Betrieblicher Datenschutz

Rechtshandbuch

Bearbeitet von
Prof. Dr. Nikolaus Forgó, Prof. Dr. Marcus Helfrich, und Prof. Dr. Jochen Schneider, Bearbeitet von den Herausgebern und von Marian Arning, LL.M., Till Baer, Dr. Benno Barnitzke, LL.M., Julia Bichlmaier, Dr. Christiane Bierekoven, Dr. Dirk Bieresborn, Prof. Dr. Georg Borges, Dr. Tobias Born, Isabell Conrad, Prof. Dr. Kai Cornelius, LL.M., Jonas Dall'Armi, Rechtsanwalt, Maria-Urania Dovas, LL.M., Dr. Eugen Ehmann, Dr. Sonja Fechtner, LL.M., Thorsten Feldmann, LL.M., Dr. Uwe Günther, Dr. Nils Christian Haag, Dr. Stefan Hanloser, Dominik Hausen, Christian Hawellek, Joerg Heidrich, Sarah Jensen, Dipl.-Jur., Wissenschaftliche Mitarbeiterin, JProf. Dr. Timoleon Kosmides, LL.M. Eur., Dr. Sebastian Kraska, Dr. Flemming Moos, Simon Quae, Rechtsanwalt, Laura Schabmair, LL.B., Dr. Gregor Scheja, Hans-Hermann Schild, Prof. Dr. Fabian Schmieder, Barbara Schmitz, Dr. Christian Schröder, Dr. Georg F. Schröder, LL.M., Dr. Robert Selk, LL.M., Dr. Axel Spies, Winfried Veil, Dr. Christoph Wegener, Dr. Hans Peter Wiesemann

3. Auflage 2019. Buch. LXXII, 1640 S. Hardcover (In Leinen)
ISBN 978 3 406 72579 1
Format (B x L): 16,0 x 24,0 cm

Japans Datenschutzgesetzgebung basiert auf dem **Personal Information Protection Act** von 2003 („PIPA") – für den privaten Sektor seit dem 1.4.2005 mit Ergänzungen, die 2017 in Kraft traten.[73] In Übereinstimmung mit der japanischen juristischen Tradition enthält PIPA nur allgemeine Anforderungen für den Datenschutz (z. B. dass die Datenübermittlung an Dritte grundsätzlich der Zustimmung des Betroffenen bedarf), sodass die Details in den Regelungen durch die Exekutive durch Verwaltungsrichtlinien zu finden sind. Einige Ministerien haben solche Regeln erlassen.[74]

Die **Richtlinien** enthalten obligatorische und freiwillige Regelungen. Unternehmen in Japan müssen sorgfältig prüfen, ob das Ministerium, unter dessen Aufsicht die Unternehmen fallen, solche Richtlinien erlassen hat. Ein Unternehmen kann auch Gegenstand mehrerer Richtlinien je nach Umfang der Geschäftstätigkeit sein, wobei die Bestimmungen einer solchen Richtlinie nicht notwendigerweise identisch sind. Verstöße gegen die Richtlinien können je nach der Art und Schwere der Verletzung durch das zuständige Ministerium sanktioniert werden. **33**

Im April 2015 verkündete Japans Regierung, dass sie sich aktiv um einen **Angemessenheitsstatus der EU** bemühen möchte. Dazu brachten sie ein Gesetzesvorhaben in das Parlament ein, welches als Novelle zu PIPA am 3.9.2015 angenommen wurde.[75] So wurde zum Inkrafttreten am 1.1.2016 Japans erste unabhängige Datenschutzbehörde („Personal Information Protection Commission" – „PIPC"), die mit dem umfassenden Schutz der persönlichen Informationen betraut ist, etabliert. Zudem enthält die Novelle eine Definition von persönlichen Daten, Angaben zum Gebrauch von anonymisierten Daten und einige Harmonisierungen mit dem internationalen Rechtsrahmen. Die EU-Kommission hat am 5.4.2018 das Verfahren zur Annahme des angemessenen Datenschutzniveaus Japans eingeleitet. **34**

Ähnliche Bestrebungen haben in **Südkorea** eingesetzt. Das südkoreanische Ministerium für Information („MOI") bekräftigte im Dezember 2015, dass das Land den EU-Angemessenheitsstatus bis zur zweiten Jahreshälfte 2017 anstrebe und gegebenenfalls Gesetze zur Anhebung des Datenschutzniveaus erlassen werde. Eine EU-Entscheidung gibt es derzeit (noch) nicht. Bislang kannte Südkorea kein umfassendes Datenschutzgesetz, obgleich ein Gesetz zum Schutz persönlicher Information seit 2011 besteht („Personal Information Protection Act" – „PIPA"), welches den Regelungen in Japan ähnelt. Flankiert wird das Gesetz von weiteren Regelungen (Guidelines), die zumindest teilweise den südkoreanischen Datenschutz beeinflussen. An erster Stelle sei der IT Network Act genannt, dessen Vollzug von der Korea Communications Commission (KCC) sichergestellt wird und zur Sicherheit der Datennetze beitragen soll. **35**

D. Südamerika

Viele südamerikanische Staaten haben das EU-Datenschutzkonzept weitgehend oder in Grundzügen übernommen. Die spanische Datenschutzbehörde arbeitet seit **36**

[73] BNA World Report, 11/2008, S. 27; vgl. die detaillierte Darstellung zu Japan in BNA World Report 12/2008, S. 3.

[74] Beispiel: Richtlinie des Ministeriums für Gesundheit, Arbeit und Beschäftigung (MHLW).

[75] *Miyashita,* Japans amends its DP Act in light of Big Data and data transfers; Privacy Laws and Business International Report 2015, S. 8–11.

Jahren eng mit vielen Ländern dieser Region zusammen.[76] Dementsprechend hat die Artikel-29-Datenschutzgruppe für die EU entschieden, dass das Datenschutzrecht in **Argentinien** aus EU-Sicht angemessen ist. Dies hat zur Folge, dass Datentransfers aus der EU nach Argentinien ohne besondere Garantien oder Restriktionen zulässig sind.[77] Im Oktober 2010 ist noch **Uruguay** mit einer Stellungnahme der Artikel-29-Datenschutzgruppe dazugekommen.[78]

37 **Chile** verfügt seit 1999 über allgemeine Datenschutzvorschriften.[79] Ein EU-kompatibles Datenschutzgesetz steht allerdings noch aus. **Brasilien** weist eine Verfassungsvorschrift zum Schutz von personenbezogenen Daten auf (in Form einer „Habeas Data"-Vorschrift, die den Datenzugang für die Bürger sicherstellt) und hat seit dem 14.8.2018 ein neues Datenschutzgesetz (LGPD).[80] Am 27.1.2016 veröffentliche das brasilianische Justizministerium einen Änderungsentwurf zum „Marco Civil da Internet", der sich mit den Themen der Netzneutralität und Sicherheitsmechanismen für gespeicherte Daten im Internet befasst.[81] Der brasilianische Supreme Court entschied 2011, dass das Bankgeheimnis nicht ohne Gerichtsbeschluss „gebrochen" werden darf.[82]

38 **Peru** hat 2011 ein neues Datenschutzrecht erlassen, das ebenfalls nach dem europäischen Konzept gestaltet ist.[83] Es folgt damit **Uruguay** und **Kolumbien.**[84] **Mexikos** neue Ausführungsvorschriften zum Datenschutzgesetz traten am 22.12.2011 in Kraft.[85] Wie ernst es Mexiko meint, verdeutlicht eine Geldstrafe in Höhe von 2 Mio. US-Dollar, die eine mexikanische Bank wegen der Verletzung der Datenschutzvorschriften treffen soll. Wann diese Länder von der Europäischen Kommission die „Angemessenheit" des Datenschutzniveaus bescheinigt bekommen (Adequacy), steht noch nicht fest.

---

[76] Siehe das Netzwerk Red Iberoamericana de Protección de Datos, abrufbar unter http://www.redipd.org/noticias_todas/2011/novedades/news/15_07_2011-ides-idphp.php (Stand: 3/2016).

[77] EU-Kommissionsentscheidung C(2003) 1731 v. 30.6.2003, ABl. L 168 v. 5.7.2003, abrufbar unter http://ec.europa.eu/transparency/regdoc/rep/3/2003/DE/3–2003-1731-DE-F1–2.pdf (Stand: 2/2018). Ganz gibt die EU die Kontrolle jedoch nicht auf. Nach Art. 3 der Entscheidung können die europäischen Datenschutzbehörden jedoch zum Schutz von Privatpersonen bei der Verarbeitung ihrer personenbezogenen Daten die Datenübermittlung an einen Empfänger in Argentinien auszusetzen, „wenn Grund zur Annahme besteht, dass die zuständige argentinische Behörde nicht rechtzeitig angemessene Maßnahmen ergreift bzw. ergreifen wird, um den betreffenden Fall zu lösen …".

[78] *Artikel-29-Datenschutzgruppe,* Opinion 6/2010 on the level of protection of personal data in the Eastern Republic of Uruguay (WP 177), abrufbar unter http://collections.internetmemory.org/haeu/20171122154227/http:/ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm (Stand: 2/2018).

[79] Ley 19.628 Sobre Protección a la Vida Privada del 28 de Agosto de 1999. Modificada por la Ley 19.812 de 13 de Junio de 2002 – basierend auf Art. 19 (4) der Chilenischen Verfassung, abrufbar unter http://www.redipd.org/documentacion/legislacion/common/legislacion/Chile/legislacion/ley_19812.pdf (Stand: 3/2016).

[80] Law No 13, 709, abrufbar auf Englisch unter https://www.pnm.adv.br (Brazilian General Data Protection Law) (Stand: 9/2018).

[81] https://iapp.org/news/a/marco-civil-da-internet-presidential-draft-decree-comments-and-main-points (Stand: 3/2016).

[82] http://www.jusbrasil.com.br/noticias/busca?q=ao+RE+389.808 (Stand: 3/2016).

[83] Gesetz v. 7.6.2011, Data Protection Bill No. 4079/2009-PE.

[84] *Renuncio-Mateos,* PL&B International 2/2011, 17.

[85] Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, http://dof.gob.mx/nota_detalle.php?codigo=5226005&fecha=21/12/2011 (Stand: 2/2018).

E. Australien/Neuseeland

Der Datenschutz in Australien und Neuseeland folgt in vielerlei Hinsicht dem EU-Recht, gibt aber gleichzeitig den Unternehmen einen relativ großen Spielraum. In **Australien** besteht das Datenschutzrecht aus Bundes- und Landesgesetzen. Am 1.11.2010 wurde das Amt des Datenschutzbeauftragten in das Amt des australischen Information Commissioner (OAIC) integriert und dadurch gestärkt.[86] Der Australische **Privacy Act** von 1988 in der aktuellen Fassung ist das grundlegende Gesetz.[87] Schedule 3 (National Privacy Principles) dieses Gesetzes enthält unter Prinzip 9 einige Vorschriften zum internationalen Datentransfer aus Australien, die den Regeln der DSRL nachgestaltet sind. Die Datentransferregeln sind etwas liberaler als in der EU. Insbesondere ist der Datentransfer danach zulässig, wenn „die Organisation [der Datenexporteur] vernünftigerweise der Ansicht ist, dass die Empfänger der Informationen einem Gesetz, bindenden Regelungen oder Verträgen unterliegen, die wirksam Grundsätze für einen fairen Umgang mit den Informationen aufrechterhalten, die substantiell den National Privacy Principles ähnlich sind." Kleinere private Gesellschaften mit Jahresumsätzen unter drei Millionen australische Dollar (AUD) sind von vielen Vorschriften ausgenommen.[88] **39**

Das Amt des **Information Commissioner** wurde erneut durch den Privacy Amendment Act aus 2012, welcher am 12.3.2014 in Kraft getreten ist, gestärkt. Fortan kann der Commissioner selbstständig Ermittlungen einleiten und – zum ersten Mal – bei schwerwiegenden oder wiederholten Verstößen Geldbußen aussprechen. Ein Gesetzesvorhaben aus Dezember 2015 möchte Befugnisse weiter ausdehnen.[89] Dreh- und Angelpunkt wird jedoch ein „schwerwiegender Datenverstoß" („serious data breach") bleiben, der dann angenommen wird, wenn ein „reales Risiko für schwerwiegende Verstöße" besteht. Seit dem 18.2.2018 besteht eine neue Pflicht für Verarbeiter mit mehr als 3 Mio. AU-Dollar Umsatz, einen Bruch der Datensicherheit bei der Behörde anzuzeigen.[90] **40**

Inhaltlich hat der Commissioner festgelegt, dass Metadaten, die aus Telefongesprächen stammen, auch zu den persönlichen Daten zählen.[91] In dem Fall wollte ein Journalist Zugang zu allen Metadaten seines Telefonanbieters erlangen, die dieser über ihn gesammelt hat. Der Begriff der **„Metadaten"** wurde in dem am 26.3.2015 erlassenen „Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 („Data Retention Law")[92] per Gesetz definiert und bezieht verschiedene Gruppen (bspw. „die Quelle der Information") ein. Gleichzeitig ermöglicht das „Data Retention Law" den Zugang zu Metadaten für insgesamt 20 **41**

[86] http://www.privacy.gov.au/ (Stand: 2/2018).

[87] http://www.comlaw.gov.au/details/C2013C00231 (Stand: 2/2018).

[88] *Fuchs,* Law360 v. 16.8.2011, abrufbar unter http://www.law360.com/privacy/articles/245851?utm_source=newsletter&utm_medium=email&utm_campaign=privacy (Stand: 2/2018).

[89] https://www.ag.gov.au/consultations/pages/serious-data-breach-notification.aspx (Stand: 2/2018).

[90] *Privacy Amendment* (Notifiable Data Breaches) Act 2017.

[91] Royal Assent, v. 22.2.2017, abufbar unter ttp://www8.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/AICmr/2015/35.html (Stand: 2/2018).

[92] http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fbills%2Fr5375_aspassed%2F0000%22;rec=0 (Stand: 2/2018).

Organisationen ohne gerichtliche Entscheidung. Die Begrenzungslinien des Gesetzes bleiben jedoch unscharf, da eine gerichtliche Entscheidung für den „Inhalt" der Metadaten weiterhin obligatorisch bleibt.

42 Das grundlegende Datenschutzgesetz in **Neuseeland** ist der Privacy Act 1993, der stark von den OECD-Leitlinien von 1980 für den Schutz der Privatsphäre und den grenzüberschreitenden Verkehr personenbezogener Daten beeinflusst wurde. Nach dem Privacy Act hat der Privacy Commissioner als unabhängige Behörde eine Reihe von Richtlinien, Merkblätter und andere Informationen herausgegeben, welche die Rechte und Pflichten für Organisationen und Einzelpersonen sowie Regeln für Beschwerden umfassen.[93] Die Artikel-29-Datenschutzgruppe (→ *Spies*, VI.2. Rn. 3) hat Neuseeland in einer Stellungnahme vom 4.4.2011 die Angemessenheit des Datenschutzes aus EU-Sicht bescheinigt.[94]

---

[93] http://privacy.org.nz/ (Stand: 2/2018).

[94] *Artikel-29-Datenschutzgruppe*, Opinion 11/2011 on the level of protection of personal data in New Zealand (WP 182), abrufbar unter http://collections.internetmemory.org/haeu/20171122154227/http:/ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm (Stand: 2/2018).

Kapitel 5. Grundsätze der datenschutzrechtlichen Prüfung

Übersicht

Literatur: *Astheimer,* Im Zweifel löschen?, fas-net.de, 4.4.2018, abrufbar unter http://www.faz.net/aktuell/wirtschaft/diginomics/datenschutz-warum-vor-allem-der-mittelstand-die-dsgvo-fuerchtet-15523443.html (Stand:8/2018); *Auer-Reinsdorff/Conrad,* Handbuch IT- und Datenschutzrecht, 2.Auflage 2016 (zit. Auer-Reinsdorff/Conrad/*Bearbeiter*); *Beuth/Böhm/Breithut/Gruber,* Datenschutz-Grundverordnung: Endlich verständlich – was die neuen EU-Regeln für die Bürger bedeuten, 14.5.2018, Spiegel online, abrufbar unter http://www.spiegel.de/netzwelt/web/dsgvo-das-sollten-sie-zur-datenschutz-grundverordnung-der-eu-wissen-a-1205985.html (Stand: 8/2018); *Ehmann/Kranig,* Fünf nach zwölf im Datenschutz, ZD 2018, 199; *Ehmann/Selmayr,* DS-GVO, 2017; *Jarass,* Charta der Grundrechte der EU, 3. Aufl. 2016; *Gola,* Datenschutz-Grundverordnung, 2. Aufl. 2018 (zit. Gola/*Bearbeiter*); *Grabitz/Hilf/Nettesheim,* Das Recht der Europäischen Union, 63. EL, Stand: 12/2017 (zit. Grabitz/Hilf/Nettesheim/*Bearbeiter*); *Hamann,* Europäische Datenschutz-Grundverordnung – neue Organisationspflichten für Unternehmen, BB 2017, 1090; *Hansen/Brechtel,* KUG vs. DS-GVO: Kann das KUG anwendbar bleiben?, GRUR-Prax 2018, 369; *Jehle,* Das DSGVO-Chaos ist angerichtet, Telepolis, heise online, 3.5.2018, abrufbar unter https://www.heise.de/tp/features/Das-DSGVO-Chaos-ist-angerichtet-4037911.html (Stand: 8/2108); *Johannes,* Der BDSG-Entwurf und das Mysterium der „23", ZD-Aktuell, 2017, 05533; *Jung,* Datenschutz-(Compliance-)Management-Systeme – Nachweis- und Rechenschaftspflichten nach der DS-GVO, ZD 2018, 208; *Kühling/Buchner,* DS-GVO BDSG, 2. Aufl. 2018 (zit. Kühling/Buchner/*Bearbeiter*); *Lauber-Rönsberg/Hartlaub,* Personenbildnisse im Spannungsfeld zwischen Äußerungs- und Datenschutzrecht, NJW 2017, 1057; *Niklas/Faas,* Der Datenschutzbeauftragte nach der Datenschutz-Grundverordnung, NZA 2017, 1091; *Oberlin,* Die Implementation der Datenschutzgrundverordnung (DS-GVO) in ein Compliance Management System (CMS), CB 2018, 51; *Paal/Pauly* (Hrsg.), Datenschutz-Grundverordnung Bundesdatenschutzgesetz, 2. Aufl. 2018 (zit. Paal/Pauly/*Bearbeiter*); *Roßnagel,* Gesetzgebung im Rahmen der Datenschutz-Grundverordnung, DuD 2017, 277; *Sydow* (Hrsg.), Europäische Datenschutzgrundverordnung, 2. Aufl. 2018 (zit. Sydow/*Bearbeiter*); *Wiedekind,* Datenschutzgrundverordnung: Was Nutzer jetzt wissen müssen, 22.5.2018, n-tv.de, abrufbar unter https://www.n-tv.de/technik/Was-Nutzer-jetzt-wissen-muessen-article20445218.html (Stand: 8/2018).

A. Woran erkennt man die datenschutzrechtliche Relevanz?

1 Mit dem Wirksamwerden der DS-GVO zum 25.5.2018 konnte man bei der Lektüre der Tagespresse[1] den Eindruck gewinnen, dass sowohl die Unternehmen als

[1] Vgl. beispielhaft *Beuth/Böhm/Breithut/Gruber,* 14.5.2018, Spiegel online, abrufbar unter http://www.spiegel.de/netzwelt/web/dsgvo-das-sollten-sie-zur-datenschutz-grundverordnung-der-eu-wissen-a-1205985.html (Stand: 8/2018); *Wiedekind,* 22.5.2018, n-tv.de, abrufbar unter https://www.n-tv.de/technik/Was-Nutzer-jetzt-wissen-muessen-article20445218.html (Stand: 8/2018); *Jehle,* Telepolis, heise online, 3.5.2018, abrufbar unter https://www.heise.de/tp/features/Das-DSGVO-

auch Private in der Bundesrepublik Deutschland erstmals mit dem Phänomen des Datenschutzes und der damit einhergehenden rechtlichen Regelungen konfrontiert seien.

Sowohl die ersten Reaktionen auf das Inkrafttreten als auch die seit der Verab- **2**
schiedung der DS-GVO im April 2016 in den betroffenen Kreisen der Wirtschaft festzustellende nur zögerliche Auseinandersetzung mit den gesamteuropäischen Rechtsänderungen[2] zeigen, dass auf breiter Ebene offenbar Zugangsschwierigkeiten zur Regelungsmaterie des Datenschutzes bestehen. Diese möglichen Verunsicherungen sind nicht zuletzt auch auf die nunmehr deutlich verschärften Bußgelddrohungen zurückzuführen und die damit verbundene Sorge vor unternehmerischen und persönlichen Haftungsrisiken.

Mit diesem Kapitel soll zunächst der Versuch unternommen werden, eine allge- **3**
meine Orientierung zu vermitteln, unter welchen Voraussetzungen datenschutzrechtliche Regelungen zu beachten sind. Mit dem vorliegenden Kapitel sollen zugleich die Bezüge zu den folgenden vertiefenden Kapiteln des Handbuchs hergestellt und so ein Überblick über die Dimensionen des betrieblichen Datenschutzes verschafft werden.

B. Welche Regelungen sind heranzuziehen?

Ausgangsfrage jeder datenschutzrechtlichen Orientierung ist stets, ob der Sach- **4**
verhalt, der nach einer rechtlichen Einordnung fragt, überhaupt dem Datenschutzrecht zuzuordnen ist. Diese Frage ist durchaus von Bedeutung, da das Datenschutzrecht nur einen – wenn auch wirtschaftlich wichtigen – Teil des Schutzes der Persönlichkeit des Einzelnen[3] darstellt. Die Verarbeitung von Informationen erfolgt beispielsweise regelmäßig auch im journalistischen Kontext oder auch im Rahmen wissenschaftlicher Betätigungen. Wollte man diese Tätigkeiten, die ihrerseits ebenfalls grundrechtlichen Schutz[4] genießen, ohne Weiteres ausschließlich dem Datenschutz unterstellen, würden diese besonderen grundrechtlichen Aspekte verkannt werden. Ebenso muss der Regelungsanspruch des Datenschutzrechts im Verhältnis zu dem Schutz des Privat- und Familienlebens gesehen werden, die ihrerseits durch Art. 7 GRCh einen besonderen grundrechtlichen Schutz genießen, der u. a. auch die hoheitliche Regelungsgewalt des Staates begrenzt.[5]

I. Verhältnis der DS-GVO zu nationalen Datenschutzbestimmungen

Mit der DS-GVO hat der europäische Gesetzgeber nach der RL 46/95/EG eine **5**
Regelung geschaffen, die den Anspruch erhebt, im gesamten Geltungsbereich der

---

Chaos-ist-angerichtet-4037911.html (Stand: 8/2108); *Astheimer,* fas-net.de, 4.4.2018, abrufbar unter http://www.faz.net/aktuell/wirtschaft/diginomics/datenschutz-warum-vor-allem-der-mittelstand-die-dsgvo-fuerchtet-15523443.html (Stand: 8/2018).

[2] Vgl. hierzu *Ehmann/Kranig,* ZD 2018, 199.

[3] → *Schneider/Forgó/Helfrich,* I.1. Rn. 29 ff.

[4] Siehe hierzu Art. 11, 13 GRCh.

[5] *Jarass,* Charta Der Grundrechte der EU, 3. Aufl. 2016, Art. 7 Rn. 34 f.; *EuGH,* Urt. v. 6.10.2015 – C-362/14 – Schrems, Rn. 94, ZD 2015, 549 m. Anm. *Spies* = MMR 2015, 752 m. Anm. *Bergt.*

Europäischen Union ein **einheitliches Datenschutzrecht** zu schaffen (→ *Forgó,* I.2.). Als Verordnung kommt der DS-GVO nach Art. 288 Abs. 2 AEUV unmittelbare Geltung in allen Mitgliedstaaten zu.[6] Wegen des Vorrangs europarechtlicher Bestimmungen gegenüber nationalen Regelungen[7] stellt sich grundsätzlich die Frage, woran sich der Rechtsanwender zu orientieren hat, sollten neben den Vorschriften der EU (DS-GVO) auch Bestimmungen auf nationaler Ebene als geltendes Recht den Anspruch erheben, in der Lebenswirklichkeit von den Rechtsanwendern befolgt zu werden (→ *Forgó,* I.2.; → *Borges,* I.3.).

6 Die DS-GVO hat davon abgesehen, das Datenschutzrecht in allen Aspekten vollständig und umfassend zu regeln. Zwar folgt die DS-GVO dem **Anspruch der Vollharmonisierung.**[8] Jedoch sieht die DS-GVO an etlichen Stellen die Möglichkeit vor, dass die Mitgliedstaaten im Rahmen der DS-GVO spezifischere Vorschriften beibehalten oder schaffen, mit denen die datenschutzrechtlichen Vorgaben[9] der DS-GVO ausgeformt werden.

7 Für den Anwender hat dies die durchaus missliche Folge, dass er zwar zunächst von den Vorschriften der DS-GVO auszugehen hat. Je nachdem, in welchem Kontext Daten verarbeitet werden, muss zudem ermittelt werden, ob auf nationaler Ebene zusätzlich spezifischere Regelungen zu beachten sind. Während der ursprüngliche Entwurf der Kommission zur DS-GVO noch vorsah, dass auf der europäischen Ebene selbst durch sog. „delegierte Rechtsakte" nach Art. 290 AEUV die Kommission selbst den datenschutzrechtlichen Rahmen spezifizierend ausformen sollte, zeigten die Verhandlungen über die DS-GVO, dass die Mitgliedstaaten erhebliche Vorbehalte gegen eine damit einhergehende Stärkung der Kommission hatten und sich über **„Öffnungsklauseln"** jedenfalls teilweise die gestalterische Kompetenz auf dem Gebiet des Datenschutzes vorbehalten wollten. Im Ergebnis führt dies nicht nur zu den bereits erwähnten zahlreichen Klauseln, mit denen die DS-GVO den Mitgliedstaaten datenschutzrechtliche Regelungsaufgaben belässt oder einräumt. In der Praxis bedeutet dies zudem, dass bei grenzüberschreitenden Datenverarbeitungen durchaus zusätzlich zu den Vorschriften der DS-GVO die jeweiligen **nationalen Besonderheiten** zu beachten sind.[10] Insoweit löst die gegenwärtige datenschutzrechtliche Situation in Europa den Anspruch auf Vollharmonisierung jedenfalls nicht in vollem Umfang ein.

8 Da es sich bei den nationalen Vorschriften allerdings nur um solche handeln kann, die aufgrund ausdrücklicher Kompetenznormen der DS-GVO erlassen oder beibehalten wurden, folgt hieraus für den Rechtsanwender, dass er **zunächst** danach zu suchen hat, ob der einzuschätzende Sachverhalt durch die **Bestimmungen der DS-GVO** hinreichend geregelt wird. Nur soweit dort auf nationale Vorschriften verwiesen wird, beispielsweise über Art. 6 Abs. 2 DS-GVO oder im Zusammenhang mit dem Beschäftigtendatenschutz,[11] der Nutzung personenbezogener Daten im Rah-

---

[6] Grabitz/Hilf/Nettesheim/*Nettesheim,* Das Recht der Europäischen Union, Art. 288 Rn. 101 f.

[7] Grabitz/Hilf/Nettesheim/*Nettesheim,* Das Recht der Europäischen Union, Art. 288 Rn. 47 ff.

[8] Ehmann/Selmayr/*Selmayr/Ehmann,* DS-GVO, Einf. Rn. 75 ff.; zur Diskussion, ob es sich um eine Vollharmonisierung oder lediglich einen Mindeststandard handelt Kühling/Buchner/*Maschmann,* DS-GVO, Art. 88 Rn. 30 f.

[9] Ehmann/Selmayr/*Selmayr/Ehmann,* DS-GVO, Einf. Rn. 82 ff.

[10] Siehe hierzu die in diesem Band enthaltenen Länderberichte zu den jeweiligen nationalen Besonderheiten in der Ausgestaltung des durch die DS-GVO vorgegebenen Rahmens.

[11] Art. 88 DS-GVO.