterin Daten verarbeite? 14
3. Weitere Fallbeispiele 15

§ 2. Grundsätze der Datenverarbeitung für mein Unternehmen 17
I. Wie wird der Schutz personenbezogener Daten sichergestellt? 17
1. Allgemeine Grundsätze der Datenverarbeitung 17
2. Rechtmässigkeit der Datenverarbeitung 19
3. Transparenz 20
4. Rechte der Betroffenen 21
5. Datenschutzkonforme Organisation 22
6. Kontrolle 23
7. Sanktionen 24
8. Öffnung 24
II. Welche konkreten Grundsätze müssen bei der Datenverarbeitung beachtet werden? 24
1. Grundsätze nach DSGVO und revDSG 25
2. Rechtmässigkeit, Verarbeitung nach Treu und Glauben und Transparenz 26
3. Zweckbindung 26

4. Datenminimierung ... 27
5. Richtigkeit ... 28
6. Speicherbegrenzung ... 28
7. Integrität und Vertraulichkeit ... 29
8. Rechenschaftspflicht ... 30

§ 3. Zulässigkeit der Datenverarbeitung ... 31
I. Zulässigkeit der Datenverarbeitung unter dem revDSG? ... 31
II. In welchen Fällen dürfen personenbezogene Daten verarbeitet werden? ... 32
1. Wann ist die Datenverarbeitung durch eine Einwilligung gedeckt? ... 35
a) Worauf muss bei vorformulierten Einwilligungserklärungen geachtet werden? ... 37
b) In welcher Form muss die Einwilligung erfolgen? ... 38
c) Bleiben bisherige Einwilligungen unter dem alten Datenschutzgesetz gültig? ... 38
d) Kann die Einwilligung durch die Betroffene widerrufen werden? ... 39
2. Wann ist die Datenverarbeitung zur Erfüllung eines Vertrages oder Durchführung vorvertraglicher Massnahmen erlaubt? ... 40
a) Erfüllung eines Vertrags ... 40
b) Vorvertragliche Massnahmen ... 41
3. Wann ist die Datenverarbeitung zur Erfüllung rechtlicher Verpflichtungen erlaubt? ... 41
4. Wann ist die Datenverarbeitung zum Schutze von lebenswichtigen Interessen der betroffenen Person oder einer anderen Person erlaubt? ... 42
5. Wann ist die Datenverarbeitung aufgrund eines öffentlichen Interesses oder zur Ausübung öffentlicher Gewalt erlaubt? ... 42
6. Wann kann sich die Verantwortliche für die Datenverarbeitung auf ihre berechtigten Interessen berufen, die eine Datenverarbeitung erlauben? ... 42
a) Die berechtigten Interessen ... 43
b) Interessenabwägung ... 45
III. Dürfen Daten auch zu einem anderen Zweck verarbeitet werden, als denjenigen, für den sie erhoben wurden? ... 46
IV. Was ist bei der Bearbeitung von besonderen Kategorien personenbezogener Daten zu beachten? ... 48
V. Was ist bei der Verarbeitung von Daten über Straftaten zu beachten? ... 49
VI. Ist die Datenverarbeitung zur automatisierten Entscheidfindung und zum Profiling zulässig? ... 51
a) Wie verhält es sich unter dem revDSG? ... 51
b) Wie verhält es sich unter der DSGVO? ... 53
VII. Beispiele und Fragen aus der Praxis ... 55
1. Was muss bei der Verwendung von Cookies beachtet werden? ... 55
2. Was gilt es beim Versand von Newslettern zu beachten? ... 58
3. Worauf muss bei der Verwendung von Tracking-Tools geachtet werden? ... 61
a) Google Analytics ... 61
b) Andere Tracking-Dienste ... 62

4. Können Social-Media-Plugins datenschutzkonform verwendet werden? ... 63

§ 4. Auftragsdatenverarbeitung ... 66
I. Was wird unter der Auftragsdatenverarbeitung verstanden? ... 66
1. Hohe praktische Relevanz der Auftragsdatenverarbeitung ... 66
2. Sinn und Zweck der Auftragsdatenverarbeitung ... 67
II. Bin ich Verantwortlicher oder Auftragsverarbeiter? ... 68
III. Ich bin Auftragsverarbeiter. Welche Folgen hat das für mich? ... 70
1. Abschluss eines Datenverarbeitungsvertrages ... 70
2. Weisungsgebundenheit des Auftragsverarbeiters und Dokumentationspflicht ... 71
3. Ergreifen von technischen und organisatorischen Massnahmen ... 72
4. Protokollierung und Bearbeitungsreglement ... 72
5. Führung eines Verzeichnisses über die Verarbeitungstätigkeit ... 73
6. Transparenz beim Beizug von Sub-Auftragsverarbeitern ... 74
7. Verpflichtung zur Vertreterbestellung (DSGVO) ... 75

§ 5. Datenexport ins Ausland ... 76
I. Warum ist das Thema «Datenexport ins Ausland» für meine Unternehmung relevant? ... 76
II. Wann ist die Übermittlung von Daten ins Ausland gestattet? ... 77
III. Wann liegt eine qualifizierte Einwilligung vor? ... 79
IV. Was ist ein «Angemessenheitsbeschluss»? ... 79
1. Was ist unter «anderen geeigneten Garantien» zu verstehen? ... 80
2. Ist die Bekanntgabe von Daten in die USA probemlos? ... 81
a) Ausgangslage ... 81
b) Welche rechltichen Folgen hat die Ungültigkeitserklärung des Privacy Shields? ... 81
c) Was beinhalten die Standardvertragsklauseln? ... 82
d) Was ist das Transfer Impact Assessment? ... 83
e) Wer muss das Transfer Impact Assessment erstellen? ... 83
V. Was sind die Sanktionen bei der Missachtung der Datenexportbestimmungen? ... 84

§ 6. Informationspflicht des Verantwortlichen ... 86
I. Welche Informationspflichten bestehen für den Verantwortlichen? ... 86
1. Hohe praktische Relevanz der Informationspflichten ... 86
2. Sinn und Zweck der Informationspflicht ... 87
3. Die verschiedenen Informationspflichten ... 87
II. Welches sind die einzelnen Informationspflichten, wenn die Daten beim Betroffenen erhoben werden? ... 89
1. Form der Mitteilung ... 90
2. Zeitpunkt der Mitteilung ... 91
3. Inhalt der Informationspflichten ... 91
4. Ausnahme von der Informationspflicht ... 96
III. Welche Informationspflichten bestehen, wenn die Daten nicht beim Betroffenen erhoben werden (Dritterhebung)? ... 97
1. Zeitpunkt der Mitteilung an den Betroffenen ... 97
2. Inhalt der Informationspflichten ... 98

3. Ausnahmen von der Informationspflicht 99
IV. Welche Melde- und Benachrichtigungspflichten bestehen im Zusammenhang mit einer Datenverarbeitung zur Wahrnehmung eines öffentlichen Interesses, zur Wahrung der berechtigten Interessen des Verantwortlichen sowie der Direktwerbung? 101
V. Welche Melde- und Benachrichtigungspflichten bestehen bei einer Datenschutzverletzung? 101
1. Meldung an die Aufsichtsbehörde 102
2. Benachrichtigung der betroffenen Person 103

§ 7. Rechte der Betroffenen 106
I. Welche Rechte haben die Betroffenen nach der DSGVO und dem revDSG? 106
II. Wie sieht das Auskunftsrecht der Betroffenen aus? 107
1. Zuverlässige Identifikation der auskunftsersuchenden Person 108
2. Form des Antrags 108
3. Zu liefernde Informationen 108
4. Form der Auskunft 109
5. Frist der Auskunft 109
6. Kosten der Auskunft 110
7. Ausnahmen der Auskunftserteilung 110
III. Wann besteht das Recht auf Berichtigung? 112
IV. Wann besteht ein Recht auf Löschung? 113
1. Voraussetzungen der Löschung 114
2. Ausnahmen der Löschung 114
3. Technische Massnahmen und Information Dritter 115
V. Was beinhaltet das Recht auf Einschränkung der Verarbeitung (DSGVO)? 117
VI. Was beinhaltet das Recht auf Unterlassung künftiger Datenbearbeitungen oder Bekanntgabe an Dritte (revDSG)? 117
VII. Was beinhalten die Rechte auf Datenübertragbarkeit und -herausgabe und wann können sie angerufen werden? 118
VIII. Was beinhaltet das Widerspruchsrecht und wann kann es angerufen werden? 120
1. Widerspruch gegen Datenverarbeitung in Wahrnehmung einer öffentlichen Aufgabe oder der berechtigten Interessen der Verantwortlichen 123
2. Widerspruch bei Direktwerbung 124
3. Widerspruchsrecht bei Verarbeitung zu Forschungszwecken oder zu statistischen Zwecken 124
4. Ausübung des Widerspruchsrechts 124
5. Hinweispflicht auf das Widerspruchsrecht 125

§ 8. Anforderungen an die Unternehmensstruktur 126
I. Zu schaffende Positionen und Verantwortungsbereiche 126
1. Allgemeines 126
2. Datenschutzbeauftragter nach DSGVO 127
a) Was sind die Aufgaben des Datenschutzbeauftragten? 129
b) Wer kann Datenschutzbeauftragter sein? 129

3. Datenschutzberater nach revDSG ... 131
4. Weitere Positionen und Verantwortungsbereiche ... 131
II. Zu definierende Prozesse ... 132
1. Verzeichnis der Verarbeitungstätigkeiten ... 132
2. Datenschutzfolgeabschätzung ... 133
III. Umsetzung in kleineren und grösseren Unternehmen ... 135
IV. Sicherheitsanforderungen für die Datenverarbeitung ... 135
1. Die Regelungen zur Datensicherheit ... 136
2. Die Schutzziele ... 137
a) Technische und organisatorische Massnahmen ... 137
b) Bedeutung der Schutzziele ... 139
c) Vertraulichkeit ... 139
d) Verfügbarkeit und Integrität ... 140
e) Nachvollziehbarkeit (nur DSV) ... 142
3. Protokollierung und Bearbeitungsreglement (nur DSV) ... 142
a) Welche Unternehmen sind zur Protokollierung und zum Bearbeitungsreglement verpflichtet? ... 143
b) Was beinhaltet die Protokollierungspflicht? ... 144
c) Was beinhaltet die Pflicht zur Führung eines Bearbeitungsreglements? ... 145
4. Allgemeine Massnahmen ... 145
a) Risiken bestimmen und ihnen begegnen ... 145
b) Sensibilisierung und Schulung ... 146
c) Regelmässige Updates ... 146
d) Berechtigungsmanagement ... 147
e) Starke Passwörter und Passworthygiene ... 147
f) Backups ... 148
g) Verschlüsselung ... 148
h) E-Mail-Kommunikation richtig verwenden ... 149
i) Physischen Zugang erschweren ... 149

§ 9. Rechtsdurchsetzung und Sanktionen ... 151
I. Rechtsdurchsetzung unter dem revDSG ... 151
1. Das öffentlichrechtliche Verfahren ... 151
2. Untersuchung ... 152
a) Verwaltungsmassnahmen ... 152
b) Beschwerde ... 153
3. Das strafrechtliche Verfahren ... 153
a) Bussen der Schweizerischen Behörden ... 154
b) Welche Handlungen sind nach dem revDSG strafbar? ... 155
aa) Informations-, Auskunfts-, und Mitwirkungspflichten ... 155
bb) Sorgfaltspflichten ... 155
cc) Berufliche Schweigepflicht ... 156
dd) Missachtung von Verfügungen ... 157
ee) Verjährung ... 157
c) Wie wird die Bussenhöhe berechnet? ... 157
d) Welche Rolle spielt der EDÖB im Strafverfahren? ... 158
4. Das zivilrechtliche Verfahren ... 158

II. Rechtsdurchsetzung unter der DSGVO ... 158
1. Befugnisse der Aufsichtsbehörden ... 159
2. Bussen von Aufsichtsbehörden von Mitgliedstaaten der EU, Norwegen, Island und Liechtenstein ... 159
3. Welche Faktoren werden bei der Berechnung der Busse durch die Aufsichtsbehörden berücksichtigt? ... 160
4. Was kann gegen Beschlüsse der Aufsichtsbehörden getan werden? ... 161
III. Welche Aufsichtsbehörde ist zuständig? ... 161
1. Wie regelt die DSGVO die internationale Zuständigkeit? ... 161
2. Wie regelt das revDSG die innerschweizerischen Zuständigkeiten? ... 162
3. Was passiert, wenn ein Zuständigkeitskonflikt zwischen dem EDÖB und einer EU-Aufsichtsbehörde vorliegt? ... 162
4. Praxisbeispiele ... 163
IV. Wie kann Beschwerde bzw. Anzeige bei der Aufsichtsbehörde erhoben werden und was sind die Folgen? ... 164
1. Anzeige nach revDSG ... 164
2. Beschwerde nach DSGVO ... 164
V. Inwiefern können Bussen von Aufsichtsbehörden der DSGVO gegen Schweizer Unternehmen durchgesetzt werden? ... 165

§ 10. Checklisten DSGVO/revDSG-Konformität ... 166
I. Vorfrage ... 166
II. Checkliste DSGVO ... 166
III. Checkliste revDSG ... 168

§ 11. Gesetzgebung / Ausblick ... 171
I. Weshalb wurde das Schweizerische Datenschutzgesetz (DSG) revidiert? ... 171
1. Wann wird das neue Schweizerische Datenschutzgesetz in Kraft treten? ... 171
2. Welche Änderungen wird das neue Schweizerische Datenschutzgesetz bringen? ... 171
II. Ausblick ... 172
1. EU ... 172
2. Schweiz ... 173

Wichtigste Links ... 174
I. Datenschutz.law ... 174
II. Grundsätze Datenschutz ... 175
III. Datenexporte ... 175
IV. Auskunftsanspruch ... 175
V. Datensicherheit ... 176
VI. Behörden ... 176

Die wichtigsten Begriffe ... 177