

Formularhandbuch Datenschutzrecht

Herausgegeben von

Dr. Ansgar Koreng
Leipzig

Dr. Matthias Lachenmann
Bonn

Bearbeitet von
den Herausgebern und von

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

C.H.BECK

Inhaltsverzeichnis

	Seite
Vorwort	V
Bearbeiterverzeichnis	XIII
Abkürzungsverzeichnis	XV
Literaturverzeichnis	XXV

A. Organisationsstruktur Datenschutz

I. Rechenschaftspflicht (Art. 5, 24 DS-GVO)	1
II. Datenschutz-Compliance	11
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 IDWPS 980	16
III. Datenschutzorganisation im Unternehmen	20
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 Datenschutz-Abteilungen	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
IV. Code of Conduct und Selbstverpflichtung zum Datenschutz	51
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

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

II. Verträge mit externen Datenschutzbeauftragten	91
1. Dienstvertrag mit einem externen Datenschutzbeauftragten	91
2. Beratungsvertrag mit einem Dienstleistungsunternehmen	109
3. Aufhebungsvertrag der Parteien	120
III. Tätigkeiten des Datenschutzbeauftragten	123
1. Entbindung von der Schweigepflicht	123
2. Antwort auf ein Auskunftsverlangen der Aufsichtsbehörde	127
3. Typische auf den Datenschutzbeauftragten des Vertragspartners bezogene Klauseln anderer Verträge	131
C. Dokumentationspflichten im Unternehmen	
I. Datenschutzaudit	137
II. Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DS-GVO)	156
III. Datenschutz-Folgenabschätzung und Konsultation (Art. 35 f. DS-GVO)	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
IV. Verhaltensregeln und Zertifizierungen	185
1. Verhaltensregeln (Art. 40 DS-GVO)	185
2. Zertifizierungen (Art. 42 f. DS-GVO)	198
V. Sicherheit der Verarbeitung und risikobasierter Ansatz	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 datenschutzfreundlicher Voreinstellungen	218
VI. Meldung von Verletzungen des Schutzes personenbezogener Daten (Art. 33 f. DS-GVO)	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
VII. Vertraulichkeitspflichten der Beschäftigten	233
1. Verpflichtung auf das Datengeheimnis mit Merkblatt	233
2. Verpflichtung auf das Telekommunikationsgeheimnis mit Merkblatt	245
3. Deklaratorische Belehrung über die Verpflichtung zur Wahrung von Geschäfts- und Betriebsgeheimnissen mit Merkblatt und Protokoll	250
4. Vereinbarung über die Wahrung von Geschäfts- und Betriebsgeheimnissen mit Merkblatt und Protokoll	256

5. Vereinbarung zur datenschutzrechtlichen Hingliederung 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

I. Konzernrichtlinie der Geschäftsleitung	297
1. Gesellschafterbeschluss zur Einführung einer Datenschutz-Organisation	297
2. Konzernrichtlinie Datenschutz-Organisation	298
II. Unternehmensrichtlinie Datenschutz für Mitarbeiter	304
III. Richtlinien zur Nutzung durch Beschäftigte	319
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
IV. Löschkonzepte	395

E. Technische und organisatorische Datensicherheit

I. Überblick: Rationalisierung von Datenschutzthemen im Unternehmen	401
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
II. Technische und organisatorische Maßnahmen (Art. 32, 25 DS-GVO) ...	456
1. Anwendung bei interner Verarbeitung und Auftragsverarbeitung	456
2. Formular zur Prüfung der technischen und organisatorischen Maßnahmen	459
III. Prüfkontrolle	491
IV. Formular zur Prüfung von Berechtigungskonzepten	499

F. Rechte der betroffenen Person

I. Informationspflicht bei Erhebung von personenbezogenen Daten (Art. 13 f. DS-GVO)	509
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
II. Auskunftsrecht der betroffenen Person (Art. 15 DS-GVO)	579
1. Auskunftsverlangen der betroffenen Person	579
2. Antwort auf Auskunftsverlangen mit Recht auf Kopie (Art. 15 DS-GVO)	583
III. Recht auf Berichtigung (Art. 16 DS-GVO)	591
IV. Rechte auf Löschung und Mitteilung (Art. 17,19 DS-GVO)	595
1. Recht auf Löschung und „Recht auf Vergessenwerden“ (Art. 17 DS-GVO)	595
2. Informationspflicht an Dritte bei einem Löschungsersuchen (Art. 17 Abs. 2 DS-GVO)	598
V. Recht auf Einschränkung der Verarbeitung (Art. 18 DS-GVO)	603
VI. Recht auf Datenübertragbarkeit (Art. 20 DS-GVO)	606
G. Zusammenarbeit mit anderen Unternehmen	
I. Vereinbarung der Auftragsverarbeitung (Art. 28 f. DS-GVO)	611
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
II. Formulare während der Laufzeit der Auftragsverarbeitung (Art. 28 DS-GVO)	685
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
III. Fernwartung durch Drittunternehmen	704
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
IV. Vertraulichkeitsvereinbarungen	722
1. Vertraulichkeitsvereinbarung bei Dienstleistungsverträgen	722
2. Vertraulichkeitsvereinbarung bei M&A-Transaktionen	730
V. Gemeinsam für die Verarbeitung Verantwortliche (Art. 26 DS-GVO) ...	747
VI. Einsatz von Cloud Computing im Unternehmen	754

VII. Datentransfers in Drittstaaten	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	
I. Einwilligung durch Beschäftigte	803
1. Einwilligungserklärung zur Veröffentlichung von Mitarbeiterfotos ...	803
2. Einwilligungserklärung zur Speicherung von Bewerberdaten	809
II. Beschäftigtendatenschutz bei Arbeitsunfähigkeit und betrieblichem Eingliederungsmanagement	817
1. Betriebsvereinbarung zu Kranken- und BEM-Unterlagen	825
2. Einladungsschreiben zum BEM	848
III. Videoüberwachung auf Firmengeländen	854
1. Checkliste zur Videoüberwachung	856
2. Richtlinie und Betriebsvereinbarung zur Videoüberwachung im Betrieb	859
3. Eestlegungen vor Inbetriebnahme der Videoüberwachung	877
4. Maßnahmen zum Schutz der betroffenen Personen	883
5. Protokoll zur Auswertung von Videoaufnahmen	885
IV. Tor- und Spindkontrollen bei Beschäftigten	887
1. Checkliste zu Tor- und Spindkontrollen	889
2. Betriebsvereinbarung über die Durchführung von Tor- und Spindkontrollen	890
V. Detektiveinsatz gegen Beschäftigte	901
VI. Betriebsvereinbarung zum Terrorlisten-Screening	910
I. Kundendatenschutz	
I. Organisation des Kundendatenschutzes	927
II. Einwilligungen durch betroffene Personen	937
III. Einwilligung in Werbeversand/Newsletter	945
IV. Bonitätsprüfung natürlicher Personen	959
1. Bonitätsprüfung und Informationen bei Kaufverträgen	960
2. Darlehen-Selbstauskunft	969
3. Mieter-Selbstauskunft	978
4. Haushaltsrechnung natürlicher Personen	985
V. Checkliste bei polizeilichen Auskunftsverlangen	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