Christian Solmecke, Sibel Kocatepe

DSGVO für Website-Betreiber

Ihr Leitfaden für die sichere Umsetzung
der EU-Datenschutz-Grundverordnung

Rheinwerk
Computing

Auf einen Blick

1	Einführung	13
2	Neuordnung durch Grundordnung: Das neue europäische Datenschutzrecht	27
3	Praxischeck I: Website und Online-Shop DSGVO-konform gestalten	109
4	Praxischeck II: Die 30 am häufigsten gestellten Fragen (FAQ)	161
5	Mustertexte	175
6	Fazit und Ausblick	241

Inhalt

Geleitwort 11

1 Einführung 13

1.1 An wen richtet sich dieses Buch? 14

1.2 Was ist die europäische Datenschutz-Grundverordnung? 16

1.3 Was bringt die europäische Datenschutz-Grundverordnung? 18

1.4 Ist eine Anpassung an die neue Rechtslage zwingend? 19

1.5 Welche Maßnahmen müssen unbedingt eingeleitet werden? 22

1.6 Warum ist rechtliche Hilfe unverzichtbar? 24

1.7 Wie kann man sich immer auf dem neusten Stand halten? 24

1.8 Dankeschön! 25

2 Neuordnung durch Grundordnung: Das neue europäische Datenschutzrecht 27

2.1 Überblick: Wesentliche Änderungen durch die DSCVO 28

2.1.1 Datenschutz als europäisches Grundrecht der Bürger 29

2.1.2 Marktortprinzip-vereinheitlichtes Regelwerk für Unternehmen 30

2.1.3 Rechenschaftspflicht 31

2.1.4 Reformierung des Beschwerdesystems 32

2.1.5 Umsetzungsanreiz aufgrund hoher Geldbußenrahmen 33

2.2 Datenschutzprinzipien 34

2.2.1 Grundsatz der Rechtmäßigkeit und der Transparenz/ Verarbeitung nach Treu und Glauben 34

2.2.2 Grundsatz der Zweckbindung 35

2.2.3 Grundsatz der Datenminimierung 35

2.2.4 Grundsatz der Datenrichtigkeit 36

2.2.5 Grundsatz der Speicherbegrenzung 36

	2.2.6	Grundsatz der Integrität und Vertraulichkeit	37
	2.2.7	Rechenschaftspflicht	37
2.3	**Grundsätze der Verarbeitung personenbezogener Daten**		38
	2.3.1	Was sind personenbezogene Daten?	39
	2.3.2	Wann erfolgt die Datenverarbeitung auf Grundlage gesetzlicher Erlaubnisnormen?	40
	2.3.3	Wie erfolgt die Datenverarbeitung auf Grundlage einer Einwilligung des Betroffenen?	43
2.4	**Technischer und organisatorischer Datenschutz: Privacy by Design und Privacy by Default**		49
2.5	**Datenschutz-Folgenabschätzung**		52
	2.5.1	In welchen Fällen ist eine Datenschutz-Folgenabschätzung durchzuführen?	52
	2.5.2	Wie ist das Verfahren durchzuführen und was beinhaltet es?	54
2.6	**Auftragsverarbeitung**		55
	2.6.1	Was ist Auftragsverarbeitung?	55
	2.6.2	Wo spielt Auftragsverarbeitung eine Rolle?	56
	2.6.3	Worin besteht die rechtliche Problematik?	56
	2.6.4	Welche Regelungen gelten bei der Auftragsverarbeitung?	57
	2.6.5	Welche Konsequenzen hat ein Verstoß des Auftragsverarbeiters?	58
2.7	**Datentransfer in Drittstaaten**		59
	2.7.1	Unter welchen Bedingungen ist ein Datentransfer in Drittstaaten zulässig?	60
	2.7.2	In welche Drittstaaten ist ein Datentransfer zulässig?	61
	2.7.3	Ist ein Datentransfer in unsichere Drittstaaten auch ohne Kommissionsbeschluss zulässig?	62
	2.7.4	Kann ein Datentransfer in Drittstaaten auch ohne Angemessenheitsbeschluss und ohne Garantien erfolgen?	63
2.8	**Erstellung eines Verarbeitungsverzeichnisses**		63
	2.8.1	Wer muss ein Verarbeitungsverzeichnis erstellen?	64
	2.8.2	Was muss das Verarbeitungsverzeichnis beinhalten?	65
	2.8.3	Wie ist ein Verarbeitungsverzeichnis zu erstellen?	67
2.9	**Melde- und Informationspflichten bei Datenpannen**		70
	2.9.1	Was müssen Sie im Falle einer Datenpanne veranlassen?	70
	2.9.2	Welchen Inhalt muss die Meldung haben?	71

2.10 Rechte der Betroffenen 72
2.10.1 Recht auf Auskunft 73
2.10.2 Recht auf Datenübertragbarkeit 73
2.10.3 Recht auf Vergessenwerden und Recht auf Berichtigung 73
2.10.4 Recht auf Widerspruch gegen die Datenverarbeitung 74
2.10.5 Recht auf Widerspruch bei automatisierten Einzelfallentscheidungen 75

2.11 Arbeitnehmerdatenschutz 77
2.11.1 Was genau ist Arbeitnehmerdatenschutz? 77
2.11.2 Wo ist der Arbeitnehmerdatenschutz geregelt? 77
2.11.3 Was sagt die Datenschutz-Grundverordnung zum Arbeitnehmer-datenschutz? 78
2.11.4 Wann dürfen Daten nach dem neuen Bundesdatenschutzgesetz verarbeitet werden? 78
2.11.5 Was ist bei der Einholung einer Einwilligung zu beachten? 80
2.11.6 Welche Rolle spielt der Betriebsrat im Arbeitnehmerdatenschutz? 80
2.11.7 Welche Rolle spielen die Aufsichtsbehörden und welche Rechte haben sie? 81

2.12 Datenschutzbeauftragter 81
2.12.1 Welche Bedeutung hat der Datenschutzbeauftragte? 81
2.12.2 Welche gesetzlichen Normierungen regeln die Modalitäten rund um die Bestellung des Datenschutzbeauftragten? 82
2.12.3 Wer muss einen Datenschutzbeauftragten bestellen? 82
2.12.4 Wie wird der Datenschutzbeauftragte bestellt? 84
2.12.5 Welche Aufgaben hat der Datenschutzbeauftragte? 84
2.12.6 Welche Anforderungen werden an den Datenschutzbeauftragten gestellt? 85
2.12.7 Welche Person kommt als Datenschutzbeauftragter in Betracht? 86
2.12.8 Welche rechtlichen Besonderheiten bestehen bei der Bestellung eines externen Datenschutzbeauftragten? 86

2.13 Datenschutzerklärung **88**
2.13.1 Wann ist eine Datenschutzerklärung erforderlich? 89
2.13.2 Wie ist eine Datenschutzerklärung aufzubauen? 90
2.13.3 Welchen Inhalt muss eine Datenschutzerklärung haben? 91
2.13.4 Wie muss die Datenschutzerklärung übermittelt werden? 99
2.13.5 Wo muss die Datenschutzerklärung platziert werden? 101

2.14 Datenschutzaudit 102
2.14.1 Was ist ein Datenschutzaudit? 103

2.14.2 Warum ist ein Datenschutzaudit sinnvoll? 104
2.14.3 Wann sollten Sie ein Datenschutzaudit in die Wege leiten? 105
2.14.4 Wer kann ein Datenschutzaudit durchführen? 105
2.14.5 Wie wird ein Zertifizierungsverfahren ablaufen? 106
2.14.6 Was passiert nach dem Datenschutzaudit? 107

3 Praxischeck I: Website und Online-Shop DSGVO-konform gestalten 109

3.1 Webanalyse: IP-Adressen, Verträge und Widerspruch 110
3.1.1 Wann ist der Einsatz von Webanalyse-Tools zulässig? 111
3.1.2 Der rechtskonforme Umgang mit IP-Adressen 112
3.1.3 Der Vertrag mit Google Analytics und Co 116
3.1.4 Widerspruch gegen die Webanalyse 119

3.2 Newsletter-Versand: Double Opt-In und Abbestell-Link 122
3.2.1 Die Einwilligung einholen: Double Opt-In 122
3.2.2 Der rechtskonforme Widerruf: Die Abbestellmöglichkeit 126
3.2.3 Der Einsatz von Newsletter-Dienstleistern aus Drittstaaten 130

3.3 Online-Targeting, Retargeting und Remarketing: Der Einsatz von Cookies 135
3.3.1 Was sind Cookies? 136
3.3.2 Der Einsatz von Cookies nach der Datenschutz-Grundverordnung 137
3.3.3 Der Einfluss der e-Privacy-Verordnung auf das Setzen von Cookies 141

3.4 Verwendung von Social-Media-Elementen 144
3.4.1 Was ist beim Einsatz von Social Plug-ins zu beachten? 144
3.4.2 Wie sieht es mit »Facebook Custom Audiences« für Websites aus? 149
3.4.3 Ist der Einsatz von »Facebook Custom Audiences« im Listenverfahren zulässig? 156

4 Praxischeck II: Die 30 am häufigsten gestellten Fragen (FAQ) i6i

4.1 Für wen gilt die Datenschutz-Grundverordnung? 161

4.2 Welche Daten dürfen nicht erfasst werden? 162

4.3	Gilt die Datenschutz-Grundverordnung auch für Alt-Daten?	163
4.4	Was passiert bei Verstößen gegen die Datenschutz-Grundverordnung?	163
4.5	Was ist die e-Privacy-Verordnung?	163
4.6	In welchem Verhältnis steht die Datenschutz-Grundverordnung zur e-Privacy-Verordnung?	164
4.7	Wie können Daten im Unternehmen geschützt werden?	164
4.8	Benötigen Unternehmen immer ein Sicherheitskonzept?	165
4.9	Was wird aus den bisherigen Datenschutzzertifikaten?	165
4.10	Muss jede Datenschutzerklärung angepasst werden?	165
4.11	Ist der Einsatz eines Datenschutz-Generators sinnvoll?	166
4.12	Woher weiß ich, welche Plug-ins ich in meine Datenschutzerklärung aufnehmen muss?	166
4.13	Wer benötigt einen Datenschutzbeauftragten?	166
4.14	Welche Mitarbeiter sind bei der Berechnung der Zehn-Personen-Grenze für einen Datenschutzbeauftragten einzubeziehen?	167
4.15	Wer kann Datenschutzbeauftragter werden?	167
4.16	Muss der Datenschutzbeauftragte schriftlich bestellt werden?	167
4.17	Was passiert mit vor der Datenschutzreform bestellten Datenschutz-beauftragten?	168
4.18	Was ist bei der Einholung einer Einwilligung nach neuem Recht zu beachten?	168
4.19	Was ist mit Einwilligungen, die vor Inkrafttreten der Datenschutz-Grundverordnung erteilt wurden?	168
4.20	Müssen Einwilligungen protokolliert werden und wie kann dies elektronisch erfolgen?	169
4.21	Können alte Kontaktformulare weiter genutzt werden?	169
4.22	Was ist beim Einsatz einer ausländischen Cloud zu beachten?	169
4.23	Was ist das Privacy-Shield-Abkommen?	170
4.24	Was ist Big Data?	170
4.25	Muss man Abmahnungen fürchten?	171
4.26	Sollte man überhaupt auf eine Abmahnung reagieren?	171

4.27 Was passiert, wenn man keine Unterlassungserklärung abgibt? 171

4.28 Sollte man die Unterlassungserklärung der Gegenseite unterschreiben? 172

4.29 Wie kann man auf eine einstweilige Verfügung reagieren? 173

4.30 Was ist zu tun, wenn man eine Klageschrift erhält? 173

5 Mustertexte 175

5.1 Muster für Datenschutzerklärungen 175

5.1.1 Checkliste zur Datenschutzerklärung für Website und Online-Shop 177

5.1.2 Datenschutzerklärung für die Website 179

5.1.3 Datenschutzerklärung für den Online-Shop 196

5.1.4 Datenschutzerklärung für Beschäftigte 200

5.2 Muster für Einwilligungserklärungen 213

5.2.1 Einwilligung in den Erhalt eines Newsletters 213

5.2.2 Einwilligung zu Bonitätsprüfungen 214

5.3 Muster eines Verarbeitungsverzeichnisses für Verantwortliche 214

5.4 Muster eines Vertrags zur Auftragsverarbeitung 224

5.5 Aufbau eines Datenschutzkonzepts 231

5.6 Leitfaden zur Erstellung eines Datensicherheitskonzepts 236

6 Fazit und Ausblick 241

Index 245