BDSG 2018

Jochen Schneider

Datenschutz

nach der EU-Datenschutz-Grundverordnung

2. Auflage

C.H.BECK

Zum Inhalt:

Wenn Sie mit personenbezogenen Daten arbeiten, kommen Sie an diesem Buch nicht vorbei

Es bietet einen Leitfaden für den Umgang mit der Datenschutzgrundverordnung – DS-GVO, sowie des neuen BDSG 2018 als nationale Umsetzung der DS-GVO. Das Buch hat den Fokus auf dem Datenschutz im Unternehmen.

Der Inhalt – Ihr Gewinn

- Die DS-GVO im Überblick
- Anwendung der DS-GVO und des BDSG 2018
- Zulässigkeit der Datenverarbeitung ohne Einwilligung
- Einwilligung in die Datenverarbeitung
- Rechte des Betroffenen
- Pflichten des Verarbeiters
- Aufsicht, Haftung und Zertifizierung
- Checklisten
- Bußgelder und Sanktionen
- Viele nützliche Hinweise und weiterführende Quellen im Anhang sowie ein Sachverzeichnis für den schnellen, gezielten Zugriff.

Zum Autor:

Prof. Dr. Jochen Schneider ist Rechtsanwalt in München und Honorarprofessor an der LMU.

Datenschutz

nach der EU-Datenschutz-Grundverordnung

von

Jochen Schneider

2. Auflage, 2019

C.H.BECK

Zum Autor

Prof. Dr. Jochen Schneider ist Rechtsanwalt in München und Honorarprofessor an der LMU. Daneben ist er Vorsitzender des Beirats der ARGE-IT des DAV – DAVIT –, langjähriges Mitglied der DGRI und Beiratsmitglied der DSRI. Er ist weiter Mitglied der Schriftleitung der Zeitschrift „COMPUTER UND RECHT" (CR), Herausgeber des IT-Rechts-Berater (ITRB) und Mitherausgeber der Zeitschrift für Datenschutz (ZD) sowie Autor und Herausgeber diverser Handbücher zum IT-Recht. Er hält Vorträge zu IT-Vertragsrecht und Datenschutz und publiziert dazu in div. Zeitschriften

www.beck.de

ISBN E-Book 978-3-406-72862-4
ISBN Print 978-3-406-72861-7

Wilhelmstraße 9, 80801 München

Satz: Fotosatz Buck, Zweikirchener Str. 7, 84036 Kumhausen
Druck: Nomos Verlagsgesellschaft mbH & Co. KG, In den Lissen 12, 76547 Sinzheim
Umschlaggestaltung: Ralph Zimmermann – Bureau Parapluie
Bildnachweis: © Sashkin – fotolia.com

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

So nutzen Sie dieses Buch

Um Ihnen das Lesen und Arbeiten mit diesem Buch zu erleichtern, hat der Autor verschiedene Stilelemente verwendet, die Ihnen das schnellere Auffinden bestimmter Texte ermöglichen. So finden Sie die Tipps und Musterformulare sofort.


Hier finden Sie Tipps, Aufzählungen und Checklisten.


So sind „Merksätze“ gekennzeichnet.


Hier finden Sie Beispiele, die das Beschriebene plastisch erläutern und verständlich machen.


Hier finden Sie markante Textstellen aus Vorschriften, unter anderem Definitionen.


Die Zielscheibe kennzeichnet Zusammenfassungen und ein Fazit zum Kapitelende.

Vorwort

§

Anliegen des Buches ist, einen Leitfaden für den Umgang mit der Datenschutzgrundverordnung – DS-GVO – vor allem im Unternehmen (nicht-öffentlicher Bereich) zu bieten. Die DS-GVO gilt seit 25.5.2018 und dies unmittelbar. Das heißt, dass es keiner Umsetzung durch die Gesetzgeber der Mitgliedstaaten bedarf. Tatsächlich hat Deutschland mit BDSG 2018 auf Basis von „Öffnungsklauseln" der DS-GVO weitere Regelungen zu speziellen Themen geschaffen, die für einzelne Instrumente und Pflichten, etwa Datenschutzbeauftragter und v.a. Beschäftigtendatenschutz, zu berücksichtigen sind.

Diese deutsche Regelung nutzt und füllt die Spielräume aus, die die DS-GVO den Mitgliedstaaten und deren Rechtsgestaltung belässt. Dieses BDSG 2018 versucht, Regelungen der DS-GVO zu konkretisieren und zu präzisieren. Ob das immer gut gelungen ist, darf bezweifelt werden (zu europarechtswidrigen BDSG-Vorschriften s. *Franck* ZD 2018, 345).

Die DS-GVO bringt für den Datenschutz nicht nur einige inhaltliche Neuerungen, sondern auch einige neue Begriffe. In einem Fall wird die Begrifflichkeit in diesem Leitfaden **nicht** übernommen: Die DS-GVO spricht von der „***betroffenen Person***" und von der Verarbeitung deren Daten. Statt „betroffener Person" wird im Folgenden häufig die Bezeichnung „Betroffener" benutzt. „Betroffener" war gem. BDSG a.F. die Person, deren personenbezogene Daten als Einzelangaben über persönliche oder sachliche Verhältnisse erhoben, verarbeitet oder genutzt werden.

„Art.“, also Artikel-Angaben ohne Gesetzes-Bezeichnung, sind Artikel der DS-GVO. Artikel der Datenschutzrichtlinie (DS-RL) sind um die Bezeichnung „DS-RL“ ergänzt. Zur Vermeidung von Unklarheiten, insbesondere bei Vergleichen zwischen DS-GVO und DS-RL wurde die Bezeichnung „DS-GVO“ gelegentlich angefügt. Bei Zitaten aus DS-GVO (oder DS-RL) erfolgen häufig Hervorhebungen des Autors. Diese sind nicht ausdrücklich jeweils als solche gekennzeichnet. Da diese Texte im Original aber keine Hervorhebungen kennen, sollte es kein Problem sein, diese Änderungen zu erkennen.

Der Leitfaden erwähnt vereinzelt Internetfundstellen für Dokumente und Nachweise für Literatur und Rechtsprechung. Bei Rechtsprechung werden einige Urteile des BVerfG und vor allem des EuGH erwähnt, die für die DS-GVO wichtig bleiben oder bei deren Interpretation hilfreich sein können.

Der Leitfaden enthält sich weitgehend der Würdigung, Kritik oder gar Beurteilung der DS-GVO als rechtswidrig oder ähnlichem, obwohl dazu ausreichend Grund bestehen würde. Die ursprünglichen Ankündigungen werden nicht erreicht (zu Zielen s.S. 24). Das Anliegen des Leitfadens ist ein anderes: Die Materie „Datenschutz“ als Schutz der Privatsphäre des Einzelnen verdient es, konstruktiv, wenn auch in Abwägung mit anderen Rechtsgütern, gestärkt und bewahrt zu werden. Die Notwendigkeit der Umsetzung der DS-GVO ist unabweisbar; also muss man als Betrieb das Beste daraus machen: ein Instrument für das gesamte Datenmanagement, auch für die Sicherheit der IT.

Der **Bußgeldrahmen** der DS-GVO und einige Pflichten, vor allem Skandalisierung, sind zudem so massiv, dass die Bemühung lohnt, die DS-GVO trotz ihrer Defizite einzuhalten. Dabei kann Vieles aus dem BDSG-Instrumentarium bleiben, also übernommen werden, muss aber neu arrangiert und vor allem gemanagt werden: die DS-GVO stellt sehr hohe Anforderungen an die Darstellung der Pflichterfüllung, vor allem die Nachweise der Einhaltung des Datenschutzes und deshalb an das Management des Datenschutzes als System im Unternehmen.

Gegenstand der Darstellung ist die Arbeit mit der DS-GVO im Betrieb als datenverarbeitender Organisation des Privatrechts, also **nicht der öffentlichen** Verwaltung. Dieser hier behandelte Bereich wird im BDSG als der Bereich nicht-öffentlicher Stellen bezeichnet. Im Folgenden ist auch von „Betrieb“, „Unternehmen“ oder „privatem Bereich“ die Rede.

Es gibt inzwischen viele Hilfen der Aufsichtsbehörden. Davon sind einige im Anhang aufgelistet.

München, im Oktober 2018 *Jochen Schneider*

Inhalt

1. Kapitel

1 Einleitung

I. Datenschutz: BDSG von 1977

„*Datenschutz*“ gibt es als Bundesgesetz seit 1977, BDSG. Das BDSG wurde mehrfach novelliert. Gegenstand der Regelung ist der Umgang mit *personenbezogenen Daten*. Ursprünglich war der Ansatz, diese dann zu schützen, wenn besondere Gefahren bestehen, was damals bei Verarbeitung mit/aus „Dateien“ vermutet wurde.

„Vorläufer“ des BDSG waren das hessische Landesdatenschutzgesetz von 1970 und das Schwedische Datenschutzgesetz von 1973. Das BDSG gilt für alle Bereiche, also öffentliche und nicht-öffentliche Stellen. Es wurde mehrfach novelliert. Die Bundesländer haben sämtlich von der Möglichkeit Gebrauch gemacht, eigene Landesdatenschutzgesetze zu schaffen, die insoweit das BDSG verdrängen. Dieses hat also neben dem Bund vor allem für die nicht-öffentlichen Stellen Wirkung. Diese Wirkung endet weitgehend mit Geltung der DS-GVO zum 25.5.2018.

Unabhängig davon besteht das Allgemeines Persönlichkeitsrecht als Schutzposition des Einzelnen weiter, wohl auch das Recht am eigenen Bild (OLG Köln (erste Entscheidung zur DSGVO) v. 18.6.2018 – 15 W 27/18, dazu *Hansen/Brechtel*: KUG vs. DS-GVO: Kann das KUG anwendbar bleiben? GRUR-Prax 2018, 369). Microsoft etwa forderte neue Gesetze zur Bilderkennung (https://blogs.microsoft.com/on-the-issues/2018/07/13/facial-recognition-technology-the-need-for-public-regulation-and-corporate-responsibility/). In Verbindung mit autonomen Fahrzeugen, KI und Algorithmen wird zunehmend ein – evtl. zu schaffendes – Recht am eigenen Datum diskutiert (*Markendorf* ZD 2018, 409).

II. Europa, EU

Schon die Datenschutzrichtlinie (DS-RL) von 1995 strebte einen **einheitlichen Datenschutz** auf hohem Niveau in der EU an. Es entstand eine Front gegenüber den USA und deren Datenschutz mit der Durchsetzung im Rahmen der EuGH-Entscheidungen. Oft wurde angenommen, dort gäbe es keinen Datenschutz. Dabei wird übersehen, dass die Art, diesen zu regeln, völlig verschieden von dem Ansatz der EU ist, vor allem beim Ansatz, **was** zu schützen ist. Der Versuch, etwa über den Schutz der Privatsphäre und dessen Regelung ein kompatibles EU-Recht zu schaffen, wurde in der EU nicht unternommen, dagegen wurden die Gräben durch Ausbau der DS-RL nun als direkt wirkende DS-GVO vertieft (s. zu USA *Lejeune* ITRB 2016, 201 (zu Privacy Shield); *Determann,* International Compliance Field Guide, 2017, und *Determann* zum California Consumer Privacy Act of 2018, CR 2018, 114).

1. DS-RL und andere Vorgaben

Der EuGH hatte bereits 1969 ein Datenschutzproblem zu entscheiden. Der Fall erinnert etwas an die Veröffentlichung der Agrar-Subventions-Empfänger, s.S. 30. Die vorgelegte Frage des VG Stuttgart betraf den Umstand, dass bei der Abgabe verbilligter Butter an Empfänger bestimmter sozialer Hilfen die Abgabe an eine Offenbarung des Namens des Empfängers gegenüber dem Verkäufer geknüpft war (EuGH v. 12.11.1969 – C-29/69). Es gibt also schon lange eine Befassung mit dem Umgang mit personenbezogenen Daten, bevor der „Datenschutz“ formalisiert wurde.

Seit 1981 gab es die **Datenschutzkonvention** des Europarats – „Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten“. Gegenstand und Zweck sind in Art. 1 beschrieben.

§

Art. 1 Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

„Zweck dieses Übereinkommens ist es, im Hoheitsgebiet jeder Vertragspartei für jedermann ungeachtet seiner Staatsangehörigkeit oder seines Wohnorts sicherzustellen, dass seine Rechte und Grundfreiheiten, insbesondere sein Recht auf einen Persönlichkeitsbereich, bei der automatischen Verarbeitung personenbezogener Daten geschützt werden („Datenschutz“).“

Mit der **EG-Datenschutzrichtlinie** 95/46 (Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr von 1995 (EG-Datenschutzrichtlinie, **DS-RL**)) wurde eine harmonisierende Maßgabe für den Datenschutz geschaffen. Diese EG-Datenschutzrichtlinie war bis zum 24.10.1998 umzusetzen. Deutschland sah sich in der Position, bereits über die entsprechende Regelung mit dem BDSG zu verfügen. Tatsächlich war dies nicht so der Fall, sodass bei Novellierungen auch noch Umsetzungen der DS-RL in das BDSG erfolgten. Die DS-RL umfasste auch die nichtautomatisierte Verarbeitung personenbezogener Daten in oder aus Dateien.

Parallel zur Konvention Europarats und zur DS-RL gibt es die **OECD -Datenschutz- Richtlinien über Datenschutz und grenzüberschreitende Ströme personenbezogener Daten („Datenschutzrichtlinien“)** vom 23.9.1980 (OECD-Datenschutzleitlinien, überarbeitet 2013, http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm). Sie haben keine Bindungswirkung. Interessant ist, dass dort vor allem die **Gefährdung der Privatsphäre** und der Freiheiten von Personen im Focus der Regelung stehen. Auch gibt es dort bereits Grundprinzipien, die weitgehend die in Art. 6 DS-RL und Art. 5 DS-GVO vorwegnehmen.

Zu erwähnen ist noch als spezielle Datenschutz-RL die Richtlinie 97/66/EG des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation von 1997, 2002 als EG-**Telekommunikations-Datenschutzrichtlinie** 2002/58/EG novelliert, durch die Richtlinie zur Vorratsdatenspeicherung 2006/24/EG geändert. Sie gilt als sog. e-Privacy-RL (2002/58/EG), die durch die sog. Cookie-RL (2009/136/EG) ergänzt wurde. Deutschland stand auf dem Standpunkt, mit dem TMG bereits über geeignete Regelungen zu verfügen, ohne speziell eine Umsetzung vornehmen zu müssen. Nun soll die e-Privacy-Verordnung, auf der DS-GVO aufsetzend, die Thematik des Datenschutzes bei der elektronischen Kommunikation ebenfalls mit direkter Wirkung neu regeln (Vorschlag vom 10.1.2017, 2017/0003, mitgeteilt vom Rat unter 5358/17). Mit Blick auf das (fehlende) Rechtsgut bei der DS-GVO ist sehr interessant, dass sie bezeichnet wird als „Verordnung über **Privatsphäre** und elektronische Kommunikation“ (dazu s. z.B. *Spindler/Schmitz*, Vorbemerkung: Überblick zum Datenschutz nach TMG und Ausblick auf DS-GVO und ePrivacy-VO Rn. 25-29).

2. Grundrechte

Seit 1983 gibt es in Deutschland das Recht auf **informationelle Selbstbestimmung** (Urteil des BVerfG), das nie in das BDSG übernommen wurde, also vor allem über die Rechtsprechung Wirkung entfaltete. In gewissem Sinne wird es ergänzt durch das Grundrecht auf **Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme** (BVerfG v. 27.2.2008 – 1 BvR 370/07, 1 BvR595/07, NJW 2008, 822). Dieses wurde als das „neue (Computer-)Grundrecht" bezeichnet (*Krings/Sachs* JuS 2008, 481). Weitere Entscheidungen finden sich ab S. 25. Das Recht auf informationelle Selbstbestimmung und das „neue Computergrundrecht" haben inhaltlich Eingang in die DS-GVO gefunden, letzteres als **Grundsatz** in Art. 5 Abs. 1.

§

Art. 5 Abs. 1 Buchstabe f

Danach **müssen** personenbezogene Daten „…in einer Weise verarbeitet werden, die eine **angemessene Sicherheit** der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen (‚**Integrität und Vertraulichkeit**')".

Seit „Lissabon" (Vertrag von Lissabon) gibt es mit Wirkung 1.12.2009 die Grundrechte nach der EU-Charta (GRCh), hier vor allem Art. 7 und 8.

§

Art. 7 und 8 GRCh

Artikel 7 Achtung des Privat- und Familienlebens

Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation.

Art. 8 Schutz personenbezogener Daten

(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) 1) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. 2) Jede Person hat das Recht, Auskunft über

die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

Art. 7 GRCh hat den Vorteil, mit „Privatleben" einen inhaltlichen, **materiellen** Rechtsgehalt zu bieten, der das Schutzgut konkreter ausgestaltet, während Art. 8 GRCh nicht vermittelt, dass es nicht als Selbstzweck um den Schutz der Daten, sondern um den Schutz der Person vor (den Folgen) der Verarbeitung „ihrer" Daten geht.

Das Fehlen eines materiellen **Schutzguts** macht sich an vielen Stellen als schwerwiegendes Defizit bemerkbar, das eine sinnvolle, zielgerichtete Berücksichtigung der Maßgaben der DS-GVO erschwert. Besonders deutlich wird dies z.B. bei „Datenschutz durch Technikgestaltung", Art. 25. Richtig wäre und postuliert wurde und wird „Privacy by design" (s. EDSB Opinion 5/2018, https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf). „*Privatsphäre*" ist aber als Schutzgut nicht in die DS-GVO eingeführt worden, vielmehr scheint der Schutz der Daten weiterhin als **Selbstzweck** verfolgt zu werden (s.a. *Veil* VwZ 2018, 686, 691; schon vor DS-GVO: *Bull*, Sinn und Unsinn des Datenschutzes, 2015).

Die Tradition, dass die Datenschutzbehörden schlechte Datenschutz-Regeln schönen, wird also fortgesetzt. Angesichts Haftung und Bußgelddrohung sind die Defizite der DS-GVO, wenn sie durch einseitige Interpretation übertüncht werden, noch bedrohlicher, weil kaum zu beurteilen.

3. Entstehung der DS-GVO

Seit 2010 arbeitet die Kommission an der Erneuerung des Datenschutzes. In der Presse-Erklärung der Kommission vom 4.11.2010 wird die „Stärkung des EU-Datenschutzrechts" betont und angekündigt, dass die Europäische Kommission eine ***neue Strategie*** vorstellt.

Diese Strategie zeigt auf, wie sich der EU-Rahmen für den Datenschutz **modernisieren** lässt, und formuliert dazu eine Reihe von **Kernzielen**. Diese sind auszugsweise:

- **Stärkung der Rechte des Einzelnen**, damit die Sammlung und Nutzung personenbezogener Daten auf das erforderliche Mindest-

maß beschränkt wird. Jeder sollte überdies klar und in transparenter Weise darüber informiert werden, wie, warum, von wem und wie lange seine Daten gesammelt und verwendet werden. Jeder sollte die Möglichkeit haben, der Verarbeitung seiner personenbezogenen Daten nach vorheriger Aufklärung freiwillig zuzustimmen, beispielsweise beim Online-Surfen, und jeder sollte das „Recht vergessen zu werden" haben, wenn seine Daten nicht länger gebraucht werden oder er will, dass seine Daten gelöscht werden.

- **Stärkung der Binnenmarktdimension** durch Verringerung des Verwaltungsaufwands für Unternehmen und die Gewährleistung gleicher Rahmenbedingungen. Gegenwärtig herrschen Unterschiede bei der Umsetzung der Datenschutzbestimmungen der EU, und nicht immer ist klar, wessen Vorschriften gelten. Dies beeinträchtigt den freien Verkehr personenbezogener Daten in der EU und bewirkt höhere Kosten.

- Gewährleistung eines **hohen Schutzniveaus** bei außerhalb der EU übermittelten Daten durch die Verbesserung und Erleichterung von Verfahren für den internationalen Datentransfer. Die EU sollte bei der Zusammenarbeit mit Drittstaaten dasselbe Schutzniveau anstreben und sich weltweit für hohe Datenschutzstandards einsetzen.

- **Wirksamere Durchsetzung** der Vorschriften durch die Stärkung und weitere Harmonisierung der Aufgaben und Befugnisse der Datenschutzbehörden. Ferner bedarf es einer besseren Zusammenarbeit und Abstimmung, um eine konsequentere Anwendung der Datenschutzbestimmungen im gesamten Binnenmarkt zu gewährleisten.

Die DS-GVO entstand in seit Ende 2011 bekannt gewordenen, verschiedenen **Versionen**, die zum Teil erhebliche Textänderungen auswiesen. Im Folgenden wird die amtliche Version (ABl. v. 4.5.2016, L 119/34) i.V.m. Berichtigung ABl. L 314/72 zitiert und nur ab und zu darauf hingewiesen, wenn ursprünglich anderes vorgesehen war. Dies spielt etwa im Zusammenhang mit der Einwilligung eine Rolle. Vereinfacht sind folgende Versionen als Entwicklungsstufen festzuhalten und zwar nicht zuletzt auch im Hinblick auf das Verständnis, warum von den ursprünglichen Zielen wenig realisiert wurde:

- Im Dezember 2011 tauchte eine so genannte geleakte Version einer „Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezo-

gener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)“ auf, wozu

- am 25.1.2012 die Kommission dann den **offiziellen Entwurf** vorlegte: Vorschlag der Europäischen Kommission vom 25.1.2012 (KOM(2012) 11 endgültig; 2012/0011 (COD)).

- Das Europäische Parlament hat am 12.3.2014 zu diesem Vorschlag der Kommission Stellung genommen und Änderungsvorschläge beschlossen. Beschluss des Europäischen Parlaments vom 12.3.2014 im Rahmen der ersten Lesung zu dem Vorschlag der Europäischen Kommission (Interinstitutionelles Dossier des Rats der Europäischen Union vom 27.3.2014, 2012/0011 (COD); 7427/1/14, REV 1). Seit 2012 wird also der Entwurf beraten. Parlament und Rat haben erhebliche Vorschläge unterbreitet und manche durchgesetzt.

- Version des Rats der Europäischen Union vom 15.6.2015, 9565/15:

- Dazu fand ab dem 24.6.2015 der so genannte Trilog statt, Verhandlungen von Kommission, Europäischem Parlament und Europäischem Rat. Der Rat hat seinen Standpunkt beim Treffen vom 15.6.2015 dargelegt. Somit lagen bei den Trilog-Verhandlungen neben dem Kommissionsvorschlag die Versionen des Europäischen Parlaments und die des Rates vor. Im Dezember 2015 haben sich die Beteiligten auf einen Verordnungstext verständigt, (Arbeits-) Ergebnis der Trilogparteien vom 15.12.2015, Dokument des Rates 15039/15, der nun als DS-GVO nur noch redaktionell bearbeitet wurde.

- Diese **Ergebnisse** des Trilogs wurden in der Version vom 5.2.2016 auch auf Deutsch veröffentlicht, allerdings war dies noch nicht die Endfassung. Redaktionell waren noch verschiedene Bearbeitungen erforderlich, die bis dahin noch nicht vollständig konsolidiert waren. Am 4.5.2016 wurde dann die DS-GVO im Amtsblatt der Europäischen Union bekannt gemacht.

Um die verschiedenen Versionen auch in ihrer möglichen Wirkung, aber auch die Unterschiede zwischen den Versionen zu verstehen, kann es Sinn machen, sich einer der **Synopsen** zu bedienen. Eine solche Synopse hat z.B. das Bayerische Landesamt für Datenschutzaufsicht publiziert (über die Homepage www.lda.bayern.de/media/brylda_synopse.pdf erreichbar).

Der Rat hat am 19.4.2018 ein ***Corrigendum*** verschiedener Sprachfassungen der Verordnung (EU) 2016/679 (Datenschutz-Grundver-

ordnung), auch der deutschen, vorgenommen, womit diese Texte berichtigt wurden.

4. Ziele

Die Erwartungen an die DS-GVO waren möglicherweise dadurch besonders hochgeschraubt, dass 2010 das Gesamtkonzept für den Datenschutz der Kommission von dieser publiziert wurde (4.11.2010, kom_2010_609, dazu oben S. 21 ff.). Danach war schwer vorstellbar bzw. kaum zu erwarten, dass lediglich eine Art Aufblähung der DS-RL herauskommen würde, also bei weitem keine konkreten und modernen Regelungen. Zu den **Zielen** beziehungsweise zu den Ansprüchen, die in dem Zusammenhang formuliert wurden, gehörten vor allem:

- Die Beherrschung der Auswirkungen neuer Technologien, ausgehend davon, dass seit Inkrafttreten der DS-RL vom 24.10.1995 eine große technische Entwicklung stattgefunden hat.
- Die Einheitlichkeit der Regelung für den Binnenmarkt: die Binnenmarkt-Dimension des Datenschutzes sollte berücksichtigt werden.
- Der Umgang mit der Globalisierung und Verbesserung internationaler Datentransfers.
- Verstärkter institutioneller Rahmen für die wirksame Durchsetzung der Datenschutzvorschriften.
- Kohärentere Regelung für den Datenschutz.

Im Ergebnis wurde ein umfassendes, kohärentes Konzept gefordert, *„das die lückenlose Einhaltung des Grundrechts des Einzelnen auf Schutz seiner Daten in der EU und anderswo garantiert“*. Mit der Pressemitteilung zum Entwurf der Kommission von 2012 wurden die wichtigsten Änderungen, die die DS-GVO mit sich bringen wird und soll, aufgelistet. Man könnte dies als **Ziele der Reform** verstehen. Daraus sind hervorzuheben:

- **EU-weit geltendes Gesamt-Regelwerk** ohne unnötige administrative Anforderungen mit erheblichen **Einsparungen**.
- Der Verarbeiter und der Auftragsverarbeiter tragen mehr **Verantwortung** und unterliegen einer verschärften **Rechenschaftspflicht**.
- Es wird eine **Benachrichtigungspflicht** bei Verletzung des Schutzes personenbezogener Daten in schweren Fällen geben (die es schon bisher gab).

- Es gibt einen alleinigen Ansprechpartner für Organisationen mit grenzüberschreitendem Bezug. Anknüpfungspunkt ist die Hauptniederlassung.
- Die Bürger sollen **leicht** auf ihre eigenen Daten zugreifen können. Das Ziel wird partiell erreicht, viele Regelungen dabei sind neu.
- Das Recht auf **Vergessenwerden** ermöglicht eine bessere Beherrschung der DS-Risiken bei Online-Diensten. Das Recht gibt es schon auf Basis der Löschungspflichten (s. EuGH v. 13.5.2014 – C-131/12 – Google (S. 28)).
- Auch **außerhalb** der **EU** erfolgende Verarbeitungen von personenbezogenen Daten durch auf dem EU-Markt aktive Unternehmen sollen künftig den Datenschutz-Vorschriften der EU unterliegen. Das ist teilweise neu.
- Die **Unabhängigkeit** der nationalen Datenschutzbehörden soll gestärkt werden.

Diese Ziele sind in der endgültigen Fassung irgendwie angesprochen. Wesentliche Teile enthielt aber bereits die DS-RL. Dass tatsächlich erhebliche Verbesserungen insgesamt eintreten werden, ist vor allem im Bereich der Verarbeitung von Daten im Nicht-EU-Ausland zu erwarten. Es kommt nicht darauf an, dass der Verarbeiter seinen Sitz in der EU hat. Zur Effektuierung des Datenschutzes könnten die Betriebe nun gezwungen sein; Einsparungen beim Datenschutz sind nicht zu erwarten, eher erhebliche Kostensteigerungen wegen gestiegener Anforderungen u.a. an Nachweisbarkeit (Rechenschaftspflicht). In den Verlautbarungen im Rahmen des Entstehungsprozesses der DS-GVO ist von einer weiteren Richtlinie bzw. einem anderen Richtlinien-/Verordnungsvorhaben die Rede. Dabei geht es um einen Bereich, der im Folgenden nicht behandelt wird, nämlich um die Zusammenarbeit der Polizei- und Strafjustizbehörden und die dabei geltenden DS-Regeln. Erwähnt wird öfters die sog. Cookie-RL, an deren Stelle eine e-Privacy-Verordnung treten soll, die aber wohl noch längere Zeit bis zur Verabschiedung benötigt.

III. „Meilenstein"-Urteile

1. BVerfG und BGH nach 1993

Die im Folgenden aufgeführten Entscheidungen von BVerfG und BGH behandelten Bedrohungsszenarien, die früher vor allem im öffent-

lichen Bereich entstanden (zum Beispiel Ausspähen durch Polizei oder Verfassungsschutz) und mittlerweile auch im nicht-öffentlichen Bereich möglich sind. Dies macht die durch die Rechtsprechung entwickelten Schutzinstitute auch älteren Datums so interessant, wenn es nun um neue Techniken etwa bei Analysetechniken mit Big Data und Tracking der Nutzer unter Geltung der DS-GVO geht.

Von der Rechtsprechung insbesondere des BVerfG wurde das **Recht auf informationelle Selbstbestimmung** gegenüber den Bedrohungen der automatisierten Datenverarbeitung aus Art. 1 Abs. 2 und Art. 2 Abs. 1 GG entwickelt, im Laufe der Zeit weiter ausgebaut und auch konkretisiert. Besonders hervorzuheben ist dabei, was auch in Übereinstimmung mit der DS-GVO steht, dass für den Staat ein prinzipielles Verbot der Erstellung von **Persönlichkeitsprofilen** gilt (im Ansatz schon BVerfG v. 30.10.1963 – Gs 168/63 – Microzensus).

§

Dieses „Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen." (BVerfG v. 15.12.1983 – 1 BvR 209, 269, 362, 420, 440, 484/83, LS 1 Satz 2).

LS 2 erlaubt Einschränkungen dieses weitreichenden Rechts unter Bedingungen: „Einschränkungen dieses Rechts auf „informationelle Selbstbestimmung" sind nur im überwiegenden Allgemeininteresse zulässig. Sie bedürfen einer verfassungsgemäßen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muss. Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der **Verhältnismäßigkeit** zu beachten. Auch hat er organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken."

DS-RL und BDSG hatten dazu einen Teilaspekt geregelt (Art. 15 DS-RL, § 6a BDSG a.F. mit *Verbot automatisierter Entscheidungen* zum Nachteil des Betroffenen). Verboten ist auch die **Observation als systematische Beobachtung einer Person**, *„die es ermöglicht, eine Vielzahl von Informationen über den Observierten zu erlangen, was in die geschützte Privatsphäre und damit in das Persönlichkeitsrecht (Art. 2 I i.V.m. Art. 1 I GG) des Betroffenen eingreifen kann."* (BVerwG v. 21.3.1986 – 7 C 73/84, mit Verweis auf BVerfGE 65, 1, 41 ff. – Recht auf informationelle Selbstbestimmung, dazu soeben).

Auch im nicht-öffentlichen Bereich sind heimliche **Profilbildungen** grundsätzlich verboten bzw. stellen einen Eingriff in das Persönlichkeitsrecht dar. Das TMG erlaubt ausdrücklich in § 15 die Profilbildung mit Pseudonymen für bestimmte Zwecke. Ob dies noch verfassungsgemäß ist, wird bezweifelt. Das TMG wird insoweit durch die DS-GVO verdrängt (s.S. 37; zum speziellen Schutz gemäß e-Privacy VO-Entwurf *Jandt* ZD 2018, 405). Art. 15 DS-RL und § 6a BDSG a.F. erwähnten die Profilbildung nicht, sondern stellten nur auf den Prozess der Automatisierten Entscheidung als solchen ab, die auch im nicht-öffentlichen Bereich nur unter bestimmten Voraussetzungen (s.S. 150) erlaubt war. Die erwähnten Art. 15 DS-RL und § 6a BDSG a.F. galten auch für den nicht-öffentlichen Bereich. § 32 BDSG a.F. regelte und beschränkte das so genannte *Screening* mit Beschäftigtendaten und erlaubte es nur für bestimmte Fälle. Die DS-GVO lockert die Voraussetzungen weiter, s.S. 134 ff. § 26 BDSG 2018 entspricht § 32 BDSG a.F. und ist insofern ebenso eine Generalklausel und somit unionswidrig.

Es gibt auch ein **Verbot** der **Datenbevorratung**, was sich schon aus dem Urteil zum Recht auf informationelle Selbstbestimmung ergab und später konkretisiert wurde (BVerfG v. 14.7.1999 – 1 BvR 2226/94 – Fernmeldeüberwachung durch den Bundesnachrichtendienst, und v. 4.4.2006 – 1 BvR 518/02 – Rasterfahndung).

Totalerfassung wäre verboten (BVerfG v. 2.3.2010 – 1 BvR 256/08, so auch im Ansatz BGH v. 24.1.2001 – 3 StR 324/00 zu GPS-Beobachtung). Besondere Beachtung verdient danach auch die Kumulation mehrerer Arten der Erfassung. In die Richtung des Verbots der Totalüberwachung geht auch die Entscheidung des BAG zum Keylogger (v. 27.7.2017 – 2 AZR 681/16, NZA 2017, 1327 – Keylogger; dazu *Kort*, NZA 2018; s.a. S. 35, 155).

Auch die „permanente und anlasslose Aufzeichnung des Verkehrsgeschehens" etwa mittels Dashcam „ist mit den datenschutzrechtlichen Regelungen" des BDSG nicht vereinbar (BGH v. 15.5.2018 – VI ZR 233/17 zu BDSG a.F.), was aber eine Beweisverwertung nicht ausschließt. Tangiert sind damit die Themen der permanenten Beobachtung und Aufzeichnungen, aber auch der Bevorratung.

Vorratsdatenspeicherung bedarf besonderer Grundlagen (BVerfG v. 2.3.2010 – 1 BvR 256/08 – Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten; differenzierender: EuGH v. 21.12.2016 – C-203/15; kritisch: *Wollenschläger*: Die Erga-omnes-Wirkung von

EuGH-Urteilen in Vorabentscheidungsverfahren und die TK-Verkehrsdatenspeicherung, NJW 2018, 2532).

Heimliche Beobachtung, hier durch staatliche Stellen, ist verboten (BVerfG v. 2.3.2010). Das **Gefühl des (heimlich) Beobachtetwerdens** darf nicht entstehen (es geht laut BVerfG darum, dass nicht ein **diffus bedrohliches Gefühl** des Beobachtetseins hervorgerufen wird, das eine unbefangene Wahrnehmung der Grundrechte beeinträchtigen kann. Wenig beachtet ist, dass im Google-Urteil der EuGH der **Profilbildung** als Bedrohung deutlich eine **Absage** erteilt hat:

„[80] Wie bereits … ausgeführt, kann eine von einem Suchmaschinenbetreiber ausgeführte Verarbeitung personenbezogener Daten, wie die im Ausgangsverfahren in Rede stehende, die Grundrechte auf Achtung des Privatlebens und Schutz personenbezogener Daten erheblich beeinträchtigen, wenn die Suche mit dieser Suchmaschine anhand des Namens einer natürlichen Person durchgeführt wird, da diese Verarbeitung es jedem Internetnutzer ermöglicht, mit der Ergebnisliste einen strukturierten Überblick über die zu der betreffenden Person im Internet zu findenden Informationen zu erhalten, die potenziell zahlreiche Aspekte von deren Privatleben betreffen und ohne die betreffende Suchmaschine nicht oder nur sehr schwer hätten miteinander verknüpft werden können, und somit ein mehr oder weniger detailliertes Profil der Person zu erstellen. Zudem wird die Wirkung des Eingriffs in die genannten Rechte der betroffenen Person noch durch die bedeutende Rolle des Internets und der Suchmaschinen in der modernen Gesellschaft gesteigert, die den in einer Ergebnisliste enthaltenen Informationen Ubiquität verleihen (vgl. i.d.S. EuGH, EU:C:2011:685 = GRUR 2012, 300 = NJW 2012, 137 Rn. 45 – eDate Advertising).“ (EuGH v. 13.5.2014 – C-131/12 – Google).

Die DS-GVO behandelt das Profiling nicht sehr restriktiv, betont aber den Aspekt, dass der Betroffene darüber informiert sein soll. Ergänzend ist darauf hinzuweisen, was aber von der DS-GVO ohnehin nicht erfasst wird, dass es noch den Schutzbereich des **Telekommunikationsgesetzes bzw. -geheimnisses** gibt, Art. 10 Abs. 1 GG. Dieser wird auch nicht vom Recht auf informationelle Selbstbestimmung erfasst. Die Lücke, die sich eventuell ergibt, wird durch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (2008) gefüllt. Dieses so genannte

neue Grundrecht, s.S. 17, ist in seiner Tragweite bislang noch nicht genügend ausgeschöpft worden.

Sämtliche genannte Errungenschaften sind allerdings in Zukunft im Rahmen der DS-GVO allenfalls mittelbar zu berücksichtigen, soweit es nur um die Anwendung der DS-GVO geht. An die Stelle dieser Institute tritt dann weitgehend der relativ knappe Grundrechtekatalog der Charta. Dabei ist davon auszugehen, dass der Schutzbereich des Privatlebens durch Art. 7 Grundrechtscharta (s.S. 20) wesentlich unmittelbarer und konkreter geschützt ist als durch Art. 8 (s.a. EuGH v. 21.12.2016 – C-207/16 und v. 2.10.2018 – C-207/16 ergänzend zu S. 28). In Art. 7 GRCh werden 4 zentrale Bereiche aufgefächert und geschützt – ***Privatleben***, ***Familienleben***, ***Wohnung*** und ***Kommunikation***. Es geht darin also sowohl um Zurückgezogenheit als auch um Teilhabe und Außenkontakt. Art. 8 schützt wie auch die DS-RL und die DS-GVO die ***personenbezogenen Daten***, allerdings auf höherem Niveau eines Grundrechts. Der Unterschied zwischen Art. 8, Schutz der personenbezogenen Daten als Grundrecht, und Schutz der personenbezogenen Daten durch die DS-GVO ist nicht klar, da die die DS-GVO meist sehr vage bleibt und dann, wenn es um Rechtsgüter geht, auf die Charta (Grundrechte und Grundfreiheiten) zurückverweist.

Wichtig wäre eine **Abwägungs**-Modalität unter Einbeziehung der Rechte Dritter, die einschließt, dass Dritte die gleichen Rechte haben können (ein Beispiel wäre etwa, dass ein Auto verunfallt und die Daten sämtlicher Insassen erhoben werden. Alle haben das Interesse am Schutz ihrer Daten, zugleich an deren Bearbeitung im Hinblick auf die Gewährung von Versicherungsschutz und Ähnlichem, evtl. auch an der Nicht-Verwendung ihrer Daten).

Des Weiteren ist die Abwägungsmodalität gegenüber der **Informations- und Meinungsäußerungsfreiheit** zu beachten. Dieser Aspekt wird von der DS-GVO kaum berücksichtigt, nur abstrakt. Insofern weist die DS-GVO nur abstrakte Qualitäten einer allgemeinen Regelung auf, mithin den Charakter einer Richtlinie. Art. 85 verpflichtet (entsprechend Erwägungsgrund 153, der auf das Recht der Mitgliedstaaten verweist) die Mitgliedstaaten, durch Rechtsvorschriften das Recht auf den Schutz personenbezogener Daten gem. dieser Verordnung mit dem Recht auf freie Meinungsäußerung und Informationsfreiheit, einschl. der Verarbeitung zu journalistischen Zwecken und zu wissenschaftlichen, künstlerischen oder literarischen Zwecken, **in Einklang** zu bringen (Art. 85 Abs. 1). Abs. 2 räumt die Möglichkeit ein, die spezielleren Regelungen, die die Verarbeitung zu

journalistischen Zwecken oder zu wissenschaftlichen, künstlerischen oder literarischen Zwecken betrifft, Abweichungen oder Ausnahmen von den Regeln in den Abschnitten II. (grundsätzlich), III. (Rechte der betroffenen Personen), Kap. IV. (Verantwortliche und Auftragsverarbeiter), Kap. V. (Übermittlung personenbezogener Daten an Drittländer oder an intern. Organisationen), Kap. VI. (unabhängige Aufsichtsbehörden) und Kap. VII. (Zusammenarbeit und Kohärenz) sowie Kap. IX. (Vorschriften für besondere Verarbeitungssituationen) vorzunehmen, *„wenn dies erforderlich ist, um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen“*.

2. EuGH auf Basis der DS-RL

Schon immer gab es Entscheidungen des EuGH zum Datenschutz, auch vor der EU-Grundrechte-Charta (vor dem Vertrag von Lissabon 2009), die sich als Referenz auch und vor allem auf die ***Privatsphäre*** bzw. den ***privaten Lebensbereich*** beziehen und diesen schützen (s. *Roßnagel* Rz. 64; *Skouris* NVwZ 2016, 1359 zum Überblick über Datenschutz-Entscheidungen des EuGH). Basis ist dabei vor allem eine Abwägung auf der Grundlage von Art. 8 EMRK und der diesbezüglichen Rechtsprechung des EGMR. Nach Lissabon (2009) äußert sich dies darin, dass der EuGH sogar bevorzugt, sich noch vor Art. 8 (auch) auf Art. 7 GRCh zu stützen. Das heißt aber, dass die Auslegung der DS-GVO nicht nur im Lichte des Art. 8 der Charta, sondern vor allem des Art. 7 vorzunehmen ist, wenn es um die materiellrechtliche Positionierung geht. Dies wird besonders relevant, sobald Haftung geltend gemacht und Schadensersatz verlangt wird.

Die Bestimmung des **Personenbezugs** von Daten mit Referenz zu „Informationen“ hatte eine weitere Entscheidung zum Gegenstand. Die betroffenen Daten, die sich sowohl auf die von bestimmten Rechtsträgern gezahlten **Bezüge** als auch auf deren **Empfänger** beziehen, sind personenbezogene Daten im Sinne von Art. 2 Buchstabe a der DS-RL, *„da sie Informationen über eine bestimmte oder bestimmbare natürliche Person darstellen“* (EuGH v. 20.5.2003 – C-465/00 u.a. – Rechnungshof u.a.).

Anschaulich für die **Abwägung** bei Datenschutzeingriffen, die gegebenenfalls auch bei DS-GVO hinsichtlich der Grundrechte-Charta erforderlich ist, ist eine Entscheidung des EuGH zur Veröffentlichung von Agrarsubventionsempfängern (v. 9.11.2010 – C-92/09, 93/09 Volker und Markus Schecke GbR u.a.): Die Veröffentlichung von

Daten unter Nennung der Namen der betroffenen Empfänger und der genauen Beträge stellt *„eine Verletzung der durch die **Art. 7 und 8 der Charta anerkannten Rechte**"* dar. Da diese Verarbeitung personenbezogener Daten nicht auf der Einwilligung dieser Empfänger beruht, ist zu prüfen, ob diese Verletzung nach Art. 52 I der Charta gerechtfertigt ist. Dazu befasst sich der EuGH mit dem Grundsatz der **Verhältnismäßigkeit**, *„der zu den allgemeinen Grundsätzen des Unionsrechts gehört"*, und dabei mit der Frage, ob die *„eingesetzten Mittel zur Erreichung des verfolgten Ziels geeignet sind und nicht über das dazu Erforderliche hinausgehen"* (EuGH v. 9.11.2010 – C-92, 93/09, Rz. 74 mit Verweis auf EuGH v. 8. 6. 2010 – C-58/08, EuZW 2010, 539 Rn. 51 und die dort angeführte Rechtsprechung. – Vodafone u.a.). Der EuGH befand die entsprechende Verordnung zur Publikation der Agrarsubventionsempfänger teilweise ungültig, sah insofern ein Überwiegen der Rechte der Betroffenen.

Auch im Zusammenhang mit der **Vorratsdatenspeicherung** ging es um Beschränkung des Eingriffs in die Datenschutzrechte auf das „absolut Notwendige", wobei der EuGH sowohl den Eingriff in das Recht auf Achtung des Privatlebens (Art. 7 EU-GRCh) als auch den Eingriff in das Recht auf Schutz personenbezogener Daten (Art. 8 EU-GRCh) betonte (EuGH v. 8.4.2014 – C-293/12, C-594/12 – Digital Rights Ireland Ldt. und Seitlinger, Herr Tschohl u.a.; s. nun auch zu sehr engen Voraussetzungen EuGH v. 21.12.2016 – C-203/15). Ganz nahe an der Rechtsprechung des BVerfG zum **„unheimlichen Gefühl der Beobachtung"** (S. 28) ist der EuGH in Rz. 37: *„Außerdem ist der Umstand, dass die Vorratsspeicherung der Daten und ihre spätere Nutzung vorgenommen werden, ohne dass der Teilnehmer oder der registrierte Benutzer darüber informiert wird, geeignet, bei den Betroffenen – (…) – das Gefühl zu erzeugen, dass ihr Privatleben Gegenstand einer ständigen Überwachung ist."* (EuGH v. 8.4.2014 – C-293/12, C-594/12).

Die Entscheidung ist auch für die Beurteilung der Möglichkeiten zur Profilbildung und Ähnlichem im Rahmen der DS-GVO zu beachten: Es erfolgt eine **parallele** Anwendung der Art. 7 GRCh (Privatleben, Kommunikation) und Art. 8 Datenschutzgrundrecht, bzw. parallele Prüfung der Eingriffe in diese Grundrechte, zusätzlich die Erwähnung der **Abschreckungswirkung** der Vorratsdatenspeicherung für Kommunikationsprozesse, sodass auch die Meinungsfreiheit aus Art. 11 GRCh berührt sein kann. Rz. 27–29 gehen auf die Gefahren der Vorratsdatenspeicherung und der Auswertung durch Profilbildung ein (EuGH v. 8.4.2014 – C-293/12, C-594/12):