forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

FORUM PRIVATHEIT UND SELBSTBESTIMMTES LEBEN IN DER DIGITALEN WELT

Forschungsbericht

# Das Sanktionsregime der Datenschutz-Grundverordnung

## Auswirkungen auf Unternehmen und Datenschutzaufsichtsbehörden

Forschungsbericht

# Das Sanktionsregime der Datenschutz-Grundverordnung

## Auswirkungen auf Unternehmen und Datenschutzaufsichtsbehörden

**Autorinnen und Autoren:**
**Nicholas Martin[1], Tamer Bile[2], Maxi Nebel[2], Felix Bieker[3], Christian Geminn[2], Alexander Roßnagel[2], Charlotte Schöning[4]**

(1) Fraunhofer-Institut für System- und Innovationsforschung ISI, Karlsruhe
(2) Universität Kassel, Projektgruppe verfassungsverträgliche Technikgestaltung (provet)
(3) Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Kiel
(4) Universität München, Institut für Wirtschaftsinformatik und Neue Medien (WIM)

Herausgeber:
Michael Friedewald, Regina Ammicht Quinn, Marit Hansen, Jessica Heesen, Thomas Hess, Nicole Krämer, Jörn Lamla, Christian Matt, Alexander Roßnagel, Michael Waidner

# Inhalt

# 1 Einleitung

Die Datenschutz-Grundverordnung (DSGVO) hat sich zum Ziel gesetzt, einen verbesserten Schutz der Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere ihres Rechts auf Schutz personenbezogener Daten zu bewirken.[1] Hierfür ist entscheidend, wie die Einhaltung der Vorschriften der Datenschutz-Grundverordnung kontrolliert und durchgesetzt werden kann. Um bei Verstößen die Handlungsmöglichkeiten der Aufsichtsbehörden zu verbessern, wurde das Sanktionsregime der Datenschutz-Grundverordnung – im Vergleich zum bisherigen Sanktionsregimen, etwa nach der alten Fassung des Bundesdatenschutzgesetzes (im Folgenden: BDSG a. F.) – deutlich verschärft.

Die Datenschutzrichtlinie aus dem Jahr 1995 hatte die Gestaltung des Sanktionsregimes noch den Mitgliedstaaten überlassen. Dies hatte zur Folge, dass die rechtlichen Sanktionsinstrumente in den Mitgliedstaaten uneinheitlich ausgestaltet waren; in einigen Mitgliedstaaten war es Datenschutzaufsichtsbehörden (im Folgenden: Aufsichtsbehörden) etwa überhaupt nicht gestattet, Geldbußen zu verhängen. In Deutschland konnten die Aufsichtsbehörden nach § 43 BDSG a. F. je nach Art des Verstoßes lediglich Bußgelder bis zu 50.000 bzw. bis zu 300.000 Euro pro Verstoß verhängen; vereinzelt wurden gegen einzelne Unternehmen als Spitzenwert Bußgelder in einer Gesamthöhe unter 2 Mio. Euro verhängt.[2]

Die Datenschutz-Grundverordnung schreibt nunmehr einheitliche und spürbare Sanktionen vor. Seit Wirksamwerden der Datenschutz-Grundverordnung am 25. Mai 2018 beträgt die maximale Geldbuße nach Art. 83 DSGVO für Datenschutzverstöße bis zu 20 Mio. Euro. Gegen Unternehmen sind noch deutlich höhere Geldbußen möglich: Hier können die Aufsichtsbehörden Geldbußen von bis zu vier Prozent des weltweiten Umsatzes des Vorjahres verhängen. Die Regelungen zur angedrohten Bußgeldhöhe sind vom Kartellrecht geprägt und von dem Ziel geleitet, von Datenschutzverstößen „abzuschrecken".[3]

Trotz Erweiterung der Sanktionsmöglichkeiten ist die befürchtete „Sanktionswelle" seit dem 25. Mai 2018 bislang ausgeblieben: Es wurden nicht – wie vielfach kolportiert – Hunderte Bußgeldbescheide an Blogger, Bäckereien oder Sportvereine zugestellt; auch haben die Aufsichtsbehörden nicht die Zentralen von IT-Unternehmen gestürmt.[4] Dennoch sind einige Fälle bekannt geworden, die zeigen, dass die Aufsichtsbehörden in Deutschland und in anderen Mitgliedstaaten vermehrt Unternehmen prüfen und Verstöße gegen die Datenschutz-Grundverordnung konsequent ahnden: So hat der Landesbeauftragte für Datenschutz und Informationsfreiheit (LfDI) Baden Württemberg gegen das Chatportal „Knuddels" ein Bußgeld in Höhe von 20.000 Euro verhängt, da dem Portal nach einem Hacking-Angriff die Passwörter, E-Mail-Adressen und Pseudonyme von rund 330.000 Nutzern entwendet und auf einer Filesharing-Website angeboten wurden. Dass die Geldbuße eher „milde" ausfiel, hing mit der Bereitschaft des Verantwortlichen zusammen, mit der zuständigen Datenschutzbehörde zu kooperieren.[5] Ein Bußgeld-Fall, der über die Grenzen des Mitgliedstaates Aufmerksamkeit erregt hat, wurde in Portugal erlassen: Die portugiesische Aufsichtsbehörde hat einem Krankenhaus ein Bußgeld in Höhe von 400.000 Euro auferlegt, weil auf die Patientendaten, die nur für Ärzte einsehbar sein sollten, auch von Technikern zugegriffen werden konnte.[6] Deutlich höher fiel das Bußgeld gegen Google LLC aus: Die französische Datenschutzbehörde Commission Nationale de L'Informatique et des Libertés (CNIL) hat gegen Google eine Rekordstrafe in Höhe von 50 Mio. Euro verhängt. Die Behörde sieht gleich zwei Verstöße von Google gegen die Datenschutz-Grundverordnung: Zum einen missachte der Konzern die Pflicht nach Art. 5, 13 und 14 DSGVO, seine Nutzer transparent über die Datennutzung zu informieren; zum anderen könne der Konzern keine wirksame Einwilligung für die Verarbeitung der Daten für Werbezwecke vorweisen.[7]

Damit dürfte das Datenschutzrecht künftig – schon allein wegen der potentiell drohenden hohen Bußgelder und der vom Unionsgesetzgeber intendierten abschreckenden Wirkung – eine ernstzunehmende Vorgabe für Compliance sein.

Im Rahmen dieses Berichts wird einerseits untersucht, welche Auswirkungen die potentiell drohenden hohen Geldbußen auf datenverarbeitende Unternehmen haben. Andererseits wird der Frage nachgegangen, inwieweit zu erwarten ist, dass die Aufsichtsbehörden künftig Gebrauch von ihrer Befugnis machen werden, gegebenenfalls "millionenschwere" Geldbußen zu verhängen. In diesem Zusammenhang wird auch beleuchtet, welche Bedingungen erforderlich sind, damit die Aufsichtsbehörden die Sanktionsinstrumente der Datenschutz-Grundverordnung effektiv einsetzen können. Zur Beantwortung dieser Fragen wird in Kapitel 2 zunächst auf die grundsätzliche Frage eingegangen, warum sich Unternehmen (nicht) an Recht und Gesetz halten. In Kapitel 3 wird das Sanktionsregime der Datenschutz-Grundverordnung vorgestellt. Auf die Frage, wie sich die Sanktionen der Datenschutz-Grundverordnung auf die Datenschutzpraxis auswirken, wird in Kapitel 4 näher eingegangen. Anschließend werden in Kapitel 5 die notwendigen Bedingungen betrachtet, die für die Aufsichtsbehörden gegeben sein müssen, um die Sanktionen der Datenschutz-Grundverordnung effektiv umzusetzen. Schließlich erfolgen in Kapitel 6 eine Zusammenfassung sowie ein rechtspolitischer Ausblick.

# 2
# Wissenschaftliche Perspektiven auf die Frage der Compliance – Warum Unternehmen sich (nicht) an Recht und Gesetz halten

Gesellschaftswissenschaftlich betrachtet, fungieren rechtliche Sanktionen als eine Form der externen sozialen Kontrolle. Sie sollen der Geltung von Normen Ausdruck verleihen. In diesem Rahmen gelten Sanktionen als „eine negative Reaktion, die das bekräftigt, von dem abgewichen wurde. Die Bekräftigung ergibt sich aus der Missbilligung der Abweichung".[8]

Die sozialwissenschaftliche Forschung zur Frage, was Compliance-Verhalten in Unternehmen motiviert, also warum Unternehmen sich (nicht) an gesetzliche Vorschriften halten und welche Rolle rechtlichen Sanktionen dabei zukommt, hat drei grundsätzliche Erklärungsansätze entwickelt: *Erstens* der „ökonomische" Ansatz, der auf rationalen Gewinn/Verlust-Berechnungen abstellt; *zweitens* soziologische und von der Verhaltensökonomie inspirierte Theorien, welche die Rolle von sozialem Druck und inneren normativen Überzeugungen thematisieren, und *drittens* der Ansatz, die Fähigkeiten von Unternehmen, Vorschriften überhaupt sinnvoll umzusetzen, in den Vordergrund zu stellen. Empirisch hat die Forschung sich vor allem auf die Bereiche des Umwelt-, Arbeits- und Verbraucherschutzrechts konzentriert, während die Umsetzung von Datenschutzrecht in Unternehmen selbst, bis auf wenige Ausnahmen,[9] bisher wenig erforscht worden ist. Im Folgenden sollen die erwähnten Erklärungsmodelle skizziert und ihre Implikationen für die Anwendung und Wirkmöglichkeiten des neuen Sanktionsregimes herausgearbeitet werden.

## 2.1 Rationale Berechnungen

Der auf die "Law and Economics"-Bewegung zurückgehende selbsternannte "ökonomische Ansatz" (*economic approach*) betrachtet Unternehmen (und Menschen allgemein) als rational und damit amoralisch handelnde Nutzen-Maximierer.[10] Während es sich beim "Nutzen" bezogen auf private Lebensentscheidungen (z. B. über Heirat, Kinder) prinzipiell um verschiedenste Güter handeln kann (Freizeit, psychische Erfüllung usw.), wird "Nutzen" im Kontext von Unternehmens-Motivationen für (nicht) rechtskonformes Verhalten gewöhnlich mit monetärem Gewinn gleichgesetzt.[11] In der einfachsten Formulierung dieses maßgeblich von Gary Becker[12] und George Stigler[13] entwickelten Ansatzes wird die Entscheidung, Rechtsvorschriften Folge zu leisten oder Rechtsbrüche zu begehen, gefällt, indem man die bei Rechtsbruch zu erwartenden zusätzlichen Gewinne $G$ mit der für diesen Rechtsbruch fälligen Strafe $S$ vergleicht, diskontiert um die Wahrscheinlichkeit $P_S$, dass der Rechtsbruch auch entdeckt und sanktioniert wird.[14] Solange $G > S*P_S$ wird der rational handelnde Kaufmann Rechtsbrüche begehen. Weiterentwicklungen des Ansatzes haben darauf hingewiesen, dass dem Kaufmann im Entdeckungsfall neben der Strafe $S$ meist noch zusätzliche Kosten $Z$ entstehen werden (etwa für Rechtsbeistand, Umsatzeinbußen aufgrund von Reputationsverlusten u.ä.), wiederum diskontiert durch ihre Eintrittswahrscheinlichkeit $P_Z$. Vollständig lautet die Entscheidungsformel also $G <> S*P_S + Z*P_Z$.[15] Unter Umständen können die unter der Variable $Z$ subsumierten Kosten in den Kalkulationen von Unternehmen schwerer wiegen als die Strafe $S$.

Empirische Studien legen nahe, dass der Ansatz, zumindest in manchen Situationen, Unternehmensverhalten durchaus gut erklären kann. So fanden Kagan et al., dass die glaubwürdige Durchsetzung von Vorschriften in Form regelmäßiger Kontrollen und empfindlicher Geld- und Haftstrafen die Umsetzung aufwendiger Umweltschutzauflagen in US-amerikanischen Galvanik- und in *kleinen* Chemiewerken maßgeblich moti-

vierte.[16] Zu ähnlichen Ergebnissen kamen Studien zur Umsetzung von Erosionsschutzmaßnahmen im Bausektor,[17] von Arbeitsschutz in Industrie- und Bergbauunternehmen[18] und Verbraucherschutzvorschriften im Finanzsektor.[19]

Jedoch zeigen selbst manche der empirischen Studien die Grenzen der Erklärungskraft dieses Ansatzes auf. Die wesentlichen Kritikpunkte, aus denen sich alternative Erklärungsansätze ergeben, stellen auf drei in diesem Ansatz implizite Annahmen ab: Kalkulierbarkeit, Motivationen und das Modell des Unternehmens als einheitlicher Akteur, dessen Verhalten primär den Präferenzen der Unternehmensleitung entspringt.

Der "ökonomische" Ansatz nimmt an, dass Unternehmensführer die Höhe und Eintrittswahrscheinlichkeit von Sanktionen präzise berechnen und ihre Handlungen entsprechend dieser Kalkulation ausrichten. Das scheint fraglich. Tatsächlich scheinen Manager rechtliche Risiken oft falsch einzuschätzen – sie sowohl zu über- wie zu unterschätzen – und nur sehr ungefähre und oft falsche Vorstellungen der ihnen potentiell drohenden Strafen zu haben.[20] Selbst die kleinen und mittelständischen Chemie- und Galvanikwerke, die in Interviews mit Kagan et al. die Drohung von Strafen als wichtigen Grund für ihre Umsetzung von Umweltauflagen angaben, schienen keine formale „Berechnung" im Sinne der Entscheidungsformel $G <> S*P_S + Z*P_Z$ vorzunehmen. Stattdessen fußten ihre Entscheidungen auf "Daumenregeln", insbesondere der Erwartung, dass Rechtsbrüche früher oder später doch entdeckt und bestraft werden würden – aber auch auf normativen und gesellschaftlichen Motivationen.[21]

## 2.2 Gesellschaftliche Erwartungen und moralische Überzeugungen als Motivationen

Unternehmen und ihre Manager bewegen sich immer auch in einem gesellschaftlichen Umfeld, bestehend aus den Orten, wo sie ansässig sind, zivilgesellschaftlichen Akteuren, Kunden und Verbrauchern, Medien und Politik sowie nicht zuletzt den eigenen Mitarbeitern. Dieses Umfeld richtet Erwartungen an sie, z. B. bezüglich Daten- und Umweltschutz, der Sicherung von Arbeitsplätzen und „good citizenship" im Allgemeinen. Gunningham et al. haben hierfür den Begriff der „gesellschaftlichen Betriebslizenz" (*social license to operate*) geprägt.[22] Werden gesellschaftliche Erwartungen enttäuscht, kann diese "Lizenz" entzogen werden, das Unternehmen und mit ihm assoziierte Personen verlieren bisher genossenes gesellschaftliches Ansehen, es kann sogar zu Protesten, gerichtlichen Klagen und politischer Obstruktion kommen.

In Interviews mit Managern von Zellstofffabriken und Chemiewerken stellten Gunningham et al. fest, dass Sorge um ihre „gesellschaftliche Lizenz" oft mehr Einfluss auf Compliance-Entscheidungen hatte als rechtliche Risiken. Vor allem *große* Werke schienen den Entzug der *social license* als *größtes* Risiko wahrzunehmen, weit mehr als Rechtsstrafen. Bei kleinen Werken hingegen, wie etwa den erwähnten Galvanikern, die sich weniger öffentlicher Aufmerksamkeit ausgesetzt sahen, schienen rechtliche Risiken samt Strafen schwerer zu wiegen.[23] Eine Ausnahme bildeten große Unternehmen in strukturschwachen Standorten, die als Hauptarbeitgeber der Region hohen politischen und gesellschaftlichen Einfluss besaßen.[24]

Zwar wurde die Idee der *social license to operate* in Abgrenzung zum „ökonomischen" Ansatz von Becker/Stigler entwickelt, letztlich geht die Idee aber weiterhin von implizit rational-kalkulierten Nutzen-Kosten – somit im Sinne Beckers[25] „ökonomischen" – Abwägungen aus. Der Unterschied zum klassischen "ökonomischen" Ansatz liegt darin, dass der Nutzen weniger gegen mögliche Rechtsstrafen aufgewogen wird, als gegen ein breiteres Portfolio monetärer und psycho-sozialer Kosten (Ansehensverlust, Scham, Kostensteigerungen aufgrund von durch gesellschaftliches Misstrauen langwierigerer gewordene oder politisierte Zulassungsprozessen etc.) und neben Gewinnerwartungen psycho-soziale Beweggründe wie Reputation expliziter in die Idee des „Nutzens" einbezogen werden. Gleichzeitig grenzt sich der Ansatz von Gunningham et al.[26]

von Erklärungsmodellen ab, die *innere* normative Überzeugungen in den Vordergrund rücken.[27]

Menschen sind jedoch nicht nur rationale Nutzen-Maximierer, sondern haben meist auch moralische Werte verinnerlicht. Ein weiterer Erklärungsansatz führt Gesetzestreue hierauf zurück. Demzufolge halten sich Menschen (somit auch Manager) an Gesetze nicht primär, weil sie rechtliche oder gesellschaftliche Sanktionen fürchten, sondern weil sie die durch das Gesetz operationalisierten Werte bejahen. Auch hierfür gibt es empirische Evidenz. So fanden etwa May und Winter[28] heraus, dass sich dänische Bauern und amerikanische Baufirmen relativ penibel an Umwelt- und Sicherheitsvorschriften hielten, obwohl beide Gruppen die Gefahr, dass Verstöße entdeckt und rechtlich oder gesellschaftlich sanktioniert werden würden, als niedrig einschätzten.[29] Zu ähnlichen Ergebnissen kamen Studien australischer Pflegeheime.[30] Sowohl im Fall der Bauern als auch der Pflegeheime und der Baufirmen ging Gesetzestreue auf normative Überzeugungen von der Richtigkeit und Wichtigkeit der Vorschriften zurück, die oft auch in Berufsethiken integriert waren.

Jedoch scheinen Menschen bei der Bewertung von Gesetzen und der subjektiven „Vertretbarkeit" von Rechtsbrüchen oft private, emotional begründete Maßstäbe anzulegen, die mit dem aus dem Rechtsbruch entstandenen *objektiven* gesellschaftlichen Schäden nicht zwangsläufig eng korrespondieren. Sichtbare, leicht verständliche und direkte Schäden scheinen für Menschen oft subjektiv schwerer zu wiegen – somit höheren Hemmschwellen zu unterliegen – als indirekte, augenscheinlich unscheinbare, aber vielleicht *objektiv* schwerere Schäden. Experimentelle Studien mit amerikanischen Managern und MBA-Studenten etwa fanden, dass die Bereitschaft der Probanden, auch ernste wirtschaftsrechtliche Delikte zu begehen (z. B. Preisabsprachen), wesentlich höher war, als gegen Umweltvorschriften zu verstoßen, die zu *direkten* Schäden an Ökosystemen führten (etwa Gewässerverschmutzung). Verstöße gegen umweltrechtliche Verwaltungsauflagen („Papierkram") hingegen unterlagen keiner vergleichbaren Hemmschwelle.[31]

Das Problem möglicher Missverhältnisse zwischen der objektiven und der von Verursachern *subjektiv* wahrgenommenen Schadenshöhe dürfte gerade im Datenschutz relevant sein. Objektiv sind Datenschutzverstöße Eingriffe in durch Grundrechte besonders geschützte Rechtsgüter. Gleichzeitig ist der durch sie verursachte Schaden oft indirekter oder sogar abstrakter Natur oder tritt erst mit Zeitverzögerung auf und ohne, dass die kausale Verknüpfung zwischen Verstoß (z. B. unbefugter Datenweitergabe) und Folgen (z. B. Absagen in Bewerbungsprozessen) selbst für Verursacher und Geschädigte leicht durchschaubar ist. In der Tat galten Datenschutzverstöße in der Wahrnehmung von Unternehmen und Öffentlichkeit bislang oft eher als Kavaliersdelikte, bei denen sich die Leute „mal locker machen" sollten.[32]

## 2.3 Kapazitäten für Compliance

Die obigen Ansätze führen Compliance auf individualpsychologische Motivationen des höheren Managements zurück. Gesetzes(un)treue wird mit bewussten Entscheidungen des Managements, sich an Recht zu halten oder nicht, erklärt. Das Unternehmen als Organisation tritt in den Hintergrund, es wird implizit als einheitlicher Akteur verstanden.

Diese Perspektive ist vielfach kritisiert worden. Seit den Arbeiten von James March, Herbert Simon und Richard Cyert[33] betont die Organisationsforschung, dass Unternehmen selten sinnvoll als einheitlicher Akteur verstanden werden können, dessen Verhalten direkt dem Willen und Anreizen der Unternehmensführer entspringt. Diese sind vielmehr komplexe Organisationen, die aus multiplen Untereinheiten bestehen. Übergeordnete Ziele (z. B. Gewinn) werden in untergeordnete heruntergebrochen und auf die jeweiligen Untereinheiten verteilt. Deren Verhalten richtet sich nun primär an ihren jeweiligen Unterzielen aus – nicht den übergeordneten Gesamtzielen. Insofern Sanktio-

nen (z. B. Geldbußen) jedoch primär auf übergeordnete Unternehmensziele einwirken, kann ihre Steuerungswirkung nachlassen.

Aufgrund der Informationsflut, der Manager ausgesetzt sind, kann ihr Verhalten meist nur als eingeschränkt rational (*boundedly rational*) gelten: Die Grenzen menschlicher kognitiver Fähigkeiten und schlichter Zeitmangel bedeuten, dass selten auf Basis aller prinzipiell erhältlichen Information entschieden wird. Stattdessen bedienen sich Organisationen und Entscheidungsträger kognitiver Hilfsmittel, um Information einzuordnen und zu begrenzen; z. B. vorgefertigte Berichtsstrukturen und Key Performance Indicators (KPIs), aber auch implizite und sogar unbewusste Scripte, Frames und Heuristiken. Diese machen die Welt bewältigbar, können aber auch dazu führen, dass eigentlich relevante Informationen ausgeblendet werden. Kognitive Verzerrungen (Bestätigungsfehler, Gruppendenken etc.) schmälern die Objektivität und Rationalität von Entscheidungen weiter.[34]

Aus dieser Perspektive resultieren Rechtsverstöße ebenso oft aus informationeller Überforderung der beteiligten Akteure und ihrer Systeme wie aus absichtlicher Entscheidung, Rechtsbruch als rationales Mittel zum Zweck zu begehen. Als Beispiel für diese Phänomene gilt etwa Fords langjähriges Versäumnis, das Modell Pinto zurückzurufen, obwohl Ingenieuren des Unternehmens gefährliche Konstruktionsfehler bekannt waren. Fehlender Informationsaustausch zwischen Unternehmenseinheiten und problematische Entscheidungsheuristiken (Scripte) führten dazu, dass falsche Schlüsse aus Unfallberichten gezogen wurden und die besonderen Risiken des Pintos unbehandelt blieben.[35] Banaler, aber vermutlich noch häufiger, resultieren Rechtsverstöße aus Unkenntnis der Rechtslage, mangelnder Sensibilität für ethische Fragen und fehlendem Wissen um praktische Alternativen, mittels derer Geschäftsziele unter Einhaltung der Rechtsvorschriften erreicht werden können.

Gemäß dieser Argumentation genügt es zur Eindämmung von Rechtsbrüchen daher nicht, die Anreize von Managern, etwa über Sanktionsandrohungen, zu erhöhen. Ebenso wichtig ist der Aufbau unternehmensinterner Compliance-Management-Systeme (CMS), über die Compliance-Risiken identifiziert, (Gegen-)Maßnahmen eingeleitet und Mitarbeiter für rechtlich-ethische Risiken und praktische Gestaltungsalternativen sensibilisiert werden können. Das CMS soll die besprochenen kognitiven und informationellen Schwächen von Organisationen sowie schlichtes Unwissen eindämmen, so dass Rechtsbrüche nicht eintreten.[36]

Parker und Gilad[37] definieren mehrere Schlüsselfaktoren für das Zustandekommen eines effektiven CMS. Dreh- und Angelpunkt sind ausgebildete Compliance-Fachkräfte, die die nötige technische und juristische Expertise sowie das unternehmensinterne Standing haben, um Compliance um- und auch durchzusetzen. Beim Datenschutz könnten dies neben Fachleuten in einer Compliance-Abteilung vor allem die betrieblichen Datenschutzbeauftragten sein.[38] Weitere Faktoren sind eine Selbstverpflichtung der Unternehmensleitung und externer Druck des Gesetzgebers – oft nötig, um Compliance-Fachkräften die nötige unternehmensinterne Autorität zu verleihen – die effektive Überführung von Compliance-Anforderungen in die täglichen Geschäftsabläufe, externe Audits und der Einbezug der Stimmen der Betroffenen bzw. ihrer Repräsentanten (etwa Verbraucherschutzverbände, Gewerkschaften, NGOs oder Betriebsräte), um etablierte Sichtweisen in Unternehmen aufzubrechen und zu hinterfragen.[39] Zu ähnlichen Schlüssen kommen Ken Bamberger und Deidre Mulligan[40] in ihren Untersuchungen von Chief Privacy Officers und Datenschutz-Management-Systemen in amerikanischen Unternehmen und Verwaltungsbehörden. Sie betonen ferner strukturelle Faktoren im Aufbau des Managementsystems wie die dezentralisierte Verteilung von Compliance-Expertise innerhalb der Organisation.

## 2.4 Zwischenfazit: Implikationen für die Wirkmöglichkeiten des Sanktionsregimes der Datenschutz-Grundverordnung

Die besprochenen Erklärungsmodelle liefern scheinbar widersprüchliche Ergebnisse. Während manche die Androhung empfindlicher Sanktionen als zentralen Motivationsfaktor für Compliance herausstellen, betonen andere die Rolle gesellschaftlicher und normativer (Selbst-)Erwartungen oder verweisen auf die Rolle von Compliance-Management-Systemen. Für alles finden sich empirische Belege. Wie sind diese verschiedenen Perspektiven zu werten und welche Implikationen ergeben sich daraus für die Wirkmöglichkeiten des Sanktionsregimes der Datenschutz-Grundverordnung?

Zumindest bisher haben Instrumente der Selbstregulierung wie moralische (Selbst-)Erwartungen und "gesellschaftliche Betriebslizenzen" offensichtlich nicht ausgereicht, um datenschutzfreundliches und rechtskonformes Verhalten zu sichern. Auch gilt die Position des Datenschutzbeauftragten in Unternehmen bislang selten als prestigeträchtig, seine realen Einflussmöglichkeiten scheinen eher begrenzt zu sein. Die Anhebung möglicher Strafmaße war nicht zuletzt diesen Tatsachen geschuldet.

Die zitierten Studien liefern dafür Anhaltspunkte, warum soziale und normative Erwartungen im Datenschutz bisher nur geringe Steuerungswirkung entfalten konnten. Sorge um ihre "gesellschaftliche Betriebslizenz" scheint vor allem auf große bzw. gesellschaftlich exponierte und "sichtbare" Unternehmen disziplinierend zu wirken, weniger auf kleine (weniger sichtbare) Unternehmen. Aber auch bei großen Unternehmen mag diese Wirkung nachlassen, wenn Marktmacht oder andere Umstände ihnen besonderen Einfluss sichern. In der Datenökonomie verfügen aber Großkonzerne aufgrund von Netzwerkeffekten oft über sehr erhebliche Marktmacht ihren Nutzern und Kunden gegenüber. Die in der Literatur besprochenen Fälle, wo normative Selbsterwartungen besonders starke Steuerungswirkung entfaltet zu haben scheinen – Pflegeheime, Wohnungsbau und Landwirtschaft – stammen aus Branchen, in denen Berufsethiken und nicht-monetäre/nicht-instrumentelle Überlegungen (Patientenwohl, Bausicherheit, Nachhaltigkeit/Langfristigkeit über Generationen hinweg) möglicherweise stärker als gewöhnlich ausgeprägt sind. Gerade die datenintensive und kulturell einflussreiche Technologiebranche hat hingegen Privatheit und Datenschutz bisher bestenfalls einen untergeordneten Wert beigemessen.[41]

Jedoch stehen harte rechtliche Sanktionen und gesellschaftliche Erwartungen und Normen in einem Wechselspiel. Die Verletzung moralischer Normen impliziert meist die Enttäuschung gesellschaftlicher Erwartungen und rechtlicher Anforderungen, die wiederum rechtliche Konsequenzen nach sich zieht. Das wirft die Frage auf, welchen Einfluss rechtliche Sanktionen auf die Herausbildung neuer gesellschaftlicher Erwartungen und Normen haben kann. Auf Grundlage ihrer Forschung zu Compliance im Umweltbereich kommen Kagan et al. etwa zum Schluss, dass „Gesetze, und die realistische Aussicht auf Durchsetzung und Bestrafung, die wesentlichen Maßstäbe und Erwartungen bilden, an denen sich der gesellschaftliche und moralische Druck, compliant zu sein, orientiert und herausbildet".[42] Mit anderen Worten: Rechtliche Sanktionen haben eine Kalibrierungsfunktion: Sie setzen nicht nur instrumentell-ökonomische Anreize, sondern bieten eine Messlatte, anhand derer Menschen einordnen können, wie Handlungen *moralisch* zu bewerten sind, und wie schwer Fehltritte moralisch wiegen. Eine besondere Rolle kommt hierbei der Rechtsdurchsetzung zu. Sie hat für Kagan et al.[43] eine „Vergewisserungsfunktion" (*reassurance function*): Sanktionierung von Rechtsbrüchen bestätigt gerade rechtstreue Akteure, die um der Compliance Willen Nachteile (wie höhere Kosten) in Kauf genommen haben, in der moralischen Richtigkeit ihres Handelns.

Diese „kalibrierende" Funktion von rechtlichen Sanktionen dürfte gerade im Datenschutz wichtig werden. Wie besprochen, ist der aus Datenschutzverstößen für die Betroffenen, über die Verletzung ihrer Rechte als solche, hinausgehende *konkrete* Scha-

den nicht immer leicht ersichtlich. Dies ist der Ausbildung eines auch ethisch-moralischen Datenschutzbewusstseins ebenso hinderlich, wie der Wahrnehmung von Datenschutzverstößen als *moralische* Fehltritte. Entsprechend bildet sich die Wahrnehmung heraus, Datenschutzverstöße seien Kavaliersdelikte. Die dramatische Erhöhung des maximal möglichen Strafmaßes unter der Datenschutz-Grundverordnung hat somit auch gesellschaftliche Signalwirkung: Sie impliziert, dass Datenschutzverstöße eben keine Bagatellen sind. Gleichzeitig stellt das die Aufsichtsbehörden vor besondere Herausforderungen: Sie sollten die Strafmaße auch mit Blick auf die Setzung neuer gesellschaftlicher Normen anwenden, müssen aber gleichzeitig verhindern, dass in der Öffentlichkeit als „exzessiv" wahrgenommene Sanktionen die Legitimität des Sanktionsregimes und der Datenschutz-Grundverordnung untergräbt

Die glaubwürdige Androhung spürbarer rechtlicher Sanktionen kann Auswirkungen auch auf die Effektivität von Compliance haben. Wie besprochen, kommt den Compliance-Fachkräften (z. B. den betrieblichen Datenschutzbeauftragten) in diesen Systemen eine Schlüsselrolle zu. Der Grad, zu dem sie diese Rolle adäquat ausüben können, ist wiederum eng mit dem Grad organisationsinterner Autorität, die sie genießen, verbunden. Das Risiko empfindlicher Strafen kann den Status und Einfluss auf Unternehmensentscheidungen von Compliance-Fachkräften merklich steigern, und somit ihre Möglichkeiten verbessern, positiv auf Datenschutz hinzuwirken.

Darüber hinaus können auch die haftungsrechtlichen Risiken, die mit der Tätigkeit des Datenschutzbeauftragten einhergehen, zu einer Erhöhung der Sensibilität für Datenschutz im (datenverarbeitenden) Unternehmen führen. Der Datenschutzbeauftragte ist nach Art. 39 Abs. 1 lit. b DSGVO verpflichtet, die Einhaltung der Vorgaben der Datenschutz-Grundverordnung zu überwachen. Dem Datenschutzbeauftragten kommt damit eine umfassende Überwachungspflicht zu, die nicht nur darauf zielt, Datenverstöße im Unternehmen zu verhindern, sondern auch, um das Unternehmen vor Datenmissbräuchen und daraus resultierenden Schäden durch einzelne Mitarbeiter oder Dritten zu schützen.[44] Dies ist in jedem Unternehmen mit den Untersuchungs- und Gestaltungskompetenzen der Compliance-Abteilungen, die für alle anderen Compliance-Themen zuständig sind, abzugleichen.[45]

Die Haftung des Datenschutzbeauftragten wird weder in der Datenschutz-Grundverordnung noch im Bundesdatenschutzgesetz näher geregelt, obwohl sie angesichts der hohen Bußgeldandrohungen von zentraler Bedeutung ist.[46] Art. 83 Abs. 4, 5 und 6 DSGVO sehen Geldbußen gegenüber dem Datenschutzbeauftragten bei Verstoß gegen seine Pflichten aus Art. 39, 38 Abs. 4 und 47 Abs. 2 lit. h DSGVO nicht vor.

Aus zivilrechtlicher Sicht kommt eine Haftung des Datenschutzbeauftragten wegen Pflichtverletzung gem. §§ 280 ff. BGB in Betracht, wobei für den internen Datenschutzbeauftragten wiederum die Grundsätze des innerbetrieblichen Schadensausgleichs maßgeblich sind.[47] Dieser würde also nur bei einem vorsätzlichen und grob fahrlässigen Verstoß voll für den Schaden haften. Darüber hinaus kommt auch eine deliktische Haftung des Datenschutzbeauftragten nach §§ 823 ff. BGB in Betracht; allerdings wird diese nur der Ausnahmefall sein.[48] Eine deliktische Haftung kann ausgelöst werden, wenn der Verstoß unmittelbar auf den Datenschutzbeauftragten zurückzuführen ist, wie etwa, wenn die Pflicht zur Verschwiegenheit verletzt wird.

Schließlich kommt eine Haftung nach Straf- und Ordnungswidrigkeitenrecht des Datenschutzbeauftragten insbesondere gemäß §§ 41, 42 BDSG in Betracht. So kann der Datenschutzbeauftragte als Täter, Mittäter oder Anstifter handeln und damit gegen §§ 41, 42 BDSG verstoßen. Denkbar wären Fälle, in denen sich der Datenschutzbeauftragte über seine Befugnis hinwegsetzt und etwa ein unzulässiges Massenscreening von Mitarbeitern veranlasst.[49]

# 3
# Sanktionen nach der Datenschutz-Grundverordnung und dem Bundesdatenschutzgesetz

Die Datenschutz-Grundverordnung sieht einige Instrumente vor, um den Verantwortlichen bei der Einhaltung der Regelungen zu unterstützen. Dazu gehören die Umsetzung von technischen und organisatorischen Maßnahmen nach Art. 25 und 32 DSGVO, die Erstellung eines Verarbeitungsverzeichnisses nach Art. 30 DSGVO, die Meldung von Datenschutzverletzungen nach Art. 33 und 34 DSGVO, die Durchführung einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO oder die Benennung eines Datenschutzbeauftragten nach Art. 37 DSGVO.

Um die Einhaltung der Vorgaben der Datenschutz-Grundverordnung sicherzustellen, sieht diese verschiedene Kontroll- und Sanktionsbefugnisse vor. So haben die Aufsichtsbehörden zum einen verschiedene Untersuchungs- und Genehmigungs-, vor allem aber Abhilfebefugnisse, um Datenschutzverstöße zu verhindern oder zu beenden, und zum anderen die Möglichkeit, Bußgelder gegenüber Verantwortlichen zu verhängen, um Datenschutzverstöße zu ahnden.

## 3.1 Abhilfebefugnisse der Aufsichtsbehörden

Um die Einhaltung der Datenschutz-Grundverordnung sicherzustellen, haben die Aufsichtsbehörden gemäß Art. 58 Abs. 2 lit. a bis j DSGVO verschiedene Abhilfebefugnisse, die sie im Falle einer (vermuteten) Verletzung der Datenschutz-Grundverordnung gegenüber dem Verantwortlichen oder Auftragsverarbeiter ausüben können. Diese Befugnisse umfassen etwa, Verantwortliche oder Auftragsverarbeiter zu warnen, dass ihre beabsichtigten Verarbeitungsvorgänge voraussichtlich gegen die Vorgaben der Datenschutz-Grundverordnung verstoßen oder diese zu verwarnen, wenn sie mit einem Datenverarbeitungsvorgang gegen die Vorgaben der Datenschutz-Grundverordnung verstoßen haben. Diese beiden Mittel stellen die am wenigsten restriktiven Eingriffsmöglichkeiten dar, da sie dem Verantwortlichen oder Auftragsverarbeiter nicht unmittelbar eine Rechtspflicht auferlegen, ihre Verarbeitungsvorgänge einzustellen oder anzupassen.[50] Andere Abhilfebefugnisse sind nach Art. 58 Abs. 2 DSGVO etwa:

- den Verantwortlichen oder den Auftragsverarbeiter anzuweisen, den Anträgen der betroffenen Person auf Ausübung der ihr nach der Datenschutz-Grundverordnung zustehenden Rechte zu entsprechen,
- den Verantwortlichen oder den Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der Datenschutz-Grundverordnung zu bringen,
- den Verantwortlichen anzuweisen, die von einer Verletzung des Schutzes personenbezogener Daten betroffene Person entsprechend zu benachrichtigen,
- eine vorübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots, zu verhängen,
- die Berichtigung oder Löschung von personenbezogenen Daten oder die Einschränkung der Verarbeitung gemäß Art. 16 bis 18 DSGVO und die Unterrichtung der Empfänger, an die diese personenbezogenen Daten gemäß Art. 17

Abs. 2 und Art. 19 DSGVO offengelegt wurden, über solche Maßnahmen anzuordnen,

- eine Zertifizierung zu widerrufen oder die Zertifizierungsstelle anzuweisen, dies zu tun, oder von einer Erteilung einer Zertifizierung abzusehen, sofern die Voraussetzungen für die Zertifizierung nicht oder nicht mehr erfüllt werden,
- die Aussetzung von Datenübermittlungen an Empfänger in einem Drittland anzuordnen.

Von besonderer Bedeutung in der betrieblichen Praxis ist die Befugnis, gemäß Art. 58 Abs. 2 lit. i DSGVO – je nach den Umständen des Einzelfalls – zusätzlich oder anstelle sonstiger Abhilfebefugnisse gemäß Art. 83 DSGVO eine Geldbuße zu verhängen.

## 3.2 Gründe für Bußgelder und Bußgeldhöhen

Ausgehend von den gesetzlichen Höchstbeträgen für Bußgelder existieren nach Art. 83 Abs. 4 und 5 DSGVO zwei Kategorien von Verstößen gegen die Vorgaben der Datenschutz-Grundverordnung.[51]

Gemäß Art. 83 Abs. 4 DSGVO werden bei Verstößen gegen die folgenden Bestimmungen Geldbußen von bis zu 10 Mio. Euro oder im Falle eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt, je nachdem, welcher der Beträge höher ist: Bei Verstößen gegen

- die Pflichten der Verantwortlichen und der Auftragsverarbeiter im Zusammenhang mit:
  - den Bedingungen für die Einwilligung eines Kindes gem. Art. 8 DSGVO;
  - Art. 11 DSGVO, wonach ein Verantwortlicher, der personenbezogene Daten verarbeitet und dies nicht oder nicht mehr für die Identifizierung der betroffenen Person für seine Verarbeitungszwecke benötigt, nicht verpflichtet ist, zusätzliche Informationen aufzubewahren, einzuholen oder zu verarbeiten, um eine Identifizierung weiterhin zu ermöglichen;
  - den Anforderungen an die Datenschutzorganisation im Sinne des Art. 25 bis 39 DSGVO sowie
  - Anforderungen an die Datenschutz-Zertifizierung gem. Art. 42 und 43 DSGVO;
- die Pflichten der Zertifizierungsstelle gem. Art. 42 und 43 DSGVO sowie
- die Pflichten der Überwachungsstelle für Verhaltensregeln gem. Art. 41 Abs. 4 DSGVO.

Gemäß Art. 83 Abs. 5 DSGVO werden für die folgenden Verstöße Geldbußen von bis zu 20 Mio. Euro oder im Fall eines Unternehmens[52] von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt, je nachdem, welcher der Beträge höher ist: Bei Verstößen gegen

- die Grundsätze für die Verarbeitung, einschließlich der Bedingungen für die Einwilligung und für eine Verarbeitung von besonderen Kategorien personenbezogener Daten gemäß Art. 5, 6, 7 und 9 DSGVO;
- die Rechte der betroffenen Personen gem. Art. 12 bis 22 DSGVO;

- die Übermittlung personenbezogener Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation gemäß Art. 44 bis 49 DSGVO;
- alle Pflichten gemäß den Rechtsvorschriften der Mitgliedstaaten, die im Rahmen der Öffnungsklauseln in Kap. IX DSGVO, etwa im Rahmen des Beschäftigtendatenschutzes, erlassen wurden.

Die gleiche Sanktion kann die Aufsichtsbehörde nach Art. 83 Abs. 6 DSGVO anordnen, wenn der Adressat eine Anweisung oder einer vorübergehenden oder endgültigen Beschränkung oder Aussetzung der Datenübermittlung durch die Aufsichtsbehörde gemäß Art. 58 Abs. 2 DSGVO nicht befolgt oder den Zugang unter Verstoß gegen Art. 58 Abs. 1 DSGVO nicht gewährt.

In der Praxis dürfte vor allem Art. 83 Abs. 6 DSGVO besondere Bedeutung zukommen, weil das Nichtbefolgen einer Anweisung der Aufsichtsbehörde in der Regel klar feststellbar ist. Dies gilt nicht für alle Tatbestände, die in Art. 83 Abs. 4 und 5 DSGVO normiert sind. Einige davon sind zu abstrakt, um unmittelbar vollzogen oder sanktioniert werden zu können. Ein Verstoß etwa gegen die abstrakten Datenschutzgrundsätze in Art. 5 DSGVO wird ohne unmittelbaren eindeutigen Handlungsbefehl nicht festzustellen sein.[53] Sanktionsrechtliche Relevanz können abstrakte Tatbestände in Art. 83 Abs. 4 und 5 DSGVO nur dann erlangen, sofern sie durch eine Aufsichtsbehörde in einer datenschutzrechtlichen Anordnung nach Art. 58 Abs. 2 DSGVO konkretisiert wurden.[54] Allerdings gilt dies nicht für alle Tatbestände in Art. 83 Abs. 4 und 5 DSGVO: So lassen sich sehr wohl Verstöße gegen die Anforderungen an die Sicherheit der personenbezogenen Daten, wie dies in Art. 32 DSGVO gefordert ist, konkret benennen. Falsch gewählte, datenschutzunfreundliche Voreinstellungen, die nicht die Anforderungen nach Art. 25 Abs. 2 DSGVO erfüllen, können von den datenschutzfreundlichen Konfigurationen abgeschichtet werden. Verstöße in Bezug auf die Gestaltung einer Einwilligung nach Art. 7 DSGVO sind ebenso wie die Nicht-Erfüllung von Betroffenenrechten gemäß Art. 12 bis 22 DSGVO häufig klar feststellbar und können auch sanktioniert werden, ohne dass es weiterer – jedoch für viele Fälle sicherlich wünschenswerter – Konkretisierungen bedürfte.

Sofern ein Verantwortlicher oder Auftragsverarbeiter bei gleichen oder miteinander verbundenen Datenverarbeitungsvorgängen vorsätzlich oder fahrlässig gegen mehrere Bestimmungen der Datenschutz-Grundverordnung verstößt, so übersteigt gemäß Art. 83 Abs. 3 DSGVO der Gesamtbetrag der Geldbuße nicht den Betrag für den schwerwiegendsten Verstoß. Somit sollten Bußgelder niemals den Betrag von 20 Mio. Euro oder 4 Prozent des weltweiten Jahresumsatzes übersteigen.

## 3.3 Verhängung von Bußgeldern

Bußgelder können für die in Art. 83 Abs. 4 bis 6 DSGVO normierten Fälle verhängt werden. Die genaue Höhe des Bußgeldes wird von der Aufsichtsbehörde – je nach Einzelfall – festgelegt. Nach Art. 83 Abs. 1 DSGVO hat jede Aufsichtsbehörde sicherzustellen, dass die Verhängung von Geldbußen für Verstöße gegen die Vorgaben der Datenschutz-Grundverordnung in jedem Einzelfall „wirksam, verhältnismäßig und abschreckend" ist. Sofern Geldbußen Personen auferlegt werden, bei denen es sich nicht um Unternehmen handelt, sollte die Aufsichtsbehörde bei der Festsetzung des Bußgelds nach Erwägungsgrund 150 DSGVO das allgemeine Einkommensniveau in dem betreffenden EU-Mitgliedstaat und die wirtschaftliche Lage der Personen gebührend berücksichtigen.

Gemäß Art. 83 Abs. 7 DSGVO und § 43 Abs. 3 BDSG[55] gilt Art. 83 Abs. 4 bis 6 DSGVO nicht gegenüber Behörden und sonstige öffentlichen Stellen.[56] Gegen sie werden keine Bußgelder verhängt. Hier ist die Aufsichtsbehörde auf ihre Eingriffsbefugnisse nach

Art. 58 DSGVO beschränkt. Aber auch hier muss sie die besonderen Verfahrensvorgaben nach § 16 BDSG und in den Ländern vergleichbare Vorgaben beachten.

Bei der Festsetzung der Bußgeldhöhe haben die Aufsichtsbehörden gem. Art. 83 Abs. 2 DSGVO die vorhandenen erschwerenden oder mildernden Umstände zu berücksichtigen, wie etwa:

- die Art, Schwere und Dauer des Verstoßes;
- die Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes;
- die Maßnahmen zur Minderung des entstandenen Schadens;
- der Grad der Verantwortung;
- etwaige einschlägige frühere Verstöße des Verantwortlichen oder des Auftragsverarbeiters;
- die Einhaltung der gegen den Verantwortlichen oder Auftragsverarbeiter angeordneten Maßnahmen;
- die Einhaltung von Verhaltensregeln.

Ziel soll es sein, mittels der Geldbuße Datenschutzverstöße zu sanktionieren und für die Zukunft Verantwortliche von weiteren Verstößen abzuhalten. Die Vorgaben der Wirksamkeit und Abschreckung lassen sich nicht trennscharf gegeneinander abgrenzen. Sie sind jedenfalls im Sinne dieser Zielsetzung zu lesen. Der Grundsatz der Verhältnismäßigkeit wäre darüber hinaus auch ohne Erwähnung in Art. 83 DSGVO zu beachten. Nach ihm muss die Geldbuße erforderlich, geeignet und angemessen sein.[57] Eine wichtige Aufgabe wird sein, unionsweit soweit wie möglich für vergleichbare Verstöße vergleichbare Bußgeldrahmen zu entwickeln, um auch in diesem Bereich eine harmonische Umsetzung der Verordnung zu erreichen und dem Gleichheitsgrundsatz der Grundrechtecharta zu entsprechen.[58] Dabei ist jedoch zu beachten, dass das Verfahrensrecht sowie das Strafrecht inklusive der Ordnungswidrigkeiten in der Kompetenz der jeweiligen Mitgliedstaaten verbleiben und deren jeweiligen Rechtstraditionen ausreichend berücksichtigt werden müssen. Auch muss es möglich sein, weiterhin die Besonderheiten der einzelnen Fälle angemessen zu würdigen. Es wäre kontraproduktiv, wenn Firmen ähnlich einem Budget für Geschwindigkeitsübertretungen, die sich etwa nach detaillierten und öffentlich verfügbaren Bußgeldkatalogen bemessen, auch Bußgelder für Datenschutzverstöße in ihre Kalkulationen einpreisen, statt sich um das Einhalten des Datenschutzrechts zu kümmern.

## 3.4 Sanktionen und Verfahrensvorschriften nach dem BDSG

Die Datenschutz-Grundverordnung sieht in verschiedenen Öffnungsklauseln eine nähere Ausgestaltung des Rechts durch die Mitgliedstaaten vor. Eine solche besteht auch im Hinblick auf Sanktionen bei Datenschutzverstößen. So ermächtigt Art. 84 Abs. 1 DSGVO die Mitgliedstaaten, neben den soeben beschriebenen Regelungen zu Bußgeldern und Sanktionen zusätzliche Sanktionen für Verstöße gegen die Datenschutz-Grundverordnung festzulegen. Das Bundesdatenschutzgesetz trifft entsprechende Regelungen zu Sanktionen in Deutschland.

Nach § 41 Abs. 2 BDSG gelten für das in der Zuständigkeit der Aufsichtsbehörden liegende Verfahren im Hinblick auf Verstöße gegen Art. 83 Abs. 4 bis 6 DSGVO das Gesetz über Ordnungswidrigkeiten (OWiG), die Strafprozessordnung (StPO) und das Gerichtsverfassungsgesetz (GVG) entsprechend. Dies gilt auch für die auf Grundlage von Öffnungsklauseln geschaffenen nationalen Sanktionstatbestände. Allerdings gelangen bestimmte Regelungen angesichts der abschließenden Regelung der Vorgaben in der Datenschutz-Grundverordnung nicht zur Anwendung, wie etwa § 17 OWiG für Bußgeldhöhen.[59]

Die §§ 42 und 43 BDSG sehen zusätzliche Sanktionstatbestände vor. So führt § 42 BDSG als Ergänzung zu den Bußgeldtatbeständen der Datenschutz-Grundverordnung strafrechtliche Sanktionen ein. Diese sind – im Gegensatz zu den Bußgeldvorschriften – in ihrem persönlichen Anwendungsbereich nicht begrenzt, sondern finden für jedermann Anwendung. Gem. § 42 Abs. 1 BDSG wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft, wer wissentlich nicht allgemein zugängliche personenbezogen Daten einer großen Zahl von Personen übermittelt oder auf andere Art und Weise zugänglich macht, ohne hierzu berechtigt zu sein und dabei gewerbsmäßig handelt. Nach § 42 Abs. 2 BDSG wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wer personenbezogene Daten, die nicht allgemein zugänglich sind, verarbeitet oder durch unrichtige Angaben erschleicht und dabei gegen Entgelt oder mit Bereicherungs- oder Schädigungsabsicht handelt. § 43 BDSG enthält ergänzende Bußgeldtatbestände für die vorsätzliche oder fahrlässige Verletzung von Pflichten aus § 30 BDSG im Kontext mit Verbraucherkrediten. Dies kann gemäß § 42 Abs. 2 BDSG die Verletzung etwaiger Pflichten mit einer Geldbuße bis zu 50.000 Euro geahndet werden.[60]

## 3.5 Gewinnabschöpfung

Verstöße gegen datenschutzrechtliche Vorgaben führen häufig zu einem nicht zu unterschätzenden direkten finanziellen Vorteil. Um Unternehmen keinen Anreiz zu bieten, mittels einfacher Kosten-Nutzen-Rechnung trotz Bußgeldandrohung Datenschutzverstöße zu begehen, sieht das Bundesdatenschutzgesetz an verschiedenen Stellen als zusätzliche Sanktion vor, den entstandenen Gewinn abzuschöpfen.

Nach § 43 Abs. 3 Satz 2 BDSG a. F. durften Geldbußen den wirtschaftlichen Vorteil, den der Verantwortliche aus einer Ordnungswidrigkeit gezogen hat, übersteigen; hierfür durften nach Satz 3 sogar der vorgesehene Bußgeldrahmen von 50.000 bis 300.000 Euro überschritten werden. Ähnlich formuliert § 17 Abs. 4 OWiG, dass die Geldbuße den wirtschaftlichen Vorteil, den der Täter aus der Ordnungswidrigkeit gezogen hat, übersteigen soll. Noch deutlicher erlaubt etwa § 73 StGB die Einziehung des erlangten Gewinns oder Nutzens (bei Straftaten), nach § 10 des Gesetzes gegen den unlauteren Wettbewerb (UWG) die Herausgabe des Gewinns sowie nach § 29a Abs. 1 OWiG die Einziehung eines Geldbetrages bis zu der Höhe, die dem Wert des Erlangten entspricht.

Die Datenschutz-Grundverordnung enthält keine solch explizite Regelung. Aber auch die Bußgeldvorschriften der Verordnung sehen eine Berücksichtigung des daraus gezogenen Gewinns vor. Nach Art. 83 Abs. 2 lit. k DSGVO stellt der durch den Verstoß erlangte finanzielle Vorteil oder vermiedene Verlust einen erschwerenden Umstand im Einzelfall dar, der bei der Höhe des zu verhängenden Bußgeldes zu berücksichtigen ist, damit dieses nach Art. 83 Abs. 1 DSGVO „wirksam, verhältnismäßig und abschreckend“ ist. Dies kann aber dazu führen, dass das Bußgeld zwar höher ausfällt, es wird aber nicht zwingend der gesamte erlangte finanzielle Gewinn abgeschöpft, da Abs. 2 lit. k nur einer unter vielen genannten Abwägungsgesichtspunkten darstellt. Letztlich liegt die Bestimmung der Höhe des Bußgeldes im Ermessen der Behörde. Außerdem obliegen die Geldbußen des Art. 83 Abs. 4 bis 6 DSGVO den dort genannten Obergrenzen.

Um eine effektive Sanktionierung zu erreichen und von Datenschutzverstößen abzuschrecken, ist es durchaus sinnvoll, den durch den Datenschutzverstoß erlangten Gewinn zu entziehen. Dabei bietet es sich an, im Rahmen des Art. 83 Abs. 2 lit. k DSGVO im Rahmen des Auswahlermessens den Umstand der Gewinnerzielung unberücksichtigt zu lassen und dafür zusätzlich auf § 29a OWiG zurückzugreifen, um den – dann jedoch genau zu ermittelnden – Gewinn zugunsten der Staatskasse einzuziehen.

# 4
# Auswirkungen der Sanktionen auf die Datenschutzpraxis

## 4.1 Auswirkungen der Sanktionen auf Aufsichtsbehörden

Um zu verstehen, wie die Aufsichtsbehörden mit den neuen Sanktionsmöglichkeiten umgehen und welche Auswirkungen die Sanktionen voraussichtlich auf die Datenschutzaufsicht in Deutschland haben werden, wurden zwischen Februar und September 2018 Interviews mit Landesdatenschutzbeauftragten, im Datenschutz tätigen zivilgesellschaftlichen Organisationen, Rechtsanwälten sowie betrieblichen Datenschutzbeauftragten geführt.[61] Die zentrale Forschungsfrage war, ob die neuen Sanktionsmöglichkeiten zu nachhaltigen Veränderungen in der bestehenden Aufsichtspraxis der Behörden führen würden und welche Faktoren ausschlaggebend für den Umgang mit dem neuen Bußgeldrahmen sein würden.

### 4.1.1 Die bisher bestehende Aufsichtspraxis der Aufsichtsbehörden

Die Tätigkeitsberichte der Aufsichtsbehörden aus Hamburg, Niedersachsen, Hessen, Bayern (Landesamt für Datenschutzaufsicht), Sachsen, Brandenburg und Berlin enthalten Statistiken zu den verhängten Bußgeldern. Allerdings unterscheiden sich die Berichtszeiträume teilweise, so dass ein direkter Vergleich einzelner Jahreszahlen nur begrenzt möglich ist. Dennoch sind die Zahlen aufschlussreich. Im Schnitt erließen die genannten Aufsichtsbehörden etwa 14 bis 19 Bußgeldbescheide pro Jahr, mit leichten Ausschlägen nach oben und unten.[62] So lag etwa die Zahl der jährlichen Bußgeldbescheide in Hamburg meist im einstelligen Bereich, während in Bayern 2015 sogar 36 Bescheide verteilt wurden. In Sachsen fielen zwischen 2013 und 2017 jährlich etwa 24 Bescheide an. Die Unterschiede dürften lokalen und zeitlichen Gegebenheiten geschuldet sein. So führte beispielsweise Hamburg eine Reihe gerichtlicher Auseinandersetzungen mit Großkonzernen wegen (vom Hamburger Datenschutzbeauftragten zum Teil mit hohen Bußgeldern geahndeten) Verstößen, was zur Bindung erheblicher personeller Ressourcen geführt haben dürfte, die somit für sonstige Rechtsdurchsetzungsaktivitäten nicht mehr zur Verfügung gestanden haben werden.

Zur Höhe der verteilten Bußgelder sind kaum systematische Daten verfügbar. Manche Behörden veröffentlichen diese auch bewusst nicht, um Fehlschlüsse darüber zu vermeiden, wie „teuer" ein gegebener Verstoß regelmäßig wird.[63] Aus Einzelberichten lässt sich entnehmen, dass die Bußgelder bisher eine große Spannweite aufwiesen, von mehreren Hundert bis zu mehreren Hunderttausend Euro, je nachdem ob es sich um kleinere Verstöße von Privatpersonen oder Kleinunternehmen oder um schwerwiegende Verstöße großer Konzerne handelte. Diese Spannbreite, gepaart mit den teilweise sehr unterschiedlichen regionalen Wirtschaftsstrukturen, macht es auch schwierig, die Gesamtsummen der durch die verschiedenen Landesämter verhängten Bußgelder sinnvoll miteinander zu vergleichen. In Bundesländern mit vielen in der Digital- und Datenwirtschaft aktiven Großkonzernen werden tendenziell höhere Bußgelder anfallen als in ländlichen oder strukturschwachen Regionen. Unterschiede in der Fallkonstellation können selbst innerhalb einzelner Länder zu erheblichen jährlichen Schwankungen führen. Beispielsweise verhängte das Bayerische Landesamt in den Jahren 2013 und 2014 Bußgelder von insgesamt etwas über 200.000 Euro, während man 2011 und 2012 – bei sogar leicht gestiegener Fallzahl – nur auf etwa 37.000 Euro kam.[64] Ähnlich Hamburg: Summierten sich die zwölf in den Jahren 2012 bis 2013 verhängten Bußgelder noch auf fast 235.000 Euro, fielen 2014 und 2015 bei vierzehn Bescheiden nur noch Bußgelder in Höhe von 21.550 Euro an.[65]

Die eher spärliche quantitative Datenlage verbietet abschließende Urteile zur bisherigen Bußgeldpraxis. Einige grundlegende Erkenntnisse lassen sich jedoch festhalten. Erstens scheint klar, dass das *Gros* der bislang verhängten Bußgelder relativ gering gewesen ist. Die weitaus meisten Bußgelder dürften sich im vier- bis niedrigen fünfstelligen (bzw. bei Privatpersonen und kleinen Unternehmen im drei- oder sogar zweistelligen) Bereich bewegt haben. Dies geht sowohl aus den in den Tätigkeitsberichten besprochenen Einzelfällen wie aus den geführten Interviews hervor und deckt sich mit Befunden in der Sekundärliteratur.[66] Gleichzeitig kam es bei Verfehlungen von Großkonzernen immer wieder zu wesentlich höheren Strafen. Beispielsweise verhängte der Hamburgische Datenschutzbeauftragte Bußgelder von 145.000 Euro gegen Google und von 200.000 Euro gegen die Hamburger Sparkasse.[67]

Die „gefühlte" Schwere eines Bußgeldes ergibt sich letztlich aus seiner Relation zum Unternehmensgewinn. Insofern stellte auch ein Bußgeld von 145.000 Euro für Google mit einem Unternehmensgewinn 2013 von über 12,7 Milliarden US-Dollar[68] eine verschwindend geringe Summe dar, von der kaum Verhaltensänderungen zu erwarten sind. Derartige Missverhältnisse begründen die verbreitete Wahrnehmung eines „Vollzugsdefizits" im Datenschutz oder aus Unternehmenssicht, dass Datenschutzverstöße nur „Kavaliers- und Bagatelldelikte" seien.[69] Der bisherige Bußgeldrahmen, der eine Obergrenze von 300.000 Euro pro mit Bußgeld belegtem Verstoß vorsah, setzte hier auch den aktivsten Datenschützern Grenzen. Dennoch konnte sich über die Kumulierung bußgeldbewehrter Verstöße bisweilen wesentlich höhere Gesamtsummen ergeben. So belegte der Rheinland-Pfälzische Datenschutzbeauftragte die Debeka 2014 mit Bußgeldern in Höhe von insgesamt 1,3 Mio. Euro.[70]

Zweitens gibt es keine Anhaltspunkte für grundsätzliche Unterschiede in der Sanktionspraxis der verschiedenen Landesbehörden etwa aufgrund verschiedener Amtsauffassungen. Wie weiter unten ausgeführt, gibt es unter den Landesbeauftragten durchaus Verschiedenheiten im Amts- und Aufgabenverständnis, die sich auch in unterschiedlichen Gewichtungen und Priorisierungen von Aufgaben widerspiegeln – nur eben nicht in der Bußgeldpraxis, zumindest soweit dies empirisch nachvollziehbar ist. Im Gegenteil hat man sich hier um möglichst große Einigkeit und Abstimmung in der Vorgehensweise bemüht. Unterschiede bezüglich der Zahl und Höhe der verhängten Bußgelder sind wohl eher auf Verschiedenheiten in den örtlichen Wirtschaftsstrukturen und den damit vorliegenden Fallkonstellationen zurückzuführen.

Drittens haben Bußgelder in der Aufsichtspraxis und dem Amtsverständnis der Landesbehörden bislang eine untergeordnete Rolle gespielt. Der Fokus der Behörden lag eher auf Aufklärung, Sensibilisierung und Beratung der Öffentlichkeit und der Verantwortlichen sowie auf der Bearbeitung von Eingaben und Beschwerden betroffener Personen. Gerade bei kleinen und mittleren Unternehmen (KMUs) scheint der Schwerpunkt eher darauf gelegen zu haben, datenschutzkonforme Zustände (wieder-)herzustellen – und nicht, eventuelle Verstöße möglichst stark zu sanktionieren. Vorausgesetzt, dass sich die Verantwortlichen kooperativ und reformwillig zeigten (und Verstöße nicht mutwillig begangen oder die betroffenen Personen hohen Risiken ausgesetzt haben), blieben Bußgelder bisher niedrig oder es wurde ganz auf sie verzichtet. Eine partielle Ausnahme bildeten Großkonzerne der Digitalökonomie, etwa Facebook oder Google, deren Aktivitäten vielfach für grundsätzlich problematisch erachtet und, entsprechend der aufsichtsrechtlichen Möglichkeiten, aktiv verfolgt wurden, wobei dies nicht immer über Bußgelder geschehen ist. Dieser eher auf Sensibilisierung und Beratung als auf aktivem „Eintreiben" von Bußgeldern fokussierte Ansatz grenzte sich auch vom aufsichtsbehördlichen „Stil" mancher anderer EU-Mitgliedstaaten ab, in denen Bußgeldern schon vor der Datenschutz-Grundverordnung eine zentralere Rolle zukam, auch zur Finanzierung der Behörden.[71]

Der neue Bußgeldrahmen hat die Aufsichtsbehörden nun mit widerstreitenden Forderungen aus Politik, Wirtschaft, Öffentlichkeit und Datenschutz-Community konfrontiert. Einerseits kamen aus (nicht-amtlichen) Datenschutz-Kreisen laute Forderungen,

bei Verstößen, in den Worten Jan Philipp Albrechts, „kein[en] Pardon“ zu gewähren,[72] hart durchzugreifen und mittels „rigorose[r] Durchsetzung“ dafür zu sorgen, dass Disziplin im Markt einkehrt.[73] Andererseits plädierten deutsche und europäische Politiker wiederholt für eine nachsichtige Herangehensweise und für vorübergehenden Sanktionsverzicht, um mit der Umsetzung von Datenschutzregeln überforderte KMUs und Vereine nicht in Existenzprobleme zu stürzen,[74] oder stellten den Datenschutz an sich in Frage.[75] Währenddessen scheint unbestreitbar, dass die Datenschutz-Grundverordnung – gerade aufgrund des neuen Bußgeldrahmens – zumindest in den Jahren 2017 und 2018 zu großer Verunsicherung bei Unternehmen, Vereinen und öffentlichen Institutionen führte, was in Absurditäten wie geschwärzten Gesichtern in Kita-Erinnerungsalben gipfelte.[76] Die Umsetzung der (in erheblichen Teilen auch nach altem Recht längst gültigen) Regeln der Datenschutz-Grundverordnung verlief in der Wirtschaft derweilen schleppend. Umgekehrt forderten Unternehmen, die in Datenschutz investiert hatten und dafür Kosten und mögliche Geschäftsnachteile in Kauf genommen hatten, aber auch eine deutlich härtere und sichtbarere Sanktionierung jener Unternehmen, die dies nicht getan hatten.[77]

Angesichts dieser komplexen Ausgangslage und der medialen Aufmerksamkeit, die das Thema auf sich zog, überrascht es nicht, dass die deutschen Aufsichtsbehörden vorsichtig mit den neuen Sanktionsbefugnissen umgegangen sind – auch wenn sie sich vehement gegen politische Forderungen nach einem temporären Sanktionsverzicht wehrten[78]. Während in anderen europäischen Staaten in den ersten acht Monaten nach Geltungsbeginn der Datenschutz-Grundverordnung bereits Bußgelder in Höhe von mehreren Hunderttausend oder sogar Millionen Euro beschieden wurden, belief sich das höchste in Deutschland bislang für Verstöße nach dem 25. Mai 2018 bis Februar 2919 verhängte Bußgeld auf 80.000 Euro. In diesem Zeitraum haben nur fünf Bundesländer insgesamt 41 Bußgeldbescheide auf Basis der Datenschutz-Grundverordnung verhängt, wobei eine erhebliche Zahl weiterer Verfahren anhängig ist.[79] Die weitaus meisten dieser Bußgelder scheinen sich weiterhin im drei- bis unteren fünfstelligen Bereich zu bewegen,[80] wobei die große Zahl laufender Verfahren (allein in Berlin und Bayern jeweils über 150) abschließende Aussagen verbietet. Dass trotz der vorherigen Panikmache um die Datenschutz-Grundverordnung scheinbar nur ein Bußgeld öffentliche Kritik hervorgerufen hat, spricht dafür, dass es den Behörden bislang gelungen ist, sensibel und, mit Blick auf die vorherige Panikmache und überzogene Kritiken, „deeskalierend“ mit den Bußgeldern umzugehen.

Diese auf Umsicht und Sensibilität angelegte Herangehensweise wurde in Interviews mit Landesdatenschutzbeauftragten deutlich. So sprach etwa ein Interviewpartner vom neuen Bußgeldrahmen als einem „sehr scharfen Schwert“, mit dem man jetzt zeigen müsse, „vernünftig umgehen“ zu können. Einerseits fühle man sich „sehr stark unter Druck zu liefern“, d. h. das Vollzugsdefizit im Datenschutz auch über merklich höhere Bußgelder zu beheben. Andererseits stehe man jedoch ebenso unter Druck, Unternehmen mit prinzipiell legitimen Geschäftsmodellen nicht mutwillig mit überzogenen Bußgeldern zu zerstören oder kleine Organisationen wegen Bagatellverstößen wie einer „blöde[n] Geburtstagsliste“ zu gängeln.[81] Konkret bedeutete das für diesen Gesprächspartner, dass bei der Sanktionierung Fälle vorerst „sehr klug“ ausgewählt werden müssten. Es käme darauf an, Verstöße zu finden, die sich „gut nach Außen darstellen lassen“, bei denen die Öffentlichkeit, aber auch die Wirtschaft verständnisvoll nachvollziehen können, warum sanktioniert wurde. Bei diesen Fällen müssten dann aber auch deutliche Bußgelder, im fünfstelligen oder noch höheren Bereich, fallen, um Signalwirkung zu entfalten. Trotz der nochmals gestärkten Unabhängigkeit der Datenschutzbehörden war es diesem Interviewpartner ein „eminent wichtiges Anliegen“, dass die Handlungen der Aufsichtsbehörden „im politischen Raum nicht nur wahrgenommen, sondern auch verstanden werden“.[82] Im Ergebnis – also auf der Ebene der eigentlichen Bußgeldpraxis – würden die Aussagen dieses Landesbeauftragten bedeuten, dass mit der Datenschutz-Grundverordnung die beschiedenen Bußgelder einerseits merklich steigen sollten, sich diese aber andererseits stärker als vielleicht zuvor auf ekla-

tante Verstöße konzentrieren müssten – insbesondere auf solche, die die Betroffenen gravierenden Risiken aussetzten – und weniger auf formale Verstöße oder Bagatellen.

In unseren Interviews offerierte keiner der weiteren Interviewpartner eine solch dezidiert politische Beschreibung ihrer Handlungslogiken wie der eben zitierte. Ihre Beschreibungen, wie sie bei der Verhängung von Bußgeldern künftig umgehen wollten, waren jedoch weitgehend deckungsgleich.

Eindeutig für alle war, dass Bußgelder mit der Datenschutz-Grundverordnung steigen müssen und werden. Wie Landesbeauftragte wiederholt erklärten, war dies schon „arithmetisch" vorgegeben: Der Bußgeldrahmen war gestiegen; entsprechend müssten auch die Bußgelder steigen. Alle sahen höhere Bußgelder als notwendiges Mittel, um dem Datenschutz die notwendige (aber bisher oft nicht genossene) Aufmerksamkeit in Unternehmen zu sichern. Hier stellt sich die Frage, inwiefern Behörden sich auch gezwungen sehen könnten zu versuchen, ihre weiterhin faktisch sehr knappe Personal- und Mittelausstattung auch durch hohe Bußgelder zu kompensieren, um so in der Breite Abschreckungseffekte zu erzeugen. In der Tat deutete ein Behördenleiter diese Möglichkeit öffentlich an.[83]

Gleichzeitig wurde aber in den Interviews auch betont, dass Bußgelder weiterhin mit Augenmaß und im Sinne der Verhältnismäßigkeit beschieden würden. Sie würden *nicht* einfach um das 67-fache steigen.[84] Grundsätzlicher noch unterstrichen die Interviewpartner, dass sie ihre Amtsaufgabe weiterhin *nicht* primär im Verteilen von Bußgeldern sehen. So erklärte ein Gesprächspartner, dass er die Aufmerksamkeit, die den Bußgeldern in der öffentlichen Debatte zukam, für „nicht gerechtfertigt" hielt, da es den Behörden „nicht vordringlich darum geht, möglichst viele Geldbußen zu verteilen".[85] In einem Interview mit einer weiteren Behörde wurde sogar betont, dass für sie die Anordnung nach Art. 58 Abs. 2 DSGVO ein sehr viel interessanteres Instrument darstelle als das Bußgeld, weil erstere gestaltend in die Zukunft hineinwirke, um datenschutzkonforme Zustände herzustellen, während letzteres lediglich retrospektiv Fehlverhalten aburteilt.[86]

Alle Gesprächspartner betonten ferner, dass auch nach dem 25. Mai 2018 keineswegs bei jedem Verstoß automatisch ein Bußgeld verhängt wird. Ob eines fällig würde und wie hoch es ausfiele, würde weiterhin stark vom Einzelfall abhängen. Kooperatives Verhalten sowie eine insgesamt um Datenschutz und Rechtskonformität bemühte Haltung würden belohnt und ehrliche Fehler und Missverständnisse, gerade bei kleineren Unternehmen und Organisationen, weitaus weniger streng geahndet werden als bewusst und absichtlich eingegangene Rechtsbrüche. Fehlern und Missverständnissen würde man – soweit insgesamt ernsthaftes Bemühen um den Datenschutz erkennbar sei – weiterhin vornehmlich mit Hilfestellungen und Anweisungen, wie die Sache besser zu machen sei, begegnet werden, nicht mit Bußgeldern. Inakzeptabel hingegen wäre es, ob aus Kostengründen oder aus Bequemlichkeit, offensichtliche Datenschutzverstöße billigend in Kauf zu nehmen. Hier wären Bußgelder definitiv zu erwarten.

Zusammenfassend ist also zu konstatieren, dass die befragten Landesbeauftragten sowohl höhere – und zwar potentiell *wesentlich* höhere – Bußgelder für eklatante Verstöße, als auch eine weiterhin eher auf Hilfestellung ausgerichtete Herangehensweise bei aus ehrlichem Unvermögen oder Missverständnissen resultierenden Unzulänglichkeiten in Aussicht stellten. Insgesamt waren die Gesprächspartner aber darauf bedacht, die Rolle der Bußgelder in ihrer Amts- und Aufsichtspraxis eher zu relativieren, verglichen mit anderen Aufgaben wie beispielsweise öffentlicher Sensibilisierung oder auch Beratung. Inwiefern sich diese aus den Interviews abgeleitete Prognose mit den bislang bekannt gewordenen Daten zu bereits verhängten Bußgeldern deckt, ist aufgrund der hohen Zahl laufender Verfahren zu Beginn des Jahres 2019 noch nicht zuverlässig zu beantworten. Verlässliche Schlüsse werden erst in ein bis zwei Jahren möglich sein.

In den Interviews deutete sich jedoch auch an, dass die Bußgeld- und Aufsichtspraxis voraussichtlich durch zwei weitere Faktoren signifikant geprägt werden würde: Auf-

wand für Gerichtsprozesse sowie die Eingaben und Beschwerden Dritter. Während die Interviewpartner die Auswirkungen dieser Faktoren sehr ähnlich beschrieben, gingen die Meinungen bei der Frage auseinander, welche Rolle die Beratung der Verantwortlichen (Unternehmen) in der Aufsichtspraxis nach dem 25. Mai 2018 zu spielen habe.

### 4.1.2 Gerichtsprozesse

Interviewpartner erwähnten wiederholt, dass die aus Bußgeldern eventuell resultierenden gerichtlichen Auseinandersetzungen notgedrungen auch in ihre Erwägungen einfließen müssten. Bei hohen Bußgeldbescheiden wäre zu erwarten, dass der beschiedene Verantwortliche im Zweifel gegen das Bußgeld klagen würde. Für die Gesprächspartner stand dabei weniger die Gefahr im Vordergrund, Prozesse zu verlieren, als die Bindung von Personalressourcen. Ein Behördenleiter meinte, dass er von seinen Mitarbeitern zwar erwarte, nur das zu bescheiden, von dem man überzeugt sei, vor Gericht auch zu bestehen, dass im Zweifel für ihn aber die Herstellung von Rechtsklarheit das wichtigste Ziel wäre. Insofern seien Urteile gegen seine Behörde nicht das „Ende der Welt".[87] Während der eben Zitierte sogar erklärte, dass es ihm mitunter lieber wäre, wenn Unternehmen vor Gericht zögen und so zur Rechtsklarheit beitragen würden, anstatt gleich „einzuknicken" und zu zahlen, betonten andere die mit komplexen Fällen und Gerichtsprozessen einhergehende Personalbindung. Vor allem für kleinere Aufsichtsbehörden, so ein anderer Landesbeauftragter, sei es angesichts – trotz bereits im Zuge des Geltungsbeginns der Datenschutz-Grundverordnung deutlich aufgestockter Personaldecke weiterhin – knapper Personalausstattung schlicht nicht möglich, „sieben bis acht Grundsatzstreitigkeiten mit jedem [zu führen], die dann jeweils Jahre laufen", da dies zu viel andere Arbeit blockieren würde.[88]

Die Auswirkung knapper Ressourcen wird vermutlich sein, dass gerade kleinere Behörden sich *tendenziell* bei der Bescheidung von Bußgeldern und Anordnungen auf eklatante, rechtlich weniger schwierige Fälle konzentrieren und sich gezwungen sehen, bei komplexen Fällen und unklaren Rechtslagen mit der Aussicht auf schwierige und langwierige Gerichtsprozesse zurückzuhalten. Dieser – angesichts der ihnen aufgrund Ressourcenmangels drohenden massiven Arbeitsüberfrachtung[89] – für die Behörden möglicherweise einzig vertretbare Schritt müsste aus gesamtgesellschaftlicher Warte jedoch als problematisch gewertet werden. Schließlich dürfte gerade die gerichtliche Entscheidung komplexer Fälle für die allgemeine Rechtsklarheit besonders wichtig sein.

### 4.1.3 Auswirkungen von Beschwerden Betroffener

Die Bearbeitung von Eingaben und Beschwerden betroffener Personen stellte auch unter der Datenschutzrichtlinie eine wichtige Aufgabe der Aufsichtsbehörden dar. Die Vorgaben der Datenschutz-Grundverordnung in Bezug auf die Frage, wie mit einer Eingabe zu verfahren ist, sind allerdings deutlich strenger: Die Aufsichtsbehörden sind nach Art. 77 und 78 DSGVO verpflichtet, sich mit jeder eingehenden Beschwerde zu befassen, diese „angemessen" zu untersuchen und den Beschwerdeführer innerhalb von drei Monaten über Fortgang und Ergebnis der Beschwerde zu unterrichten. Geschieht dies nicht, können Beschwerdeführer sie auf Untätigkeit verklagen.[90] Neu hinzu kommt zudem die Möglichkeit der Verbandsklage nach Art. 80 Abs. 1 DSGVO. Zur Vertretung der betroffenen Personen sind in Deutschland nur Verbraucherschutzverbände im Sinne von § 3 und 4 Unterlassungsklagegesetz (UKlaG) berechtigt. Ein eigenständiges Klage- und Beschwerderecht gibt es in Deutschland nicht.[91] Als Vertreter betroffener Personen können die Verbände aber alle Ansprüche betroffener Personen, etwa auf Löschung, Berichtigung oder Schadenersatz, geltend machen. Durch den dadurch entstehenden größeren öffentlichen Druck auf die Verantwortlichen entsteht ein Anreiz zu datenschutzkonformen Verhalten.[92] Zudem dürfte die Möglichkeit auf Musterfeststellungsklagen nach dem Gesetz zur Einführung einer zivilprozessualen Musterfeststellungsklage den Druck auf die Verantwortlichen weiter erhöhen.

Presseberichte deuten auf einen sprunghaften Anstieg der Beschwerden hin. So sprach etwa die Berliner Datenschutzbeauftragte von einer Vervierfachung seit dem 25. Mai 2018.[93] Der Baden-Württembergische Landesbeauftragte verzeichnete eine Verdoppelung.[94] Europaweit gingen nach Angaben der Europäischen Kommission zwischen Mai 2018 und Januar 2019 über 95.000 Beschwerden bei den Aufsichtsbehörden ein.[95] Diese Tendenz zeichnete sich bereits in unseren Interviews im Sommer 2018 ab. So verzeichneten interviewte Landesdatenschutzbeauftragte innerhalb der ersten Monate nach Inkrafttreten der Datenschutz-Grundverordnung Verdoppelungen oder sogar Verzehnfachungen der Eingaben und Beschwerden.[96] Aufgrund des wachsenden öffentlichen Bewusstseins um Datenschutz, Betroffenenrechte und die Bedrohungen, die aus Datenverarbeitungen entstehen können, ist anzunehmen, dass Beschwerden weiterhin eher zu- als abnehmen werden. Unterstützt wird dies zusätzlich durch die vereinfachten Möglichkeiten: Beschwerden können in der Regel sehr einfach und schnell über die Webseite der jeweiligen Aufsichtsbehörden des jeweiligen Bundeslandes eingereicht werden.

Für die Aufsichtspraxis der Behörden hat dieser Umstand zwei wesentliche Auswirkungen. Erstens bindet die Bearbeitung von Beschwerden Personalressourcen, die somit für andere Vorhaben (z. B. proaktive anlasslose Kontrollen, Gerichtsprozesse) nicht mehr zur Verfügung stehen. Zwei Landesbeauftragte sprachen sogar von einer drohenden „Lahmlegung" oder „Blockierung" ihrer Behörden durch die Flut von Eingaben.[97] Wenn andere Interviewpartner auch weniger dramatische Worte bemühten, so zeichneten sie doch ein konsistentes Bild von stetig wachsenden Beschwerde-Zahlen, die immer mehr Arbeitskapazität beanspruchten.[98] Insofern Beschwerden auf wachsende öffentliche Sensibilisierung hindeuteten, werteten die Befragten das Phänomen prinzipiell positiv, sahen sich aber gezwungen, neue Lösungen zu entwickeln, um Ressourcen zu erhalten. Sie zogen unter anderem in Erwägung, Beschwerden stärker risikogewichtet zu bearbeiten, vermehrt auf den privaten Rechtsweg zu verweisen und Arbeitsprozesse weiter zu standardisieren.[99]

Die zweite Auswirkung ist, dass der Inhalt der Beschwerden droht, die Stoßrichtung der Aufsichtspraxis zu bestimmen. Je mehr Zeit- und Personalressourcen der Behörden von der Beschwerden-Bearbeitung aufgezehrt werden, desto weniger stehen diese Ressourcen für eigene strategische Schwerpunktsetzungen zur Verfügung, wie z. B. für Kontrollen bestimmter Branchen oder das Führen komplexerer Gerichtsprozesse. Was kontrolliert und gegebenenfalls sanktioniert wird, droht stattdessen de facto vom Inhalt der eingehenden Beschwerden vorgegeben zu werden. Das wirft die Frage auf, ob hieraus Lücken in der Aufsichtspraxis entstehen. Damit stellt sich die Frage, ob nicht gerade jetzt, wo Grundrechte von immer invasiveren, technisch fortgeschrittenen Verarbeitungen bedroht werden, der aufsichtsbehördliche Fokus durch eine Flut von Beschwerden auf relative Bagatellen gelenkt wird, die gerade *nicht* die risikoreichsten oder strategisch signifikantesten Datenverarbeitungen zum Inhalt haben, sondern eben jene, die von Nicht-Fachleuten leicht erkannt und verstanden werden.

Diese Gefahr scheint real, muss aber auch qualifiziert werden. Einerseits berichteten die meisten, aber nicht alle Interviewpartner, dass sich das Gros der Beschwerden in der Tat bislang um eher einfache Verarbeitungen gedreht hatte, die nicht unbedingt die höchsten Risiken darstellten, dafür aber leicht erkannt und verstanden würden: insbesondere Videoüberwachung und unerwünschte Werbung.[100] Andererseits können auch technisch einfache Verarbeitungen ernste Risiken für Betroffene darstellen, beispielsweise im Beschäftigtendatenschutz, wo Sensibilisierungskampagnen der Behörden zu einem nachhaltigen Anstieg der Beschwerden geführt haben.[101] Auch scheinen zumindest exponierte Großunternehmen der Internetwirtschaft einen nicht unerheblichen Anteil an Eingaben und Beschwerden aus der Bevölkerung auf sich zu ziehen, die sich zum Teil auch um technisch komplexere, risikobehaftetere Verarbeitungen drehen.[102]

Grundsätzlicher stellt sich auch die Frage, was eine „Bagatelle" ist. Interviewpartner betonten wiederholt, dass sie – bei aller Sorge um Fremdsteuerung ihrer Arbeit und

„Lahmlegung" durch Eingaben – sich sehr wohl ebenfalls für „kleinere" Fälle, etwa Ausspähung durch die Videokamera des Nachbarn, zuständig sehen, da diese Fälle für den Betroffenen eben *keine* Bagatellen sind. Außerdem formulierte ein Interviewpartner, ist „es für die Zufriedenheit der Leute nicht unwichtig, dass die scheinbar ganz kleinen Dinge behandelt werden – beispielsweise unverlangt zugesendete E-Mail".[103]

Wichtig für diese Frage dürfte auch sein, inwieweit Unternehmen von der Beschwerdemöglichkeit Gebrauch machen, um Wettbewerber, deren Geschäftsmodelle auf datenschutzrechtlich fragwürdigen Verarbeitungen fußen oder die einfach davon abgesehen haben, für den Datenschutz notwendige Investitionen zu tätigen, bei Behörden „anzuschwärzen". Zumindest einer interviewten Rechtsanwältin war genau solch ein Fall bekannt, in dem etablierte Unternehmen die Datenschutzbehörde auf einen neuen Wettbewerber aufmerksam machten, dessen Geschäftsmodell auf sehr invasiven Verarbeitungen beruhte.[104] Im europäischen Wettbewerbsrecht spielen Eingaben von geschädigten Marktteilnehmern schon länger eine wichtige Rolle[105] und etliche der spektakulärsten Fälle im Wettbewerbsrecht der vergangenen Jahre gehen auf Beschwerden von Unternehmen über ihre Wettbewerber zurück, denen die Behörden dann nachgegangen sind. Datenschutzbehörden berichten zumindest davon, dass ihnen von Unternehmen, die entsprechende Investitionen getätigt haben, wiederholt angetragen wird, gegenüber anderen hart durchzugreifen.[106] Für Datenschutzbehörden würde eine Zunahme von Beschwerden von Unternehmen über ihre Wettbewerber vermutlich Chancen wie Herausforderungen bieten: einerseits das Problem, sich nicht illegitim instrumentalisieren zu lassen, andererseits die Chance, an Informationen über technisch anspruchsvolle und relativ verborgene Datenschutzverstöße zu kommen, die ansonsten unerkannt blieben.

### 4.1.4 Beratung von Verantwortlichen

Während sich bei der Bußgeldpraxis der Aufsichtsbehörden weitgehend Einigkeit abzeichnete, gab es klare Differenzen in der Frage, welche Rolle die Beratung der Verantwortlichen (d.h. Unternehmen und Verwaltungsbehörden) in der Aufsichtspraxis unter der Datenschutz-Grundverordnung zu spielen habe.

„Beratung" umfasst in diesem Kontext vor allem vier Tätigkeitsbereiche, deren Umsetzung den Aufsichtsbehörden prinzipiell obliegt:

- Erstens die Bereitstellung von Leitlinien, Handlungsempfehlungen, Stellungnahmen,[107] Auslegungshilfen, Orientierungshilfen und Anwendungshinweisen[108] zur Umsetzung der – zum Teil hochabstrakten – materiellrechtlichen Vorgaben der Datenschutz-Grundverordnung.

- Zweitens die Durchführung von Informationsveranstaltungen und Workshops für betriebliche und behördliche Datenschutzbeauftragte sowie sonstige zuständige Mitarbeiter der Verantwortlichen (z. B. Software-Entwickler), entweder bei der Aufsichtsbehörde selbst oder im Rahmen von Tagungen und Schulungsveranstaltungen von Verbänden oder sonstigen Veranstaltern.

- Drittens die Beantwortung von individuellen Beratungsanfragen und Diskussion von datenschutzrechtlichen Problemen und möglichen Lösungen mit einzelnen Verantwortlichen oder ihren Datenschutzbeauftragten, etwa auf Anfrage der Ratsuchenden bei der Aufsichtsbehörde oder im Rahmen von regelmäßigen „Sprechstunden", wie sie manche Aufsichtsbehörden z. B. für Startups anbieten.

- Viertens regelmäßige Treffen (in jährlichem bis vierteljährlichem Turnus) mit den größten und datenverarbeitungsintensivsten Unternehmen des jeweiligen

Bundeslandes, um ihre Vorgänge, Vorhaben, Herausforderungen und mögliche Lösungen zu besprechen.

Insbesondere die erste, zweite und dritte Form von Beratung wurde von allen interviewten Aufsichtsbehörden bisher angeboten. In den Monaten vor und unmittelbar nach dem 25. Mai 2018 wurde das Beratungsangebot in der Regel erheblich ausgeweitet, auch als Reaktion auf die dramatisch gestiegene Nachfrage, die das Angebot meist um ein Vielfaches überstieg. Alle Interviewpartner glaubten ferner, dass die gezielte Beratung von Verantwortlichen einen erheblichen Mehrwert erzeugt, und zwar für beide Seiten: Die Verantwortlichen erhielten ein besseres Verständnis, welche Maßnahmen nötig seien, um Datenschutzkonformität sicherzustellen (auch wenn die Interviewpartner klarstellten, dass sie im Rahmen von Beratungen grundsätzlich keine verbindliche Gewährleistung für die Rechtskonformität einer besprochenen Verarbeitung übernehmen könnten und würden). Umgekehrt erhielten die Aufsichtsbehörden bessere Einblicke in die Verarbeitungen, die tatsächlich stattfinden, und in damit verbundene Probleme. Sie könnten so direkt auf die Anhebung des allgemeinen Datenschutzniveaus hinwirken.

Wo die Positionen der Interviewpartner zum Teil auseinandergingen, war die Frage, welche Rolle Beratung vor allem von Unternehmen künftig zu spielen habe. Während manche Interviewpartner Beratung weiterhin als einen sehr wichtigen Teil ihrer Aufsichtspraxis verstanden, die sie auch institutionell von anderen Aufgaben (z. B. Kontrollen, Bußgeldern) zu trennen versuchten, sahen andere die Beratung von nichtöffentlichen Verantwortlichen als eine bestenfalls periphere Aufgabe. Hier traten auch unterschiedliche Interpretationen der Datenschutz-Grundverordnung zum Vorschein. So argumentierte ein Landesbeauftragter, dass unter der Datenschutz-Grundverordnung die Beratung von Unternehmen schlicht nicht länger in seinen „primären Befugniskatalog und Zuständigkeits- und Funktionsbereich" falle. Während man schon versuche, auch Beratungstätigkeit zu leisten, könne das jetzt nur noch „bedingt" geschehen. Vorrang müsse die Abarbeitung des in Art. 57 DSGVO definierten, verpflichtenden Aufgabenkatalogs haben. Soweit nach der Erfüllung dieser Aufgaben noch Kapazität frei sei, könnte die Aufsichtsbehörde auch Beratung leisten – aber nicht vorher.[109] Diese Position wurde keineswegs von allen geteilt. Mehrere andere Gesprächspartner betonten ganz im Gegenteil, dass für sie Beratung weiterhin eine zentrale Aufgabe sei, die sich ihrer Lesart zufolge auch aus dem Art. 57 DSGVO ergäbe und für die sie zum Teil auch dedizierte Personalkapazitäten bereitstellten.

Eine noch offene Frage ist, wie sich Beratung mit einer härteren Sanktionspraxis vereinbaren lässt. Interessanterweise betonten gerade mehrere der Landesbehörden, die weiterhin Beratung als wichtigen Teil ihrer Arbeit sehen, ebenfalls die Notwendigkeit wesentlich höherer Bußgelder und intensivere Kontrollen. In der Tat haben gerade diese Behörden auch in der Vergangenheit keineswegs vor der Durchsetzung vergleichsweise hoher Bußgelder zurückgeschreckt. Insofern dürfte die – prinzipiell plausible – Sorge, dass intensivierte Beratung am Ende zur Vereinnahmung der Behörde durch die Wirtschaft („regulatory capture")[110] führt, eher unbegründet sein. Im Gegenteil berichteten gerade Behörden, die einen Schwerpunkt auf Beratung nichtöffentlicher Stellen legen, wiederholt, von betrieblichen Datenschutzbeauftragten und der Industrie allgemein, geradezu aufgefordert worden zu sein, doch gegenüber nichtdatenschutzkonformen Unternehmen hart durchzugreifen.

Es stellt sich jedoch die Frage, ob harte Sanktionierung einer effektiven Beratungspraxis nicht insofern im Wege stehen könnte, als dass Unternehmen aus Angst vor Bußgeldern künftig davon absehen könnten, den Rat der Aufsichtsbehörden zu suchen. Dies birgt insofern Risiken, als dass nach Art. 83 Abs. 2 lit. h DSGVO bei einer Entscheidung über die Verhängung einer Geldbuße und über deren Höhe insbesondere zu berücksichtigen ist, ob und gegebenenfalls in welchem Umfang der Verantwortliche oder der Auftragsverarbeiter den Verstoß mitgeteilt hat. Wird der Verstoß also letztlich dennoch

aufgedeckt, kann der Umstand des Verschweigens zu einem noch höheren Bußgeld führen.

Sollten Verantwortliche oder Auftragsverarbeiter zudem darauf verzichten, sich anderweitig beraten zu lassen, könnte dies letztlich sogar zu einer Senkung des Datenschutzniveaus führen. Diese Sorgen scheinen eher begründet, wobei das Bild keineswegs eindeutig ist. Einerseits ist die Zahl der Beratungsanfragen von Unternehmen bei den Aufsichtsbehörden mit der Datenschutz-Grundverordnung zunächst deutlich angestiegen. Auch plante keiner der von uns interviewten Datenschutzbeauftragten, künftig zurückhaltender zu sein, was Anfragen bei den Aufsichtsbehörden anging. Eine betriebliche Beauftragte ging sogar von einer weiteren Zunahme und Intensivierung des Kontakts mit den Behörden aus, insbesondere aufgrund der Abstraktheit der Datenschutz-Grundverordnung.[111] Aber es gibt auch gegenteilige Beispiele, die auf erhebliches Misstrauen der Privatwirtschaft gegenüber den Aufsichtsbehörden schließen lassen. Als beispielsweise der Thüringische Datenschutzbeauftragte im Dezember 2018 eine Umfrage unter Unternehmen durchführen wollte, um sich ein Bild vom Umsetzungsstand der Datenschutz-Grundverordnung und den Hauptproblemen, die Unternehmen damit haben, zu machen, warnten mehrere IHKs ihre Mitglieder vor einer Teilnahme, mit Verweis auf die Gefahr, dass Verstöße ans Licht kommen und zu Bußgeldern führen könnten.[112]

Ein im Januar 2019 bekannt gewordener Hamburger Bußgeld-Fall unterstreicht die kommunikativen Herausforderungen, die sich für die Aufsichtsbehörden aus der gleichzeitigen Rolle als Berater wie strafenden Aufsehern ergeben. Laut Medienberichten hatte ein kleines Versandhaus sich ratsuchend an die hessische Landesbehörde mit dem Problem gewandt, dass sein spanischer Dienstleister nicht bereit sei, einen Auftragsverarbeitungs-Vertrag anzufertigen.[113] Die Details der Interaktion zwischen dem Unternehmen und der hessischen Behörde sind nicht bekannt, aber offensichtlich nutzte das Versandhaus die ihm von der hessischen Behörde bereitgestellten Hilfsmittel nicht,[114] und erweckte zumindest den klaren Anschein, der hessischen Einschätzung seiner Rechtspflichten zu widersprechen und nicht bereit zu sein, diesen nachzukommen.[115] Daraufhin übergab die hessische Aufsichtsbehörde den Fall an die für das Unternehmen eigentlich zuständige Hamburger Behörde, die es schließlich mit einem Bußgeld von 5.000 Euro belegte.[116]

Ob das Bußgeld gerechtfertigt war, soll mangels Kenntnis der genauen Sachlage hier nicht bewertet werden. Interessant ist vor allem die kommunikative Herausforderung. Die Schlagzeile „Bei Aufsichtsbehörde angefragt – Bußgeld kassiert!“ (wie ein Datenschutz-Blog titelte) schrieb sich quasi von selbst.[117] Online-Kommentaren ist zu entnehmen, dass diese spezielle Interpretation des Vorfalls bei mehr als einem Kommentator hängen geblieben sein dürfte – auch wenn das sozial-mediale Echo keineswegs nur negativ war. Die offenen Fragen des Falls, die für eine fundierte Bewertung nötig wären – z. B. mögliche Verweigerungshaltung des Unternehmens, die Qualität seiner Rechtsberatung, aber auch das Vermögen eines Klein(st)unternehmens, die ihr von den Behörden offerierten Hilfsmittel zu nützen, die Schwere des aus der fraglichen Verarbeitung hervorgehenden Risikos für die betroffenen Personen, die Verfügbarkeit praktikabler Alternativen, und das Machtgefälle zwischen Klein(st)unternehmen und großen Auftragsverarbeitern – gingen in der Debatte eher unter und bleiben öffentlich unbeantwortet (möglicherweise auch aus rechtlichen Gründen). Entsprechend groß ist der Raum für Spekulation, Halbwahrheiten und Panikmache.

Sofern Behörden die Beratung von Verantwortlichen weiterhin als einen wichtigen Teil ihrer Arbeit sehen, wird es wichtig werden, Kommunikationsstrategien für potentiell kontroverse Fälle zu entwickeln. Ebenfalls müssen klare Regeln kommuniziert werden, wie Beratung und (strafende) Aufsicht sich zueinander verhalten und insbesondere wie mit beratungsresistenten oder strategisch motivierten vermeintlichen „Ratsuchenden“ umgegangen wird.[118] Die striktere – auch institutionelle – Trennung der für Beratung

einerseits und Kontrollen und Bußgelder andererseits zuständigen Einheiten (z. B. getrennte Aktenvorgänge), wie sie manche Aufsichtsbehörden implementiert und kommuniziert haben, könnte hier ein Mittel sein – auch um strategischem Vorgehen von Unternehmen vorzubeugen (etwa in „letzter Minute" vor dem Bekanntwerden eines gravierenden Verstoßes „Beratung" zu suchen, um Sanktionen zuvorzukommen).

## 4.2 Auswirkungen der Sanktionen auf die betriebliche Datenschutzpraxis

Viele der durch die Datenschutz-Grundverordnung normierten Pflichten bestanden schon vor deren Geltung; diese wurden aber weitgehend nicht umgesetzt.[119] Daher stellt sich die Frage, ob die potentiell hohen Bußgeldbeträge geeignet sind, zu einer besseren Durchsetzung und Einhaltung der Vorgaben der Datenschutz-Grundverordnung beizutragen. Zur Beantwortung dieser Frage wurden vor Geltungsbeginn der Datenschutz-Grundverordnung am 25. Mai 2018 Interviews mit neun verschiedenen Unternehmen durchgeführt. Dabei wurden bewusst Unternehmen verschiedener Branchen und Größe ausgewählt, um die Konsequenzen der Geldbußen möglichst differenziert abbilden zu können (vgl. Tabelle 1).

| Unternehmen | Branche | Mitarbeiter | Position des Befragten |
|---|---|---|---|
| A | Medien, Technologie | > 10.000 | Projektleitung DSGVO |
| B | Personalberatung | 30-50 | Geschäftsführung |
| C | Personalberatung | 30-50 | Geschäftsführung |
| D | Unternehmensberatung | 5-10 | Geschäftsführung |
| E | Personalberatung | 1 | Geschäftsführung |
| F | Gesundheit/Medizin | > 10.000 | Betriebliche Datenschutzbeauftragte |
| G | Gesundheit/Medizin | N/A | Externe betriebliche Datenschutzbeauftragte |
| H | Kommunikation | > 10.000 | Betriebliche Datenschutzbeauftragte |
| I | Handel | > 10.000 | Im Datenschutz tätiger Mitarbeiter |

Tabelle 1: Überblick über die Unternehmen

Hinsichtlich der Frage, ob Geldbußen oder andere Faktoren der Antrieb für die Umsetzung der neuen Vorgaben seien, wiesen die Unternehmen den Geldbußen eine entscheidende Rolle zu, führten aber auch andere Faktoren an, die für sie eine zentrale Rolle spielen. Die neuen Sanktionen sind nach Aussagen der Interviewpartner der Motor, andererseits wurde von den Unternehmen nicht erwartet, dass mit Geltung der

Auswirkungen der Sanktionen auf die Datenschutzpraxis

Datenschutz-Grundverordnung im großen Stil Bußgelder verteilt werden; zunächst wurde erst einmal eine „Abmahnungswelle" befürchtet.

Als wichtigsten Faktor führen einige Unternehmen zum Beispiel einen drohenden Imageverlust an, da für diese Unternehmen eine geschädigte Reputation zu gewaltigen finanziellen Schäden führt – ähnlich der Schäden durch Geldbußen. Zwar führen diese Unternehmen die Reputation als wichtigsten Faktor an, allerdings zeigen zahlreiche Aussagen aller befragten Unternehmen, dass sich ganz ohne die Anhebung der Geldbußen vermutlich eher weniger verändert hätte: „Ich glaube, dass sonst vielleicht gar keine Veränderung stattgefunden hätte, ohne die Geldbußen".[120]; „Das Bundesdatenschutzgesetz wurde natürlich nicht ganz so intensiv umgesetzt wie die Datenschutz-Grundverordnung jetzt – einfach weil die Strafen nicht so hoch waren".[121]; „Die Androhung dieser Strafe als Worst Case hat dazu geführt, dass jedes Unternehmen sich damit beschäftigen muss".[122] „Es gibt sehr wenige Dinge in der Datenschutz-Grundverordnung, die neu sind (wie die verstärkten Rechenschaftspflichten). Bisher haben sich die Unternehmen nicht davon überzeugen lassen, das Bußgeld wirkt disziplinsteigernd."[123]

Für die Unternehmen hängt ihr künftiges Handeln stark davon ab, wie hart die Geldbußen in der Realität durchgesetzt werden – also davon, welche Durchsetzungspraxis sich bei den Aufsichtsbehörden entwickelt. Allerdings halten Unternehmen die Datenschutzbehörden auch für kooperativ und erwarten nicht sofort die Nutzung des vollen Bußgeldrahmens, sondern Zwischenschritte in Form von Warnungen, Verwarnungen oder ähnlichen Maßnahmen. Gerade kleine Unternehmen fühlen sich nicht als Ziel der Aufsichtsbehörden und erwarten, dass die Behörden gerade kurz nach Geltungsbeginn der Verordnung erst einmal mit der Durchsetzung der Datenschutz-Grundverordnung überfordert sein werden. Dennoch sind sich alle Befragten einig, dass die angedrohten hohen Bußgelder dafür verantwortlich sind, dass Datenschutz nun auch auf Vorstands- und Managementebene ernst genommen wird. Nicht zuletzt dadurch hat das Thema Datenschutz in den Unternehmen einen neuen Stellenwert bekommen.

Bei der Befragung der Unternehmen zur direkten Handhabung drohender Geldbußen wurde schnell klar, dass bislang wenig bis nichts unternommen wurde, um sich gegen mögliche Bußgeldzahlungen abzusichern. Rücklagen wurden nach Kenntnis der jeweils befragten Person nicht gebildet, teilweise werden die angedrohten hohen Bußgelder auch eher als „Abschreckung" gesehen und eine tatsächliche Verhängung dieser Gelder nicht erwartet. Für einige Unternehmen wäre eine Bildung der Rücklagen auch schlichtweg viel zu hoch, um sie tatsächlich zu tätigen.

Zu möglichen Versicherungen konnten sich die Unternehmen nicht im Detail äußern. Ein „Rundum-sorglos-Versicherungspaket" bei (schuldhaften) Verstößen gegen die Datenschutz-Grundverordnung wird es jedenfalls auch künftig wohl kaum geben. Zwar gilt in Deutschland kein direktes Versicherungsverbot; allerdings argumentieren deutsche Versicherungsunternehmen in diesem Zusammenhang, dass der Ersatz einer Geldbuße einer Förderung von rechtswidrigem Verhalten gleichkäme und damit als sittenwidriges Rechtsgeschäft gegen § 138 BGB verstoße.[124] Umso mehr gilt für Unternehmen, den Anforderungen der Datenschutz-Grundverordnung ausreichend Rechnung zu tragen.

# 5
# Notwendige Bedingungen für ein effektives Sanktionsregime

Das Sanktionsregime der Datenschutz-Grundverordnung ist kein Selbstzweck, sondern dient der effektiven Umsetzung des Datenschutzrechts und dazu, ein hohes Schutzniveau für die Rechte und Freiheiten natürlicher Personen zu erreichen.[125] Dies verdeutlicht, dass die Abhilfe- und Sanktionsbefugnisse dahingehend auszuüben sind, dass ein (grund-)rechtskonformer Zustand hergestellt wird.

## 5.1 Voraussetzungen

Um dies zu erreichen, müssen die Aufsichtsbehörden zunächst grundsätzlich in der Lage sein, ihre Abhilfebefugnisse effektiv auszuüben. Die Wichtigkeit dessen zeigt sich nicht zuletzt in den Aussagen einiger Unternehmen ihr eigenes Handeln in Abhängigkeit der Durchsetzungsfähigkeit der Behörden zu stellen. Wesentlich für die Effektivität der Behörden ist demnach, dass mögliche Verstöße umfassend untersucht und Verarbeitungsverfahren geprüft werden können. Die Befugnisse der Aufsichtsbehörden gemäß Art. 58 Abs. 1 lit. a und b DSGVO sind zwar bezüglich der Überprüfung der Verarbeitungstätigkeiten der Verantwortlichen und Auftragsverarbeiter umfassend ausgestaltet. Allerdings erfordern solche Überprüfungen die Analyse komplexer Zusammenhänge und die Untersuchung sowohl technischer als auch rechtlicher Aspekte der Verarbeitung.

Dabei sind die Aufsichtsbehörden in vielen Fällen auf die Verantwortlichen und Auftragsverarbeiter angewiesen, da diese die Verarbeitung vornehmen und damit auch über die entsprechenden Informationen verfügen. Daher haben die Aufsichtsbehörden gemäß Art. 58 Abs. 1 lit. a DSGVO die Untersuchungsbefugnis bezüglich der Bereitstellung aller erforderlichen Informationen.

Bezüglich der Mitwirkungspflicht des Verantwortlichen gilt allerdings der „Nemotenetur"-Grundsatz, der sich aus Art. 47 Abs. 2 und Art. 48 Abs. 1 Grundrechtecharta (GrCh) ergibt und nach dem sich Beschuldigte nicht selbst belasten müssen.[126] Allerdings entbindet dieser Grundsatz den Verantwortlichen nicht von der Pflicht, der Aufsichtsbehörde Informationen bereitzustellen. Auskunftsverweigerungsrechte dürfen nur geltend gemacht werden, wenn verlangt würde, dass der Verantwortliche das Vorliegen einer Zuwiderhandlung eingesteht, für die die Aufsichtsbehörde beweispflichtig ist.[127] Dies ist etwa in § 42 Abs. 4 BDSG umgesetzt, wonach Meldungen und Benachrichtigungen nach Art. 33 f. DSGVO in einem Strafverfahren nur mit Zustimmung des Meldepflichtigen oder Benachrichtigenden verwendet werden dürfen.

Damit die Untersuchungen der Aufsichtsbehörden in der von Art. 8 Abs. 3 GrCh geforderten Unabhängigkeit geschehen können, müssen diese mit den Ressourcen ausgestattet werden, die erforderlich sind, um sie in der gebotenen Tiefe und in einer angemessenen Vielzahl von Fällen durchführen zu können.[128] Dabei muss sichergestellt sein, dass die Behörden nicht nur reaktiv auf Beschwerden betroffener Personen hin handeln, sondern auch proaktiv eigene Überprüfungen anstoßen können.

Allerdings ist es nicht in jedem Fall realistisch, dass die Aufsichtsbehörden auf externe Ressourcen verzichten können. Wenn im Rahmen einer datenschutzrechtlichen Überprüfung Verstöße festgestellt werden, schließt sich ein Verfahren gegen den entsprechenden Verantwortlichen an. Kommt es dabei zu einer gerichtlichen Auseinandersetzung, muss sichergestellt sein, dass die Aufsichtsbehörde vor Gericht angemessen vertreten ist. Aufgrund der Komplexität und Eigenheiten des Prozessrechts, das im Datenschutzrecht neben den nationalen Instanzen auch Verfahren vor den Gerichten der Europäische Union beinhalten kann, kann es geboten sein, dass sich eine Aufsichtsbe-

Notwendige Bedingungen für ein effektives Sanktionsregime

hörde anwaltlich vertreten lässt. Dies kann sich jedoch schwierig gestalten, wenn zwischen Kanzleien und Verantwortlichen bereits Mandatsverhältnisse bestehen und die Kanzleien sich daher gehindert sehen, die Aufsichtsbehörden zu vertreten. Zudem ist die öffentliche Verwaltung mit einem geringen Budget für solche Zwecke ausgestattet und kann bei der Vergütung anwaltlicher Leistungen nicht mit großen oder multinationalen Unternehmen konkurrieren.

Zudem ist es von großer Bedeutung, dass in gerichtlichen Verfahren die komplexen Fragestellungen des Datenschutzrechtes ausreichend gewürdigt werden können. Nach § 41 Abs. 1 BDSG in Verbindung mit § 68 OWiG sind auch Geldbußen nach Art. 83 Abs. 4 bis 6 DSGVO vor dem Amtsgericht zu verhandeln. Erst ab einer Geldbuße über 100.000 Euro ist nach § 41 Abs. 1 S. 3 BDSG das Landgericht zuständig. Allerdings sind nach den internen Ressourcenplänen für Ordnungswidrigkeitenverfahren vor den Amtsgerichten nur geringe Bearbeitungszeiten vorgesehen. Aufgrund der Komplexität des Datenschutzrechtes und den Unterschieden zu anderen Ordnungswidrigkeiten sollte diese Zuweisung erweitert oder generell in Frage gestellt werden. Würden sämtliche Geldbußen vor dem Landgericht verhandelt werden, könnten zudem über eine Sonderzuständigkeit einer Kammer sämtliche Datenschutzverfahren zugewiesen werden. Dadurch würde sich die Einarbeitungszeit verringern.

Weiterhin wäre es sinnvoll, wenn bei Verfahren, die sich mit europarechtlichen Fragen, wie etwa der Auslegung der Datenschutz-Grundverordnung befassen, auch untere Instanzen von ihrer Vorlagemöglichkeit nach Art. 267 Abs. 2 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) Gebrauch machen. Auch dies könnte die Gesamtdauer eines Verfahrens erheblich reduzieren.

Um diesen Problemen, die auf fehlende Ressourcen auf Seiten der Aufsichtsbehörden zurückzuführen sind, zu begegnen und eine effektive Erfüllung der Aufgaben und Abhilfebefugnisse der Aufsichtsbehörden zu gewährleisten, ist eine Aufstockung der Ressourcen unerlässlich.[129] Als eine Möglichkeit zur adäquaten Aufstockung der Ressourcen könnte man überlegen, verhängte Geldbußen – nicht wie bisher – in den Haushalt der Bundesländer, sondern vielmehr direkt in den Haushalt der Aufsichtsbehörden fließen zu lassen. Allerdings wären mögliche Nachteile und Nebenwirkungen zu bedenken: Würden Stellenbewilligungen von Geldbußen abhängig gemacht oder müssen Beschäftigte sogar den Gegenwert ihrer Stelle selbst durch Prüfungen eintreiben, falls sie auch im nächsten Jahr in der Aufsichtsbehörde arbeiten wollen, würde sich der Charakter der Prüfungen ändern. Insbesondere wären Prüfungen unattraktiv, die sich über einen längeren Zeitraum hinziehen und die möglicherweise erst nach mehreren Gerichtsinstanzen entschieden werden. Noch unbekannte Sachverhalte, die erst neu durchdacht und technisch und rechtlich gut argumentiert werden müssten, die aber eine erhebliche Signalwirkung für die Zukunft entfalten könnten, könnten vernachlässigt werden, um lieber im Schnellverfahren die bekannten Fälle durchzuziehen. Es darf nicht der Effekt entstehen, dass diejenigen Datenverarbeiter, deren Anwälte das Verfahren in die Länge ziehen, aus dem Fokus geraten, weil es sich finanziell nicht lohnt. Auch muss die Aufsichtsbehörde den langen Atem haben, um Fälle mit grundsätzlichem Charakter bis vor den Gerichtshof der Europäischen Union zu bringen. Ein Sachbearbeiter, der daran denken muss, wie er seinen nächsten Personenmonat refinanziert, müsste andere Prioritäten setzen. Auch ein je nach Prüferfolg andauernd wechselnder Personalkörper bringt mehr Nachteile als Vorteile mit sich, weil ständig Wissen verloren geht. Schließlich spielt auch eine Rolle, ob in einem Bundesland wirtschaftsstarke Unternehmen sitzen oder ob es sich lediglich um Kleinstunternehmen handelt, die von einem Bußgeld in nennenswerter Höhe sofort mit der Insolvenz bedroht würden.

## 5.2 Auswahl und Ausübung der Abhilfe- und Sanktionsbefugnisse

Die Ausübung der Abhilfebefugnisse richtet sich nach den allgemeinen rechtsstaatlichen Grundsätzen. Bei jeglicher Form staatlicher Sanktionen ist dabei insbesondere der Grundsatz der Verhältnismäßigkeit zu beachten. Die Maßnahme muss also geeignet, erforderlich und angemessen sein, um ein legitimes Ziel zu erreichen. Das Ziel der Abhilfebefugnisse ist dabei durch die Datenschutz-Grundverordnung bereits vorgegeben: Die Wahrung der Rechte und Freiheiten natürlicher Personen. Die Ausübung der Abhilfebefugnisse muss sich also an der Erreichung dieses Ziels dahingehend messen lassen, ob sie dazu förderlich und das mildeste effektive Mittel sind und ob sie in einem angemessenen Verhältnis zu dem Verstoß stehen.

Laut Erwägungsgrund 148 DSGVO sollen im Interesse einer konsequenteren Durchsetzung des Datenschutzrechtes neben den Abhilfemaßnahmen, die die Aufsichtsbehörden treffen können, auch Sanktionen einschließlich Geldbußen verhängt werden. Nach Art. 83 Abs. 1 DSGVO sollen Geldbußen wirksam und verhältnismäßig sein sowie abschreckend wirken. Damit soll sichergestellt werden, dass die Mitgliedstaaten die Interessen der Europäischen Union ausreichend berücksichtigen. Schließlich soll verhindert werden, dass rein symbolische Strafen erfolgen.[130]

Aufgrund der besonderen Bedeutung des Grundsatzes der Verhältnismäßigkeit steht nicht zu befürchten, dass bei geringen Verstößen das vielzitierte Höchstmaß der Geldbuße nach Art. 83 Abs. 4 und 5 DSGVO zum Tragen kommt. Der Kriterienkatalog des Art. 83 Abs. 2 DSGVO lenkt das Ermessen, welches den Aufsichtsbehörden bei der Bemessung einer Geldbuße zukommt. Bei Verhängung eines besonders hohen Bußgeldes ist es zudem wahrscheinlicher, dass sich der Verantwortliche gerichtlich zur Wehr setzt. Aufgrund vieler auslegungsbedürftiger Konzepte und Begriffe der Datenschutz-Grundverordnung können solche gerichtlichen Verfahren sehr lange dauern. Allerdings sind Musterverfahren zur Herstellung von Rechtssicherheit wesentlich. Um begrenzte Ressourcen sinnvoll zu verwenden, ist es daher geboten, dass sich die Aufsichtsbehörden (weiterhin) untereinander koordinieren, um Verfahren zu rechtswidrigen Praktiken aufzuteilen. Dabei kann auch eine Abstimmung mit Verbraucherschutzorganisationen, die durch ihre Abmahnmöglichkeiten selbst eine Vielzahl von gerichtlichen Entscheidungen herbeiführen, oder mit Kartellbehörden hilfreich sein.

Allerdings dürfen auch die milderen Abhilfebefugnisse nicht vernachlässigt werden. Art. 58 DSGVO stellt den Aufsichtsbehörden ein breites Instrumentarium zur Verfügung, das zur Herstellung eines (grund-)rechtskonformen Zustands umfänglich genutzt werden sollte. Auch die Verwarnung und Warnung können dabei sinnvolle Mittel sein, um Verstöße gegen das Datenschutzrecht zu beseitigen. Verwarnungen sind auf vergangenes Handeln gerichtet, während Warnungen in die Zukunft gerichtet sind.

Im Fall von Verwarnungen gilt dies insbesondere bei Verstößen, die nicht so schwerwiegend sind, dass eine Geldbuße verhältnismäßig wäre.[131] Zum Beispiel kann es vorkommen, dass ein Verantwortlicher eine E-Mail an eine Vielzahl von Personen mit offenem E-Mail-Verteiler versendet, d. h. ohne dabei die Adressen in „BCC“ zu setzen. In den meisten Fällen wird dies als Verstoß von geringer Schwere zu werten sein. Insbesondere wenn der Verantwortliche einsichtig ist und etwa Schulungsmaßnahmen als Konsequenz zieht oder künftig Mailinglisten ohne offenen Verteiler nutzt, wäre ein Bußgeld im Einzelfall voraussichtlich unverhältnismäßig.

Warnungen können dagegen ausgesprochen werden, um drohende Verstöße zu verhindern. Im Gegensatz zu einem Verbot einer Verarbeitungstätigkeit besteht bei der Warnung der Vorteil, dass diese bereits ausgesprochen werden kann, wenn eine Stelle beabsichtigt, eine voraussichtlich rechtswidrige Verarbeitung durchzuführen. Durch eine Warnung kann ein Verstoß also noch verhindert werden. Im Gegensatz dazu muss die Aufsichtsbehörde bereits detaillierte Informationen über eine geplante Verarbeitung

Notwendige Bedingungen für ein effektives Sanktionsregime

haben, um ein Verbot aussprechen zu können. Von Fällen der vorherigen Konsultation gemäß Art. 36 DSGVO bei Verarbeitungen mit hohem Restrisiko abgesehen wird dies jedoch im Voraus vermutlich selten der Fall sein.

Kommt es nach einer Verwarnung oder einer Warnung jedoch zu einem – im Fall der Verwarnung erneuten – Verstoß, so fließt dies gemäß Art. 83 Abs. 2 lit. i DSGVO in die Bewertung des (erneuten) Verstoßes mit ein. Dieser wird in einem solchen Fall als schwerwiegender zu beurteilen sein und die Begründung einer Geldbuße erleichtern.

Bezüglich jeglicher Sanktionen gilt das Verbot der Doppelbestrafung („ne bis in idem") gemäß Art. 50 GrCh. Danach darf dieselbe Tat nicht mehrfach durch Strafmaßnahmen sanktioniert werden. Der Grundsatz gilt dabei sowohl für nach deutschem Recht als strafrechtliche als auch als Ordnungswidrigkeiten eingeordnete Sanktionen.[132]

Neben den Geldbußen finden jedoch auch weitere Sanktionsmittel nach dem nationalen Recht Anwendung, wie etwa die Zwangsmittel zur Abstellung von Gesetzesverstößen nach §§ 6 ff. Verwaltungsvollstreckungsgesetz (VwVG).[133] So können Aufsichtsbehörden etwa zur Durchsetzung eines Verarbeitungsverbots nach Art. 58 Abs. 2 lit. f DSGVO auch ein Zwangsgeld gemäß § 11 VwVG verhängen.[134] Diese fallen nicht unter das Doppelbestrafungsverbot, da sie nicht der Ahndung eines Verstoßes dienen, sondern auf die Herbeiführung einer Handlung oder Unterlassung gerichtet sind.[135] Nach § 11 Abs. 3 VwVG kann das Zwangsgeld bis zu 25.000 Euro betragen und kann gemäß § 13 Abs. 6 VwVG wiederholt werden, wenn das vorherige Zwangsgeld erfolglos war.

# 6
# Zusammenfassung und rechtspolitischer Ausblick

Zusammenfassend ist festzustellen, dass sich eine gewisse Zweigleisigkeit in der Aufsichtspraxis der Behörden unter der Datenschutz-Grundverordnung abzeichnet. Einerseits ist damit zu rechnen, dass der neue Bußgeldrahmen sowie die allgemeinere Erwartung, Vollzugsdefizite zu beheben, zumindest mittelfristig zu einer schärferen Sanktionierung von Datenschutzverstößen führen wird. Denn die neuen Regelungen ermöglichen eine effektive Sanktionierung von Rechtsverstößen und damit genau den Grad an Rechtsdurchsetzung, dessen Fehlen unter der Datenschutzrichtlinie stets beklagt wurde. Durch die Erhöhung des Bußgeldrahmens ist es nun möglich, bei gravierenden oder wiederholten Verstößen deutlich höhere Geldbußen zu verhängen.

Andererseits sind die Aufsichtsbehörden insgesamt mit der Durchsetzung des Datenschutzrechts beauftragt und damit nicht auf die Rolle als Bußgeldstelle reduziert. Die Geldbußen stellen nur ein Mittel zum Zweck dar. Bei Unternehmen und anderen Organisationen, die sich ernsthaft bemühen, Datenschutz umzusetzen, werden die Aufsichtsbehörden voraussichtlich bei offenen Fragen weiterhin zunächst auf Hilfestellung setzen. Wie geschildert, ist der Spagat zwischen Berater und Aufseher, den die Aufsichtsbehörden dabei zum Teil auszuführen versuchen, nicht einfach, und wird viel Kommunikationsgeschick erfordern.

Ein dynamisches Element in dem sich unter der Datenschutz-Grundverordnung entwickelnden Aufsichtsregime sind die Eingaben und Beschwerden aus der Bevölkerung. Der massive Anstieg von Beschwerden könnte ein Zeichen für ein geschärftes Datenschutzbewusstsein in der Bevölkerung sein. Scheinbar machen zumindest jene Menschen, die das Ausmaß der alltäglichen Verarbeitung ihrer personenbezogener Daten als störend empfinden, zunehmend Gebrauch vom Beschwerdeweg, anstatt die fraglichen Datenverarbeitungen einfach hinzunehmen.

Für die Aufsichtsbehörden bedeutet die steigende Anzahl an Beschwerden einerseits massive Mehrarbeit und eine (ressourcenbedingte) Beschränkung ihrer Möglichkeiten, eigene Prioritäten in der Aufsicht zu setzen. Andererseits zeigen die Beschwerden, dass die Regelungen der Datenschutz-Grundverordnung auf erhebliche Resonanz stoßen und es einen großen Bedarf für Datenschutzaufsicht gibt. Zudem bieten die Beschwerden den Aufsichtsbehörden die Möglichkeit, Informationen zu Verstößen zu erlangen, die ihnen sonst womöglich entgangen wären. Auch nutzen zunehmend Unternehmen die Beschwerdemöglichkeiten, um Aufsichtsbehörden auf für Außenstehende nur schwer einsehbare Verstöße hinzuweisen. Dabei wird es wichtig sein, dass die Aufsichtsbehörden standardisierte und rechtssichere Abläufe entwickeln, um häufig auftretende Beschwerden oder Bagatellfälle möglichst ressourcenschonend zu bearbeiten.

Die begrenzten Ressourcen der Aufsichtsbehörden erschweren auch die effektive Rechtsdurchsetzung. Soweit es keine signifikanten Mittelerhöhungen geben sollte, ist es für viele Aufsichtsbehörden eine kaum zu bewältigende Herausforderung, für einen effektiven Datenschutz zu sorgen. Dazu gehört auch die Notwendigkeit, komplexe Fälle in oft langwierigen Prozessen gerichtlich klären zu lassen. Aufgrund dieser Beschränkungen und der durch die Datenschutz-Grundverordnung ohnehin erweiterten Abstimmungserfordernisse zwischen den Behörden können mangelnde Ressourcen jedoch teilweise durch vertiefte Zusammenarbeit und Abstimmung ausgeglichen werden. Dabei ist zum Beispiel denkbar, dass sich Aufsichtsbehörden bezüglich der Verfolgung systematischer Verletzungen in bestimmtem Maße spezialisieren. Dies geschieht heute schon im Rahmen von Arbeitsgruppen oder Taskforces und kann zukünftig noch erweitert werden. Nichtsdestotrotz ist es unabdingbar, dass den Datenschutzaufsichtsbehörden ausreichend Ressourcen (finanzielle Mittel und Personal) zur Verfügung gestellt

werden, damit diese effektiv ihre von der Datenschutz-Grundverordnung übertragenen Aufgaben und Befugnisse wahrnehmen können.[136]

Wichtig für eine effektive Rechtsdurchsetzung erscheint aber auch der Grad, zu dem betroffene Personen von ihrem Beschwerde- und Klagerecht nach der Datenschutz-Grundverordnung Gebrauch machen. Interviews mit Vertretern dieser Gruppen lassen in der Tat Interesse erkennen, die neuen Rechte zu nutzen. Verbraucherinteressen und -rechte, und damit auch Datenschutzrechte, sind Felder, mit denen sich die Verbraucherverbände aktiv beschäftigen, so dass es durchaus auch zu Klagen durch diese kommen könnte. Jedoch ist Datenschutz nur ein (eher untergeordneter) Teilbereich der Digitalthemen, mit denen sich die Verbraucherverbände beschäftigen. Eine dezidierte „Datenschutz-Rechtsdurchsetzungs-NGO" wie die österreichische Datenschutzorganisation „NOYB (none of your business) – europäisches Zentrum für digitale Rechte" um Max Schrems hat sich in Deutschland noch nicht formiert.

Es ist zu hoffen, dass jedes sanktionierte Unternehmen zumindest nach einem signifikant hohen Bußgeldbescheid sein zukünftiges Verhalten datenschutzkonform gestalten wird, allein um damit weiteren Kosten in Form von Geldbußen zu entgehen. Zudem können hohe Bußgelder eine erhöhte mediale Aufmerksamkeit erzielen, was gegebenenfalls zu einem in doppelter Weise negativen Ergebnis für das sanktionierte Unternehmen führt und abschreckende Wirkung auf die ganze Branche haben kann.

Diese Ausarbeitung kann nur ein grobes und vorläufiges Bild vom Sanktionsregime im Datenschutz zeigen – es handelt sich zunächst um eine erste Momentaufnahme in dem frühen Stadium nach Wirksamwerden der Datenschutz-Grundverordnung. Die nächsten Monate und Jahre werden zeigen, ob die Erwartungen an die Datenschutz-Grundverordnung und an die Akteure, die für Kontrollen und Sanktionen sorgen können, in Erfüllung gehen. Dabei werden neben den Datenschutzaufsichtsbehörden auch Verbraucherschützer, Kartellämter und die Zivilgesellschaft eine wichtige Rollen spielen können.

# Nachweise und Literaturverzeichnis

1 Hinweis: Aus Gründen der leichteren Lesbarkeit wird die männliche Sprachform bei personenbezogenen Substantiven und Pronomen verwendet. Dies impliziert jedoch keine Benachteiligung anderer Geschlechter, sondern soll im Sinne der sprachlichen Vereinfachung als geschlechtsneutral zu verstehen sein.

2 S. etwa LfDI Rheinland-Pfalz (29.12.2014).

3 Gemäß Art. 83 DSGVO hat die betroffene Aufsichtsbehörde sicherzustellen, „dass die Verhängung von Bußgeldern in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist". Damit setzt der Unionsgesetzgeber auf eine negative General- und Spezialprävention, s. hierzu Nemitz, in: Ehmann/Selmayr 2018, Art. 83 DSGVO, Rn. 1.

4 Golla, CR 2018, 353.

5 Anger und Neuerer 2019. Zu diesem Fall ausführlich Braun, ZD-aktuell 2019, 06445.

6 FAZ 2018.

7 CMS 2019.

8 Popitz 1980, S. 28

9 Z. B. Bamberger und Mulligan 2015.

10 Becker 1976.

11 Parker und Lehmann Nielsen 2011.

12 Becker 1968; Becker 1976.

13 Stigler 1970.

14 Siehe auch Scholz 1997; Faure et al. 2009.

15 Faure et al. 2009.

16 Kagan et al. 2011; Gunningham et al. 2005.

17 Burby und Paterson 1993.

18 Ko et al. 2010; Lewis-Beck und Alford 1980.

19 Gilad 2011.

20 Thornton et al. 2005; Kagan et al. 2011; Edelman und Talesh 2011.

21 Gunningham et al. 2005.

22 Gunningham et al. 2004, S. 308.

23 Gunningham et al. (2004, 2005).

24 Kagan et al. 2011.

25 Becker 1976.

26 Gunningham et al. 2004.

27 Vgl. auch Kagan et al. 2011.

28 May und Winter 1999.

29 Vgl. auch Winter und May 2001; May 2005.

30 Braithwaite und Makkai 1991; Makkai und Braithwaite 1994.

31 Simpson und Piquero 2002; Craig Smith et al. 2007; Simpson und Rorie 2011.

32 Interview mit Rechtsanwalt.

33 March et al. 1994; Cyert und March 2006.

34 Bamberger 2006, S. 409-425; Parker 2002, S. 33-35.

35 Gioia 1992; Parker 2002, S. 34.

36 Bamberger 2006; Parker und Gilad 2011; Parker 2002.

37 Parker und Gilad 2011.

38 Zur Konkurrenz beider Stellen hinsichtlich der innerbetrieblichen Durchsetzung des Datenschutzes s. Jaksch/Alt, in: Roßnagel/Hornung, Datenschutz im Smart Car, 2019, i.E.

39 Parker und Gilad 2011; Parker und Nielsen 2008.

40 Bamberger und Mulligan (2008, 2011, 2015).

41 Waldman 2018.

42 Kagan et al. 2011, 41.

43 Kagan et al. 2011, S. 46-47.

44 Niklas/Faas, NZA 2017, 1096.

45 Jaksch/Alt, in: Roßnagel/Hornung, Datenschutz im Smart Car, 2019, i.E.

46 Drewes, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 39 DSGVO, Rn. 41.

47 Lantwin, ZD 2017, 412.

48 S. ausführlich zur deliktischen Haftung des Datenschutzbeauftragten Drewes, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 39 DSGVO, Rn. 48.

49 Drewes, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 39 DSGVO, Rn. 57.

50 Hullen, in: Plath 2016, Art. 58 DSGVO, Rn. 12.

51 Braun/Hohmann, in: Roßnagel 2018, § 6 Rn. 129 ff.

52 Zum kartellrechtlichen Unternehmensbegriff s. Braun/Hohmann, in: Roßnagel 2018, § 6 Rn. 133.

53 Roßnagel, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 5 DSGVO, Rn. 189.

54 Roßnagel 2017, 132.

55 In den Landesdatenschutzgesetzen finden sich vergleichbare Regelungen.

56 Braun/Hohmann, in: Roßnagel 2018, § 6 Rn. 146.

57 Nemitz, in: Ehmann/Selmayr 2018, Art. 83 DSGVO, Rn. 8.

58 S. dazu auch die Leitlinien der Art.-29-Datenschutzgruppe (2017).

59 Braun/Hohmann, in: Roßnagel 2018, § 6 Rn. 141 ff.

60 Braun/Hohmann, in: Roßnagel 2018, § 6 Rn. 143 ff.

61 Insgesamt wurden vierzehn Interviews geführt, davon sechs mit Landesdatenschutzbeauftragten bzw. in einem Fall mit der zuständigen Mitarbeiterin, vier mit zivilgesellschaftlichen Organisationen, und vier mit betrieblichen Datenschutzbeauftragten beziehungsweise im betrieblichen Datenschutz tätigen Mitarbeitern. Zusätzlich wurden öffentliche Veranstaltungen besucht, auf denen Landesdatenschutzbeauftragte über ihre Aufsichtspraxis sprachen, und die einschlägige Berichterstattung

in Medien und Fachzeitschriften sowie die Tätigkeitsberichte der Landesdatenschutzbehörden seit 2010 konsultiert. Allen Interviewpartnern wurde Anonymität zugesichert.

62 Die Gesamtzahl der Bußgeldverfahren lag dabei stets höher, da nicht jedes Verfahren auch zum Erlass eines Bußgeldbescheids (d. h. eines zu zahlenden Bußgeldes) führt.

63 So verweist das Bayerische Landesamt für Datenschutzaufsicht in seinem Tätigkeitsbericht 2013/2014 darauf, dass gleiche Sachverhalte unter Umständen mit deutlich unterschiedlichen Bußgeldern geahndet werden können, da bei der Bemessung auch die wirtschaftlichen Verhältnisse des Adressaten eine Rolle spielen, und der Bußgeldrahmen für vorsätzliche Ordnungswidrigkeiten doppelt so hoch ist wie für lediglich fahrlässig begangene Ordnungswidrigkeiten (Bayerisches LDA 2015, S. 15-16).

64 Bayerisches LDA 2015, S. 15; Bayerisches LDA 2013, S. 12.

65 HamBfDI 2014, S. 259; HamBfDI 2016, S. 259.

66 Bignami 2011; Bamberger and Mulligan 2015.

67 HamBfDI 2014, S. 190-191; HamBfDI 2012, S. 185-187.

68 Statista 2019.

69 So der Hamburgische Landes-Datenschutzbeauftragte Johannes Caspar in seinem Vortrag auf dem CAST-Forum am 15. März 2018 in Darmstadt.

70 LfDI Rheinland-Pfalz (29.12.2014).

71 Bamberger und Mulligan 2013.

72 Rosenbach 2018.

73 Nemitz 2018, S. 313.

74 dts (14.03.2018); dts (22.05.2018); Rundblick 2018.

75 Stenzel 2018.

76 Die Welt (02.08.2018); Gassmann und Fuest 2018.

77 LfDI Rheinland-Pfalz 2014, S. 98.

78 dts (22.05.2018).

79 Anger und Neuerer 2019; Fahrun 2019.

80 Dies ergibt sich aus den verfügbaren Eckdaten zur Zahl und Gesamthöhe verhängter Bußgelder. Vgl. Anger/Neuerer 2019; Heidrich 2019.

81 Interview mit der Datenschutzbehörde

82 Interview mit der Datenschutzbehörde

83 So erklärte der Hamburgische Landes-Datenschutzbeauftragte, Johannes Caspar, dass „[d]ie schwache Behörde gezwungen [ist], fehlende sachliche und personelle Mittel durch entsprechend hohe Bußgelder zu kompensieren." Vortrag auf dem CAST-Forum am 15. März 2018 in Darmstadt.

84 Interview mit der Datenschutzbehörde. Der Faktor 67 ergibt sich aus der Steigerung des Bußgeldrahmens um das 67-fache von 300.000 auf 20 Mio. Euro.

85 Interview mit der Datenschutzbehörde

86 Interview mit der Datenschutzbehörde

87 Interview mit der Datenschutzbehörde.

88 Interview mit der Datenschutzbehörde. Zur engen Ausstattung der Behörden mit Personal- und Finanzmitteln siehe auch Schütz 2018.

89 Vgl. Roßnagel 2017.

90 Roßnagel 2017, 42-43.

91 Geminn, in Jandt/Steidle, VII Rn. 103 ff.

92 Gierschmann, ZD 2016, 53.

93 Fahrun 2019.

94 Peteranderl 2019.

95 Europäische Kommission 2019.

96 Interviews mit der Datenschutzbehörden.

97 Interview mit der Datenschutzbehörde; Bemerkungen von Thomas Kranig, Präsident des Bayerischen Landesamtes für Datenschutzaufsicht, am 30.01.2018, Europäische Akademie in Berlin.

98 Interviews mit den Datenschutzbehörden.

99 Interviews mit den Datenschutzbehörden.

100 Interviews mit der Datenschutzbehörden. Laut dem European Data Protection Board sind unerwünschte Werbung (einschließlich Telemarketing) und Videoüberwachung auch europaweit die häufigsten Beschwerde-Ursachen (Europäische Kommission 2019).

101 Interview mit der Datenschutzbehörde.

102 Interviews mit den Datenschutzbehörden.

103 Interviews mit den Datenschutzbehörden.

104 Interview mit der Datenschutzbehörde.

105 Kelemen 2011, S. 143-194.

106 Interviews mit der Datenschutzbehörden.

107 Leitlinien, Handlungsempfehlungen und Stellungnahmen können die Aufsichtsbehörden alleine oder in Zusammenarbeit mit der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder sowie dem Europäischen Datenschutzausschuss erstellen.

108 Zu den Auslegungshilfen, Orientierungshilfen und Anwendungshinweisen etwa der Datenschutzkonferenz s. https://www.datenschutzkonferenz-online.de/orientierungshilfen.html.

109 Interview mit der Datenschutzbehörde.

110 Vgl. Stigler 1971.

111 Interview mit betrieblicher Datenschutzbeauftragten.

112 Thüringer Allgemeine 2018; IHK Südthüringen 2019.

113 Ob ein Auftragsverarbeitungs-Verhältnis wirklich vorlag, bleibt zwischen den Parteien umstritten.

114 Ob der Grund hierfür in Unvermögen, Unverständnis, Machtgefälle zwischen dem Versandhaus und dem spanischen Dienstleister oder aus Kostengründen liegt, ist ebenfalls unklar.

115 Die Gründe hierfür (schlechte Rechtsberatung, Verweigerungshaltung, oder schlichte Fehlkommunikation) sind ebenfalls unklar.

116 Heidrich 2019. Für die Darstellung des Falls aus Sicht des Unternehmens siehe https://kolibri-image.com/causa-datenschutz, zuletzt geprüft am 05.02.2019

117 https://www.datenschutzbeauftragter-info.de/bei-aufsichtsbehoerde-angefragt-bussgeld-kassiert/. Zuletzt geprüft am 05.02.2019

118 Zur grundsätzlichen Herausforderung, Beratung und strafende Aufsicht unter einen behördlichen Hut zu bringen siehe auch Wolff 2017, S. 110.

119 Zu den Vollzugsdefiziten im Bereich der Telemedien s. etwa Kühling/Sivridis/Schwuchow/Burghard, DuD 2009, 335 ff.

120 Interview mit dem Unternehmen (E).

121 Interview mit dem Unternehmen (A).

122 Interview mit dem Unternehmen (B).

123 Interview mit dem Unternehmen (G).

124 BDJ 2018.

125 Erwägungsgründe 11 und 13 DSGVO.

126 Eser, in: Meyer 2014, Art. 48 GrCh, Rn. 10a.

127 Vgl. die standige Rechtsprechung zum Wettbewerbsrecht: EuG, Rs. T-112/98 Mannesmannröhren-Werke, Urteil vom 20.2.2001, ECLI:EU:T:2001:61, Rn. 66 f.; EuGH, Rs. 374/87 Orkem, Urteil vom 18.10.1989, ECLI:EU:C:1989:387, Rn. 34 f.

128 Vgl. Roßnagel 2017.

129 Roßnagel 2017, 1.

130 Boehm, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 83 DSGVO, Rn. 20.

131 Erwägungsgrund 148 Satz 2 DSGVO.

132 Boehm, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 84 DSGVO, Rn. 9.

133 Boehm, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 84 DSGVO, Rn. 12.

134 Frenzel, in: Paal/Pauly 2018, Art. 83 DSGVO, Rn. 26.

135 Troidl, in: Engelhardt/App/Schlatmann 2017, § 11 VwVG, Rn. 1.

136 Roßnagel 2017, 1.

# Literaturverzeichnis

Anger, Heike; Neuerer, Dietmar (2019): Behörden verhängen erste Bußgelder wegen Verstößen gegen DSGVO. In: *Handelsblatt*, 18.01.2019. Online verfügbar unter https://www.handelsblatt.com/politik/deutschland/datenschutzgrundverordnung-behoerden-verhaengen-erste-bussgelder-wegen-verstoessen-gegen-dsgvo/23872806.html?ticket=ST-2213537-uaP4TgvVDzFlg9TLfpRP-ap2, zuletzt geprüft am 24.01.2019.

Art.-29-Datenschutzgruppe (2017): Leitlinien für die Anwendung und Festsetzung von Geldbußen im Sinne der Verordnung (EU) 2016/679. Working Paper 253, angenommen am 03.10.2017

Bamberger, Kenneth A. (2006): Regulation as Delegation. Private Firms, Decisionmaking, and Accountability in the Administrative State. In: *Duke Law Journal* 56 (2), S. 377–468.

Bamberger, Kenneth A.; Mulligan, Deidre K. (2008): Privacy Decisionmaking in Administrative Agencies. In: *University of Chicago Law Review* 75 (1), S. 75–108.

Bamberger, Kenneth A. and Mulligan, Deirdre K. (2011): New Governance, Chief Privacy Officers, and the Corporate Management of Information Privacy in the United States. An Initial Inquiry. In: *Law & Policy* 33 (4), S. 477–508. DOI: 10.1111/j.1467-9930.2011.00351.x.

Bamberger, Kenneth A. and Mulligan, Deirdre K. (2013): Privacy in Europe: Initial Data on Governance Choices and Corporate Practices. In: *George Washington Law Review* 81 (5), S. 1529–1664.

Bamberger, Kenneth A. and Mulligan, Deirdre K. (2015): Privacy on the ground. Driving corporate behavior in the United States and Europe. Cambridge, Massachusetts: The MIT Press (Information policy series).

Bayerisches Landesamt für Datenschutzaufsicht (2013): 5.Tätigkeitsbericht des Bayerischen Landesamtes für Datenschutzaufsicht für die Jahre 2011 und 2012. Hg. v. Bayerisches Landesamt für Datenschutzaufsicht. Ansbach. Online verfügbar unter https://www.lda.bayern.de/media/baylda_report_05.pdf, zuletzt geprüft am 20.01.2019.

Bayerisches Landesamt für Datenschutzaufsicht (2015): 6. Tätigkeitsbericht des Bayerischen Landesamtes für Datenschutzaufsicht für die Jahre 2013 und 2014. Hg. v. Bayerisches Landesamt für Datenschutzaufsicht. Ansbach. Online verfügbar unter https://www.lda.bayern.de/media/baylda_report_06.pdf, zuletzt geprüft am 20.01.2019.

BDJ (2018). Newsletter No. 1. Hg. v. BDJ Versicherungsmakler GmbH & Co. KG. Online abrufbar unter https://www.bdj.de/fileadmin/files/newsletter/BDJ_No1_Ausgabe28.pdf, zuletzt geprüft am 20.02.2019.

Becker, Gary S. (1968): Crime and Punishment. An Economic Approach. In: *Journal of Political Economy* 76 (2), S. 169–217. DOI: 10.1086/259394.

Becker, Gary S. (1976): The economic approach to human behavior. Chicago: University of Chicago Press.

Bignami, Francesca (2011): Cooperative Legalism and the Non-Americanization of European Regulatory Styles: The Case of Data Privacy. In: *American Journal of Comparative Law* 59 (2), S. 411–461.

Braithwaite, John; Makkai, Toni (1991): Testing an Expected Utility Model of Corporate Deterrence. In: *Law & Society Review* 25 (1), S. 7. DOI: 10.2307/3053888.

Braun, Steffen (2019): Kooperation oder Konfrontation? Erste Bußgelder nach DS-GVO. In: *Newsdienst ZD-aktuell*. Nr. 06445.

Braun, Steffen; Hohmann, Carolin (2018): Sanktionen, in: Roßnagel, Alexander (Hg.), Das neue Datenschutzrecht. Europäische Datenschutz-Grundverordnung und deutsche Datenschutzgesetze. Baden-Baden: Nomos, § 6 Rn. 126 – 161.

Bundesamt für Justiz (2019). Hg. v. Bundesamt für Justiz. Bundesamt für Justiz. Bonn. Online verfügbar unter https://www.bundesjustizamt.de/DE/SharedDocs/Publikationen/Verbraucherschutz/Liste_qualifizierter_Einrichtungen.pdf?__blob=publicationFile&v=32, zuletzt geprüft am 05.04.2019.

Burby, Raymond J.; Paterson, Robert G. (1993): Improving Compliance with State Environmental Regulations. In: *Journal of Policy Analysis and Management* 12 (4), S. 753. DOI: 10.2307/3325349.

CMS (2019): CNIL verhängt EUR 50 Mio. DSGVO-Bußgeld gegen Google LLC. In: CMS Blog, 23.01.2019. Online verfügbar unter: https://www.cmshs-bloggt.de/tmc/datenschutzrecht/dsgvo-bussgeld-google-cnil-eur-50-mio/, zuletzt geprüft am 20.02.2019.

Craig Smith, N.; Simpson, Sally S.; Huang, Chun-Yao (2007): Why Managers Fail to do the Right Thing. An Empirical Study of Unethical and Illegal Conduct. In: *Bus. Ethics Q.* 17 (04), S. 633–667. DOI: 10.1017/S1052150X00002633.

Cyert, Richard Michael; March, James G. (2006): A behavioral theory of the firm. 2. ed., [Nachdr.]. Malden, Mass.: Blackwell.

Die Welt (02.08.2018): Kita schwärzt Gesichter in Fotoalben. Online verfügbar unter https://www.welt.de/vermischtes/article180429010/Datenschutz-Kita-schwaerzt-Gesichter-in-Fotoalben.html, zuletzt geprüft am 23.01.2019.

dts (14.03.2018): EU-Datenschutz-Grundverordnung: Rufe nach Sanktionsverzicht. Online verfügbar unter https://www.hasepost.de/eu-datenschutz-grundverordnung-rufe-nach-sanktionsverzicht-74867/, zuletzt geprüft am 23.01.2018.

dts (22.05.2018): Datenschützer widersprechen EU-Kommission: Keine Nachsicht.

Edelman, Lauren B.; Talesh, Shauhin A. (2011): To Comply or Not to Comply – That Isn't the Question. How Organizations Construct the Meaning of Compliance. In: Christine Parker, Vibeke Lehmann Nielsen und Neil Gunningham (Hg.): Explaining Compliance // Strategizing Compliance and Enforcement. Business Responses to Regulation // Responsive Regulation and Beyond. Cheltenham: Edward Elgar Publishing.

Ehmann, Eugen; Selmayr, Martin (2018): DS-GVO, Kommentar. Hg. v. Ehmann, Eugen; Selmayr, Martin. 2. Auflage. München: C.H.Beck. Zitiert als Autor, in: Ehmann/Selmayr 2018.

Engelhardt, Hanns; App; Schlatmann, Arne (2017): Verwaltungsvollstreckungsgesetz, Verwaltungszustellungsgesetz, Kommentar. Hg. v. Schlatmann, Arne. 11. Auflage. München: C.H.Beck.

Europäische Kommission (2019): GDPR in Numbers. Hg. v. European Commission. European Commission. Brüssel. Online verfügbar unter https://ec.europa.eu/commission/sites/beta-political/files/190125_gdpr_infographics_v4.pdf, zuletzt geprüft am 05.02.2019.

Fahrun, Joachim (2019): Berliner fordern mehr Datenschutz. In: *Berliner Morgenpost*, 22.01.2019. Online verfügbar unter unter https://www.morgenpost.de/berlin/article216261597/In-Berlin-gibt-es-mehr-Beschwerden-zum-Datenschutz.html, zuletzt geprüft am 05.02.2019.

Faure, Michael; Ogus, Anthony; Philipsen, Niels (2009): Curbing Consumer Financial Losses. The Economics of Regulatory Enforcement. In: *Law & Policy* 31 (2), S. 161–191. DOI: 10.1111/j.1467-9930.2009.00299.x.

FAZ (2018): 400.000 Euro Strafe für DSGVO-Verstoß. In: *Frankfurter Allgemeine Zeitung*, 23.10.2018. Online verfügbar unter https://www.faz.net/aktuell/wirtschaft/diginomics/dsgvo-strafe-krankenhaus-in-portugal-muss-400-000-euro-zahlen-15852321.html, zuletzt geprüft am 20.02.2019.

Gassmann, Michael; Fuest, Benedikt (2018): Datenschutzregeln versetzen Mittelständler in Panik. In: *Die Welt*, 12.05.2018. Online verfügbar unter https://www.welt.de/wirtschaft/article176287537/DSGVO-Datenschutzregeln-versetzen-Mittelstaendler-in-Panik.html, zuletzt geprüft am 23.01.2018.

Gierschmann, Sybille (2016): Was „bringt" deutschen Unternehmen die DS-GVO? Mehr Pflichten, aber die Rechtsunsicherheit bleibt. In: Zeitschrift für Datenschutz (ZD), Heft 2, 51-55.

Gilad, Sharon (2011): Institutionalizing fairness in financial markets. Mission impossible? In: *Regulation & Governance* 5 (3), S. 309–332. DOI: 10.1111/j.1748-5991.2011.01116.x.

Gioia, Dennis A. (1992): Pinto fires and personal ethics. A script analysis of missed opportunities. In: *J Bus Ethics* 11 (5-6), S. 379–389. DOI: 10.1007/BF00870550.

Golla, Sebastian J. (2018): Das Opportunitätsprinzip für die Verhängung von Bußgeldern nach der DSGVO. Oder: How I Learned to Stop Worrying about Fines and Love the GDPR. In: Computer und Recht (CR), Heft 6, 353-357.

Gunningham, Neil; Kagan, Robert A.; Thornton, Dorothy (2004): Social License and Environmental Protection. Why Businesses Go Beyond Compliance. In: *Law & Social Inquiry* 29 (2), S. 307–341. DOI: 10.1111/j.1747-4469.2004.tb00338.x.

Gunningham, Neil; Thornton, Dorothy; Kagan, Robert A. (2005): Motivating Management. Corporate Compliance in Environmental Protection*. In: *Law & Policy* 27 (2), S. 289–316. DOI: 10.1111/j.1467-9930.2005.00201.x.

Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (2012): 23. Tätigkeitsbericht Datenschutz des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit zugleich Tätigkeitsbericht der Aufsichtsbehörde für den nicht-öffentlichen Bereich 2010 / 2011. Hg. v. Hamburgische Beauftragte für Datenschutz und Informationsfreiheit. Hamburg. Online verfügbar unter https://datenschutz-hamburg.de/assets/pdf/23._Taetigkeitsbericht_Datenschutz_2010-2011.pdf, zuletzt geprüft am 20.01.2019.

Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (2014): 24. Tätigkeitsbericht Datenschutz des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit 2012 / 2013. Hg. v. Hamburgische Beauftragte für Datenschutz und Informationsfreiheit. Hamburg. Online verfügbar unter https://datenschutz-hamburg.de/assets/pdf/24._Taetigkeitsbericht_Datenschutz_2012-2013.pdf, zuletzt geprüft am 20.01.2019.

Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (2016): 25. Tätigkeitsbericht Datenschutz des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit 2014 / 2015. Hg. v. Hamburgische Beauftragte für Datenschutz und Informationsfreiheit. Hamburg. Online verfügbar unter https://datenschutz-hamburg.de/assets/pdf/25._Taetigkeitsbericht_Datenschutz_2014-2015_HmbBfDI_01.pdf, zuletzt geprüft am 04.02.2019.

Heidrich, Joerg (2019): DSGVO: 5000 Euro Bußgeld für fehlenden Auftragsverarbeitungsvertrag. In: *heise online*, 20.01.2019. Online verfügbar unter https://www.heise.de/-4282737, zuletzt geprüft am 01.02.2019.

IHK Südthüringen (18.01.2019): Reden ist Silber, Schweigen ist Gold. Suhl. Online verfügbar unter https://www.ihk-suhl.de/www/ihkst/data/artikel-detail.html?recordid=1686020164F, zuletzt geprüft am 05.02.2019.

Jaksch, Christoph; Alt Christian (2019) Rolle des Datenschutzbeauftragten und der Datenschutzorganisation bei der Implementierung des vernetzten Fahrzeuges, in: Roßnagel, Alexander; Hornung, Gerrit (Hg.): Grundrechtsschutz im Smart Car, Wiesbaden: Springer Vieweg (Research), i.E.

Jandt, Silke; Steidle, Roland (2018): Datenschutz im Internet. Hg. v. Jandt, Silke; Steidle, Roland. Baden-Baden: Nomos.

Kagan, Robert A.; Gunningham, Neil; Thornton, Dorothy (2011): Fear, Duty, and Regulatory Compliance. Lessons from Three Research Projects. In: Christine Parker, Vibeke Lehmann Nielsen und Neil Gunningham (Hg.): Explaining Compliance // Strategizing Compliance and Enforcement. Business Responses to Regulation // Responsive Regulation and Beyond. Cheltenham: Edward Elgar Publishing.

Kelemen, R. Daniel (2011): Eurolegalism. The transformation of law and regulation in the European Union. Cambridge, Mass: Harvard University Press.

Ko, Kilkon; Mendeloff, John; Gray, Wayne (2010): The role of inspection sequence in compliance with the US Occupational Safety and Health Administration's (OSHA) standards. Interpretations and implications. In: *Regulation & Governance* 4 (1), S. 48–70. DOI: 10.1111/j.1748-5991.2010.01070.x.

Krempl, Stefan (2018): DSGVO: Bundesdatenschutzbeauftragte meldet „beachtliche" Zahl an Beschwerden. In: *heise online*, 14.12.2018. Online verfügbar unter https://www.heise.de/-4250411, zuletzt geprüft am 22.01.2019.

Kühling, Jürgen; Sivridis, Anastasios; Schwuchow, Mathis; Burghard, Thorben (2009): Das datenschutzrechtliche Vollzugsdefizit im Bereich der Telemedien — ein Schreckensbericht. In: *Datenschutz und Datensicherheit* (DuD), Heft 6, 335-342.

Landesbeauftragte für den Datenschutz und die Informationsfreiheit in Rheinland-Pfalz (2014): Datenschutzbericht 2012/2013. Hg. v. Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit in Rheinland-Pfalz. Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit in Rheinland-Pfalz. Mainz. Online verfügbar unter https://www.datenschutz.rlp.de/fileadmin/lfdi/Taetigkeitsberichte/ds_tb24.pdf, zuletzt geprüft am 01.02.2019.

Landesbeauftragte für den Datenschutz und die Informationsfreiheit in Rheinland-Pfalz (29.12.2014): Bußgeldverfahren gegen die Debeka einvernehmlich abgeschlossen. Mainz. Online verfügbar unter https://www.datenschutz.rlp.de/de/aktuelles/detail/news/detail/News/bussgeldverfahren-gegen-die-debeka-einvernehmlich-abgeschlossen-debeka-akzeptiert-geldbusse-und-gar/, zuletzt geprüft am 20.01.2019.

Lantwin, Tobias (2017): Risikoberuf Datenschutzbeauftragter? Die Haftung nach der neuen DS-GVO. In: *Zeitschrift für Datenschutz* (ZD), Heft 9, 411-414.

Lewis-Beck, Michael S.; Alford, John R. (1980): Can Government Regulate Safety? The Coal Mine Example. In: *Am Polit Sci Rev* 74 (03), S. 745–756. DOI: 10.2307/1958155.

Makkai, Toni; Braithwaite, John (1994): The Dialectics of Corporate Deterrence. In: *Journal of Research in Crime and Delinquency* 31 (4), S. 347–373. DOI: 10.1177/0022427894031004001.

March, James G.; Simon, Herbert Alexander; Guetzkow, Harold (1994): Organizations. 2. ed., reprinted (twice). Cambridge, Mass.: Blackwell.

May, Peter J. (2005): Compliance Motivations. Perspectives of Farmers, Homebuilders, and Marine Facilities*. In: *Law & Policy* 27 (2), S. 317–347. DOI: 10.1111/j.1467-9930.2005.00202.x.

May, Peter J.; Winter, Søren C. (2011): Regulatory Enforcement Styles and Compliance. In: Christine Parker, Vibeke Lehmann Nielsen und Neil Gunningham (Hg.): Explaining Compliance // Strategizing Compliance and Enforcement. Business Responses to Regulation // Responsive Regulation and Beyond. Cheltenham: Edward Elgar Publishing.

May, Peter J.; Winter, Sren (1999): Regulatory enforcement and compliance. Examining Danish agro-environmental policy. In: *Journal of Policy Analysis and Management* 18 (4), S. 625–651. DOI: 10.1002/(SICI)1520-6688(199923)18:4<625::AID-PAM5>3.0.CO;2-U.

Meyer, Jürgen (2014): Charta der Grundrechte der Europäischen Union. Hg. v. Meyer, Jürgen. 4. Auflage. Baden-Baden: Nomos. Zitiert: Autor, in: Meyer 2014.

Nemitz, Paul F. (2018): Die Datenschutz-Grundverordnung als Vertrauensrahmen für Innovation in der Digitalen Gesellschaft. In: Alexander Roßnagel, Michael Friedewald und Marit Hansen (Hg.): Die Fortentwicklung des Datenschutzes. Zwischen Systemgestaltung und Selbstregulierung. Wiesbaden: Springer Vieweg (DuD-Fachbeiträge), S. 311–314.

Niklas, Thomas; Faas, Thomas (2017): Der Datenschutzbeauftragte nach der Datenschutz-Grundverordnung. In: *Neue Zeitschrift für Arbeitsrecht* (NZA), Heft 17, 1091-1097.

Paal, Boris P.; Pauly, Daniel A. (2018): Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, Kommentar. Hg. v. Paal, Boris P; Pauly, Daniel A. 2. Auflage. München: C.H.Beck. Zitiert als Autor, in: Paal/Pauly 2018.

Parker, Christine (2002): The Open Corporation. Cambridge and New York: Cambridge University Press. DOI: 10.1017/CBO9780511550034.

Parker, Christine; Gilad, Sharon (2011): Internal Corporate Compliance Management Systems. Structure, Culture and Agency. In: Christine Parker, Vibeke Lehmann Nielsen und Neil Gunningham (Hg.): Explaining Compliance // Strategizing Compliance and Enforcement. Business Responses to Regulation // Responsive Regulation and Beyond. Cheltenham: Edward Elgar Publishing.

Parker, Christine; Lehmann Nielsen, Vibeke (2011): Introduction. In: Christine Parker, Vibeke Lehmann Nielsen und Neil Gunningham (Hg.): Explaining Compliance // Strategizing Compliance and Enforcement. Business Responses to Regulation // Responsive Regulation and Beyond. Cheltenham: Edward Elgar Publishing.

Parker, Christine; Nielsen, Vibeke Lehmann (2008): Corporate Compliance Systems. In: *Administration & Society* 41 (1), S. 3–37. DOI: 10.1177/0095399708328869.

Peteranderl, Sonja (2019): „Fehler werden jetzt teuer". In: *Spiegel Online*, 24.01.2019. Online verfügbar unter http://www.spiegel.de/netzwelt/netzpolitik/dsgvo-strafen-fehler-werden-jetzt-teuer-a-1249443.html, zuletzt geprüft am 25.01.2019.

Plath, Kai-Uwe (2016): DSGVO/BDSG, Kommentar. Hg. v. Plath, Kai-Uwe. 2. Auflage. Köln: Verlag Dr. Otto Schmidt.

Popitz (1980): *Die normative Konstruktion von Gesellschaft*. Tübingen: Mohr Siebeck Gmbh & Co. KG.

Rosenbach, Marcel (2018): „Es wird kein Pardon geben". Neue Datenschutzregeln. In: *Spiegel Online*, 02.02.2018. Online verfügbar unter http://www.spiegel.de/netzwelt/netzpolitik/datenschutz-verordnung-deutsche-unternehmen-sind-schlecht-vorbereitet-a-1191075.html, zuletzt geprüft am 23.01.2019.

Roßnagel, Alexander (2017): Datenschutzaufsicht nach der EU-Datenschutz-Grundverordnung. Neue Aufgaben und Befugnisse der Aufsichtsbehörden. Wiesbaden: Springer Vieweg (Research).

Roßnagel, Alexander (2018): Das neue Datenschutzrecht. Europäische Datenschutz-Grundverordnung und deutsche Datenschutzgesetze. Hg. v. Roßnagel, Alexander. Baden-Baden: Nomos.

Roßnagel, Alexander; Hornung, Gerrit (2019): Grundrechtsschutz im Smart Car, Hg. v. Roßnagel, Alexander und Hornung, Gerrit. Wiesbaden: Springer Vieweg (Research).

Rundblick (2018): Schadet der Datenschutz dem Ehrenamt? SPD und CDU wollen den Vereinen helfen. In: *Rundblick. Politikjournal für Niedersachsen*, 13.09.2018. Online verfügbar unter https://www.rundblick-niedersachsen.de/schadet-der-datenschutz-

dem-ehrenamt-spd-und-cdu-wollen-den-vereinen-helfen/, zuletzt geprüft am 23.01.2019.

Scholz, John T. (1997): Enforcement Policy and Corporate Misconduct. The Changing Perspective of Deterrence Theory. In: *Law and Contemporary Problems* 60 (3), S. 253. DOI: 10.2307/1192014.

Schütz, Philip (2018): Zum Leben zu wenig, zum Sterben zu viel? Die finanzielle und personelle Ausstattung deutscher Datenschutzbehörden im Vergleich. In: Alexander Roßnagel, Michael Friedewald und Marit Hansen (Hg.): Die Fortentwicklung des Datenschutzes. Zwischen Systemgestaltung und Selbstregulierung. Wiesbaden: Springer Vieweg (DuD-Fachbeiträge), S. 251–268.

Simitis, Spiros; Hornung, Gerrit; Spiecker, gen. Döhmann, Indra (2019): Datenschutzrecht, DSGVO mit BDSG, Kommentar. Hg. v. Simitis, Spiros; Hornung, Gerrit; Spieker, gen. Döhmann, Indra. Baden-Baden: Nomos. Zitiert als Autor, in: Simitis/Hornung/Spiecker gen. Döhmann 2019.

Simpson, Sally S.; Piquero, Nicole Leeper (2002): Low Self-Control, Organizational Theory, and Corporate Crime. In: *Law & Society Review* 36 (3), S. 509. DOI: 10.2307/1512161.

Simpson, Sally S.; Rorie, Melissa (2011): Motivating Compliance. Economic and Material Motives for Compliance. In: Christine Parker, Vibeke Lehmann Nielsen und Neil Gunningham (Hg.): Explaining Compliance // Strategizing Compliance and Enforcement. Business Responses to Regulation // Responsive Regulation and Beyond. Cheltenham: Edward Elgar Publishing.

Statista (2019): Google's net income from 2001 to 2015 (in million U.S. dollars). Online verfügbar unter https://www.statista.com/statistics/266472/googles-net-income/, zuletzt geprüft am 20.01.2019.

Stenzel, Christian (2018): „Unsere Kinder müssen programmieren lernen wie lesen und schreiben". Die neue Digitalministerin Dorothee Bär im Bild-Interview. In: *Bild*, 05.03.2018. Online verfügbar unter https://www.bild.de/politik/inland/dorothee-baer/im-interview-55009410.bild.html, zuletzt geprüft am 23.01.2018.

Stigler, George J. (1970): The Optimum Enforcement of Laws. In: *Journal of Political Economy* 78 (3), S. 526–536. DOI: 10.1086/259646.

Stigler, George J. (1971): The Theory of Economic Regulation. In: *The Bell Journal of Economics and Management Science* 2 (1), S. 3. DOI: 10.2307/3003160.

Thornton, Dorothy; Gunningham, Neil A.; Kagan, Robert A. (2005): General Deterrence and Corporate Environmental Behavior*. In: *Law & Policy* 27 (2), S. 262–288. DOI: 10.1111/j.1467-9930.2005.00200.x.

Thüringer Allgemeine (2018): IHK warnt vor Umfrage zum Datenschutz: Große Verunsicherung bei Thüringer Unternehmen. In: *Thüringer Allgemeine*, 19.12.2018. Online verfügbar unter https://www.thueringer-allgemeine.de/web/zgt/wirtschaft/detail/-/specific/IHK-warnt-vor-Umfrage-zum-Datenschutz-Grosse-Verunsicherung-bei-Thueringer-Unte-1522889861, zuletzt geprüft am 05.04.2019.

Waldman, Ari Ezra (2018): Designing Without Privacy. In: *Houston Law Review* 55 (3).

Winter, Sren C.; May, Peter J. (2001): Motivation for Compliance with Environmental Regulations. In: *Journal of Policy Analysis and Management* 20 (4), S. 675–698. DOI: 10.1002/pam.1023.

Wolff, Heinrich A. (2017): „Die überforderte Aufsichtsbehörde". In: *PinG Privacy in Germany* 03, S. 109–111. Online verfügbar unter https://www.pingdigital.de/PinG.03.2017.109, zuletzt geprüft am 05.02.2019.

## IMPRESSUM

**Presse und Kommunikation:**
Barbara Ferrarese
Fraunhofer-Institut für System- und Innovationsforschung ISI
Breslauer Straße 48
76139 Karlsruhe

Telefon +49 721 6809-678
E-Mail presse@forum-privatheit.de

**Projektkoordination:**
Michael Friedewald
Fraunhofer-Institut für System- und Innovationsforschung ISI
Breslauer Straße 48
76139 Karlsruhe

Telefon +49 721 6809-146
Fax +49 721 6809-315
E-Mail info@forum-privatheit.de

www.isi.fraunhofer.de
www.forum-privatheit.de

**Schriftenreihe:**
Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt
ISSN-Print 2199-8906
ISSN-Internet 2199-8914

1. Auflage
März 2019

**Zitiervorschlag:**
Martin et al. (2018): Das Sanktionsregime der Datenschutz-Grundverordnung: Auswirkungen auf Unternehmen und Datenschutzaufsichtsbehörden. Hrsg.: Michael Friedewald et al., Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt, Karlsruhe: Fraunhofer ISI.

forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

PROJEKTPARTNER

Fraunhofer

Natur Technik Kultur Gesellschaft
UNIKASSEL VERSITÄT

provet
Projektgruppe verfassungsverträgliche Technikgestaltung

UNIVERSITÄT DUISBURG ESSEN
Offen im Denken

EBERHARD KARLS UNIVERSITÄT TÜBINGEN
INTERNATIONALES ZENTRUM FÜR ETHIK IN DEN WISSENSCHAFTEN

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein