

## Datenschutz im Unternehmen

Bearbeitet von  
Von Dr. Michael Wächter

5. Auflage 2017. Buch. XX, 483 S. Kartoniert  
ISBN 978 3 406 71525 9  
Format (B x L): 14,1 x 22,4 cm

[Recht > Handelsrecht, Wirtschaftsrecht > Telekommunikationsrecht, Postrecht, IT-Recht > Datenschutz, Postrecht](#)

Zu [Leseprobe](#) und [Sachverzeichnis](#)

schnell und portofrei erhältlich bei



Die Online-Fachbuchhandlung beck-shop.de ist spezialisiert auf Fachbücher, insbesondere Recht, Steuern und Wirtschaft. Im Sortiment finden Sie alle Medien (Bücher, Zeitschriften, CDs, eBooks, etc.) aller Verlage. Ergänzt wird das Programm durch Services wie Neuerscheinungsdienst oder Zusammenstellungen von Büchern zu Sonderpreisen. Der Shop führt mehr als 8 Millionen Produkte.

Aktuelles Recht  
für die Praxis

**beck-shop.de**  
DIE FACHBUCHHANDLUNG

**beck-shop.de**  
DIE FACHBUCHHANDLUNG

# Datenschutz im Unternehmen

von

**Dr. Michael Wächter**

5., neu bearbeitete Auflage

**beck-shop.de**  
DIE FACHBUCHHANDLUNG





The logo for beck-shop.de features the word "beck" in a bold, black, sans-serif font, followed by "shop" in a larger, bold, black, sans-serif font. A small ".de" is positioned at the end of "shop". Above the letter "i" in "shop", there are three light blue dots of increasing size from left to right, suggesting motion or a stylized "i". Below the main text, the words "DIE FACHBUCHHANDLUNG" are written in a smaller, black, sans-serif font.

**beck-shop.de**  
DIE FACHBUCHHANDLUNG

**www.beck.de**

ISBN 9783406715259

© 2017 Verlag C.H. Beck oHG  
Wilhelmstraße 9, 80801 München  
Druck: Druckhaus Nomos  
In den Lissen 12, 76547 Sinzheim

Satz: jürgen ullrich typosatz, Nördlingen  
Umschlaggestaltung: Druckerei C.H. Beck Nördlingen

Gedruckt auf säurefreiem, alterungsbeständigem Papier  
(hergestellt aus chlorfrei gebleichtem Zellstoff)

## Vorwort

Mit Inkrafttreten der DSGVO in 2016 wurde es erforderlich, das Werk grundlegend zu überarbeiten. Es musste neu ausgerichtet werden. Dabei kommt die neue Konzeption der DSGVO dem Werk entgegen. Denn die *Prinzipienorientierung der DSGVO* als Basis einer zukunftsorientierten Ausdifferenzierung des Datenschutzrechts zielt auf eine technisch-organisatorische Umsetzung von Datenschutz ab. Mit der Ausrichtung der DSGVO, Datenschutz durch Technik zu gestalten, wurde dieser Ansatz vertieft. Dies entspricht der Zielsetzung des Werks von Anfang an. Dies beginnend mit Müller 1981 und Müller/Wächter 1991 unter dem Buchtitel *Der Datenschutzbeauftragte*. Dann von Wächter 2003 und 2014 unter dem Titel *Datenschutz im Unternehmen*. Unter dem Gesichtspunkt des betrieblich-organisatorischen Datenschutzes wurde der Text der 4. Auflage durchgesehen und für die 5. Auflage auf Basis der neuen Rechtslage gründlich überarbeitet.

Das Konzept des Datenschutzrechts nach der DSGVO und anderen Vorschriften über den Datenschutz macht es für Unternehmen erforderlich, neue Lösungskonzepte für ihre Organisation zu entwickeln, um den *neuen rechtlichen Vorgaben* nachzukommen. Das bedeutet, dass Datenschutz wiederum neu und innovativ in die Arbeitsorganisation und die Geschäftsmodelle des jeweiligen Unternehmens einzupassen ist. Datenschutz muss neu gedacht werden. Dies betrifft im Besonderen auch neue Entwicklungen in der Automatisierung und Digitalisierung. *Industrie 4.0* und *Arbeiten 4.0* sind hierbei neue Technikleitbilder für Wirtschaft und Gesellschaft. Datenschutz steht an zentraler Stelle zwischen moderner Datenökonomie und individueller Datensouveränität. Im Arbeitnehmerdatenschutz kommt ergänzend hinzu, dass neue Formen der IT-Arbeit interessengerecht zu handhaben sind. Zu der Frage, wie solche Themen im Unternehmen zu implementieren sind und in welcher Weise Datenschutz und Datensicherheit sowie *Compliance* und *Integrität* zu gewährleisten sind, werden im Werk Vorschläge entwickelt.

Für den Datenschutz werden in der Zukunft sicherlich Vorschriften auf europäischer und nationaler Ebene geschaffen werden, die das Datenschutzrecht materiell-rechtlich fortentwickeln werden. Der europäische Datenschutz bewegt sich hierbei in einem *offenen Wettbewerb* von Interessen und Meinungen. Datenschutz muss insofern diesem pluralistischen Modell der unterschiedlichsten kurzfristigen Interessen zur Lösung anstehender wirtschaftlicher und gesellschaftlicher Problemstellungen gerecht werden. Dabei ist Datenschutz aber nach dem vorliegenden

Verständnis eines Schutzes von Grundrechten und Grundfreiheiten unter Berücksichtigung eines freien Datenverkehrs auch auf eine langfristige Wahrung von Freiheits- und Persönlichkeitsrechten von Betroffenen hin angelegt.

Die rechtspolitische Zielsetzung der DSGVO liegt im Aufbau eines *einheitlichen Datenschutzregimes* in Europa. Dies hat unmittelbare Implikationen für die Gewährleistung von Datenschutz in den Unternehmen. Denn dieser Schutz von personenbezogenen Daten muss sich nunmehr verstärkt an der gesamteuropäischen und auch internationalen Entwicklung dieses Rechtsgebiets orientieren. Wesentlich ist es hierbei, mit den neuen Begrifflichkeiten der DSGVO, aber auch den Begrifflichkeiten des IT-Marktes zu arbeiten, die für die rechtliche Bewertung und die Fassung von Sachverhalten hilfreich sind.

Das Sachverzeichnis im Werk wurde grundlegend überarbeitet, um die Zugangswege zu datenschutzrechtlichen Fragestellungen, die oftmals vielseitige rechtliche und tatsächliche Bezüge aufweisen, zu erleichtern. Dabei konzentriert sich das Werk auf Kernpunkte der neuen Rechtslage. Rechtliche Debatten auf Basis des BDSG wurden in der Neuauflage des Werkes nicht mehr weiter geführt. Denn für die Verantwortlichen in Unternehmen ist es wichtig, die sich ihnen stellenden Fragestellungen im Unternehmensdatenschutz auf der neuen Grundlage anzugehen und zu lösen. Insofern müssen Unternehmen die für sie *zutreffende Rechtslage* kennen. Deshalb wurde sehr zeitnah das Gesetz zur Anpassung des Datenschutzrechts an die DSGVO (DSAnpUG-EU) als *BDSG-neu* eingearbeitet. Dies ist auch rechtlich konsistent, weil die DSGVO und das BDSG-neu beide zeitgleich ab dem 25. Mai 2018 gelten.

Drei Schwerpunkte werden in dieser Auflage vertieft. Zunächst soll Datenschutz als *ganzheitliche Organisation* betrachtet werden. Dann soll der Ansatz *Datenschutz durch Technik* die Gewährleistung der Zulässigkeiten der personenbezogenen Datenverarbeitung unterstützen. Und schließlich soll Datenschutz als *risikoorientierter Ansatz* eine interessengerechte Vorgehensweise im Verhältnis von Unternehmen und Betroffenen unterstützen. Dies bedeutet, Datenverarbeitung im Rahmen von Zulässigkeiten weitgehend zuzulassen. Datenschutz ist aber immer dann konsequent umzusetzen, wenn IT nachteilige Folgen oder besondere Risiken für Rechte und Interessen von Betroffenen beinhaltet.

Sindelfingen, im Mai 2017

*Michael Wächter*

## Inhaltsverzeichnis

	Seite
Abkürzungsverzeichnis .....	XIII
Literaturverzeichnis .....	XIX
<b>A. Datenschutz im Unternehmen</b>	
<b>I. Datenschutz als Unternehmensaufgabe .....</b>	<b>1</b>
1. Schwerpunkte des Unternehmensdatenschutzes .....	1
1.1 Datenschutz als gesetzliche Anforderung .....	1
1.2 Nationale Anpassung europäischen Rechts .....	17
1.3 IT-Bezug und Globalität des Datenschutzes .....	22
1.4 Methodisches Vorgehen im Datenschutzrecht .....	31
1.5 Technologieentwicklung als Rechtskriterium .....	38
1.6 Geschäftliche Medien und Social Computing .....	43
1.7 Virtuelle Welten und 3D-Geschäftsprozesse .....	54
2. Management des Unternehmensdatenschutzes .....	57
2.1 Geschäftsdaten und Daten von Beschäftigten .....	57
2.2 Datenschutzorganisation und Management .....	63
2.3 Compliance und Revision im Datenschutz .....	67
2.4 Datenschutz-Integrität und Corporate Rules .....	73
<b>II. DSGVO als Regelungsvorgabe im Datenschutz .....</b>	<b>76</b>
1. Inhalte der DSGVO als Handlungsanweisung .....	76
2. Systemdatenschutz als Organisationsprinzip .....	81
3. Einwilligung, Anonymität und Pseudonymität .....	84
4. Bilder und Videos in Marketing und Vertrieb .....	88
5. Datenschutz bei Meinungs- und Pressefreiheit .....	90
<b>III. Datenschutz bei IT-Nutzung im Arbeitsverhältnis .....</b>	<b>92</b>
1. Aufgabenstellung des Arbeitnehmerdatenschutzes .....	92
1.1 Sachverhalte zum Arbeitnehmerdatenschutz .....	92
1.2 Chancengleichheit und Gleichbehandlung .....	96
1.3 Sozialgeheimnis und Sozialdatenschutz .....	97
2. Unternehmensprozesse und Persönlichkeitsschutz .....	99
2.1 Datenverarbeitung als Organisationsmittel .....	99
2.2 Datenverarbeitung als Hauptleistungspflicht .....	101
2.3 Datenverarbeitung für Beschäftigungszwecke .....	103
3. Maßnahmen der Arbeitnehmerüberwachung .....	106
3.1 Screening, Scoring, Profiling von Personen .....	106
3.2 Videoüberwachung und technische Ortung .....	109
3.3 Systemvorgaben für Personalentscheidungen .....	111
<b>IV. Datenschutz bei Nutzung von Telemedien .....</b>	<b>111</b>
1. Persönlichkeitsschutz bei Telemedien .....	111
2. Fernmeldegeheimnis und Kontrollen .....	113
3. Sonderfall Arbeitnehmerdatenschutz .....	114

<b>V. Electronic Commerce und Social Business .....</b>	115
1. E-Commerce und Privacy Protection .....	115
2. Fairness und Datenschutzerklärungen .....	117
 <b>B. Datenschutzkontrolle</b>	
<b>I. Selbst-, Eigen- und Fremdkontrolle .....</b>	119
1. Unternehmensverantwortung im Datenschutz .....	119
1.1 DSGVO und Rechtsgüter für Betroffene .....	119
1.2 Verfassungsrechtliche Basis der Kontrolle .....	126
1.3 Metabetrachtung der Datenschutz-Compliance .....	127
1.4 Qualitätsmanagement und Datenschutzaudit .....	128
1.5 Kybernetisches Modell der Rechtsfindung .....	131
2. Zulässigkeiten der Informationsverarbeitung .....	134
2.1 Geltungsumfang der DSGVO .....	134
2.2 Zulässigkeitsrahmen der DSGVO .....	137
2.2.1 Steuerung durch Datenschutzkontrolle .....	141
2.2.2 Steuerung durch Einwilligungserklärung .....	142
2.2.3 Mitbestimmung durch Kollektivrecht .....	144
3. Selbstkontrolle der Betroffenen .....	145
3.1 Handlungsautonomie des Betroffenen .....	145
3.2 Auskunft einschließlich Datenkorrektur .....	147
3.3 Ambivalenz der Rechte-Wahrnehmung .....	149
4. Eigenkontrolle der verantwortlichen Stelle .....	153
4.1 Selbstverständnis und Aufgabe des DSB .....	153
4.2 Implementierung der IT-Compliance .....	155
5. Fremdkontrolle durch Aufsichtsbehörden .....	155
5.1 Unabhängige externe Datenschutzkontrolle .....	155
5.2 Zentrale Aufgaben der Aufsichtsbehörden .....	156
5.3 Zentrale Befugnisse der Aufsichtsbehörden .....	157
<b>II. Verzeichnis der Verarbeitungstätigkeiten .....</b>	158
1. Aufzeichnung der Verarbeitungsvorgänge .....	158
2. Erfassung und Pflege des Verzeichnisses .....	163
2.1 Erfassung der automatisierten Verfahren .....	163
2.2 Beteiligung der Geschäftsbereiche .....	165
2.3 Mobile und verteilte Datenverarbeitung .....	167
3. Persönliche berufliche Verarbeitung .....	169
<b>III. Datengeheimnis und Vertraulichkeit .....</b>	171
1. Wahrung des Datengeheimnisses .....	171
2. Datengeheimnis und Geheimnisschutz .....	172
3. Verpflichtung auf das Datengeheimnis .....	175
3.1 Abgrenzung der Verpflichtungen .....	175
3.2 Sonderfall Verpflichtung nach AGG .....	176
4. Austausch vertraulicher Informationen .....	177
<b>IV. Datenschutz und die Rolle der Mitbestimmung .....</b>	178
1. Betriebsratsarbeit und Datenschutz .....	178
2. Arbeitsrechtliches Koordinatensystem .....	182
3. Datenschutzbeauftragter und BetrVG .....	183
4. Tools und Datenschutzdokumentation .....	184
5. Digitale Arbeitswelt in Industrie 4.0 .....	187

**C. Pflichten der verantwortlichen Stelle**

<b>I. Rechtmäßige Verarbeitung von Daten</b> .....	191
1. Digitalisierung und Konzerndatenschutz .....	191
2. People Analytics und Datenschutz-Risiken .....	201
3. Erfüllung der Bedingungen der Rechtmäßigkeit .....	205
3.1 Faire Speicherung von Kundendaten .....	205
3.2 Faire Speicherung von Lieferantendaten .....	208
3.3 Nachweisführung und Rechenschaftspflicht .....	209
4. Verarbeitung von Arbeitnehmerdaten .....	211
4.1 Umgang mit Arbeitnehmerdaten .....	211
4.2 Fallkonstellationen zum Fragerecht .....	214
4.3 Betriebsarzt und Gesundheitsdaten .....	220
4.4 Sozialdaten und Wiedereingliederung .....	223
4.5 Medien-Nutzung und Überwachung .....	224
<b>II. Rechtmäßige Übermittlung von Daten</b> .....	226
1. Grundstrukturen der Datenübermittlung .....	226
2. Datenaustausch in globalen Unternehmen .....	229
3. Datenübermittlung an Geschäftspartner .....	234
4. Übermittlung von Arbeitnehmerdaten .....	236
<b>III. Informationspflicht und Benachrichtigung</b> .....	241
1. Informationspflicht und Transparenz .....	241
2. Umsetzung der Informationspflicht .....	246
3. Sonderfall Datenschutzverletzungen .....	248
<b>D. Umsetzung der IT-Sicherheit im Unternehmen</b>	
<b>I. Maßnahmen zur Sicherheit der Verarbeitung</b> .....	251
1. Datensicherheit im Unternehmensdatenschutz .....	251
1.1 Datenschutz durch Technik und Sicherheit .....	251
1.2 Datensicherheit bei intensiver Datennutzung .....	265
1.3 Schutzanforderungen für Arbeitnehmerdaten .....	270
1.4 Nutzungsregelungen für mobiles Arbeiten .....	279
1.5 Verhinderung ungewollter Datenverwendung .....	281
1.6 Sicherheitsbestimmungen für IT-Equipment .....	289
2. Maßnahmen zur Organisationskontrolle .....	293
2.1 Sicherheit von Anwendungen und Prozessen .....	293
2.2 Katalog der Maßnahmen zur Datensicherheit .....	303
3. Datensicherheit bei Datenverwendung im Web .....	312
3.1 Internetsicherheit und Abwehr von Angriffen .....	312
3.2 Sichere Durchführung des Geschäftsverkehrs .....	318
4. System zu Datensicherheit und Compliance .....	325
4.1 Integrität und Compliance von IT-Systemen .....	325
4.2 Einsatz und Nutzen von Firewall-Systemen .....	328
4.3 Asset-Management und Eigentumsschutz .....	330
5. Richtlinien zur Datensicherheit im Unternehmen .....	334
5.1 Zielsetzungen für Organisationsanweisungen .....	334
5.2 Schutz von E-Mails, Intranet und Internet .....	338
5.3 Datengeheimnis und Fernmeldegeheimnis .....	339
5.4 Sicherheit bei individueller Datenverarbeitung .....	340
5.5 Organisationsanweisung zur IT-Sicherheit .....	341
6. Überprüfung der Datensicherheit durch Führungskräfte .....	342

<b>II. Handhabung der Unterlagensicherheit .....</b>	344
1. Behandlung von Unterlagen und Datenträgern .....	344
2. Handhabung von Personalunterlagen .....	350
3. Archivierung von Geschäftsunterlagen .....	355
4. Klassifikation der Unterlagen und Datenträger .....	356
4.1 Interner Gebrauch .....	357
4.2 Vertraulich .....	358
4.3 Streng Vertraulich .....	358
4.4 Persönlich Registriert .....	358
4.5 Persönlich .....	359
4.6 Zusammenfassung .....	359
5. Handhabung von Unterlagen und Datenträgern .....	360
6. Angemessenheit der Maßnahmen .....	363
<b>E. Rechte der Betroffenen</b>	
<b>I. Wahrnehmung von Datenschutzrechten .....</b>	365
1. Datenschutz als soziale Errungenschaft .....	365
2. Betroffenenrechte und Mitbestimmung .....	368
3. Datenschutz und Gleichbehandlung .....	369
<b>II. Recht auf Transparenz und Auskunft .....</b>	371
1. Auskunft als Basisrecht für Betroffene .....	371
2. Gesichtspunkte der Auskunftsbearbeitung .....	374
2.1 Erfordernisse der Auskunftserteilung .....	374
2.2 Konsistente Datenschutz-Organisation .....	375
2.3 Beschränkungen der Auskunftserteilung .....	376
3. Datenschutz-Management zur Auskunft .....	377
<b>III. Recht auf Korrektur und Mitteilung .....</b>	378
1. Datenkorrektur als Gestaltungsrecht .....	378
2. Berichtigung und Mitteilungspflicht .....	379
3. Löschung und Mitteilungspflicht .....	381
4. Einschränkung und Mitteilungspflicht .....	382
5. Recht auf Übertragung von Daten .....	383
6. Widerspruch bei besonderer Situation .....	384
<b>F. Datenverarbeitung außer Haus</b>	
1. Sachverhalte der Auftragsverarbeitung .....	387
2. Cloud Computing und IT-Ressourcen .....	397
3. Struktur der Auftragsverarbeitung .....	400
4. Pflichten des Auftraggebers .....	401
5. Pflichten des Auftragnehmers .....	403
5.1 Überblick zu den Pflichten .....	403
5.2 Verzeichnis der Verarbeitungen .....	405
5.3 Weisungsgebundene Verarbeitung .....	405
5.4 Wahrung der Vertraulichkeit .....	406
5.5 Dienst von Unterauftragnehmern .....	407
5.6 Wahrung der Datensicherheit .....	409
6. Struktur des Pflichtenspektrums .....	409

**G. Haftung im Datenschutzrecht**

<b>I. Funktion der Haftung im Datenschutz .....</b>	411
1. Haftung bei Verletzung von Privatsphäre .....	411
2. Wettbewerbsverhalten und Urheberrecht .....	428
3. Betriebsrisiko und Arbeitnehmerhaftung .....	432
4. Verstöße gegen Diskriminierungsverbote .....	434
5. Nichteinhaltung von Geschäftsgrundsätzen .....	437
6. Sicherheitsverstöße und Internet-Kriminalität .....	439
<b>II. Haftungsansprüche im Datenschutzrecht .....</b>	443
1. Grundstruktur der Haftungsansprüche .....	443
2. Haftungsansprüche im Vertragsverhältnis .....	449
3. Haftungsansprüche im Vertrauensverhältnis .....	450
4. Haftungsansprüche ohne Vertragsverhältnis .....	451
5. Haftung bei Tätigwerden von Mitarbeitern .....	454
6. Haftung bei gemeinsamer Verantwortung .....	456
<b>III. Versicherung im Datenschutz .....</b>	460
1. Grundstrukturen der Versicherungspraxis .....	460
2. Datenschutzversicherung und IT-Haftpflicht .....	465
3. Organisation des Versicherungsschutzes .....	466
Sachverzeichnis .....	469

**beck-shop.de**  
DIE FACHBUCHHANDLUNG

**beck-shop.de**  
DIE FACHBUCHHANDLUNG