Praxishandbuch

DSGVO

einschließlich BDSG und spezifischer Anwendungsfälle

Herausgegeben von

Dr. Flemming Moos

Rechtsanwalt, Fachanwalt für IT-Recht, Hamburg

Dr. Jens Schefzig

Rechtsanwalt, Hamburg

Dr. Marian Alexander Arning

LL.M., Dozent, Türkisch-Deutsche Universität, Istanbul

2., komplett überarbeitete und erweiterte Auflage 2021

Bearbeitet von

Dr. Marian Alexander Arning, LL.M.; Dr. Ulrich Baumgartner, LL.M. (King's College London); Ingo Braun; Cay Lennart Cornelius; Eva Gardyan-Eisenlohr, D.I.A.P. (ENA, Paris); Dr. Tina Gausling, LL.M. (Columbia University); Stephan Hansen-Oest; Carmen Heinemann; Per Meyerdierks; Dr. Flemming Moos; Leif Rohwedder; Dr. Tobias Rothkegel; Dr. Jens Schefzig; Laurenz Strassemeyer; Dr. Anna Zeiter, LL.M. (Stanford)

Fachmedien Recht und Wirtschaft | dfv Mediengruppe | Frankfurt am Main

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

ISBN 978-3-8005-1728-2

dfv Mediengruppe

© 2021 Deutscher Fachverlag GmbH, Fachmedien Recht und Wirtschaft, Frankfurt am Main
www.ruw.de

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Satzkonvertierung: Lichtsatz Michael Glaese GmbH, 69502 Hemsbach

Druck und Verarbeitung: Eberl & Koesel GmbH & Co. KG, 87452 Altusried-Krugzell

Printed in Germany

Kapitel 2

Grundlagen des Datenschutzrechts

Übersicht

	Rn.
I. Datenschutz im Anwendungsbereich des EU-Rechts	1
II. Schutzgut des Datenschutzrechts	3
1. Schutz der natürlichen Personen	4
2. Schutz des freien Datenverkehrs	7
III. Grundbegriffe des Datenschutzrechts	10
1. Personenbezug	10
2. Datenverarbeitung	14
3. Verantwortlicher	15
IV. Zusammenspiel mit anderen Rechtsmaterien	17
1. Wettbewerbsrecht	19
2. Kartellrecht	21
a) Missbräuchliche Nutzung von Kundendaten	22
b) Missbräuchliche Zugangsverweigerung zu Daten	25
c) AGB-Recht	26
3. Besonderer Geheimnisschutz	30
a) Berufsrechtliche Schweigepflichten	31
b) Strafrechtliche Schweigepflichten	32
c) Fernmeldegeheimnis	34
d) Schutz von Geschäftsgeheimnissen	36
4. Arbeits- und Mitbestimmungsrecht	39
a) Umfang von Datenerhebungen im Bewerbungsgespräch	40
b) Betriebsvereinbarungen als datenschutzrechtliche Erlaubnisvorschrift	43
c) Einsicht in Personalakten	44
d) Kündigungsschutz für Datenschutzbeauftragte	46

I. Datenschutz im Anwendungsbereich des EU-Rechts

Für die Unternehmenspraxis, an die sich dieses Buch maßgeblich richtet, ist vor allem derjenige Teil des Datenschutzrechts relevant, der die Verarbeitung von Daten eben durch private Wirtschaftsunternehmen betrifft. Dieser Bereich ist durch einen grundsätzlichen **Vorrang des Europarechts** – und mit ihm sowohl des Sekundärrechts (einschließlich der DSGVO) als auch der EU-Grundrechtsverbürgungen – vor dem nationalen Recht geprägt. Die relevanten Grundlagen des Datenschutzrechts – einschließlich der jeweiligen Grundrechtsverbürgungen – ergeben sich insoweit aus dem Unionsrecht. **1**

Praxishinweis

Deshalb gelten nur für Datenverarbeitungsvorgänge außerhalb des Anwendungsbereichs des primären und sekundären Unionsrechts weiter direkt etwaige nationale Grundrechtsverbürgungen, also z. B. auch das vom BVerfG

entwickelte „Recht auf informationelle Selbstbestimmung". Im Anwendungsbereich des EU-Rechts gilt hingegen ein grundsätzlicher Vorrang der EU-Datenschutzgrundrechte.

2 Eine Einschränkung von diesen Grundsätzen gilt dort, wo das Unionsrecht Umsetzungsspielräume eröffnet – im Falle der DSGVO also bei den Öffnungsklauseln, die den Mitgliedstaaten konkretisierende Regelungen gestatten. Bei nationalen Gesetzen, die von diesen Öffnungsklauseln Gebrauch machen, können auch die nationalen Grundrechtsverbürgungen beachtenswert sein.[1]

II. Schutzgut des Datenschutzrechts

3 Das EU-Datenschutzrecht verfolgt im Wesentliche zwei Ziele: Zum einen dient es dazu, die Menschen (also im juristischen Sprachgebrauch „natürliche Personen") bei der Verarbeitung der sie betreffenden Daten zu schützen. Zum anderen soll die das Datenschutzrecht mittlerweile sehr wesentlich prägende DSGVO aber auch den freien Datenverkehr innerhalb der EU sicherstellen.[2]

1. Schutz der natürlichen Personen

4 Im Kern des Datenschutzrechts steht der **Schutz der natürlichen Personen, auf die sich die Daten beziehen**. Anders als der Begriff „Datenschutz" es nahelegt, geht es primär also nicht um den Schutz der Daten an sich, sondern um die dahinterstehende Person. Teilweise besteht hier freilich eine Wechselwirkung: So umfasst das Datenschutzrecht z. B. auch Vorgaben für die Gewährleistung der Datensicherheit,[3] weil durch eine ungewollte Veröffentlichung von Daten nicht nur deren Integrität, sondern auch die Rechte der betroffenen Person beeinträchtigt werden können.

5 Das Schutzgut ist sogar grundrechtlich verankert: namentlich in dem **Grundrecht auf Schutz personenbezogener Daten** nach **Art. 8 der EU-Grundrechte-Charta (GrCh)**.[4] Danach hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten. Hierauf nehmen die ErwG 1 und 2 DSGVO

1 Zu Einzelheiten dieser „konkurrierenden Mehrfachbindung" und der einschlägigen Rechtsprechung des BVerfG ausführlich: BeckOK-DS/*Schneider*, Syst. B Rn. 11.

2 Vgl. Art. 1 Abs. 1 DSGVO.

3 Zur Datensicherheit siehe Kap. 13.

4 Quasi als Vorbilder für diese Grundrechtsverbürgung gelten im Wesentlichen die Europarats-Konvention Nr. 108 und auch Art. 8 EMRK; daneben gibt es teilweise vergleichbare Grundrechtsverbürgungen in den mitgliedstaatlichen Verfassungen; vgl. *Knecht*, in: Schwarze/Becker/Hatje/Schoo, EU-Kommentar, 4. Aufl. 2019, Art. 8 GrCh Rn. 1.

unmittelbar Bezug und legen es als das Hauptziel der DSGVO fest, das Grundrecht auf Schutz personenbezogener Daten ungeachtet der Staatsangehörigkeit und des Aufenthaltsortes der betroffenen Person zu wahren.

Der **grundrechtliche Kerngehalt** des „Rechts auf Datenschutz" besteht aus drei Säulen und ergibt sich aus Art. 8 Abs. 2 GrCh. Danach dürfen diese Daten nur (1) nach Treu und Glauben, (2) für festgelegte Zwecke und (3) mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Auch das Recht jeder Person, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken, ist grundrechtlich verankert. Schließlich ist grundrechtlich die Überwachung durch eine unabhängige Stelle vorgegeben. **6**

Praxishinweis

Der EuGH legt die DSGVO regelmäßig im Lichte der GRCh einschließlich des Art. 8 GrCh aus; so hat er zuletzt in seinem Urteil vom 16.7.2020 (Rs. C-311/18) in Sachen *Schrems II*[5] Art. 45 DSGVO im Lichte der in Art. 7, 8 und 47 verbrieften Garantien der GRCh ausgelegt und konstatiert, dass die verfahrensgegenständliche Übermittlung personenbezogener Daten in einen Drittstaat regelmäßig u. a. in das Recht auf Schutz personenbezogener Daten (Art. 8 Abs. 1 GRCh) eingreife.

2. Schutz des freien Datenverkehrs

Ein weiteres Schutzgut der DSGVO besteht in der Gewährleistung eines **freien Datenverkehrs** innerhalb der EU. Nach Art. 1 Abs. 3 DSGVO darf der freie Verkehr personenbezogener Daten in der Union aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden. **7**

Die DSGVO untersagt es also Mitgliedstaaten, eigenständig nationale Maßnahmen zum Schutz personenbezogener Daten zu ergreifen und diese Beschränkung der Grundfreiheiten mit dem Bestreben nach einem höheren Schutzniveau zu rechtfertigen.[6] Ebenso ist es den Mitgliedstaaten verwehrt, das Datenschutzniveau eines anderen Mitgliedstaats als nicht ausreichend zu qualifizieren; Datenverarbeitungen in einem anderen Mitgliedstaat müssen identisch zu solchen innerhalb des eigenen Mitgliedstaates behandelt werden.[7] **8**

5 Siehe Kap. 19 Rn. 96.
6 BeckOK-DS/*Schantz*, Art. 1 DSGVO Rn. 9.
7 Paal/Pauly/*Ernst*, Art. 1 DSGVO Rn. 14.

Beispiel

Aus diesem Grund sind z. B. mitgliedstaatliche Vorschriften untersagt, die aus Gründen eines besseren Datenschutzes eine Speicherung von Daten im Inland verlangen.

9 Zulässig bleiben jedoch solche Schutzmaßnahmen der Mitgliedstaaten, die anderen Zielsetzungen als einem höheren Datenschutzstandard folgen, auch wenn sie de facto zu einer Einschränkung des freien Datenverkehrs führen.[8] Die Abgrenzung kann in Einzelfall sehr schwierig sein.[9]

III. Grundbegriffe des Datenschutzrechts

1. Personenbezug

10 Das wichtigste Merkmal zur Definition des Anwendungsbereichs – und damit auch zur Abgrenzung von anderen Rechtsmaterien – ist der „Personenbezug" der Daten. Nur wenn Daten einen solchen Personenbezug aufweisen, unterfallen sie der DSGVO und den sonstigen Datenschutzvorschriften.

11 Der für das gesamte Datenschutzrecht zentrale Begriff des „**personenbezogenen Datums**" ist in Art. 4 Nr. 1 DSGVO definiert. Demnach ist Personenbezug dann gegeben, wenn sich die jeweilige Information auf eine natürliche Person und nicht ausschließlich auf Sachen bezieht. Die Person muss durch die Information identifiziert oder zumindest identifizierbar sein.

Beispiel

In Abgrenzung zu personenbezogenen Daten haben Sachdaten keinen Personenbezug; bspw. „Das Handy ist mit einer 16 Megapixel Kamera ausgestattet." Entsprechend kann auch keine Person identifiziert werden.[10]

12 Wenn die natürliche Person nicht unmittelbar aus den Informationen des Datums identifiziert werden kann, ist ein Bezug dennoch gegeben, wenn eine entsprechende Identifizierung mit Hilfe von Verknüpfungen mit weiteren Informationen hergestellt werden kann.[11]

---

8 Mitteilung der Europäischen Kommission, Building a European Data Economy, COM(2017) 9 final, S. 5; Ehmann/Selmayr/*Zerdick*, Art. 1 DSGVO Rn. 13.

9 BeckOK-DS/*Schantz*, Art. 1 DSGVO Rn. 9.

10 Taeger/Gabel/*Arning/Rothkegel*, Art. 4 DSGVO Rn. 9.

11 Taeger/Gabel/*Arning/Rothkegel*, Art. 4 DSGVO Rn. 30.

Das Gegenstück zu personenbezogenen Daten sind **anonyme Daten**. Wann ein ausreichender „Grad an Anonymität" gegeben ist, so dass die DSGVO unanwendbar ist, ist in der Praxis häufig nicht leicht festzustellen. Grundsätzlich gilt, dass Anonymität bei Informationen vorliegt, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder bei personenbezogenen Daten, die (nachträglich) in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Anonyme Daten sind gemäß Erwägungsgrund 26 Satz 5 und 6 nicht vom Anwendungsbereich der DSGVO umfasst.[12] **13**

Praxishinweis

Denkbare Vorgehensweisen zur Anonymisierung:[13]

- Löschung von identifizierenden Merkmalen (Name, Adresse, Bankverbindung),
- Aggregation von Daten,
- Bildung von Gruppen und/oder die kontrollierte Einbringung von Zufallsfehlern.

2. Datenverarbeitung

Ein weiteres bedeutsames Merkmal zur Bestimmung des Anwendungsbereichs ist die „Datenverarbeitung" gem. Art. 4 Nr. 2 DSGVO. Die DSGVO fasst unter dem Merkmal der Datenverarbeitung eine ganze Reihe von Nutzungsvorgängen zusammen:[14] Umfasst ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie **14**

- das Erheben;
- das Erfassen;
- die Organisation;
- das Ordnen;
- die Speicherung;
- die Anpassung oder die Veränderung;
- das Auslesen;
- das Abfragen;
- die Verwendung;
- die Offenlegung durch Übermittlung;

12 Taeger/Gabel/*Arning/Rothkegel*, Art. 4 DSGVO Rn. 47.
13 Kühling/Buchner/*Klar/Kühling*, Art. 4 DSGVO Rn. 34.
14 Paal/Pauly/*Ernst*, Art. 4 DSGVO Rn. 20.

- die Verbreitung oder eine andere Form der Bereitstellung;
- der Abgleich oder die Verknüpfung;
- die Einschränkung;
- das Löschen oder die Vernichtung.

Praxishinweis

Ein automatisiertes Verfahren liegt vor, wenn bestimmte Aufgaben mit Hilfe einer informationstechnischen Infrastruktur, wie z. B. Hardware, Software oder Übertragungsnetze, unter Einbeziehung personenbezogener Daten wahrgenommen werden (bspw. über PCs, Netzwerke mit Servern, Notebooks, Smartphones oder auch den Einsatz digitaler Kamerasysteme etc.).

Weiterhin sollte darauf geachtet werden, dass das „aufbau- und ablauforganisatorische Umfeld" in seiner Gesamtheit berücksichtigt wird. Dazu zählen Speichermedien, wie Disketten, USB-Sticks, externe Festplatten und CDs, aber auch Videokameras, Kopierer, Multifunktionsgeräte sind Datenverarbeitungsanlagen. Diese spielen bei der Beurteilung eine Rolle, da dort personenbezogene Daten zwischengespeichert oder gar langfristig gespeichert werden können.[15]

Ein nicht-automatisiertes Verfahren ist bei einer manuellen Verarbeitung gegeben. Trotz manueller Verarbeitung werden von der DSGVO dennoch sog. Dateisysteme gem. Art. 4 Nr. 6 DSGVO erfasst, also z. B. Karteien. Nicht umfasst bleiben allerdings unstrukturierte Akten, Aufzeichnungen oder Notizen, wie z. B. Papierakten, in denen die Daten selbst nicht strukturiert sind.[16]

3. Verantwortlicher

15 Der zentrale Begriff zur Bestimmung des persönlichen Anwendungsbereichs der DSGVO ist derjenige des Verantwortlichen. Der Verantwortliche ist der hauptsächliche Träger der Pflichten nach der DSGVO. Der Begriff des Verantwortlichen ist in Art. 4 Nr. 7 DSGVO definiert. Verantwortlicher ist danach derjenige, der alleine oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.[17] Dies kann eine natürliche oder juristische Person, eine Behörde, Einrichtung oder andere Stelle sein. Eine solche Verantwortlichkeit kann sich für jeden, der Daten für *sich* verarbeitet, ergeben. Letzteres unterscheidet den Verantwortlichen auch vom Auftragsverar-

15 BeckOK-DS/*Schild*, Art. 4 DSGVO Rn. 34.
16 BeckOK-DS/*Schild*, Art. 4 DSGVO Rn. 33.
17 Paal/Pauly/*Ernst*, Art. 4 DSGVO Rn. 55.

beiter,[18] der Daten nicht für sich selbst, sondern lediglich „im Auftrag" und auf Weisung eines Verantwortlichen verarbeitet.

Der Begriff des Verantwortlichen ist auch nicht auf eine einzelne Stelle limitiert. Denkbar ist gem. Art. 26 Abs. 1 Nr. 1 DSGVO eine **gemeinsame Verantwortlichkeit**.[19] Eine solche ist dann gegeben, wenn zwei oder mehrere Stellen gemeinsam über die Zwecke und Mittel der Datenverarbeitung entscheiden. Dies ist gekennzeichnet durch eine gemeinsame Kontrolle über die Datenverarbeitungsprozesse, wobei die Verantwortlichen hierbei grundsätzlich auch einen gemeinsamen Zweck verfolgen müssen.[20] Für die gemeinsame Kontrolle bedarf es keiner gleichberechtigten oder gleichmäßigen Verantwortung, vielmehr können die Verantwortlichen unterschiedlich stark und in unterschiedlicher Weise in die Datenverarbeitung eingebunden sein.[21] **16**

IV. Zusammenspiel mit anderen Rechtsmaterien

Das Datenschutzrecht fokussiert – wie gezeigt – auf den Schutz natürlicher Personen bei der Verarbeitung der auf sie bezogenen Daten. Vor allem der vorstehend erläuterte „**Personenbezug**" grenzt das Datenschutzrecht von anderen rechtlichen Vorgaben im Umgang mit Informationen (ohne Personenbezug) im Unternehmen ab. Daneben grenzt der Begriff der „**Datenverarbeitung**" das Datenschutzrecht von anderen rechtlichen Vorgaben im Hinblick auf den Umgang mit den jeweiligen Personengruppen – also im Wesentlichen Kunden und Mitarbeiter (ohne Bezug zu einer **Datenverarbeitung**) – ab. **17**

In der Unternehmensrealität müssen die **verschiedenen rechtlichen Anforderungen** aber zumeist in Deckung gebracht werden und das Datenschutzrecht bildet nur eine Facette, die bei der Umsetzung einer konkreten Maßnahme zu beachten ist. Nachfolgend soll deshalb ein grober Überblick über typische „**Schnittmengen**" mit anderen Rechtsbereichen gegeben werden, um für das Zusammenspiel mit anderen Regelungsmaterien die notwendige Sensibilität zu erzeugen: **18**

1. Wettbewerbsrecht

Eine Schnittmenge des Datenschutzrechts zum Wettbewerbsrecht besteht insbesondere im Bereich der Werbung. In Deutschland gilt es im Hinblick auf belästi- **19**

18 Zur Auftragsverarbeitung siehe Kap. 7.
19 Zur gemeinsamen Verantwortlichkeit s. Kap. 8 Rn. 3 ff.
20 BeckOK-DS/*Spoerr*, Art. 26 DSGVO.
21 BeckOK-DS/*Spoerr*, Art. 26 DSGVO; EuGH, EuZW 2018, 534, 537 Rn. 43.

gende Werbung, die lauterkeitsrechtliche Regelung des § 7 UWG zu berücksichtigen. Dabei gilt, dass gem. § 7 UWG z. B. E-Mail-Werbung nur zulässig ist, soweit eine vorherige ausdrückliche Einwilligung i. S. v. § 7 Abs. 2 Nr. 3 UWG vorliegt oder die Voraussetzungen des § 7 Abs. 3 UWG erfüllt sind. Im Verhältnis zur DSGVO ergeben sich im Hinblick auf die Voraussetzungen der Einwilligung im Direktmarketing hierbei spezielle Anforderungen.[22]

Praxishinweis

Gerade bei Werbeaktionen, wie z. B. Gewinnspielen und Newslettern etc., muss den Anforderungen beider Rechtsbereiche entsprochen werden. Bei einer Zusendung von Werbung via E-Mail handelt es sich gemäß § 7 Abs. 1, Abs. 2 Nr. 3 UWG um eine unzulässige Belästigung, es sei denn, es liegt eine vorherige ausdrückliche Einwilligung des Adressaten hierzu vor. Selbiges gilt z. B. bei Werbung mit einem Telefonanruf gegenüber einem Verbraucher, § 7 Abs. 1, Abs. 2 Nr. 2 UWG.

20 Die datenschutzrechtliche Wertung folgt dabei grundsätzlich der wettbewerbsrechtlichen Bewertung: Soweit das UWG eine (z. B. postalische) Kontaktaufnahme ohne vorherige Einwilligung explizit gestattet, wird regelmäßig auch die Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO zugunsten des Verantwortlichen ausgehen. Insoweit ist zu berücksichtigen, dass die Regelung in § 7 UWG großteils der Umsetzung des Art. 13 RL 2002/58/EG dient – es sich europarechtlich also um datenschutzrechtliche Regelungen handelt, auch wenn der deutsche Gesetzgeber sich für eine Umsetzung im UWG entschieden hat.

2. Kartellrecht

21 Auch das Kartellrecht weist Schnittmengen mit dem Datenschutzrecht auf. Vor allem steht hierbei die Fragestellung des Marktmissbrauchs durch unfaire Datenverarbeitungspraktiken oder durch Verweigerung des Zugangs zu bestimmten Daten im Vordergrund.[23]

a) Missbräuchliche Nutzung von Kundendaten

22 Dies verdeutlichte das Bundeskartellamt mit seiner Facebook-Entscheidung, in der es erstmals einen sog. Konditionenmissbrauch aus einer Datenschutzverletzung ableitete.[24] Die Behörde untersagte dem sozialen Netzwerk, Nutzungsbe-

22 Auer-Reinsdorff/Conrad/*Conrad/Treeger*, § 34 Rn. 503.
23 Taeger/*Louven*, DSRITB 2019, 703, 708 f.
24 BKartA, BeckRS 2019, 4895.

dingungen zu verwenden, die ohne Einwilligung der Nutzer eine Zusammenführung von Nutzerdaten über verschiedene Produkte und Drittangebote hinweg beinhalteten.

Nach Auffassung des Bundeskartellamts verstieß Facebook als marktbeherrschendes Unternehmen für soziale Netzwerke für private Nutzer in Deutschland dadurch gegen das kartellrechtliche Verbot des Missbrauchs einer marktbeherrschenden Stellung gem. § 19 Abs. 1 GWB, dass die Registrierung von einer Einwilligung in Nutzungskonditionen abhängig gemacht wurde, die mit datenschutzrechtlichen Anforderungen unvereinbar sei. Infolgedessen sei die Einwilligung nicht wirksam und entsprechende Datenverarbeitungen unzulässig. **23**

Die aufschiebende Wirkung der Verfügung ist zwar vom OLG Düsseldorf mit Entscheidung vom 26.8.2019 im Eilverfahren wieder hergestellt worden, so dass das Unternehmen bis zum Abschluss des Beschwerdeverfahrens die Untersagungsverfügung nicht umsetzen muss.[25] Dies begründete das OLG Düsseldorf damit, dass Facebook zwar womöglich marktbeherrschend sei, aber die Datenverarbeitung keinen relevanten Wettbewerbsschaden bewirke.[26] Weiterhin sei der erforderliche Kausalzusammenhang zwischen Nutzungsbedingungen und Marktstellung nicht hinreichend nachgewiesen worden.[27] Mit anderen Worten: Selbst wenn die beanstandete Datenverarbeitung gegen Datenschutzbestimmungen verstößt, liege darin nicht zugleich ein Verstoß gegen das Kartellrecht. Diese Entscheidung wird im Schrifttum kritisiert[28]; das letzte Wort ist hier also noch nicht gesprochen. **24**

b) Missbräuchliche Zugangsverweigerung zu Daten

Auch unter dem Aspekt der missbräuchlichen Verweigerung des Zugangs zu bestimmten (ggf. auch personenbezogenen) Daten besteht ein Berührungspunkt zum Kartellrecht. Hierzu gibt es jedoch erst wenige Entscheidungen; ein praxisrelevantes Beispiel bildet der Zugang unabhängiger Marktteilnehmer auf dem Kfz-Teilemarkt zu bestimmten bei Fahrzeugherstellern vorhandenen Daten einschließlich der Fahrzeugidentifikationsnummer.[29] **25**

25 OLG Düsseldorf, Beschl. v. 26.8.2019 – VI-Kart 1/19 (V), MMR 2019 Rn. 742.
26 OLG Düsseldorf, Beschl. v. 26.8.2019 – VI-Kart 1/19 (V), MMR 2019 Rn. 18.
27 OLG Düsseldorf, Beschl. v. 26.8.2019 – VI-Kart 1/19 (V), MMR 2019 Rn. 45.
28 Vgl. *Bunte*, EWiR 2019, 575.
29 OLG Frankfurt, GRUR-RR 2017, 231.

Praxishinweis

Beide Entscheidungen sind für die Praxis von höchster Relevanz: Die Entscheidungen des Bundeskartellamts und des OLG Düsseldorf offenbaren, wie kartellrechtliche Wertungen durch die DSGVO (insbesondere über die Auslegung von Erlaubnistatbeständen der DSGVO) beeinflusst werden können.

c) AGB-Recht

26 Auch das AGB-Recht hat starke Bezüge zum Datenschutzrecht. Dies ist dem Umstand geschuldet, dass die Verarbeitung personenbezogener Daten durch Unternehmen in vielen Fällen im Zusammenhang mit privatrechtlichen Vertragsverhältnissen erfolgt, z. B. mit Kunden oder Mitarbeitern. Besonders beachtenswert ist hierbei, dass vor allem „datenschutzrechtliche" Vereinbarungen, allen voran vorformulierte Einwilligungserklärungen, im Regelfall einer AGB-Kontrolle i. S. d. §§ 305 ff. BGB unterliegen.[30]

27 In der Praxis ist festzustellen, dass viele Unternehmen sich auch unnötig durch eine falsche Gestaltung eine vermeidbare AGB-Kontrolle einfangen; das gilt vor allem für **Datenschutzerklärungen** nach Art. 13 und 14 DSGVO. Dienen Datenschutzerklärungen ausschließlich der gesetzlich verlangten Informationserteilung, können sie einer AGB-Kontrolle nicht unterzogen werden.[31] Soweit eine Datenverarbeitung jedoch Entgeltcharakter aufweist oder eine Datenschutzerklärung zusätzliche Pflichten der betroffenen Person begründen soll, schließt dies einen rein informativen Inhalt der Datenschutzerklärung aus und sie kann als Vertragsbestimmung i. S. d. § 305 Abs. 1 S. 1 BGB qualifiziert werden, die wiederum in vollem Umfang einer AGB-Kontrolle unterliegt.[32] Schädlich kann in diesem Zusammenhang insbesondere eine zu starke Verzahnung der Datenschutzerklärung mit den Nutzungsbedingungen sein. In diesem Sinne hat das LG Berlin entschieden, dass eine „Privacy Policy" der AGB-Kontrolle unterliegt, wenn diese nach ihrem objektivem Wortlaut bei dem Empfänger den Eindruck hervorruft, mit ihr solle der Inhalt eines vertraglichen oder Rechtsverhältnisses bestimmt werden.[33]

30 So für Einwilligungserklärungen: Forgó/Helfrich/Schneider/*Ehmann*, Teil IX Kap. 1 Rn. 27 unter Verweis u. a. auf BGH, Urt. v. 1.2.2018, GRUR 2018, 545.

31 OLG Hamburg, GRUR-RR 2015, 361 Rn. 48 ff.

32 *Wendehorst/Graf von Westphalen*, NJW 2016, 3745, 3750.

33 LG Berlin, Urt. v. 16.1.2018, MMR 2018, 328, 330.

Praxishinweis

Es sollte deshalb dringend vermieden werden, von dem Nutzer zu verlangen, dass er sich „mit den Datenschutzhinweisen einverstanden erklärt".

Gegenstand der AGB-Kontrolle können auch vom Unternehmen vorformulierte Leistungsbeschreibungen sein, die eine Datenverarbeitung überhaupt erst zur Erfüllung des Vertrags erforderlich machen.[34] **28**

Praxishinweis

Ein in der Praxis ebenfalls sehr häufig anzutreffender Fehler besteht darin, den Nutzer auf der Grundlage eines allgemein vorformulierten Hinweises bestätigen zu lassen, dass er die **Datenschutzerklärung gelesen** oder zur Kenntnis genommen habe. Bereits eine solche Klausel ist i. S. d. § 309 Nr. 12b BGB als formularmäßig erteilte Tatsachenbestätigung unwirksam.[35]

Soweit eine Klausel der AGB-Kontrolle nicht standhält, können Unternehmen in vertragsrechtlicher Hinsicht nicht auf sie zurückgreifen. Dann könnte es passieren, dass Datenverarbeitungen ohne die notwendige Rechtsgrundlage stattfinden. Die Verwendung unwirksamer AGB kann zudem zu empfindlichen Folgen im Hinblick auf das UKlaG und UWG führen und eine Schadensersatzhaftung aus culpa in contrahendo nach sich ziehen.[36] **29**

3. Besonderer Geheimnisschutz

In manchen Fällen werden personenbezogene Daten nicht nur durch die DSGVO und die bereichsspezifischen Datenschutzgesetze geschützt, sondern zusätzlich durch besondere gesetzliche **Geheimhaltungs- und Verschwiegenheitspflichten**. **30**

a) Berufsrechtliche Schweigepflichten

So unterliegen z. B. Geheimnisse, die einem Arzt, Apotheker, Rechtsanwalt, Notar, Steuerberater oder Wirtschaftsprüfer in dessen jeweiliger Funktion anvertraut worden sind, einer gesetzlichen Schweigepflicht, die auch über den Tod der betroffenen Person hinaus gilt. Diese Pflicht bestimmter Berufsträger zur Verschwiegenheit ergibt sich primär aus den jeweils für sie geltenden berufsrechtlichen Vorschriften, also z. B. der Berufsordnung für Ärzte (vgl. § 9 MBO-Ä), **31**

34 LG Berlin, Urt. v. 16.1.2018, MMR 2018, 328, 330.
35 So ausdrücklich LG Berlin, Urt. v. 16.1.2018, MMR 2018, 328, 331.
36 *Wendehorst/Graf von Westphalen*, NJW 2016, 3745, 3750.

für Rechtsanwälte aus § 43a Abs. 2 BRAO und § 2 BORA, für Notare aus § 18 BNotO, für Steuerberater aus § 57 Abs. 1 StBerG und für Wirtschaftsprüfer aus § 43 Abs. 1 S. 1 WiPrO. Solche Geheimnisse werden oftmals auch personenbezogene Daten umfassen; also z. B. soweit sie sich auf eine natürliche Person als Patient oder Mandant beziehen.

b) Strafrechtliche Schweigepflichten

32 Daneben und grundsätzlich unabhängig von den berufsrechtlichen Pflichten folgt eine gesetzliche Schweigepflicht – wiederum für Angehörige bestimmter Berufe – auch aus dem Strafrecht, und zwar aus § 203 StGB. Neben den oben genannten Berufsgruppen unterfallen dieser Klausel zusätzlich z. B. auch Angehörige von privaten Unfall-, Kranken- und Lebensversicherungen sowie die jeweils für sie **berufsmäßig tätigen Gehilfen** (z. B. Sprechstundenhilfen, Referendare etc.).

Praxishinweis

Im hiesigen Kontext besonders wichtig ist auch die Erstreckung der Geheimhaltungspflicht auf die jeweils bei den Verpflichteten bestellten (betrieblichen) Datenschutzbeauftragten: Nach § 203 Abs. 4 S. 1 StGB macht sich der **Datenschutzbeauftragte** einer Stelle, die dem Geheimhaltungsregime unterfällt, selbst strafbar, wenn er ein ihm in seiner Eigenschaft bekannt gewordenes Geheimnis offenbart.

33 In der Praxis wirkt sich die Überschneidung von Datenschutzrecht und gesetzlichen Schweigepflichten oft aus, wenn nach beiden Rechtsmaterien geschützte Informationen einem Dritten bekannt gegeben werden sollen, ohne dass eine gesetzliche Vorschrift dies anordnen oder gestatten würde. Wird hier datenschutzrechtlich also auf das Instrument einer **Einwilligung** gesetzt, ist die Erklärung parallel als eine wirksame **Befreiung von der Schweigepflicht** auszugestalten.[37]

c) Fernmeldegeheimnis

34 Eine auch in der Unternehmenspraxis relevante Berührung gibt es ferner zum **Fernmeldegeheimnis** nach § 88 TKG. Nach § 88 Abs. 2 S. 1 TKG ist jeder Diensteanbieter zur Wahrung des Fernmeldegeheimnisses verpflichtet. Diensteanbieter ist nach § 3 Nr. 6 TKG jeder, „der ganz oder teilweise geschäftsmäßig a) Telekommunikationsdienste erbringt oder b) an der Erbringung solcher Dienste“

37 Siehe hierzu das Muster von *Arning*, in: Moos, Datenschutz- und Datennutzungsverträge, 2. Aufl. 2018, § 41.