

Big Data und Recht

Einführung für die Praxis

von

Dr. iur. Maria Cristina Caldarola, LL.M., MBA

Prof. Dr. iur. Joachim Schrey

2019



Inhaltsverzeichnis

Vorwort	V
Abkürzungsverzeichnis	XIII
Legende	XV
Literaturverzeichnis	XVII
Abbildungsverzeichnis	XIX
A. Einführung	1
I. Warum Big Data?	1
II. Welche Daten sind betroffen?	1
III. Welche Unterschiede bestehen zwischen den Datenarten?	3
IV. Welche Prüfschritte sind bei einer Big Data-Anwendung zu beachten?	6
B. Datenarten	9
I. Personenbezogene Daten	10
1. Definition „Personenbezogene Daten“ gemäß Art. 4 Nr. 1 DS-GVO	10
2. Identifizierbarkeit bei personenbezogenen Daten (Beispiele)	12
a) Dynamische IP-Adressen	12
b) Personal- oder Kundennummern	13
c) VIN / KFZ-Kennzeichen	13
d) Besondere Kategorien personenbezogener Daten	13
e) Standort-, Verkehrs- und Nutzungsdaten	14
f) Besonderheiten spezifischer Datenquellen:	16
(1) Social-Media	16
(2) Open Data	18
(3) Datengewinnung durch Apps	18
II. Nicht-Personenbezogene Daten	19
III. Datenbanken und Sammelwerke	20
1. Sammlungen von Werken, Daten oder anderen unabhängigen Elementen, § 4 UrhG	21
2. Datenbankschutzrecht, §§ 87a, 87b UrhG	22
3. Schutz einzelner Elemente einer Datenbank oder eines Sammelwerks	24
a) Datenbankmodell	24
b) Datenformat	25
c) Schnittstelle	26
IV. Schutz als Geschäfts- oder Betriebsgeheimnis, § 17 UWG	26
V. Hausrecht in Bezug auf Sammeln von Sachdaten	27
VI. Virtuelles Hausrecht	28
VII. Mit IP-Adressen oder sonstigen identifizierenden Merkmalen verknüpfte Sachdaten	29
VIII. Kein Eigentum an Daten	30
C. Verantwortliche Stelle	33
I. Auftragsverarbeitung	34
1. Auftragsverarbeitungsvereinbarung	36
2. Pflicht zur Trennung der Datenbestände	37
3. Sonstige Pflichten eines Auftragsverarbeiters	37

4.	Sicherungsinstrumente zur Einhaltung datenschutzrechtlicher Verpflichtungen eines Auftraggebers von Big Data-Anwendungen in Bezug auf Auftragsverarbeiter	38
a)	Auswahl und Vorabkontrolle	38
b)	Auftragsverarbeitungsvereinbarung	39
II.	Gemeinsame Verantwortlichkeit für die Verarbeitung, Art. 26 DS-GVO	40
1.	Innerbetriebliches Verhältnis zwischen den gemeinsam Verantwortlichen	41
2.	Zurverfügungstellung der internen Vereinbarung	42
3.	Außerbetriebliches Verhältnis zwischen den gemeinsamen Verantwortlichen und den betroffenen Personen	42
III.	Dynamische Matrixstrukturen	42
1.	Projektbeteiligungen verschiedener verantwortlicher Stellen	42
2.	Arbeitnehmerabordnung / -überlassung	43
3.	Gemeinsame Verantwortlichkeit im Sinne von Art. 26 DS-GVO in Hinblick auf die Projektbeteiligungen.	44
IV.	Cloud Computing	44
1.	Speichern in der eigenen Cloud	45
2.	Nutzung von Cloud Storage Dritter	45
D.	Spezifische Anforderungen und Aufgaben des Datenschutzbeauftragten in Hinblick auf Big Data-Anwendungen	47
I.	Fachkunde	47
II.	Organisatorische und operative Einbindung des Datenschutzbeauftragten	47
III.	Kommunikation mit Betroffenen.	48
IV.	Informations- und Überwachungspflichten	48
V.	Kooperations- und Kontrollpflichten	49
VI.	Innerbetrieblicher Ablauf bei einer Datenschutzverletzung	49
E.	Legitimationsgrundlagen für die Verarbeitung von Daten (Erhebung, Bezug, Übermittlung, Auswertung und Kommerzialisierung)	51
I.	Gesetzliche Legitimationstatbestände für personenbezogene Daten	52
1.	Vertragserfüllungstatbestand	55
2.	Interessensabwägungstatbestand	56
3.	Betriebsvereinbarungen	57
4.	Einwilligung	58
a)	Einwilligungserklärung	60
b)	Formale Anforderungen	60
c)	Freiwilligkeit	61
d)	Hinweis auf den Zweck der Erhebung und Verarbeitung.	62
e)	Übermittlung an Dritte insbesondere in das EU-Ausland	63
f)	Widerruflichkeit	64
g)	„Opt in“- und „Opt out“-Lösungen	66
II.	Verarbeitung von nicht personenbezogenen Sachdaten.	66
1.	Verarbeitung von Sachdaten.	66
2.	Bezug von Daten aus Datensammlungen/Datenbanken.	67
3.	Bezug von Daten aus Open Data-Projekten	68
4.	Daten aus öffentlich zugänglichen Quellen.	68
F.	Datenverarbeitung und Datenzyklus (Ebene des Datenzwecks)	69
I.	Datenverarbeitung	69
II.	Lebenszyklus eines Datums	69
III.	Erhebung personenbezogener Daten zu ursprünglich anderen Zwecken als ihre Verwertung in Big Data-Anwendungen – die Zweckänderung	71

1. Der Zweck der Datenerhebung und -verarbeitung	71
2. Der „Zweck“ bei Verträgen über die Lieferung und Nutzung von Daten	72
3. Das Problem der dynamischen Zweckänderung bei Big Data- Anwendungen	73
a) Die Verbindung zwischen dem ursprünglichen und dem neuen Zweck	74
b) Der Zusammenhang der Datenerhebung	75
c) Die Art der personenbezogenen Daten	75
d) Die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen	75
e) Das Vorhandensein geeigneter Garantien	75
G. Drittstaatentransfer / Anwendbares Recht (Ebene des anwendbaren Rechts)	77
H. Aufbau einer Big Data-Anwendung	81
I. Erhebung von Daten	82
II. Bezug und Erwerb von Daten bei Datendienstleistern	82
1. Rechtmäßigkeit der Erhebung Daten durch den Datenlieferanten	82
2. Rechtmäßigkeit des Datenbezugs von Dritten	83
3. Heilung von Mängeln	83
III. Kombination von Daten	84
1. Zulässigkeit der Kombination von unterschiedlichen Datenkategorien auf der Ebene des Datenbezugs	87
2. Kombination von personenbezogenen Daten aus verschiedenen Datenquellen	87
3. Kombination von personenbezogenen Daten mit Sachdaten bzw. anonymen Daten	88
4. Kombination von personenbezogenen Daten aus unterschiedlichen Herkunftsländern	88
5. Kombination von unterschiedlichen personenbezogenen Daten, die aufgrund von unterschiedlichen Zwecken erhoben wurden	89
6. Heilung von Mängeln	92
IV. Den Spielraum erweitern: Anonymisierung/Pseudonymisierung der in einer Big Data-Datenbank gespeicherten Daten	94
1. Pseudonymisierung (Art. 4 Nr. 5 DS-GVO)	94
2. Anonymisierung	97
3. Verschlüsselung und Geheimhaltung	100
4. Reanonymisierung bei hoher Menge von Daten, die eine Re-Identifizierung erlauben	100
5. Data Trustee	101
a) Anforderungen an einen Datentreuhänder	102
b) Vertragsstrafe bei Verletzung der Pflichten oder zur Überwindung von gemeinsamen Managementkontrollen	103
V. Übermittlung von Daten mehrerer verantwortlicher Stellen an eine zentrale Big Data-Anwendung	103
VI. Auswertung und Analyse von Daten	104
1. Legitimationstatbestände für die Auswertung und Analyse personenbezogener Daten	104
2. Big Data-Anwendungen zur Analyse von Daten mit Bezug auf Beschäf- tigte oder Bewerber	105
a) Bewerberanalyse	105
aa) Erhebung und Verarbeitung von Beschäftigendaten zur Erarbei- tung von Algorithmen in People Analytics-Anwendungen	106
(1) Für Beschäftigendaten spezifische Legitimation:	106

(2) Legitimation durch Interessenabwägungstatbestand:	106
(3) Legitimation durch Einwilligung:	107
bb) Analyse von Bewerberdaten in People Analytics-Anwendungen .	108
b) Arbeitnehmeranalyse	108
aa) Analysen zum Zweck der Mitarbeiterbindung	109
bb) People Analytics-Anwendung mit Bezug auf Daten aus sozialen Netzwerken	109
cc) People Analytics-Anwendung mit Bezug auf sonstige öffentlich zugängliche Daten	109
dd) Grenzen von People Analytics-Anwendungen	109
c) Stress- und Stimmungsanalysen	110
d) Datenbanken zur Analyse von Projekten	110
e) Verbot von ausschließlich automatisiert generierten Einzelentschei- dungen	111
3. Betriebsvereinbarungen	111
4. Mitwirkungsrechte des Betriebsrats in Hinblick auf § 87 Abs. 1 Nr. 6 BetrVG	112
5. Sonderfälle	113
a) Scoring	113
b) Nutzerprofile	114
VII. Fortbestand des Personenbezugs nach Auswertung und Analyse von Daten	114
1. Analyse von personenbezogenen Datensätzen, soweit Personenbezug noch vorhanden oder wiederherstellbar	114
2. Auswertung von pseudonymisierten Datensätzen	115
3. Auswertung von nicht personenbezogenen Daten, Sachdaten oder anonymisierten Daten	115
VIII. Verwertung von personenbezogenen Daten bzw. personenbezogenen Aus- wertungs-/Analyseergebnissen	116
I. Löschungspflichten	117
I. Erarbeitung eines Löschkonzeptes	120
II. Umsetzung des Löschkonzeptes	121
III. Was sind die notwendigen Inhalte eines Löschkonzeptes?	121
1. Beschreibung von Aufbewahrungs- und Löschpflichten	121
2. Was ist das maßgebliche Recht zur Bestimmung von Aufbewahrungs- und Löschpflichten	121
3. Gesetzliche Aufbewahrungspflichten	122
4. Löschfristen bei Archivierung von Daten aufgrund einer Einwilligung	122
5. Herleitung von Löschfristen dem Verwendungszweck, den dafür geltenden gesetzlichen Bestimmungen und dem Geschäftsprozessbezug der verarbeiteten Daten	123
6. Datenarten, bei denen der Verwendungszweck die Maßgabe für die Bemessung der Aufbewahrungsdauer abgibt	123
a) Bestimmung eines Zwecks und dazugehörige Legitimationsgrundle- ge bei personenbezogenen Daten	123
b) Verwendungszweck und Aufbewahrung von nicht personenbezoge- nen Daten	123
IV. Startzeitpunkte von Aufbewahrungs- und Löschpflichten	124
V. Zuordnung von Datenarten zu Löschklassen	125
VI. Auflösung von Konflikten bei Verwendung einer Datenart in verschiede- nen Datenobjekten	125
VII. Was bedeutet „Löschen“ von Daten und was dagegen deren „Sperrung“, „Maskierung“, „Pseudonymisierung“ oder „Anonymisierung“?	126

VIII.	Pflicht zur Löschung personenbezogener Daten gegenüber der betroffenen Person	128
	1. Lösungsgründe	128
	a) Personenbezogene Daten	128
	b) Nicht personenbezogene Daten	129
	2. Lösungszeitpunkt	130
	3. Ausschlussgründe	130
	4. Recht auf „Vergessenwerden“	131
	5. Recht auf Einschränkung der Verarbeitung	131
IX.	Löschpflichten gegenüber Lizenzgebern, Datenlieferanten etc. unabhängig vom Dateninhalt	132
X.	Generalisierende Festsetzung einer einheitlichen Löschfrist über alle Dokumente und Daten	132
XI.	Löschpflichten bei länderübergreifender Datenverarbeitung	133
XII.	Speicherorte und Löschpflichten	134
XIII.	Vier-Augen-Prinzip und Dokumentation	135
J.	Typischerweise bei Big Data-Anwendungen besonders relevante Betroffenenrechte nach der DS-GVO	137
I.	Informationspflichten gemäß § 4 Abs.3 BDSG bzw. Art. 13, 14 DS-GVO ..	137
II.	Betroffenenrechte gemäß Art. 15 ff. DS-GVO	139
	1. Auskunftsrechte	140
	2. Berichtigungsrecht	140
	3. Recht auf Löschung und „Vergessenwerden“	140
	4. Recht auf Einschränkung der Verarbeitung	141
	5. Recht auf Datenübertragbarkeit	141
	6. Beschwerderecht	141
III.	Verarbeitungsverzeichnis gemäß Art. 30 DS-GVO	142
IV.	Umsetzung technischer und organisatorischer Maßnahmen zum Schutz personenbezogener Daten vor unbefugtem Zugriff	143
	1. Zutrittskontrolle	144
	2. Zugangskontrolle	145
	3. Zugriffskontrolle	145
	4. Datenträgerkontrolle	146
	5. Zugriffs- und Benutzerkontrolle	146
	6. Weitergabe-, Übertragungs- und Transportkontrolle	146
	7. Eingabe- und Speicherkontrolle	147
	8. Auftragskontrolle	147
	9. Verfügbarkeitskontrolle	147
	10. Trennungskontrolle	148
	11. Wiederherstellbarkeit	148
	12. Zuverlässigkeit	148
	13. Datenintegrität	149
	14. Sanktion bei nicht vorhandenen oder unzureichenden technischen und organisatorischen Maßnahmen	149
V.	Allgemeine Grundsätze für die Verarbeitung personenbezogener Daten in Art.5 DS-GVO	149
	1. Allgemeine Grundsätze der Verarbeitung personenbezogener Daten ..	149
	2. Grundsatz der Rechenschaftspflicht (Art. 5 Abs.2 DS-GVO)	150
	3. Sanktionierung der Verletzung auch dieser Grundsätze trotz ihrer allgemeinen Formulierung	150
K.	Datenschutzfolgeabschätzung	151

L. Systemdatenschutz beim Betrieb von Big Data-Anwendungen	153
I. Systemdatenschutz bei personenbezogenen Daten	153
1. Grundrecht auf informationelle Selbstbestimmung	153
2. Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme.	154
3. Mittelbare Grundrechtswirkung zwischen Privaten; Auslegung von Normen.	154
4. Sicherstellung der Vertraulichkeit durch technisch-organisatorische Maßnahmen	155
II. Systemdatenschutz bei ausschließlich nicht personenbezogenen Daten in einer Big Data-Anwendung	157
M. Schutz von Big Data-Anwendungen im Unternehmen	159
I. Technische und organisatorische Maßnahmen	159
II. Schutz der der Big Data-Anwendung zugrunde liegenden Algorithmen.	159
III. Compliance Management-System	160
IV. Urhebervertragsrechtliche Aspekte beim genutzten Datenbankmanage- mentsystem	161
N. Rechtsfolgen bei Missachtung der in diesem Leitfaden erläuterten rechtli- chen Anforderungen	163
I. Sanktionen bei Verletzung datenschutzrechtlicher Bestimmungen	164
1. Bußgeld	164
2. Materieller und immaterieller Schadenersatz ergänzt durch Ver- bandsklagebefugnis.	166
3. Ordnungswidrigkeiten gemäß §§ 30, 130 OWiG	166
4. Eintrag in Gewerbezentralregister (Verlust der Berechtigung zur Teil- nahme an öffentlichen Ausschreibungen).	166
5. Strafbarkeiten gemäß BDSG n. F.	167
6. Aufsichtliche Eingriffsrechte der Datenschutzaufsichtsbehörden	167
II. Rechtsfolgen bei der Verletzung von Urheberrechten an Sammelwerken oder Datenbankschutzrechten	168
1. Unterlassungsansprüche	168
2. Schadenersatzansprüche	168
3. Durchsetzung urheberrechtlicher Ansprüche	169
4. Vernichtungsanspruch	169
5. Haftung des Unternehmens	170
6. Hilfsansprüche	170
7. Straftatbestände	170
III. Verletzung des virtuellen Hausrechts.	170
1. Unterlassungsansprüche	170
2. Schadenersatzansprüche	171
3. Hilfsansprüche	171
4. Strafrechtliche Relevanz	171
IV. Sanktionen wegen des Verrats von Geschäfts- oder Betriebsgeheimnissen gemäß § 17 UWG	171
1. Vorrangig strafrechtliche Sanktionen	171
2. Zivilrechtliche Ansprüche	172
V. Vertragliche Ansprüche	172
O. Big Data-Anwendungen als Service	175
P. Handlungsempfehlungen	181
Stichwortverzeichnis	183