

Formularhandbuch Datenschutzrecht

von

Dr. Ansgar Koreng, Matthias Lachenmann, Matthias Bergt, Nikolaus Bertermann, Jörg Jaenichen, Dr. Olaf Koglin,
Sascha Kremer, Dr. Joachim Müller, Dr. Carlo Piltz, Stefan Sander, Steffen Weiß

1. Auflage



Verlag C.H. Beck München 2015

Verlag C.H. Beck im Internet:

www.beck.de

ISBN 978 3 406 66502 8

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

schnell und portofrei erhältlich bei beck-shop.de DIE FACHBUCHHANDLUNG

beck-shop.de

Koreng/Lachenmann
Formularhandbuch Datenschutzrecht

beck-shop.de

Formularhandbuch Datenschutzrecht

Herausgegeben von

Dr. Ansgar Koreng
Berlin

Matthias Lachenmann
Elchingen

Bearbeitet von
den Herausgebern und von

Matthias Bergt, Berlin; *Nikolaus Bertermann*, Berlin;
Jörg Jaenichen, Bielefeld; *Dr. Olaf Koglin*, Berlin;
Sascha Kremer, Köln; *Dr. Joachim Müller*, Bielefeld;
Dr. Carlo Piltz, Berlin; *Stefan Sander*, LL. M., B. Sc., Köln;
Steffen Weiß, LL. M., Bonn

2015

beck-shop.de

Zitiervorschlag: Koreng/Lachenmann/*Bearbeiter*

www.beck.de

ISBN 978 3 406 66502 8

© 2015 Verlag C.H. Beck oHG
Wilhelmstraße 9, 80801 München
Druck: CPI – Clausen & Bosse GmbH
Birkstraße 10, 25917 Leck

Satz: Druckerei C.H.Beck, Nördlingen

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

beck-shop.de

Vorwort

Das Datenschutzrecht ist geprägt von restriktiven gesetzlichen Regelungen, die in der Praxis jedoch oft nur rudimentär umgesetzt werden. Es wäre allzu leicht, den Grund hierfür nur in dem Umstand zu suchen, dass die gesetzlichen Regelungen in ihrer Entwicklung kaum mit dem technischen Fortschritt Schritt halten konnten. Denn es ist nicht zuletzt auch die Komplexität der Rechtsmaterie, die ihrer praktischen Akzeptanz entgegensteht. Dieses Buch soll eine Bresche durch das Dickicht des geltenden Datenschutzrechts schlagen und Unternehmen sowie deren Beratern eine Hilfe bei dessen praxisbezogener Umsetzung sein. Dabei war es uns ein besonderes Anliegen, das Datenschutzrecht nicht als einsame Insel im großen Ozean der Anforderungen an die unternehmensinterne IT- und Datensicherheit zu betrachten, sondern seine Wechselwirkungen und Synergien etwa mit den Aspekten IT-Sicherheit, Know-how-Schutz, Compliance und Arbeitsrecht aufzuzeigen.

Das Buch richtet sich damit insbesondere an interne wie externe Datenschutzbeauftragte, denen es eine Hilfestellung bei der alltäglichen Ausübung ihres Amtes sein soll. Ebenso soll es Rechtsabteilungen bzw. Geschäftsführungen als praxisbezogener Leitfaden beim Aufbau einer Datenschutzorganisation im Unternehmen dienen. Formulare zum Thema Arbeitnehmerrechte, Online-Datenschutz sowie verwaltungsbehördliche und verwaltungsgerichtliche Verfahren bieten darüber hinaus auch Rechtsanwälten eine Hilfestellung in den meisten datenschutzrechtlichen Fragen, unabhängig davon, ob der Datenschutz einen Beratungsschwerpunkt darstellt oder nur unregelmäßig behandelt wird.

Bei der Gestaltung des Buches haben sowohl Juristen als auch Autoren mit technischem Hintergrund mitgewirkt. Es war uns bei seiner Konzeption ebenso ein Anliegen, datenschutzrechtlich interessierten Nichtjuristen Kenntnisse zu vermitteln, wie wir auch hoffen, dem juristisch gebildeten Publikum neue Erkenntnisse auf technischem Gebiet vermitteln zu können. Ob uns dieser Spagat gelungen ist, bitten wir den geneigten Leser zu beurteilen. Für Rückmeldungen zu diesem oder jedem anderen Aspekt dieses Buches sind die Herausgeber dankbar (koreng@jbb.de; matthias@kanzlei-lachenmann.de).

Unser Dank gilt den Autoren für die stets freundliche, unkomplizierte und kompetente Zusammenarbeit. Dank gilt weiterhin Frau Ruth Schrödl und Herrn Dr. Johannes Wasmuth aus dem Lektorat des Verlags C.H.Beck, die die Entstehung des Buches stets konstruktiv begleitet und unterstützt haben.

Berlin/Elchingen, Oktober 2014

*Dr. Ansgar Koreng
Matthias Lachenmann*

beck-shop.de

Inhaltsverzeichnis

	Seite
Vorwort	V
Bearbeiterverzeichnis	VII
Abkürzungsverzeichnis	IX
Literaturverzeichnis	XVII

A. Der Datenschutzbeauftragte

I. Beauftragung eines Datenschutzbeauftragten	1
1. Bestellung zum Datenschutzbeauftragten	1
2. Dienstvertrag mit einem externen betrieblichen Datenschutz- beauftragten	15
3. Beratungsvertrag mit einem Dienstleistungsunternehmen	31
II. Tätigkeiten des Datenschutzbeauftragten	43
1. Dateistatut/Verfahrensverzeichnis	43
2. Antwort auf das Auskunftsverlangen eines Betroffenen	48
3. Entbindung von der Schweigepflicht	52
4. Typische auf den Datenschutzbeauftragten des Vertragspartners bezogene Klauseln anderer Verträge	55
5. Antwort auf Auskunftsverlangen der Aufsichtsbehörde	60
III. Datenschutzaudit	64

B. Datenschutz im Unternehmen

I. Datenschutzorganisation im Unternehmen	77
1. Organisatorischer und strategischer Aufbau	77
2. Pflichtübung, Kür oder Manager: Möglicher Verantwortungsumfang von Datenschutzabteilungen	83
3. Dienstleister oder Kontrolleur: Die zwei Gesichter von Datenschutz- abteilungen	85
4. Von der Auftragsdatenverarbeitung bis zur Verbandsarbeit: Zuständig- keitsbereiche im Einzelnen	87
5. Risikoverständnis und Reifegrad einer Datenschutzorganisation	90
6. Umgang mit Anfragen und Audits der Aufsichtsbehörden	93
II. Code of Conduct und Selbstverpflichtung zum Datenschutz	96
1. Datenschutz im Code of Conduct	96
2. Übersicht zu Hinweisgebersystemen (Whistleblower-Hotlines)	97
3. Hinweisgebersystem (Whistleblower-Hotline) im Code of Conduct	100
4. Datenschutzerklärung für ein elektronisches Hinweisgeberportal	101
5. Richtlinie zum Einsatz eines Hinweisgebersystems	101
6. Internal Investigations: Unternehmenspflicht vs. Datenschutz	109

III. Unternehmensrichtlinie Datenschutz	112
IV. Projekt- und Produktfragen	125
1. Klassische Vorabkontrolle oder Teameinbindung	125
2. Kundendatenschutz	129
3. Einrichtung automatisierter Abrufverfahren gemäß § 10 BDSG	134
4. Einsatz von Cloud Computing im Unternehmen	137
5. Löschkonzepte	147
V. Auftragsdatenverarbeitung im Unternehmen	150
1. Abgrenzung Funktionsübertragung von Auftragsdatenverarbeitung	150
2. Auftragsdatenverarbeitung oder Funktionsübertragung: Richtlinie für Unternehmen und Konzerne	153
3. Richtlinie Auftragsdatenverarbeitung	164
VI. Fernwartung durch Drittunternehmen	175
1. Anlage zur Fernwartung für externe Dienstleister	176
2. Datenschutzvereinbarung für den Remotezugriff	188
3. Allgemeine Bestimmungen	190
4. Arbeitsanweisung zur Fernwartung für Dienstleister	191
VII. Videoüberwachung im Betrieb	194
1. Checkliste zur Videoüberwachung	196
2. Richtlinie zur Videoüberwachung im Betrieb	198
3. Prüftabelle vor Inbetriebnahme einer Videoüberwachung	212
4. Maßnahmen zum Schutz der Betroffenen	217
VIII. Vertraulichkeitsvereinbarung	220
IX. Datenschutzerklärungen	229
1. Datenschutzerklärung für Websites und Apps bei rein informativ-scher Nutzung	230
2. Besondere Nutzungsformen von Websites	237
3. Newsletter	248
4. Webtracking	254
5. Social Media Plug-ins	259
6. Online Behavioral Advertising	263
7. Datenschutzerklärung für mobile Apps	268
8. Besondere Nutzungsformen der mobilen Apps	272
X. Datenschutzhinweise und Einwilligungen	277
1. Datenschutzhinweise bei Kaufverträgen	277
2. Datenschutzhinweise bei Portalverträgen	281
3. Einwilligung in Werbeversand/Newsletter	284
 C. Formulare zur Verwendung gegenüber Mitarbeitern	
I. Einwilligung durch Beschäftigte	295
1. Einwilligungserklärung zur Veröffentlichung von Mitarbeiterfotos	295
2. Einwilligungserklärung zur Speicherung von Bewerberdaten	302
II. Vertraulichkeitspflichten	307
1. Verpflichtung auf das Datengeheimnis mit Merkblatt	307
2. Verpflichtung auf das Telekommunikationsgeheimnis mit Merkblatt	316

3. Deklaratorische Belehrung über die Verpflichtung zur Wahrung von Geschäfts- und Betriebsgeheimnissen mit Merkblatt	320
4. Vereinbarung über die Wahrung von Geschäfts- und Betriebs- geheimnissen mit Merkblatt und Protokoll	325
5. Vertraulichkeitsvereinbarung für freie Mitarbeiter	332
6. Merkblatt zur Wahrung der Vertraulichkeit in der sozialen Arbeit	346
III. Richtlinien zur EDV-Nutzung	354
1. Richtlinie zur Nutzung von Internet und E-Mail	354
2. Richtlinie Home Office/Mobile Office (Telearbeit)	375
3. Richtlinie zur Fernwartung durch eigene Mitarbeiter	385
4. Nutzungsvereinbarung zu „Bring Your Own Device“ (BYOD)	392
5. Social Media Guideline	406
D. Behördliches und verwaltungsgerichtliches Verfahren	
I. Verwaltungsverfahren	415
1. Eingabe an eine Aufsichtsbehörde	417
2. Widerspruch gegen einen Bescheid einer Datenschutzaufsichts- behörde	421
3. Antrag auf Genehmigung der Übermittlung personenbezogener Daten in ein Drittland ohne ausreichendes Datenschutzniveau	426
4. Mitteilung einer Datenpanne gemäß § 42a BDSG	429
5. Anzeige an die Behörde gemäß § 80 Abs. 3 SGB X	431
II. Verwaltungsgerichtliches Verfahren	435
1. Antrag auf Wiederherstellung der aufschiebenden Wirkung	436
2. Klage gegen eine Anordnung der Aufsichtsbehörde	442
3. Einstweiliger Rechtsschutz gegen die Informationstätigkeit der Auf- sichtsbehörde	448
E. Technische und organisatorische Datensicherheit	
I. Überblick: Rationalisierung von Datenschutzthemen im Unternehmen	457
1. Methodischer Aufbau	457
2. Richtlinien zur Ermittlung von Schnittmengen zu anderen Funktionen	471
3. Checkliste der Rollen und ihrer Funktionen	477
4. Tabellarische Aufstellung von Rollenüberdeckungen	485
5. Vermeidung unrationeller Arbeitsweisen	492
II. Vorabkontrolle vor Vertragsabschluss einer Auftragsdatenverarbeitung	504
III. Formular zur Prüfung der technischen und organisatorischen Maßnahmen gemäß § 9 BDSG	510
1. Anwendung bei interner Verarbeitung und Auftragsdatenverarbeitung	510
2. Prüfliste	513
IV. Prüfprotokolle	541
1. Einleitung	541
2. Formular	545
V. Formulare während der Laufzeit der Auftragsdatenverarbeitung	550
1. Genehmigung von Unterauftragnehmern	550
2. Änderung der Weisungsberechtigten/-empfänger	552

beck-shop.de

X	Inhaltsverzeichnis	
	3. Änderung des betrieblichen Datenschutzbeauftragten	553
	4. Änderungen in den Verfahren	555
	5. Meldebogen Datenschutz- oder IT-Sicherheitsvorfall im Innenverhältnis	556
	6. Prüfliste für Auftragsdatenverarbeitung bei Insolvenz des Auftraggebers/Auftragnehmers	564
	VI. Formular zur Prüfung von Berechtigungskonzepten	568
	Sachverzeichnis	577