

# Formularhandbuch Datenschutzrecht

Bearbeitet von

Herausgegeben von Dr. Ansgar Koreng, Rechtsanwalt, und Dr. Matthias Lachenmann, Rechtsanwalt,  
Bearbeitet von den Herausgebern und von Bilal Abedin, Dr. Holger Achtermann, Matthias Bergt, Nikolaus  
Bertermann, Dr. Martin Braun, Dr. Stefan Brink, Christian Diekmann, LL.M., Michael Huth, Jörg Jaenichen,  
Dr. Olaf Koglin, Sascha Kremer, Dr. Joachim Müller, Malaika Nolde, LL.M., Dr. Carlo Piltz, Dr. Frederike  
Rehker, Stefan Sander, LL.M., B.Sc., Stephan Schmidt, Sebastian Schwiering, Steffen Weiß, LL.M., und  
Bernhard C. Witt

2. Auflage 2018. Buch inkl. Online-Nutzung. XXVIII, 1042 S. Mit Zugang zur Online-Version in beck-online  
DIE DATENBANK für einen Nutzer. In Leinen

ISBN 978 3 406 69542 1

Format (B x L): 16,0 x 24,0 cm

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

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

schnell und portofrei erhältlich bei

The logo for beck-shop.de features the text 'beck-shop.de' in a bold, red, sans-serif font. Above the 'i' in 'shop' are three red dots of varying sizes, arranged in a slight arc. Below the main text, the words 'DIE FACHBUCHHANDLUNG' are written in a smaller, red, all-caps, sans-serif font.

**beck-shop.de**  
DIE FACHBUCHHANDLUNG

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.

Koreng/Lachenmann  
Formularhandbuch Datenschutzrecht

  
**beck-shop.de**  
DIE FACHBUCHHANDLUNG

**beck-shop.de**  
DIE FACHBUCHHANDLUNG

# Formularhandbuch Datenschutzrecht

Herausgegeben von

**Dr. Ansgar Koreng**  
Leipzig

**Dr. Matthias Lachenmann**  
Bonn

**beck-shop.de**  
Bearbeitet von  
den Herausgebern und von  
DIE FACHBUCHHANDLUNG

*Bilal Abedin, Aachen; Dr. Holger Achtermann, Leer; Matthias Bergt, Berlin; Nikolaus Bertermann, Berlin; Dr. Martin Braun, Frankfurt a. M.; Dr. Stefan Brink, Stuttgart; Christian Diekmann, LL. M., Essen; Michael Huth, Bonn; Jörg Jaenichen, Köln; Dr. Olaf Koglin, Berlin; Sascha Kremer, Pulheim; Dr. Joachim Müller, Köln; Malaika Nolde, LL. M., Düsseldorf; Dr. Carlo Piltz, Berlin; Dr. Frederike Rehker, Langenhagen; Stefan Sander, LL. M., B. Sc., Duisburg; Stephan Schmidt, Mainz; Sebastian Schwiering, Aachen; Steffen Weiß, LL. M., Bonn; Bernhard C. Witt, Ulm*

2. Auflage 2018



Zitiervorschlag: Koreng/Lachenmann/*Bearbeiter*

  
**beck-shop.de**  
DIE FACHBUCHHANDLUNG

[www.beck.de](http://www.beck.de)

ISBN 978 3 406 69542 1

© 2018 Verlag C.H. Beck oHG  
Wilhelmstraße 9, 80801 München  
Druck und Bindung: Kösel GmbH & Co. KG  
Am Buchweg 1, 87452 Altusried-Krugzell

Satz und Umschlaggestaltung: Druckerei C.H. Beck, Nördlingen

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

## Vorwort

Der Regelungsanspruch des Datenschutzrechts ist im Zeitalter von künstlicher Intelligenz, Big Data und Wearables allgegenwärtigen Herausforderungen ausgesetzt und praktisch umfassend. Gleichwohl ist dieses Rechtsgebiet nach wie vor von einer erheblichen Sein-Sollen-Dichotomie geprägt.

Maßgebliche Akteure interessieren sich häufig nicht für das Europäische Datenschutzrecht, insbesondere die im außereuropäischen Ausland ansässigen. Dies führt bei anderen Wettbewerbern zu Frustration und setzt nicht selten hinsichtlich der datenschutzrechtlichen Compliance eine Abwärtsspirale in Gang. Hinzu kommt ein gewisses, allgemeines Akzeptanzdefizit. Das gilt für den privatwirtschaftlichen und den öffentlich-rechtlichen Bereich gleichermaßen. Während sich die Aufsichtsbehörden mit privaten Akteuren teilweise erbitterte und für den Normalbürger kaum nachvollziehbare Auseinandersetzungen über Social Plug-ins und die Verschlüsselung von Messenger-Apps liefern, greifen staatliche Akteure mit immer größerer Nonchalance nach den Daten der Bürger. Diese wiederum lassen das nicht nur größtenteils widerstandslos geschehen, sondern rufen teilweise sogar, beeinflusst durch das staatliche Versprechen nach mehr Komfort und Sicherheit, nach weiteren Einschränkungen der Privatsphäre. Für einen jüngst gestarteten Test einer automatischen Gesichtserkennung am Berliner Bahnhof Südkreuz fanden sich innerhalb kurzer Zeit 300 Freiwillige, die bereit waren, gegen einen Amazon-Gutschein (sic!) in Höhe von 25 Euro an der Erprobung dieser datenschutzrechtlich mehr als zweifelhaften Technologie mitzuwirken.

Den Defiziten des geltenden Rechts und den bisweilen erkennbaren datenschutzrechtlichen Dismembrationsbewegungen hat der europäische Gesetzgeber nun die Datenschutz-Grundverordnung (DS-GVO) entgegengesetzt. Sie stellt den Versuch dar, das nach 22 Jahren etwas angestaubte Datenschutzrecht in Europa den heutigen Gegebenheiten anzupassen und ihm gleichzeitig zu stärkerer Durchsetzung zu verhelfen. Noch keine datenschutzrechtliche Reform war derart umfassend. Es wird viel Zeit in Anspruch nehmen, bis alle Akteure ihre Prozesse an die Erfordernisse des geltenden Rechts vollständig angepasst haben. Umso mehr Zeit wird es brauchen, dem neuen Regelwerk tatsächlich zur Geltung zu verhelfen.

Es liegt in der Natur der Sache, dass die Datenschutz-Grundverordnung sehr unterschiedlich rezipiert wird. Gleichwohl kann es sicherlich nicht geleugnet werden, dass Unternehmen sich mit Blick auf die erheblichen Sanktionsandrohungen und Eingriffsmittel der Aufsichtsbehörden eine stiefmütterliche Behandlung des Datenschutzrechts spätestens jetzt nicht mehr erlauben können. Es liegt im Interesse eines jeden Unternehmens, der datenschutzrechtlichen Compliance künftig einen großen Stellenwert zuzuweisen. Bei der unternehmensinternen Umsetzung des neuen Rechts soll dieses Formularhandbuch als Hilfestellung dienen.

Im Vergleich zur ersten Auflage wurde die Gliederung vollständig neu konzipiert, eine Reihe von Formularen wurde neu entwickelt und sämtliche Kapitel wurden intensiv überarbeitet. Die zweite Auflage ist konsequent am neuen Recht ausgerichtet.

Auf die bisherige Rechtslage wird nur dort Bezug genommen, wo es zum besseren Verständnis des neuen Rechts geboten erscheint. Einige Muster schildern die Organisation des Datenschutzes und die Anpassung bestehender Prozesse an das neue Recht. Die meisten Formulare des Buches sind zum Einsatz unter Geltung der DS-GVO bestimmt und können daher unter Geltung des BDSG a. F. nicht mehr eingesetzt werden.

Als Herausgeber bedanken wir uns an erster Stelle bei den Autoren dafür, dass sie gerade in Zeiten, in denen ihre datenschutzrechtliche Expertise am Markt ohnehin stark nachgefragt ist, neben ihrer erheblichen Arbeitsbelastung viel Zeit und Mühe für das Buch aufgebracht haben. Bedanken möchten wir uns auch bei den Mitarbeiterinnen und Mitarbeitern des Verlags C. H. Beck, in erster Linie bei Frau Ruth Schrödl, die uns stets mit Rat und Tat zur Seite standen.

Wir hoffen, dass dieses Buch dem Rechtsanwender eine Hilfestellung sein wird, um die aus der Datenschutz-Grundverordnung resultierenden Herausforderungen in der unternehmerischen Praxis zu meistern. Das Buch ist im Wesentlichen auf dem Stand von August 2017. Sollten trotz aller Anstrengungen noch Fehler verblieben sein, so bitten wir dafür um Entschuldigung und bedanken uns für entsprechende Hinweise – ebenso wie freilich für alle anderen Kommentare, Anmerkungen und Anregungen (lachenmann@paulypartner.de; ansgar@koreng.eu).

Leipzig/Bonn, November 2017

*Dr. Ansgar Koreng*  
*Dr. Matthias Lachenmann*

## Inhaltsverzeichnis

	Seite
Vorwort .....	V
Bearbeiterverzeichnis .....	XIII
Abkürzungsverzeichnis .....	XV
Literaturverzeichnis .....	XXV

### A. Organisationsstruktur Datenschutz

<b>I. Rechenschaftspflicht (Art. 5, 24 DS-GVO) .....</b>	<b>1</b>
<b>II. Datenschutz-Compliance .....</b>	<b>11</b>
1. Vorstandspflichten – Die Lücke zwischen Datenschutzbeauftragtem und Datenschutz-Compliance .....	11
2. Pflichten und Haftung bei Vorständen bzw. Geschäftsleitung sowie bei Aufsichtsräten .....	13
3. Anforderungen an ein Compliance Management System nach IDW PS 980 .....	16
<b>III. Datenschutzorganisation im Unternehmen .....</b>	<b>20</b>
1. Organisatorischer und strategischer Aufbau .....	20
2. Pflichtübung, Kür oder Privacy-Manager: Vom Datenschutzbeauftragten zu Datenschutz-Compliance .....	27
3. Dienstleister oder Kontrolleur: Die zwei Gesichter von Datenschutzabteilungen .....	31
4. Von der Auftragsverarbeitung bis zur Verbandsarbeit: Zuständigkeitsbereiche im Einzelnen .....	34
5. Risikoverständnis und Reifegrad einer Datenschutzorganisation .....	38
6. Umgang mit Anfragen und Audits der Aufsichtsbehörden .....	41
7. Formale Datenschutz-Folgenabschätzung oder Teamarbeit .....	44
<b>IV. Code of Conduct und Selbstverpflichtung zum Datenschutz .....</b>	<b>51</b>
1. Datenschutz im Code of Conduct .....	51
2. Übersicht zu Hinweisgebersystemen (Whistleblower-Hotlines) .....	54
3. Hinweisgebersystem (Whistleblower-Hotline) im Code of Conduct .....	56
4. Datenschutzerklärung für ein elektronisches Hinweisgeberportal .....	58
5. Richtlinie zum Einsatz eines Hinweisgebersystems .....	58
6. Internal Investigations: Unternehmenspflicht vs. Datenschutz .....	66

### B. Der Datenschutzbeauftragte

<b>I. Benennung und Abberufung des Datenschutzbeauftragten .....</b>	<b>69</b>
1. Benennung als Datenschutzbeauftragter .....	69
2. Abberufung durch den Arbeitgeber .....	87



<b>II. Verträge mit externen Datenschutzbeauftragten</b> .....	91
1. Dienstvertrag mit einem externen Datenschutzbeauftragten .....	91
2. Beratungsvertrag mit einem Dienstleistungsunternehmen .....	109
3. Aufhebungsvertrag der Parteien .....	120
<b>III. Tätigkeiten des Datenschutzbeauftragten</b> .....	123
1. Entbindung von der Schweigepflicht .....	123
2. Antwort auf ein Auskunftsverlangen der Aufsichtsbehörde .....	127
3. Typische auf den Datenschutzbeauftragten des Vertragspartners be- zogene Klauseln anderer Verträge .....	131

### C. Dokumentationspflichten im Unternehmen

<b>I. Datenschutzaudit</b> .....	137
<b>II. Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DS-GVO)</b> .....	156
<b>III. Datenschutz-Folgenabschätzung und Konsultation (Art. 35 f. DS-GVO)</b> .....	164
1. Übersicht über den Verlauf einer Datenschutz-Folgenabschätzung .....	166
2. Schwellenwertprüfung und Erforderlichkeit einer Datenschutz- Folgenabschätzung .....	167
3. Durchführung einer Datenschutz-Folgenabschätzung .....	168
4. Vorherige Konsultation (Art. 36 DS-GVO) .....	174
<b>IV. Verhaltensregeln und Zertifizierungen</b> .....	185
1. Verhaltensregeln (Art. 40 DS-GVO) .....	185
2. Zertifizierungen (Art. 42 f. DS-GVO) .....	198
<b>V. Sicherheit der Verarbeitung und risikobasierter Ansatz</b> .....	205
1. Ziele der Maßnahmen zur Sicherheit der Verarbeitung .....	205
2. Einführung zum risikobasierten Ansatz in der DS-GVO .....	207
3. Schema zur Ermittlung von Risiken der Verarbeitungstätigkeiten .....	211
4. Verfahren zur Durchführung von Wirksamkeitskontrollen .....	216
5. Prüfkonzept zu Datenschutz durch Technikgestaltung und daten- schutzfreundlicher Voreinstellungen .....	218
<b>VI. Meldung von Verletzungen des Schutzes personenbezogener Daten (Art. 33 f. DS-GVO)</b> .....	222
1. Mitteilung an die Aufsichtsbehörde (Art. 33 DS-GVO) .....	222
2. Mitteilung an die betroffene Person (Art. 34 DS-GVO) .....	226
3. Dokumentation der Verletzungen des Schutzes personenbezogener Daten (Art. 33 DS-GVO) .....	229
<b>VII. Vertraulichkeitspflichten der Beschäftigten</b> .....	233
1. Verpflichtung auf das Datengeheimnis mit Merkblatt .....	233
2. Verpflichtung auf das Telekommunikationsgeheimnis mit Merk- blatt .....	245
3. Deklaratorische Belehrung über die Verpflichtung zur Wahrung von Geschäfts- und Betriebsgeheimnissen mit Merkblatt und Proto- koll .....	250
4. Vereinbarung über die Wahrung von Geschäfts- und Betriebsgeheim- nissen mit Merkblatt und Protokoll .....	256

5. Vereinbarung zur datenschutzrechtlichen Eingliederung freier Mitarbeiter in den Betrieb des Verantwortlichen .....	264
6. Vertraulichkeitsvereinbarung für freie Mitarbeiter .....	270
7. Merkblatt zur Wahrung der Vertraulichkeit in der sozialen Arbeit .....	287

**D. Richtlinien des Unternehmens**

<b>I. Konzernrichtlinie der Geschäftsleitung .....</b>	<b>297</b>
1. Gesellschafterbeschluss zur Einführung einer Datenschutz-Organisation .....	297
2. Konzernrichtlinie Datenschutz-Organisation .....	298
<b>II. Unternehmensrichtlinie Datenschutz für Mitarbeiter .....</b>	<b>304</b>
<b>III. Richtlinien zur Nutzung durch Beschäftigte .....</b>	<b>319</b>
1. Richtlinie zur Nutzung von Internet und E-Mail .....	319
2. Richtlinie Home Office/Mobile Office (Telearbeit) .....	351
3. Richtlinie zur Fernwartung durch eigene Mitarbeiter .....	361
4. Nutzungsvereinbarung zu „Bring Your Own Device“ (BYOD) .....	370
5. Social-Media-Guideline .....	385
<b>IV. Löschkonzepte .....</b>	<b>395</b>

**E. Technische und organisatorische Datensicherheit**

<b>I. Überblick: Rationalisierung von Datenschutzthemen im Unternehmen .....</b>	<b>401</b>
1. Methodischer Aufbau .....	401
2. Richtlinien zur Ermittlung von Schnittmengen zu anderen Funktionen .....	417
3. Checkliste der Rollen und ihrer Funktionen .....	426
4. Tabellarische Aufstellung von Rollenüberdeckungen .....	435
5. Vermeidung unrationeller Arbeitsweisen .....	444
<b>II. Technische und organisatorische Maßnahmen (Art. 32, 25 DS-GVO) ...</b>	<b>456</b>
1. Anwendung bei interner Verarbeitung und Auftragsverarbeitung .....	456
2. Formular zur Prüfung der technischen und organisatorischen Maßnahmen .....	459
<b>III. Prüfkontrolle .....</b>	<b>491</b>
<b>IV. Formular zur Prüfung von Berechtigungskonzepten .....</b>	<b>499</b>

**F. Rechte der betroffenen Person**

<b>I. Informationspflicht bei Erhebung von personenbezogenen Daten (Art. 13 f. DS-GVO) .....</b>	<b>509</b>
1. Datenschutzerklärung für Websites .....	510
2. Datenschutzerklärung für mobile Apps .....	520
3. Besondere Nutzungsformen von Websites .....	531
4. Newsletter .....	543
5. Web Analytics .....	548

6. Social Media .....	556
7. Online-Werbung .....	565
<b>II. Auskunftsrecht der betroffenen Person (Art. 15 DS-GVO) .....</b>	<b>579</b>
1. Auskunftsverlangen der betroffenen Person .....	579
2. Antwort auf Auskunftsverlangen mit Recht auf Kopie (Art. 15 DS-GVO) .....	583
<b>III. Recht auf Berichtigung (Art. 16 DS-GVO) .....</b>	<b>591</b>
<b>IV. Rechte auf Löschung und Mitteilung (Art. 17, 19 DS-GVO) .....</b>	<b>595</b>
1. Recht auf Löschung und „Recht auf Vergessenwerden“ (Art. 17 DS-GVO) .....	595
2. Informationspflicht an Dritte bei einem Lösungsersuchen (Art. 17 Abs. 2 DS-GVO) .....	598
<b>V. Recht auf Einschränkung der Verarbeitung (Art. 18 DS-GVO) .....</b>	<b>603</b>
<b>VI. Recht auf Datenübertragbarkeit (Art. 20 DS-GVO) .....</b>	<b>606</b>

### G. Zusammenarbeit mit anderen Unternehmen

<b>I. Vereinbarung der Auftragsverarbeitung (Art. 28 f. DS-GVO) .....</b>	<b>611</b>
1. Vergleich Auftragsverarbeitung nach dem BDSG und der DS-GVO ...	611
2. Richtlinie Auftragsverarbeitung .....	618
3. Prüfliste vor Vertragsabschluss einer Auftragsverarbeitung .....	627
4. Vertragsmuster Auftragsverarbeitung .....	633
5. Ergänzungsvertrag zum Video-Ident-Verfahren .....	654
6. Maßnahmenübersicht und deren risikobasierte Bewertung bei der Auftragsverarbeitung .....	675
<b>II. Formulare während der Laufzeit der Auftragsverarbeitung (Art. 28 DS-GVO) .....</b>	<b>685</b>
1. Genehmigung von Unterauftragnehmern .....	685
2. Änderung bei den Weisungsberechtigten/-empfängern .....	687
3. Änderung beim Datenschutzbeauftragten .....	689
4. Änderungen in den Verfahren .....	690
5. Meldebogen Datenschutz- oder IT-Sicherheitsvorfall im Innenverhältnis .....	692
6. Prüfliste für Auftragsverarbeitung bei Insolvenz des Auftraggebers/Auftragnehmers .....	700
<b>III. Fernwartung durch Drittunternehmen .....</b>	<b>704</b>
1. Anlage zur Fernwartung für externe Dienstleister .....	705
2. Datenschutzvereinbarung für den Remotezugriff .....	716
3. Allgemeine Bestimmungen .....	718
4. Arbeitsanweisung zur Fernwartung für Dienstleister .....	719
<b>IV. Vertraulichkeitsvereinbarungen .....</b>	<b>722</b>
1. Vertraulichkeitsvereinbarung bei Dienstleistungsverträgen .....	722
2. Vertraulichkeitsvereinbarung bei M&A-Transaktionen .....	730
<b>V. Gemeinsam für die Verarbeitung Verantwortliche (Art. 26 DS-GVO) ...</b>	<b>747</b>
<b>VI. Einsatz von Cloud Computing im Unternehmen .....</b>	<b>754</b>

Inhaltsverzeichnis	XI
--------------------	----

<b>VII. Datentransfers in Drittstaaten</b>	764
1. Übersicht über internationale Datentransfers (Art. 44 ff. DS-GVO) ...	764
2. Anhänge zu den Standarddatenschutzklauseln	771
3. Binding Corporate Rules	778
4. Einwilligung der betroffenen Personen	793
5. Antrag auf Genehmigung des Transfers personenbezogener Daten in ein Drittland ohne ausreichendes Datenschutzniveau (Art. 46 Abs. 3 DS-GVO)	800

## H. Beschäftigtendatenschutz

<b>I. Einwilligung durch Beschäftigte</b>	803
1. Einwilligungserklärung zur Veröffentlichung von Mitarbeiterfotos	803
2. Einwilligungserklärung zur Speicherung von Bewerberdaten	809
<b>II. Beschäftigtendatenschutz bei Arbeitsunfähigkeit und betrieblichem Eingliederungsmanagement</b>	817
1. Betriebsvereinbarung zu Kranken- und BEM-Unterlagen	825
2. Einladungsschreiben zum BEM	848
<b>III. Videoüberwachung auf Firmengeländen</b>	854
1. Checkliste zur Videoüberwachung	856
2. Richtlinie und Betriebsvereinbarung zur Videoüberwachung im Betrieb	859
3. Festlegungen vor Inbetriebnahme der Videoüberwachung	877
4. Maßnahmen zum Schutz der betroffenen Personen	883
5. Protokoll zur Auswertung von Videoaufnahmen	885
<b>IV. Tor- und Spindkontrollen bei Beschäftigten</b>	887
1. Checkliste zu Tor- und Spindkontrollen	889
2. Betriebsvereinbarung über die Durchführung von Tor- und Spindkontrollen	890
<b>V. Detektiveinsatz gegen Beschäftigte</b>	901
<b>VI. Betriebsvereinbarung zum Terrorlisten-Screening</b>	910

## I. Kundendatenschutz

<b>I. Organisation des Kundendatenschutzes</b>	927
<b>II. Einwilligungen durch betroffene Personen</b>	937
<b>III. Einwilligung in Werbeversand/Newsletter</b>	945
<b>IV. Bonitätsprüfung natürlicher Personen</b>	959
1. Bonitätsprüfung und Informationen bei Kaufverträgen	960
2. Darlehen-Selbstauskunft	969
3. Mieter-Selbstauskunft	978
4. Haushaltsrechnung natürlicher Personen	985
<b>V. Checkliste bei polizeilichen Auskunftsverlangen</b>	988

**J. Behördliches und verwaltungsgerichtliches Verfahren**

I. Eingabe an eine Aufsichtsbehörde .....	1001
II. Antrag auf Wiederherstellung der aufschiebenden Wirkung .....	1007
III. Klage gegen eine Anordnung der Aufsichtsbehörde .....	1014
IV. Einstweiliger Rechtsschutz gegen Informationstätigkeit der Aufsichtsbehörde .....	1019
Sachverzeichnis .....	1029

  
**beck-shop.de**  
DIE FACHBUCHHANDLUNG