3.1 Informationssicherheit und Recht

Informationssicherheit ist letztlich ein Mittel oder Erfordernis zum Schutz von Rechtsgütern, wie bspw. der informationellen Selbstbestimmung oder des Eigentums. Doch auch wenn Informationssicherheit kein eigenständiges Rechtsgut und keinen Selbstzweck darstellt, kann ihr trotzdem eine hohe Bedeutung zukommen. So kommt es nicht von ungefähr, dass die 2007 eingeführten § 100g StPO[4] und §§ 113a f TKG[5], besser bekannt als Rechtsgrundlagen der sogenannten TK-Vorratsdatenspeicherung, am 10.03.2010 durch das Bundesverfassungsgericht nicht wegen des Eingriffs in das Telekommunikationsgeheimnis, in das Recht auf informationelle Selbstbestimmung oder in die Rechte der Provider für nichtig erklärt wurden, sondern wegen der unzureichenden Regelungen zu Sicherheitspflichten bei der Aufbewahrung, Übermittlung und Nutzung dieser Daten.[6]

Informationssicherheit wird in § 2 Abs. 2 BSIG (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik) legaldefiniert als die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen in oder bei der Anwendung von informationstechnischen Systemen, Komponenten oder Prozessen. Dies entspricht dem Verständnis, das auch in Abschnitt 1.2 dargestellt ist.

Die Sicherheitsziele lassen sich direkt aus verschiedenen Grundrechten ableiten. Das Recht auf informationelle Selbstbestimmung, die Grundlage des deutschen Datenschutzrechts, erfordert bspw. den Schutz der Vertraulichkeit, aber auch den Schutz der Verfügbarkeit und der Integrität personenbezogener Daten. Der Schutz des Eigentums (Art. 14 GG[7]) etwa der Gesellschafter von Unternehmen erfordert einerseits den Schutz von Vertraulichkeit, bspw. bezüglich der Geschäftsgeheimnisse, andererseits den Schutz der Verfügbarkeit der gesamten – heute regelmäßig essenziellen – Informationsinfrastruktur. Der Gesetzgeber erlässt daher zunehmend Regelungen von Sicherheitsanforderungen, um seiner Pflicht zum Schutz dieser Grundrechte nachzukommen.

Mit seiner Entscheidung über die Regelungen zum staatlichen Trojaner-Einsatz im Verfassungsschutzgesetz von Nordrhein-Westfalen hat das Bundesverfassungsgericht zudem aus dem allgemeinen Persönlichkeitsrecht das Grundrecht auf »Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme« abgeleitet.[8] Dieses Grundrecht, auch als »Computer-Grundrecht« oder »IT-Grundrecht« bezeichnet, schützt die IT-Systeme eines Grundrechtsträgers gegen Zugriffe des Staats. Das Grundrecht stellt heimliche staatliche Zugriffe unter einen Richtervorbehalt und fordert enge gesetzliche Eingriffsvoraussetzungen.

Wesentliche Motivation des Bundesverfassungsgerichts für die Ableitung eines neuen Grundrechts, das mit der Vertraulichkeit und Integrität zwei der generischen Sicherheits-

4 Strafprozessordnung

5 Telekommunikationsgesetz

6 BVerfGE 125, 260

7 Grundgesetz

8 BVerfG, Urteil v. 27.02.2008, AZ: 1 BvR 370/07, abrufbar unter *http://www.hrr-strafrecht.de/hrr/bverfg/07/1-bvr-370-07.php; s. weiter [HOR 2008].*

ziele verfolgt, ist die steigende Bedeutung von IT-Systemen für die Persönlichkeitsentfaltung der Nutzer. Die Informationssicherheit hat durch das oben erwähnte Urteil rechtlich eine deutliche Aufwertung erfahren.

Grundrechte wirken jedoch nicht nur gegen staatliches Handeln, sondern sind auch bei der Auslegung der Gesetze des Privatrechts heranzuziehen. Hierin liegt die sogenannte »Drittwirkung der Grundrechte«. Sie können außerdem Schutzpflichten des Staats für das geschützte Rechtsgut begründen. Daher besteht die Hoffnung, dass durch zukünftige Gesetzgebung oder Rechtsprechung die Rechtsvorschriften zur Informationssicherheit bzw. deren Auslegung ergänzt und ausgestaltet werden. Das IT-Sicherheitsgesetz stellt hier einen ersten Schritt dar, der aber auch exemplarisch die praktischen Herausforderungen des Gesetzgebers vorführt. Diese bestehen unter anderem darin, Raum für fortschreitende technische Entwicklungen sowohl mit Blick auf Risiken als auch auf Maßnahmen zu lassen, andererseits aber ein möglichst konkretes Anforderungslevel zu regeln, um Rechtssicherheit zu schaffen. Um die notwendige Flexibilität der Anforderungen zu erhalten, werden sich auch künftig die gesetzlichen Regelungen auf sehr allgemeine Anforderungen beschränken, selbst in Gesetzen, die spezifisch auf die Informationssicherheit gerichtet sind. Die konkreteren Anforderungen werden weiterhin auf Verordnungen, technische Richtlinien, Standards und Verwaltungsvorschriften verschoben werden.

Die Darstellung in den folgenden Abschnitten stellt die rechtlichen Anforderungen an die Informationssicherheit aus verschiedenen Rechtsbereichen dar. Am Anfang jeden Rechtsgebiets wird auch der Kontext skizziert, in dem diese Sicherheitsanforderungen gelten.

Rechtsbereiche mit Sicherheitsanforderungen

Die rechtlichen Anforderungen an Informationssicherheit in Unternehmen werden im Folgenden nach einzelnen Rechtsbereichen oder Branchenregulierungen untergliedert. Hierfür werden jedoch zuerst Grundlagen des Risikomanagements erläutert, da sie für einen Teil der nachfolgend erläuterten Anforderungen eine maßgebliche Rolle zum Verständnis spielen.

3.1.1 Risikomanagement als rechtliche Anforderung

Die Forderung nach einem dokumentierten, nachvollziehbaren und Sicherheit förderndem Risikomanagement hat in einige gesetzliche Vorgaben, vor allem aber in vielen Standards, die die Erfüllung unternehmensbezogener Sorgfaltspflichten näher beschreiben, Einzug gehalten. Beispiele sind etwa § 25a Abs. 1 KWG oder der Katalog von Sicherheitsanforderungen der Bundesnetzagentur nach § 109 Abs. 6 TKG im Abschnitt 3.1.3 bzw. 3.3. Die Einführung eines Risikomanagements ist jedoch selbst ebenfalls Gegenstand von Standardisierungsvorschlägen.

Grundlagen des Risikomanagements

Nach ISO 31000:2018 wird Risiko definiert als »Auswirkung von Unsicherheit auf Zielsetzungen.« Die Norm selbst dient nicht zu Zertifizierungszwecken, sondern liefert vielmehr Empfehlungen, um die Unternehmensstrategie zu verwirklichen. Durch Entwicklung einer maßgeschneiderten Risikomanagementstrategie, der Identifikation von Risiken und deren Abschwächung soll zur Unternehmenszielerreichung führen und dem Schutz von Unter-

nehmenswerten dienen. Die Norm legt Grundsätze für den Umgang mit Risiken fest. Diese Grundsätze sollten als Grundlage festgelegt, d. h. als Basis für die Gestaltung der Unternehmensprozesse berücksichtigt werden. Der Umgang mit den Risiken basiert auf dem sogenannten Deming-Kreis[9] und umfasst die Risikomanagementkomponenten Integration → Gestaltung → Implementierung → Bewertung → Verbesserung. Risikomanagement ist demnach als dynamischer Prozess zu sehen, der kontinuierlich an die Unternehmensziele und Prozessabläufe angepasst werden muss. Neben der ISO-Norm 31000:2018 gibt es einen weiteren wichtigen Risikomanagementansatz, den COSO-Ansatz[10]. 2004 veröffentlichte COSO das Enterprise Risk Management (ERM) – Integrated Framework, wobei COSO die Auffassung vertritt, dass der ERM-Ansatz umfangreicher ist als ein internes Kontrollsystem (IKS). Ein IKS umfasst sämtliche in einem Unternehmen eingesetzte Methoden und Maßnahmen, die das Unternehmensvermögen und die Einhaltung der gesetzlichen Vorschriften und definierten Unternehmensrichtlinien, d. h. Legal und Compliance, sichern sollen. COSO definiert dagegen ERM als Prozess, der bei der Festlegung von Strategien im gesamten Unternehmen angewendet wird und eine entsprechende Sicherheit in Bezug auf die Unternehmenszielerreichung ermöglichen soll.

Einer der wesentlichsten Unterschiede liegt in der unterschiedlichen Betrachtungsweise von »Auswirkungen der Risiken auf die Unternehmenszielerreichung« (ISO 31000:2018) gegenüber den »risikorelevanten Ereignissen« (COSO ERM). Ob sich ein Unternehmen also auf das versuchte Vorherbestimmen von Ereignissen im Sinne einer Compliance-basierten Funktion oder auf die Fokussierung auf Ziele im Sinne von strategischen risikobasierten Entscheidungen konzentriert, sollte vor Beginn der Aufnahme des Risikomanagements sorgfältig abgewogen und entschieden werden.

Grundlagen zur Informationssicherheit aus dem Risikomanagement

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) definiert Informationssicherheit als Synonym von Datensicherheit, d. h. dem Schutz von Daten hinsichtlich der Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität. Da jede mögliche Bedrohung ein Risiko darstellt, kommt dem Risikomanagement auch im Rahmen der Informationssicherheit eine hohe Bedeutung zu. Damit ein Mindestmaß an Sicherheit gewährleistet ist, sollten Maßnahmen zur Risikominimierung definiert und regelmäßig überprüft werden. Dieser Vorgang kann auch durch eine externe Zertifizierung, z. B. anhand ISO 27001:2015[11] erfolgen. Es gibt jedoch eine Vielzahl unterschiedlicher Standards und Verfahren, anhand derer der Nachweis über das Vorhandensein entsprechender Sicherheitsniveaus erbracht werden kann, z. B. Common Criteria, Control Objectives for Information and related Technology (COBIT) oder IT Infrastructure Library (ITIL), die teilweise zertifizierbar sind.

9 Sogenannter PDCA-Zyklus; PDCA steht für die englischen Begriffe Plan, Do, Check, Act, d. h. der kontinuierlichen Prozessverbesserung und Qualitätssicherung.

10 COSO steht für »Committee of Sponsoring Organizations of the Treadway Commission«.

11 Information technology – Security techniques – Information security management systems – Requirements.

Anforderungen an die Informationssicherheit aus dem Risikomanagement

Damit Informationssicherheit überprüf- und darstellbar wird, muss sie messbar sein. Wie bereits erläutert, gibt es unterschiedliche Ansätze, Risikomanagement zu betreiben. Dies gilt auch für den Bereich der Informationssicherheit. Allen Ansätzen ist gemein, dass sie ein strukturiertes Vorgehen fordern, anhand dessen die individuellen Sicherheitsmaßnahmen für die IT-Landschaft eines Unternehmens abgeleitet werden. Durch eine entsprechende Analyse, z. B. basierend auf ISO 27001:2013, werden die zu schützenden Unternehmenswerte ermittelt. Diese Art der Risikoanalyse liefert wertvolle Informationen, kann jedoch mit einem hohen personellen und finanziellen Aufwand verbunden sein und erfordert detailliertes Know-how. Eine Alternative zu diesem Vorgehen bietet bspw. der IT-Grundschutz des BSI, der dazu beiträgt, den Aufwand für die Informationssicherheit zu reduzieren und durch die Bündelung und Wiederverwendung bekannter Vorgehensweisen zur Entwicklung der Informationssicherheit beizutragen. Die Messbarkeit wird hierbei durch die Abfrage der Umsetzung der Katalogmaßnahmen und die Angabe des Umsetzungsgrads erreicht.

3.1.2 Anforderungen aus dem Gesellschaftsrecht

Das Gesellschaftsrecht steht für die Gesamtheit der Vorschriften, die der Regulierung von privatrechtlichen Personenvereinigungen dienen, also etwa der Aktiengesellschaften, der Gesellschaften mit beschränkter Haftung, aber auch der Gesellschaften bürgerlichen Rechts, der offenen Handelsgesellschaften oder der eingetragenen Vereine. Das Gesellschaftsrecht enthält Anforderungen an die IT-Sicherheit vor allem durch seine Vorgaben an die Unternehmensleitung und die Organpflichten innerhalb der Unternehmen sowie durch die Einführung von Pflichten zum Risikomanagement. Mit Organpflichten sind hierbei die Pflichten weiterer vom Gesetz vorgesehener Unternehmensgremien gemeint, etwa Pflichten eines Aufsichtsrats. Teil dieser Vorgaben ist auch die Kontrolle der Einhaltung sowohl der ein Unternehmen treffenden Rechtsvorgaben als auch der internen Unternehmensregeln, die sogenannte Compliance. Informationssicherheit wird deshalb auch unter dem Aspekt der IT-Compliance behandelt (weiterführend [Fal 2011, S. 35] oder [NoBe 2008]). Rechtliche Konkretisierungen mit Blick auf die Unternehmens-IT finden sich insbesondere im Recht der Aktiengesellschaften, das zum Schutz der Aktionäre besondere Pflichten (insbesondere des Vorstands) vorsieht.

Grundlagen zur Informationssicherheit im Gesellschaftsrecht

Bezüglich der Rechtsgründe, Maßnahmen zur IT-Sicherheit zu treffen, ist zunächst zwischen den Gesellschaftsformen zu unterscheiden. Für die Kapitalgesellschaften (GmbH – Gesellschaft mit beschränkter Haftung, AG – Aktiengesellschaft) ergeben sich Pflichten aus den Aufgaben und Sorgfaltspflichten der Unternehmensleitung sowie aus der Verpflichtung zum Risikomanagement. Für Personengesellschaften (GbR – Gesellschaft bürgerlichen Rechts, KG – Kommanditgesellschaft, OHG – offene Handelsgesellschaft) entfallen diese Pflichten. Für sie bestehen Sorgfaltspflichten der Geschäftsführer oder der geschäftsführenden persönlich haftenden Gesellschafter sowohl gegenüber Dritten als auch gegenüber den Mitgesellschaftern.

Die Unternehmens-IT ist in den meisten Unternehmen eine lebenswichtige Infrastruktur, ohne die der Geschäftsablauf nicht mehr möglich ist. Für viele Unternehmen ist

zudem die Vertraulichkeit der gespeicherten Daten – personen- oder geschäftsbezogen – von essenzieller Bedeutung.

Die Gewährleistung von Informationssicherheit und die Organisation diesbezüglicher Aufgaben und Zuständigkeiten gehören daher zu den bestandssichernden Kernaufgaben der Unternehmensleitung. § 93 Abs. 1 AktG[12] legt als Pflicht für den Vorstand einer Aktiengesellschaft fest, dass dieser die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden hat. Diese Pflicht ergibt sich auch aus § 43 Abs. 1 GmbHG[13] und § 347 Abs. 1 HGB[14] entsprechend für Geschäftsführer am Handelsverkehr teilnehmender juristischer Personen.

Zu dieser Sorgfalt gehört zunächst eine sorgfältige Personalauswahl bezüglich der Verantwortlichen für die Umsetzung von Informationssicherheit und gegebenenfalls des IT-Sicherheitsbeauftragten. Dann ist eine Organisationsstruktur zur Gewährleistung von Informationssicherheit zu schaffen und die informationssicherheitsbezogenen Aufgaben sind festzulegen. Der Unternehmensleitung bleibt die fortdauernde Pflicht, die Umsetzung und die Wirksamkeit der vorhandenen Organisation und Maßnahmen zu überwachen und zu kontrollieren. Hierzu gehören sowohl die regelmäßige Vorlage von Berichten als auch Kontrollen, etwa durch Audits. Angesichts der Entwicklungsgeschwindigkeit des IT-Bereichs und der kontinuierlichen Veränderung der Risiken kommt der regelmäßigen Wirksamkeitsüberprüfung und Anpassung von Maßnahmen eine hohe Bedeutung zu.

Um Haftungsrisiken zu vermeiden, sollte die Unternehmensleitung dokumentieren, mit welchen Maßnahmen sie ihre Sorgfaltspflichten erfüllt. Die Dokumentation ermöglicht auch die gesetzlich vorgesehenen Kontrollen und Überwachungen.

Unter dem Aspekt der Compliance (der Regelkonformität) gilt dies noch weitergehender für die Einhaltung sämtlicher gesetzlicher Vorgaben. Das Ziel der Regelkonformität bedingt auch die Gestaltung und Überwachung der Einhaltung der unternehmensinternen IT-Richtlinien einschließlich der Informationssicherheit.[15] Einzuschließen sind die hier und im Weiteren dargestellten gesetzlichen Vorgaben, z. B. die Bereiche Datenschutz, Banken- oder Telekommunikationsregulierung. Auch Regelungsbereiche, die nur eine indirekte Beziehung aufweisen wie das Urheberrecht (Lizenzmanagement) oder das Betriebsverfassungsrecht (Mitbestimmungspflichtigkeit von Sicherheitsmaßnahmen), sind zu beachten.

§ 91 Abs. 2 AktG[16] begründet eine weitere Handlungspflicht für den Vorstand der Aktiengesellschaft. Der Vorstand muss geeignete Maßnahmen zur Früherkennung von den Fortbestand der Gesellschaft gefährdenden Entwicklungen treffen und insbesondere ein diesbezügliches Überwachungssystem einrichten. Laut Gesetzesbegründung soll diese Pflicht auch auf andere Gesellschaftsformen, vor allem die Gesellschaft mit beschränkter

12 Aktiengesetz

13 Gesetz betreffend die Gesellschaften mit beschränkter Haftung.

14 Handelsgesetzbuch

15 Der Bereich Compliance wird auch als Gebiet des Informationssicherheitsmanagements in ISO 27002 aufgeführt, vgl. im Abschnitt 5.4. Insofern besteht inzwischen eine enge Wechselwirkung zwischen Rechtsvorgaben und Maßnahmen zur Informationssicherheit.

16 § 91 Abs. 2 AktG wurde 1998 durch das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) eingeführt (Bundesgesetzblatt (BGBl.) Teil I, S. 786 v. 27.04.1998).

Haftung, Anwendung finden.[17] Die Früherkennung bedingt, dass Entwicklungen, die nachteilige Veränderungen auf die Vermögens-, Ertrags- oder Finanzlage der Gesellschaft nach sich ziehen können (Bestandsgefährdungen), der Unternehmensleitung bekannt werden müssen [Hüf 2010, § 91 Rn. 6 ff.]. Folge des Erkennens solcher Entwicklungspotenziale ist das Ergreifen entsprechender risikobegrenzender Maßnahmen, die in der zweiten Stufe durch das insbesondere geforderte Überwachungssystem neben der Wirksamkeit der Früherkennungsmaßnahmen auf ihre Umsetzung kontrolliert werden sollen. Angesichts der oben dargestellten Bedeutung der IT-Infrastruktur ist deren Betrachtung durch das einzurichtende interne Kontrollsystem (IKS) ein wesentlicher Bestandteil.

Die Ergebnisse der Risikobewertung und ergriffene Maßnahmen sind zudem in den von mittelgroßen und großen Kapitalgesellschaften zu erstellenden Lagebericht aufzunehmen (§ 289 HGB).

Unternehmen, die in den USA börsennotiert sind, haben über die Anforderungen des deutschen Rechts hinaus die Anforderungen des Sarbanes-Oxley-Acts von 2002 zu berücksichtigen, die ebenfalls die Einrichtung eines internen Kontrollsystems beinhalten. Die hierbei zu überwachenden und zu dokumentierenden Inhalte ergeben sich aus zugehörigen Standards. Bezüglich der Standards bei der Prüfung des Abschluss- und Lageberichts und der Kooperation mit Drittstaaten sind zudem wenigstens bei der Rechtsauslegung die Bestimmungen der Richtlinie 2006/43/EG zu beachten.[18]

Anforderungen an Informationssicherheit im Gesellschaftsrecht

Weder die aufgeführten Sorgfaltspflichten der Vorstände oder Geschäftsführer noch die Verpflichtung zu einem Risikomanagement enthalten konkrete Vorgaben zu Maßnahmen zum Schutz der Informationssicherheit. Sie sind beschränkt auf allgemeine Kontroll-, Überwachungs- und Organisationspflichten.

Eine Konkretisierung der zu treffenden Maßnahmen findet sich erst in technischen Standards, die zur Auslegung der gesetzlichen Vorgaben und als Maßstab für den Stand der Technik herangezogen werden können, wie bspw.:[19]

- ISO 2700x
- Grundschutzkataloge des BSI
- Control Objectives for Information and Related Technology (CoBIT)
  IT-Infrastructure Library (ITIL)
- Common Criteria

Keiner dieser Standards hat jedoch Gesetzesrang. Standards werden überwiegend durch private, internationale oder nationale Organisationen verabschiedet und haben innerhalb des jeweiligen nationalen Rechts keine *formale Verbindlichkeit*. Da der Gesetzgeber auf ihren veränderbaren Inhalt keinen Einfluss hat, können Gesetze auch nicht direkt auf Standards verweisen. Ihre *faktische Verbindlichkeit* erlangen Standards durch die Recht-

17 Bundestagsdrucksache (BT-Drs.) 13/9712, S. 15.

18 Richtlinie 2006/43/EG des Europäischen Parlaments und des Rats vom 17.05.2006 über Abschlussprüfungen von Jahresabschlüssen und konsolidierten Abschlüssen […].

19 Zu den Standards siehe Kapitel 5, Kapitel 6 sowie die *Übersicht zu Standards der Informationssicherheit im Anhang.*

sprechung. Dort wird auf sie z. B. als Maßstab für den Stand der Technik, zur Bemessung der verkehrsüblichen Sorgfaltspflichten, als Bezugspunkt von vertraglichen Verpflichtungen, durch Bezugnahmen in Verwaltungsvorschriften oder als Ausschreibungskriterien verwiesen.

Teile der sich auf diese Weise ergebenden Pflichten der Unternehmensleitung betreffen Anforderungen an die physische und logische Sicherheit, z. B. die Notfallplanung, Klassifizierung von Informationen und Systemen, betriebliche Verfahren und Zuständigkeiten, Vorkehrungen für eine ausreichende Datensicherung und die Absicherung der Systeme gegen Angriffe usw.

Durchsetzung von Informationssicherheit im Gesellschaftsrecht

Die Durchsetzung der durch das Gesellschaftsrecht bestehenden Anforderungen an die IT-Sicherheit erfolgt in erster Linie über die für die verschiedenen Gesellschaftsformen vorgesehenen Kontrollmechanismen. Dazu gehört bspw. in einer Aktiengesellschaft die Kontrolle der vorzulegenden Berichte durch den Aufsichtsrat. Die Durchsetzung der Pflichten erfolgt außerdem über die Haftungsvorschriften für die jeweilige Unternehmensleitung.

Die Haftung des Vorstands einer Aktiengesellschaft ist in § 93 Abs. 2 AktG geregelt. Bei Verletzung der oben erläuterten Sorgfaltspflichten haften die Vorstandsmitglieder gegenüber ihrer Gesellschaft als Gesamtschuldner. Eine Entlastungsmöglichkeit besteht, wenn die Vorstandsmitglieder auf Grundlage angemessener Informationen bei einer unternehmerischen Entscheidung vernünftigerweise annehmen durften, zum Wohle der Gesellschaft zu handeln (Business Judgement Rule). Auch aus diesem Grund sind ein Berichtswesen und eine nachvollziehbare Risikoabschätzung unabdingbar. Der Nachweis, mit der erforderlichen Sorgfalt gehandelt zu haben, obliegt dem Vorstand. Aus diesem Grund reichen gut funktionierende und an sich angemessene Maßnahmen allein bei Eintritt eines Schadens nicht aus. Für den Nachweis der Pflichterfüllung benötigt der Vorstand eine Dokumentation des internen Kontrollsystems und der getroffenen Maßnahmen. Für die Geschäftsführer einer GmbH gilt Entsprechendes, auch wenn eine ausdrückliche gesetzliche Regelung lediglich für Aktiengesellschaften besteht.

Fehlt eine solche Dokumentation gänzlich, kann der Unternehmensleitung die Entlastung verweigert oder eine erteilte Entlastung mit der Folge fortbestehender Haftung angefochten werden.[20] Für Vorstände der Aktiengesellschaft sieht § 93 Abs. 2 AktG zudem bei einer durch die Gesellschaft abgeschlossenen D&O-Versicherung[21] einen zwingenden Selbstbehalt von mindestens 10 % des Schadens vor, der erst nach Erreichen der anderthalbfachen Jahresvergütung des Vorstandsmitglieds begrenzt werden kann.

Nach § 316 Abs. 1 HGB sind der Jahresabschluss und der Lagebericht durch unabhängige Wirtschaftsprüfer zu prüfen. Nach § 317 Abs. 4 HGB ist hierbei insbesondere das durch § 91 Abs. 2 AktG einzurichtende Überwachungssystem einzubeziehen, nach § 321 Abs. 4 HGB sogar in einem gesonderten Berichtsteil des Prüfungsberichts. Die Abschlussprüfer

20 LG München I, Urteil v. 5.4.2007, AZ: 5 HK O 15964/06.

21 Directors & Officers Versicherung, eine für Organe und leitende Angestellte abgeschlossene Vermögensschadenshaftpflichtversicherung.

haben hierbei über Gesetzesverstöße oder bestandsgefährdende Tatsachen zu berichten, sodass die Beseitigung der Missstände durchgesetzt werden kann.

3.1.3 Anforderungen aus dem Bankenrecht

Das Bankenrecht gilt im Vergleich zum Gesellschaftsrecht nur für einen eng begrenzten Anwenderkreis, ist aber als Orientierung und durch die Ausstrahlung auf die Dienstleister der Adressaten auch darüber hinaus relevant.

Das Kreditwesengesetz regelt die Aufsicht über die Banken. Es soll Schäden im Kreditwesen und Verluste der Bankengläubiger abwenden. Hierfür wird von den Banken gefordert, ein Risikomanagement zu betreiben und dabei die operationellen Risiken auch der Unternehmens-IT zu erfassen. Die §§ 25a und 25b KWG[22] gehen inhaltlich über die allgemeinen Anforderungen des Aktiengesetzes hinaus. Soweit[23] sie übertragbar sind, können sie deshalb zur genaueren Bestimmung und Auslegung des Pflichtenumfangs im AktG für Unternehmen außerhalb des Finanzsektors herangezogen werden.

Zur Harmonisierung der Finanzmärkte im europäischen Binnenmarkt wurde die »Markets in Financial Instruments Directive« (MiFID)[24] erlassen. 2018 wurde MiFID I durch MiFID II[25] abgelöst und verfolgt die Ziele des erhöhten Anlegerschutzes, des gestärkten Wettbewerbs und der Harmonisierung des europäischen Finanzmarkts. Die Stärkung des Anlegerschutzes und der Strukturierung der Wertpapier- und Derivatemärkte umfasst z. B. die Regulierung des Hochfrequenzhandels und die Einführung von Vor- und Nachhandelstransparenzanforderungen. MIFID II wird durch eine begleitende Verordnung (MiFIR) ergänzt[26,] die weitere Anforderungen und Durchsetzungsmittel enthält.

Die Umsetzung von MiFID in nationales Recht erfolgte mit dem Finanzmarktrichtlinie-Umsetzungsgesetz (FRUG) in Verbindung mit der Wertpapierdienstleistungs-Verhaltens- und Organisationsverordnung (WpDVerOV). MiFID gilt definitionsgemäß für Wertpapierfirmen, Kreditinstitute sowie bestimmte weitere Subjekte der Bankenregulierung durch Basel III resp. Eigenkapitalrichtlinie.

Mitte der 70er-Jahre wurde zudem der sogenannte Basler Ausschuss für Bankenaufsicht gegründet. Die aktuellen Regelungen des Ausschusses – derzeit Basel III – klären die Anforderungen an das Eigenkapital von Banken für die Kreditvergabe zur Reduktion von Insolvenzrisiken. Zu diesem Zweck werden Kreditnehmer bspw. durch Bonitätschecks überprüft und anhand der Ermittlung von Scoring-Werten bewertet. Je höher das Kreditrisiko, desto höher muss das Eigenkapital der kreditvergebenden Bank sein. Die

22 Kreditwesengesetz

23 D. h., soweit es nicht um die Besonderheiten des Finanzsektors geht.

24 Richtlinie 2004/39/EG des Europäischen Parlaments und des Rats vom 21. April 2004 über Märkte für Finanzinstrumente, zur Änderung der Richtlinien 85/611/EWG und 93/6/EWG des Rats und der Richtlinie 2000/12/EG des Europäischen Parlaments und des Rats und zur Aufhebung der Richtlinie 93/22/EWG des Rats.

25 Richtlinie 2014/65/EU des Europäischen Parlaments und des Rats vom 15. Mai 2014 über Märkte für Finanzinstrumente sowie zur Änderung der Richtlinien 2002/92/EG und 2011/61/EU.

26 Verordnung (EU) Nr. 600/2014 des Europäischen Parlaments und des Rats vom 15.05.2014 über Märkte für Finanzinstrumente und zur Änderung der Verordnung (EU) Nr. 648/2012.

Regelungen nach Basel III sind in der EU in Form der »Eigenkapitalrichtlinie«[27] umgesetzt. Aufgrund eines umfassenden Schutzmechanismus, der aus mehreren Puffern in Form einer erforderlichen Eigenkapitalquote von 8 %, eines erforderlichen Kernkapitals von 6 % sowie eines Kapitalerhaltungspuffers von 2,5 % besteht, soll dazu beigetragen werden, dass Banken auch in Krisenzeiten nicht an Stabilität einbüßen und ihre Solvenz und Liquidität gewährleistet bleiben.

Hierfür spielt wiederum die Bewertung der operationellen Risiken der kreditnehmenden Unternehmen eine Rolle. Dadurch kann sich ein nachweisbar hoher Standard bei der Informationssicherheit beim Kreditnehmer auf die Bewilligung und den Zinssatz eines Kredits auswirken. Somit besteht durch Basel II auch für normale Unternehmen ein Anreiz, sich um Informationssicherheit zu kümmern. Versäumen sie dies und weisen sie offenkundige Informationssicherheitsmängel auf, riskieren sie, ihre Kreditwürdigkeit einzubüßen.

Die für den Bankensektor konkretisierten Anforderungen strahlen außerdem auch auf die Unternehmen aus, die (IT)Dienstleistungen für Kredit- oder Finanzdienstleistungsinstitute erbringen. Diese sind von den Banken in ihr Risikomanagement einzubeziehen, sodass sie die für ihre Auftraggeber geltenden Anforderungen in weiten Teilen ebenfalls erfüllen müssen.

Grundlagen zur Informationssicherheit im Bankenrecht

Gegenüber den Banken sind Anforderungen, die auch ausdrücklich die Informationssicherheit betreffen, in den §§ 25a und 25b KWG (Fassung ab 2014) enthalten. In § 25a Abs. 1 KWG werden die Finanzinstitute zunächst zu dem besagten angemessenen und wirksamen Risikomanagement verpflichtet, zu dem die Einrichtung eines internen Kontrollsystems und einer internen Revision gehört. Zum internen Kontrollsystem wiederum gehört eine ordnungsgemäße Geschäftsorganisation in Form von aufbau- und ablauforganisatorischen Regelungen, die unter anderem eine klare Abgrenzung der Verantwortungsbereiche schaffen. Die Verantwortungszuweisungen und die zu schaffenden Regelungen müssen auch die IT umfassen. Zum internen Kontrollsystem gehört ausdrücklich eine Compliance-Funktion. Diese muss die Einhaltung der das Institut betreffenden gesetzlichen Bestimmungen gewährleisten. Die Verantwortung hierfür wird der Unternehmensleitung zugewiesen.

Für die IT wird neben dem internen Kontrollsystem auch eine angemessene personelle und technisch-organisatorische Ausstattung sowie die Festlegung und Umsetzung eines angemessenen Notfallkonzepts gefordert. Das Finanzinstitut muss insbesondere durch geeignete Maßnahmen eine angemessene Qualifikation der IT-Mitarbeiter gewährleisten. Bezüglich der technisch-organisatorischen Ausstattung wird die Angemessenheit an den gängigen technischen Standards orientiert. Sämtliche Maßnahmen sind als Teil der ordnungsgemäßen Geschäftsorganisation vollständig und nachvollziehbar zu dokumentieren.

27 Sogenannte »Richtlinie 2013/36/EU des Europäischen Parlaments und des Rats vom 26. Juni 2013 über den Zugang zur Tätigkeit von Kreditinstituten und die Beaufsichtigung von Kreditinstituten und Wertpapierfirmen, zur Änderung der Richtlinie 2002/87/EG und zur Aufhebung der Richtlinien 2006/48/EG und 2006/49/EG«, Download: *https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32013L0036*.

Eine weitere Ergänzung mit möglichen Auswirkungen für die Informationssicherheit ist die Verpflichtung zur Einrichtung eines Whistleblowing-Systems. Ein solches System muss die Vertraulichkeit der Identität von meldenden Mitarbeitern gewährleisten. Es ist daher zwangsläufig Gegenstand der Informationssicherheit. Gleichzeitig ist es auch ein Durchsetzungs- und Überwachungsinstrument für die organisatorischen Maßnahmen der Informationssicherheit.

In § 25b KWG (Fassungen seit 2014) finden sich Regelungen zur Auslagerung, die auch bei IT-Anwendungen, Infrastrukturen und -Prozessen anzuwenden sind. Inhaltlich ähneln sie den Vorschriften zur datenschutzrechtlichen Auftragsverarbeitung,[28] gelten aber auch unabhängig von personenbezogenen Daten. Die Verantwortung für die Einhaltung der gesetzlichen Bestimmungen verbleibt auch hier beim auslagernden Finanzinstitut (§ 25b Abs. 2 S. 2 KWG).[29] Die Regelungen setzen einerseits Grenzen für die Auslagerung von Aufgaben und Arbeiten und formulieren andererseits Gestaltungsanforderungen. Grundsätzlich sind Maßnahmen zu ergreifen, um übermäßige zusätzliche Risiken durch die Auslagerung zu vermeiden. Auch nach einer Auslagerung muss ein angemessenes Risikomanagement sichergestellt sein. Die Auslagerung ist schriftlich zu vereinbaren, es müssen Prüf- und Kontrollrechte, Weisungs- und Kündigungsrechte des auslagernden Unternehmens sowie die entsprechenden Pflichten des Dienstleistungsunternehmens, das mit den ausgelagerten Aufgaben betraut wird, in der Vereinbarung geregelt werden.

Der Auftraggeber muss das Risikomanagement auch auf die ausgelagerten Tätigkeiten erstrecken. Daher sind auch die beim Auftragnehmer zu treffenden technischen und organisatorischen Sicherheitsmaßnahmen in die Vereinbarung aufzunehmen. Die Vereinbarung muss so konkret gefasst werden, dass auch externe Prüfer anhand der Dokumentation entscheiden können, ob die Maßnahmen angemessen und tauglich sind. Die Vereinbarung muss außerdem geeignet sein, um die konkreten Maßnahmen einfordern zu können.

Das Kontrollrecht der BaFin[30] und der Institutsprüfer darf auch durch eine Auslagerung an ein Unternehmen mit Sitz innerhalb des Europäischen Wirtschaftsraums oder in einem Drittstaat nicht eingeschränkt werden (§ 44 Abs. 1 und 2 KWG). Damit wird der BaFin Rechnung getragen, die als Behörde in ihrer Hoheitsmacht auf Deutschland beschränkt ist. Für Finanzunternehmen ergibt sich daraus ein Hindernis, Aufgaben an beliebige Dritte auszulagern.

Anforderungen an Informationssicherheit im Bankenrecht (MaRisk)

Aus den oben dargestellten gesetzlichen Anforderungen lassen sich bereits abstrakte Anforderungen ableiten, etwa zur Prüfung der IT-Ausstattung, zur Organisation des Geschäftsbereichs IT, zum Erstellen eines Notfallplans und zur vertraglichen Gestaltung von Auslagerungen.

Eine weitere Konkretisierung erfahren diese Anforderungen durch das Rundschreiben 09/2017 (BA) vom 27.10.2017 der BaFin, das Mindestanforderungen an das Risikomanage-

28 Siehe Abschnitt 3.2.1

29 Näheres zu den diesbezüglichen Anforderungen der BaFin und der Deutschen Bundesbank, Le2019.

30 Bundesanstalt für Finanzdienstleistungsaufsicht.

ment (MaRisk)[31] definiert. Den MaRisk kommt zwar eine hohe faktische Verbindlichkeit zu, rechtlich hat das Rundschreiben, in dem sie veröffentlich wurden, aber keinen Gesetzesrang und damit keine direkte Verbindlichkeit. Die Anforderungen sind auch nicht als abschließend zu verstehen; für Institute besonderer Größe oder mit besonders komplexen Tätigkeitsfeldern können für ein angemessenes Sicherheitsniveau auch Maßnahmen über die MaRisk hinaus notwendig sein.

Die MaRisk beschreibt zunächst die Rollen und Verantwortlichkeiten der verschiedenen Funktionen wie Geschäftsleitung, Compliance, Risikocontrolling und interne Revision. Gesondert behandelt werden die geforderten Dokumentationen. Kontroll- und Überwachungsunterlagen sind danach grundsätzlich für Jahre lang aufzubewahren (MaRisk AT 6). Maßnahmen und Regelungen sind nachvollziehbar zu dokumentieren. Im allgemeinen Teil der MaRisk (MaRisk AT 7.2) werden die Anforderungen an die technisch-organisatorische Ausstattung konkretisiert. Sicherzustellen sind die Integrität, Verfügbarkeit, Authentizität und Vertraulichkeit der Daten durch Beachtung der gängigen Standards. Es sind Prozesse zur IT-Berechtigungsvergabe einzurichten, die die Rechte jedes Mitarbeiters auf das für seine Tätigkeit Erforderliche beschränken. IT-Systeme sind vor ihrem Einsatz und nach wesentlichen Veränderungen zu testen und abzunehmen sowie regelmäßig auf ihre Eignung zu prüfen. Die Produktions- und die Testumgebung sind hierbei zu trennen.

Nähere Bestimmungen ergehen auch zum Notfallkonzept. Dessen Wirksamkeit und Angemessenheit sind durch regelmäßige Notfalltests zu überprüfen. Mit Auslagerungsunternehmen sind die Notfallkonzepte gegenseitig abzustimmen. Das Konzept muss gewährleisten, dass zeitnah Ersatzlösungen zur Verfügung stehen und in angemessenem Zeitrahmen die Rückkehr zum Normalbetrieb möglich ist. Das Konzept muss für die beteiligten Mitarbeiter zur Verfügung stehen (MaRisk AT 7.3).

Die Kontrolle dieser Vorgaben obliegt der internen Revision. Schwerwiegende Mängel sind unverzüglich der Geschäftsleitung zu melden und andere Mängel bezüglich ihrer fristgerechten Beseitigung zu überwachen. Gegebenenfalls ist hierzu eine Nachschauprüfung (Follow-up-Prüfung) anzusetzen. Erfolgt die Beseitigung nicht, besteht eine Berichtspflicht an den zuständigen Geschäftsleiter, danach an die gesamte Geschäftsleitung. Diese wiederum hat über schwerwiegende und nicht beseitigte Mängel mindestens jährlich ihrem Aufsichtsorgan zu berichten.

Nebst einer regelmäßigen Risikoberichterstellung, z. B. Berichte bestimmter Risikoarten (bspw. operationelle Risiken) und Gesamtrisikoberichte, müssen die Bankinstitute auch ad hoc Berichterstellungen tätigen können, z. B. in besonderen Risikosituationen. (bspw. Gefahrenrisiken). Das Aufsichtsorgan wird durch die Geschäftsleitung mindestens vierteljährlich zur Risikosituation informiert. Die Berichterstattung beinhaltet auch eine Beurteilung der Risikoverhältnisse.

Durchsetzung von Informationssicherheit im Bankenrecht

Die Maßnahmen zum Risikomanagement werden durch die oben dargestellten Prüf- und Berichtspflichten durchgesetzt. Sie zwingen letztlich die Geschäftsleitung, vertragliche Konsequenzen und mögliche Haftungsfolgen zu vermeiden. Als Folge der Berichte an die

31 Die MaRisk enthalten die Anforderungen der BaFin, die Prüfungen von Kreditinstituten und Finanzdienstleistungsinstituten zugrunde gelegt werden, siehe [MaRisk 2012].

Unternehmensleitung greifen die oben zum allgemeinen Gesellschaftsrecht dargestellten Rechtsregeln.

Darüber hinaus unterliegen auch die der Informationssicherheit dienenden Maßnahmen der Aufsicht der BaFin, die nach § 25a Abs. 2 KWG Auflagen zu deren Durchsetzung erteilen kann. Dasselbe gilt für die Beseitigung von Beeinträchtigungen der Kontrollmöglichkeiten der BaFin durch Auslagerungen. § 25b Abs. 4 KWG gibt auch hier der BaFin das Recht, im Einzelfall Anordnungen zu treffen. Die Anordnungen erfolgen als Verwaltungsakt und können dementsprechend durch Zwangsgelder oder Ersatzvornahmen vollstreckt werden.

Wird der BaFin bekannt, dass ein Institut nicht bereit oder in der Lage ist, die erforderlichen Vorkehrungen u. a. für die Informationssicherheit zu schaffen, kann sie sogar die Betriebserlaubnis aufheben (§§ 35 Abs. 2 Nr. 3, 33 Abs. 1 Nr. 7 KWG).

3.1.4 Anforderungen aus dem Steuer- und Handelsrecht

Das Steuer- und Handelsrecht hat lediglich für einen eng begrenzten Bereich, die Buchführung und die Aufbewahrung der zugehörigen Dokumente, einen Bezug zur Informationssicherheit und auch diesen nur, wenn die Buchführung elektronisch erfolgt, was sowohl § 239 Abs. 4 Handelsgesetzbuch (HGB) als auch § 147 Abs. 2 Abgabenordnung (AO) ermöglichen.

Zur Buchführung ist handelsrechtlich jeder Kaufmann verpflichtet, der in zwei aufeinanderfolgenden Geschäftsjahren mehr als 50.000 Euro Jahresüberschuss und mehr als 500.000 Euro Umsatz erzielt (§§ 238 Abs. 1, 241a HGB). Die steuerrechtliche Buchführungspflicht nach §§ 140, 141 Abs. 1 AO entspricht dem weitestgehend.

Grundlagen zur Informationssicherheit im Steuer- und Handelsrecht

Grundsätzlich sind die Unterlagen der Buchhaltung, in der Terminologie des Steuerrechts *Bücher,* nach den Grundsätzen ordnungsmäßiger Buchführung zu führen (§ 238 Abs. 1 HGB). Sämtliche Geschäftsvorfälle müssen sich über die Bücher in ihrer Entstehung und Abwicklung nachvollziehen lassen (§ 238 Abs. 1 S. 3 HGB). Eine maßgebliche Anforderung ist hierbei, dass die Eintragungen oder Aufzeichnungen nach ihrer Eintragung nicht mehr in einer Weise verändert werden können und dürfen, dass ihr ursprünglicher Inhalt nicht mehr feststellbar ist. (§ 239 Abs. 3 HGB). Werden die Bücher auf Datenträgern geführt, muss weiter sichergestellt sein, dass sie während der Aufbewahrungsfrist von 10 Jahren verfügbar sind und jederzeit innerhalb angemessener Frist lesbar gemacht werden können.

Zu den relevanten Unterlagen gehören neben den eigentlichen Buchungen weitere Dokumente. Soweit diese elektronisch vorgehalten werden, sind auch diese angemessen zu sichern. Zu den Unterlagen zählen – ebenfalls mit einer Aufbewahrungsfrist von 10 Jahren – die buchungsbegründenden Unterlagen wie Rechnungen, Gutschriften, Quittungen oder Gehaltsabrechnungen. Mit einer kürzeren Frist von 6 Jahren müssen Handelsbriefe aufbewahrt werden. Dieser leider etwas unscharfe Begriff umfasst Unterlagen, die der Vorbereitung, Durchführung, dem Abschluss oder der Rückgängigmachung eines Geschäfts dienen, z. B. Vertragsunterlagen. Werden solche Unterlagen eingescannt oder nur elektronisch erstellt und verarbeitet, sind die oben genannten Rechtsvorschriften einschlägig. Sie gelten daher häufig nicht nur für Buchhaltungs-, sondern auch für CRM- oder Dokumentenmanagementsysteme.

Die Abgabenordnung (AO) enthält in § 146 Abs. 2a AO eine besondere Bestimmung, die bei einer Auslagerung der Buchführung an Web- oder Cloud-Dienste zu berücksichtigen ist: Elektronische Bücher und sonstige Aufzeichnungen sind innerhalb der Europäischen Union oder innerhalb des Europäischen Wirtschaftsraums zu führen. Die Aufbewahrung außerhalb Deutschlands muss von der zuständigen Finanzbehörde auf schriftlichen Antrag hin erst genehmigt werden. Für den Antrag ist unter anderem der Standort des eingesetzten Datenverarbeitungssystems und bei Beauftragung eines Dritten dessen Anschrift mitzuteilen.

Anforderungen an Informationssicherheit im Steuer- und Handelsrecht

Die Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS) umfassten Regeln zur Buchführung mit Datenverarbeitungssystemen. Diese Regeln wurden 1995 durch das Bundesfinanzministerium veröffentlicht und stellten eine Spezifizierung der Grundsätze ordnungsmäßiger Buchführung (GoB) dar. Die GoBS wurden 2015 in die Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) überführt, die vom Bundesministerium für Finanzen herausgegeben wurden. Durch die GoBD wurden nicht nur die GoBS, sondern auch die Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) abgelöst.

Die GoBD beantworten Einzelheiten zur digitalen Archivierung unter steuerlichen Gesichtspunkten und berücksichtigt deshalb auch Datenschutz-Anforderungen für die elektronische Aufbewahrung geschäftsrelevanter Unterlagen. Die zwei wichtigsten Grundsätze umfassen dabei die Aspekte »Datensicherheit« und »Datenunveränderbarkeit«, wobei ersterer Begriff den Schutz der Daten vor Verlust und unberechtigten Zugriffen, der zweite die Unveränderbarkeit im Sinne von Veränderungen, Überschreibungen, Ersetzen von Daten ohne Kennzeichnung usw. umfasst. Diese Grundsätze müssen während der gesamten Aufbewahrung nachweislich erfüllt sein, damit die Nachvollziehbarkeit und Überprüfbarkeit ununterbrochen gewahrt bleiben.

Die Beweiskraft der Buchführung wird durch die Verknüpfung von Beleg mit der Buchung herbeigeführt. Gemäß § 146 Abs. 1 AO und § 239 Abs. 2 HBG sind Buchungen zeitgerecht vorzunehmen, d. h., sie müssen so zeitnah wie möglich gebucht werden im Sinne eines engen zeitlichen Zusammenhangs. Die steuerliche Relevanz zur Feststellung, ob es sich um steuerliche relevante Daten im Sinne der GoBD handelt, muss grundsätzlich für jeden Fall einzeln geklärt werden. Daten der Finanz-, Lohn- und Anlagenbuchhaltung gehören grundsätzlich dazu. Auch liefert § 147 Abs. 1 AO diesbezüglich erste Antworten (Bücher und Aufzeichnungen, Geschäfts- und Handelsbriefe, Buchungsbelege). Gemäß BFH-Urteil vom 24.06.2009 VIII R/80/06 sind danach alle Unterlagen aufzubewahren, die zum Verständnis und zur Überprüfung der für die Besteuerung gesetzlich vorgeschriebenen Aufzeichnungen im Einzelfall von Bedeutung sein können.

Für die Unternehmen bestehen Mitwirkungspflichten bei der Datenbereitstellung, z. B. bei Überprüfung durch das Finanzamt, § 146 Abs. 6 AO. Dies kann bspw. in einem Lese-Zugriff auf das Datenverarbeitungssystem resultieren mit entsprechender Zugangs- und Zugriffsberechtigung.

Technische Anforderungen an die elektronische Erfassung der Daten ergeben sich u. a. aus der möglichen maschinellen Auswertbarkeit von Daten. Für elektronische Rechnungen z. B. PDF/A-3 (Dateiformat zur Langzeitarchivierung digitaler Dokumente), wobei

das Format aus zwei Teilen besteht (Bild der Rechnung und maschinenlesbarer Teil in XML-Format mit Rechnungsdaten). Eine maschinelle Auswertbarkeit eines Dokuments ist nur dann gegeben, wenn beide Teile vorhanden sind.

Durchsetzung von Informationssicherheit im Steuer- und Handelsrecht

Nur einer ordnungsgemäßen Buchführung kommt nach § 158 AO Beweiskraft zu. Folge einer nicht ordnungsmäßigen Buchführung kann eine Steuerschätzung nach § 162 AO sein. Unzureichende Sicherheitsmaßnahmen bergen daher große Steuerrisiken für Unternehmen. Wenn durch die nicht ordnungsgemäße Buchführung eine Steuerverkürzung möglich wird, kann dies zusätzlich als Ordnungswidrigkeit geahndet werden (§ 379 Abs. 1 AO).

In einem Ende 2018 vorgelegten Entwurf des Bundesministeriums der Finanzen (BMF) sollen die GoBD von 2015 neu gefasst werden. Der Entwurf sieht maßgebliche Erleichterungen vor, z. B. in den Bereichen Digitalisierung von Belegen mittels mobiler Endgeräte und der Konvertierung aufbewahrungspflichtiger Unterlagen in unternehmenseigene Formate. Der Entwurf verlangt weiterhin die Unveränderbarkeit elektronisch erzeugter Unterlagen, was ohne die Implementierung und Verwendung von revisionssicheren Dokumentenmanagementsystemen kaum möglich ist. Gerade für KMUs kann diese Anforderung jedoch ein kritischer finanzieller Faktor sein. Der Deutsche Steuerberaterverband (DStV) hat das BMF deshalb um Umsetzungsvorschläge zur Einhaltung der Revisionssicherheit von aufbewahrungspflichtigen Office-Unterlagen eingeladen, der sich auch ohne Implementierung eines derartigen Managementsystems umsetzen lässt.

3.1.5 Informationssicherheit für Kritische Infrastrukturen (IT-Sicherheitsgesetz)

Mit dem IT-Sicherheitsgesetz hat der deutsche Gesetzgeber die IT-Sicherheit selbst zum Hauptgegenstand seiner Gesetzgebung gemacht und gezielt bestimmte Branchen in die Pflicht genommen. Für einige der betroffenen Branchen (Telekommunikationsbranche, Energiewirtschaft) sind die bereits oben dargestellten inhaltlichen Anforderungen zwar nur geringfügig verändert worden, der Konkretisierungsgrad des Gesetzes selbst ist jedoch nicht höher als der der bisherigen Regelungen, die Nachweis- und Dokumentationspflichten sowie die Durchsetzungsmittel sind jedoch hierdurch erheblich verschärft.

Grundlagen der Regelungen für Kritische Infrastrukturen

Das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, kurz IT-Sicherheitsgesetz,[32] ist am 25.07.2015 in Kraft getreten. Der Beginn der Umsetzungsfristen für die einzelnen Pflichten der Adressaten wurde jedoch mit dem In-Kraft-Treten von Verordnungsbestimmungen (Verordnungen nach § 10 Abs. 1 BSIG) verknüpft, die den Adressatenkreis, also die Betreiber Kritischer Infrastrukturen, näher definieren sollen. Die Verordnungen bestimmen anhand eines Katalogs von Schwellenwerten die Zugehörigkeit eines Branchenunternehmens zu den Kritischen Infrastrukturen. Die Kritikalität bemisst sich dabei beinahe ausschließlich an dem Ausfallsrisiko und der Versorgungsbedeutung.

32 BGBl I Nr. 31, 24.07.2015, S. 1324.

Der erste Korb dieser sogenannten BSI-Kritisverordnung (BSI-KritisV)[33] hat die Branchen Energie, Wasser, Ernährung sowie Informations- und Kommunikationstechnik zum Gegenstand. Er ist am 3.5.2016 in Kraft getreten, sodass die, nach Schwellenwerten über den tatsächlichen Versorgungsgrad bestimmten, Adressaten die neuen Pflichten nach einer zweijährigen Umsetzungspflicht[34] ab Mai 2018 erfüllen mussten. Der zweite Korb (Erste Verordnung zur Änderung der BSI-KritisV) hat die verbleibenden Branchen Finanz- und Versicherungswesen, Transport und Verkehr sowie den Gesundheitssektor erfasst und die diesbezüglichen Schwellenwerte hinzugefügt. Dieser zweite Teil ist am 22.6.2017 in Kraft getreten, sodass diese zweijährige Umsetzungsfrist im Juni 2019 endet.

Dem heutigen Gesetz sind in Deutschland lange Beratungen des »UP-KRITIS«, einer öffentlich-privaten Kooperation von Betreibern, deren Verbänden und der zuständigen staatlichen Stellen, vor allem des Bundesamts für Sicherheit in der Informationstechnik (BSI) und des Bundesinnenministeriums vorangegangen. Ziel des Gesetzes und der vorherigen Umsetzungspläne ist es, eine signifikante Verbesserung der Sicherheit informationstechnischer Systeme in Deutschland zu erreichen sowie den Schutz der Bürger im Internet zu stärken.

Während es sich beim eigentlichen IT-Sicherheitsgesetz um ein Artikelgesetz mit Änderungen verschiedener Einzelbestimmungen handelt (Änderungen des Atomgesetzes, des Energiewirtschaftsgesetzes, des Telekommunikationsgesetzes, des Telemediengesetzes und weiterer Gesetze), liegt der Kern der Rechtsänderungen in den Einfügungen und Ergänzungen des BSI-Gesetzes (des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik). Da die weiteren Gesetzesänderungen im Wesentlichen die zusätzlichen Bestimmungen des BSIG in anderen Branchenregelungen abbilden, lässt sich das Vorgehen des Gesetzgebers am besten anhand des BSI-Gesetzes darstellen. Eingeführt wurde eine allgemeine Pflicht, angemessene technische und organisatorische Vorkehrungen nach Stand der Technik zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit bei den betriebenen Kritischen Infrastrukturen zu ergreifen (§ 8a Abs. BSIG). Diese Pflicht wird von einer Nachweispflicht flankiert, nach der die Betreiber alle zwei Jahre die Erfüllung der Anforderungen durch Sicherheitsaudits, Prüfungen oder Zertifizierungen gegenüber dem BSI oder der sonst zuständigen Aufsichtsbehörde nachzuweisen haben (§ 8a Abs. 3 BSIG). Das BSI kann die Verfahrensanforderungen für diese Nachweisformen weiter festlegen (§ 8a Abs. 5 BSIG), ist dem bislang aber lediglich mit einer Orientierungshilfe und verschiedenen Formularen zur Ergebniseinreichung nachgekommen.[35] Eine weitere Verpflichtung betrifft die beidseitige Kommunikation zu Störfällen und beinhaltet zum einen die Einrichtung einer Kontaktstelle und zum anderen eine Meldepflicht über Störungen, die zu einem durch

33 BGBl. I Nr. 20 vom 2. Mai 2016, S. 958.

34 Die zweijährige Umsetzungspflicht bezieht sich vor allem auf die Umsetzung der technischen und organisatorischen Vorkehrungen zur Störungsvermeidung nach § 8a Abs. 1 BSIG als Kernpflicht. Die Kontaktstelle nach § 8b Abs. 3 BSIG ist dagegen bereits nach sechs Monaten umzusetzen gewesen.

35 Orientierungshilfe zu Nachweisen nach § 8a Abs. 3 BSIG vom 30.06.2017, abrufbar unter *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/IT_SiG/Orientierungshilfe_8a_3.pdf?__blob=publicationFile&v=17* und Formulare abrufbar unter *https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/KRITIS/IT-SiG/Was_tun/Nachweise/Orientierungshilfe/Nachweisdokumente/Nachweisdokumente_node.html*

Schwellenwerte bestimmten Ausfall geführt haben, und über erhebliche Störungen, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der Infrastruktur führen können (§ 8b Abs. 3, 4 BSIG).

Die Inhalte des IT-Sicherheitsgesetzes haben bereits am 29.06.2017 ihre erste Überarbeitung erfahren[36], durch die die sogenannte NIS-Richtlinie[37] in nationales Recht umsetzen soll. Bezüglich der »wesentlichen Dienste«, so die Bezeichnung der Richtlinie für die Kritischen Infrastrukturen deutschen Rechts, wurden die Vorlage und Überprüfungsrechte des BSI und der Aufsichtsbehörden nochmals verschärft. Zudem wurde eine Berichtspflicht des BSI gegenüber der Europäischen Kommission ergänzt und das Meldewesen über die durch die Verordnung erfassten Betreiber hinaus ausgedehnt sowie um einen europäischen Austausch erweitert. Mit dem neuen § 8c BSIG wurden jedoch auch die »Anbieter digitaler Dienste« einer Regulierung unterworfen, die den für Kritische Infrastrukturen geltenden Anforderungen im Wesentlichen entspricht. Umfasst werden durch die in § 2 Abs. 11 und 12 BSIG definierten »Anbieter digitaler Dienste« u. a. Onlinemarktplätze, Suchmaschinenbetreiber und Cloud-Dienste.[38] Geregelt werden die Verpflichtung zu Sicherheitsmaßnahmen, eine Meldepflicht zu Sicherheitsvorfällen gegenüber dem BSI und eine Anwendungsregelung für internationale Anbieter. Die Anbieter digitaler Dienste sind jedoch nicht zur Vorlage von Auditberichten im Zweijahresturnus verpflichtet und haben lediglich bei Anhaltspunkten für die Nichteinhaltung Dokumentationen und Nachweise vorzulegen sowie Mängel zu beseitigen.[39] Zur näheren Bestimmung der Anforderungen hat die Europäische Kommission als Durchführungsrechtsakt (§ 8c Abs. 3 S.2 BSIG) eine Durchführungsverordnung erlassen.[40] Die Regulierung für die digitalen Dienste gilt ab dem 10.05.2018.

Anforderungen an die Betreiber Kritischer Infrastrukturen und Anbieter digitaler Dienste

Die Anforderungen an die Betreiber Kritischer Infrastrukturen und an die Anbieter digitaler Dienste ergeben sich aus den §§ 8 a,b BSIG bzw. § 8c BSIG für die Anbieter digitaler Dienste. Für Unternehmen, die dem Telekommunikationsgesetz unterfallen, gelten die §§ 109, 109a TKG. Die Anwendung der §§ 8a, 8b BSIG des BSIG ist in § 8d Abs. 2 Nr. 1,

36 Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rats vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union vom 23.06.2017.

37 Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rats vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, abrufbar unter https://eur-lex.europa.eu.

38 Die NIS-RL verweist für die Definition der digitalen Dienste auf die Definition der »Dienstleistungen der Informationsgesellschaft«, Art. 1 b) und Anhang I der I Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rats vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft.

39 ScTh 2018, S. 497 ff.

40 Durchführungsverordnung (EU) 2018/151 der Kommission vom 30. Januar 2018 über Vorschriften für die Anwendung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rats hinsichtlich der weiteren Festlegung der von Anbietern digitaler Dienste beim Risikomanagement in Bezug auf die Sicherheit von Netz- und Informationssystemen zu berücksichtigenden Elemente und der Parameter für die Feststellung erheblicher Auswirkungen eines Sicherheitsvorfalls, abrufbar unter *https://eur-lex.europa.eu*.

Abs. 3 Nr. 1 BSIG für diesen Bereich ausgeschlossen. Für Betreiber von Energieversorgungsnetzen oder Energieanlagen, die dem Energiewirtschaftsgesetz (EnWG) unterfallen, gelten die §§ 11 Abs. 1a -1c EnWG. Dieser Bereich wird durch § 8d Abs. 2 Nr. 2 und Abs. 333 Nr. 2 BSIG aus dem Anwendungsbereich der §§ 8a, 8b BSIG ausgenommen, so wie das allgemeiner auch für weitere Branchen und Kritische Infrastrukturen der Fall ist, die bereits einer entsprechenden Regulierung unterliegen. Ein Beispiel hierfür dürften Unternehmen des Finanzsektors sein, die mit den bereits dargestellten §§ 25a, b KWG bereits gleichwertigen Pflichten unterliegen.

Wie bereits dargestellt besteht die Kernpflicht der Betreiber im Ergreifen angemessener technischer und organisatorischer Maßnahmen, um funktionsbeeinträchtigende Störungen der Verfügbarkeit, aber auch von Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse ihrer Infrastrukturen zu vermeiden. Maßstab für die Angemessenheit der Maßnahmen ist zum einen die Einhaltung des Stands der Technik, zum anderen die Abwägung der Verhältnismäßigkeit zwischen dem erforderlichen Aufwand und den Folgen eines Ausfalls oder einer Beeinträchtigung der Kritischen Infrastruktur.

Bei dem »Stand der Technik« handelt es sich um einen unbestimmten Rechtsbegriff, der bereits auf eine lange Geschichte zurückblickt und als Maßstab in allen Bereichen des Technikrechts eingesetzt wird. Dementsprechend ist seine gängige Auslegung auch zunächst einmal nicht an der schnellen Entwicklung und Wandlungsfähigkeit der IT-Technik orientiert. Die übliche Definition der Rechtsprechung geht auf ein Urteil des Bundesverfassungsgerichts zu § 7 des Atomgesetzes und das Bundesimmissionsschutzgesetz zurück. Sie lautet: Stand der Technik in diesem Sinne ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zum Schutz der Funktionsfähigkeit von informationstechnischen Systemen, Komponenten oder Prozessen gegen Beeinträchtigungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit gesichert erscheinen lässt. Bei der Bestimmung des Stands der Technik sind insbesondere einschlägige internationale europäische und nationale Normen und Standards heranzuziehen, aber auch vergleichbare Verfahren, Einrichtungen und Betriebsweisen, die mit Erfolg in der Praxis erprobt wurden.[41]

§ 8a Abs. 2 BSIG sieht vor, dass die Betreiber Kritischer Infrastrukturen und ihre Branchenverbände eigene branchenspezifische Sicherheitsstandards vorschlagen können. Das BSI kann diese dann in Abstimmung mit den zuständigen Aufsichtsbehörden, bspw. der Bundesnetzagentur, als geeignet annehmen. Während eine Reihe von Branchenstandards bereits angenommen wurde, sind derzeit über die einschlägige Seite des BSI nur der Branchenstandard für den Bereich Datacenter & Hosting im Volltext veröffentlicht.[42] Neben diesen stehen noch die Kataloge der Bundesnetzagentur, von denen der Katalog

41 Ausführlicher zum »Stand der Technik« in den verschiedenen Regelungen zur IT-Sicherheit Kno 2017. Zur sogenannten Dreistufentheorie des Bundesverfassungsgerichts (Kalkar-Entscheidung): BVerfGE 49, 89 (135f) vom 8.8.1978. S. auch § 3 Abs. 6 BImSchG.

42 Das BSI informiert über die Standards und ihre Annahme unter *https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/KRITIS/IT-SiG/Was_tun/Stand_der_Technik/B3S_BAKs/B3S_BAKs_node.html.*

gemäß § 11 Abs. 1b EnWG abrufbar ist.[43] Die Standards orientieren sich im Wesentlichen an den ISO-27000-Standards und passen diese auf die besonderen Risikolagen und Gegebenheiten der jeweiligen Branche an. Eine der wesentlichsten gemeinsamen Forderungen ist dementsprechend die Einführung eines Informations-Sicherheitsmanagement-Systems (ISMS), das sich an der ISO/IEC 27001:2013 orientieren kann, aber nicht muss.

Über die Einhaltung des jeweiligen Branchenstandards oder, da die meisten Standards erst nach Ablauf oder kurz vor Ablauf der Umsetzungsfrist zur Verfügung standen, zunächst eigendefinierter angemessener Maßnahmen hat der Betreiber Nachweis zu führen. § 8a Abs. 3 BSIG sieht vor, dass dieser Nachweis alle zwei Jahre durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen muss. Dem BSI oder der zuständigen Aufsichtsbehörde außerhalb des Anwendungsbereichs des § 8a BSIG sind die Ergebnisse einschließlich der Feststellungen mitzuteilen. Das Bundesamt kann danach die Vorlage der gesamten Dokumentation verlangen. Es hat die Befugnis, im Anschluss die Beseitigung der aufgezeigten Mängel zu fordern. Für das Erbringen der erforderlichen Nachweise hat das BSI eine Reihe von Formularen bereitgestellt und seine Erwartungen an die Nachweisdurchführung in eine Orientierungshilfe vom 30.06.2017 gegossen. Die Orientierungshilfe stellt Anforderungen an die Dokumentation, die Scope-Beschreibung, die Prüfstelle und die Zusammensetzung des Prüfteams sowie die eigentliche Prüfungsdurchführung zusammen.[44]

Die auf das Unternehmen und auf Sicherheitsmaßnahmen bezogenen Pflichten werden ergänzt durch das mit § 8b Abs. 3 BSIG und seinen Entsprechungen eingeführte Meldewesen, in dessen Zentrum das BSI steht. Die Betreiber haben eine Kontaktstelle in ihrem Unternehmen einzurichten, über die sie jederzeit für das BSI erreichbar sind. Über diese kann das BSI über sein von ihm zu erstellendes Lagebild sowie über wesentliche Informationen zur Informationssicherheit, zu Sicherheitslücken, Schadprogrammen und aktuelle Angriffsversuche informieren. Die Betreiber haben ihrerseits über ihre Kontaktstellen über Störungen ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu berichten, soweit diese zu einem Ausfall oder einer erheblichen Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt haben. Bei erheblichen Störungen reicht auch bereits die Möglichkeit einer solchen Funktionsbeeinträchtigung für das Eintreten der Meldepflicht. Die Identität des Betreibers wird jedoch nur dann zum verpflichtenden Meldeinhalt, wenn tatsächlich eine Beeinträchtigung der Funktionsfähigkeit eingetreten ist. Die Meldung muss Angaben zu den technischen Rahmenbedingungen und möglichen grenzübergreifenden Auswirkungen, zur vermuteten oder tatsächlichen Ursache, den betroffenen Komponenten, zur durch die Stelle erbrachten kritischen Dienstleistung und zu den Auswirkungen auf diese Dienstleistung enthalten. Die Meldung hat unverzüglich zu erfolgen.

Die Pflichten der Anbieter digitaler Dienste entsprechen in ihrem Aufbau denen der Betreiber Kritischer Infrastrukturen weitgehend (§ 8c BSIG). Den Kern bildet das Ergrei-

43 Abrufbar unter *https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheitskatalog_2018.pdf?__blob=publicationFile&v=4.*

44 Das BSI stellt Formulare bereit unter *https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/KRITIS/IT-SiG/Was_tun/Nachweise/Nachweise_node.html.*

fen angemessener Maßnahmen nach Stand der Technik, wobei dem die zu berücksichtigenden Maßnahmenkategorien Sicherheitsgewährleistung für Systeme und Anlagen, die Vorfallserkennung, das Betriebskontinuitätsmanagement, Evaluation und die Beachtung internationaler Normen an die Seite gestellt sind. An Stelle der aktiven Nachweispflicht steht jedoch lediglich ein Recht des BSI, entsprechende Dokumentation und Nachweise anzufordern, wenn Anhaltspunkte für eine nicht ausreichende Erfüllung vorliegen. Die Meldepflicht dagegen entspricht bis hin zum Verweis auf den Meldeinhalt der Pflicht zu den Kritischen Infrastrukturen. Es entfällt allerdings die Pflicht, eine Kontaktstelle zu betreiben.

Nähere Ausgestaltung erhalten die Pflichten durch den in der NIS-Richtlinie vorgesehenen ergänzenden Rechtsakt der Kommission, die Durchführungsverordnung 2018/151/EU der Kommission vom 30.01.2018, die ab dem 10.05.2018 direkte Geltung in allen Mitgliedstaaten entfaltet.[45] Die Verordnung regelt inhaltliche Elemente, etwa die Vorgabe eines systematischen Managements der Netz- und Informationssysteme, die Gewährleistung physischer Sicherheit, die Notfall-Planung, die Zugriffs- und Zugangskontrolle und Maßgaben zur Bewältigung von Vorfällen, von Erkennungsverfahren über den Meldeprozess bis hin zur Reaktions- und Analyseprozessen. Die Verordnung enthält auch eine prüftaugliche Dokumentationspflicht für die getroffenen Maßnahmen. Weiter werden Maßstäbe zur Feststellung der Vorfallserheblichkeit abstrakt vorgegeben,

Durchsetzung der Anforderungen

Die Durchsetzung der gesetzlichen Pflichten sowohl der Betreiber Kritischer Infrastrukturen als auch der Anbieter digitaler Dienste liegt in den Händen des BSI und der besonderen Aufsichtsbehörden, etwa der Bundesnetzagentur. Nach § 8a Abs. 4 BSIG kann das Bundesamt selbst die Einhaltung der Anforderungen prüfen oder sich hierzu Dritter bedienen. Hierzu besteht ein Betretungs- und Einsichtsrecht des Bundesamts bezüglich der Unternehmen. Das Bundesamt kann ferner die Beseitigung von festgestellten Umsetzungsmängeln verlangen (§§ 8a Abs. 3, 8c Abs. 4 Nr. 2 BSIG).

Verstöße gegen die Pflichten aus den §§ 8a, b oder c BSIG sind zudem als Ordnungswidrigkeiten mit Bußgeldern belegt. Die Höchstsumme beträgt bei Missachtung einer Anordnung 100.000 Euro, für alle übrigen Verfehlungen 50.000 Euro, einschließlich der Verletzung der Meldepflicht.

3.2 Datenschutzrecht

Dem Datenschutzrecht kommt im Rechtsrahmen der Informationssicherheit eine besondere Rolle zu, zum einen, da es in vielen Fällen der Ursprung von Sicherheitsanforderungen ist, zum anderen, da viele Maßnahmen zur Informationssicherheit ihrerseits am Datenschutzrecht zu messen sind. Bevor die datenschutzrechtlichen Grundlagen, Anforderungen

45 Durchführungsverordnung (EU) 2018/151 DER KOMMISSION vom 30.01.2018 über Vorschriften für die Anwendung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rats hinsichtlich der weiteren Festlegung der von Anbietern digitaler Dienste beim Risikomanagement in Bezug auf die Sicherheit von Netz- und Informationssystemen zu berücksichtigenden Elemente und der Parameter für die Feststellung erheblicher Auswirkungen eines Sicherheitsvorfalls, abrufbar unter *https://eur-lex.europa.eu*.

und Durchsetzungsmittel für Informationssicherheit dargestellt werden, gibt der nächste Abschnitt einen kurzen Überblick über die Grundzüge des Datenschutzrechts.

Die Darstellung des Datenschutzrechts beschränkt sich jedoch auf den Bezug zur Informationssicherheit. Technische Gestaltungsfragen oder Organisationspflichten, die keinen Sicherheitsbezug haben, wie z. B. Zulässigkeitsprüfungen, Transparenzpflichten, Betroffenenrechte, Pflichten bei der Videoüberwachung oder Gestaltungsfragen des Konzerndatenaustauschs, bleiben außen vor.

3.2.1 Grundzüge des Datenschutzrechts

Das Datenschutzrecht dient dem Schutz des Einzelnen vor Beeinträchtigungen seines Persönlichkeitsrechts durch den Umgang mit seinen personenbezogenen Daten. Diesen Zweck hat bis Mai 2018 § 1 Abs. BDSG definiert. Art. 1 Abs. 1 und 2 DSGVO sprechen vom Schutz der Grundrechte und Grundfreiheiten sowie vom Recht auf Schutz personenbezogener Daten, führen jedoch bezüglich des Schutzzwecks zu keinen wesentlichen Änderungen.

Personenbezogene Daten und Anwendungsbereich des Datenschutzrechts

Das Verständnis von Datenschutz ist an den Begriff der personenbezogenen Daten geknüpft. Das Bundesdatenschutzgesetz aF hat personenbezogene Daten in § 3 Abs. 1 BDSG als Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person definiert. Art. 4 Nr. 1 DSGVO definiert zunächst personenbezogene Daten als »alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen«. Im 2. Halbsatz wird dann die Identifizierbarkeit, also der Personenbezug, erläutert als Möglichkeit, eine Person direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung oder zu besonderen Merkmalen, zu identifizieren. Erfasst sind damit sämtliche Informationen, die auf eine konkrete Person bezogen werden können, unabhängig von deren Bedeutung für den Betroffenen. Die bloße Möglichkeit des Personenbezugs kann jedoch zu Abgrenzungsschwierigkeiten führen. Pseudonyme Daten (§ 3 Abs. 6a BDSG aF, Art. 4 Nr. 5 DSGVO), bei denen definitionsgemäß der Name oder andere Identifikationsmerkmale der Bezugsperson durch ein Kennzeichen ersetzt werden, um die direkte Bestimmung bspw. für Gruppen von Anwendern auszuschließen oder wesentlich zu erschweren, gelten als personenbeziehbar, da das Kennzeichen die Zuordnung weiter erlaubt. Sie unterfallen damit weiterhin dem Datenschutzrecht.

Der Anwendungsbereich des Datenschutzrechts endet bei anonymen Daten. Wann Daten als anonym einzustufen sind, ist unter Umständen aber schwer zu beurteilen – eine tiefere Analyse von Datenbeständen führt immer wieder zu überraschenden Erkenntnissen. Beispielsweise können Angaben zu einer Person auch ohne bestimmte Identifikationsmerkmale personenbeziehbar werden, wenn die Angaben in ihrer Konstellation und Menge lediglich eine einzige Person zutreffend beschreiben. So kann die Kombination der besuchten Schule, des Geburtsjahrgangs, des Berufs und eines bestimmten Hobbys bereits ausreichen, um eine Person zu bestimmen. Ein Personenbezug liegt bspw. auch bei dynamischen IP-Adressen vor.[46]

46 EuGH, Urteil vom 19.10.2016, C-582/14.

Der Anwendungsbereich des Datenschutzrechts endet ebenfalls bei der Verwendung personenbezogener Daten für ausschließlich persönliche oder familiäre Tätigkeiten (Art. 2 Abs. 2 c) DSGVO).

Bei dem örtlichen Anwendungsbereich des Datenschutzrechts ist zwischen deutschen Vorschriften und der sowohl in Deutschland als auch in den übrigen Mitgliedsstaaten der Europäischen Union direkt geltenden Datenschutz-Grundverordnung zu unterscheiden. Deutsche Datenschutzvorschriften erfassen in der Regel jegliche Datenerhebung, -verarbeitung oder -nutzung in Deutschland, es sei denn, die verantwortliche Stelle hat ihren Sitz in einem anderen Staat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum. Die Datenschutz-Grundverordnung knüpft zum einen an die Tätigkeit eines Verantwortlichen oder eines Auftragsverarbeiters mit Niederlassung in der Europäischen Union an. Zum anderen ist die Datenschutz-Grundverordnung auf Verarbeitungstätigkeiten anzuwenden, die von Verantwortlichen außerhalb der Union ausgehen, aber im Zusammenhang mit Angeboten an betroffenen Personen in der Union stehen oder die der Verhaltensbeobachtung zu betroffenen Personen dienen, die sich in der Union befinden.

Adressaten des Datenschutzrechts sind der *Verantwortliche* und der *Auftragsverarbeiter*. Der Verantwortliche entscheidet allein oder gemeinsam mit weiteren Verantwortlichen über Zwecke und Mittel der Verarbeitung. Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen, unterliegt dabei jedoch eigenen Datenschutzpflichten. Verantwortlicher können natürliche und juristische Personen, Behörden oder andere Stellen sein.

Verbindungen von juristischen Personen untereinander, etwa eine Konzernzugehörigkeit oder ein mehrheitlicher Anteilsbesitz an einer anderen juristischen Person, haben keine Bedeutung – es existiert im Datenschutzrecht kein Konzernprivileg. Daran hat auch die Datenschutz-Grundverordnung im Grundsatz nichts geändert. Die natürliche Person, auf die sich die personenbezogenen Daten beziehen, ist der Betroffene. Alle Personen oder Stellen außerhalb der verantwortlichen Stellen und des Betroffenen sind sogenannte Dritte mit Ausnahme der Auftragsdatenverarbeiter, auf die weiter unten eingegangen wird. Die entscheidende Handlung für die Anwendung des Datenschutzrechts ist das Verarbeiten der personenbezogenen Daten. Die Verarbeitung umfasst das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung (Art. 4 Nr. 2 DSGVO). Im Gegensatz zum früheren BDSG umfasst damit der Verarbeitungsbegriff der DSGVO den gesamten Umgang mit personenbezogenen Daten und definiert die einzelnen aufgezählten Handlungen nicht weiter. Der Begriff des Offenlegens macht deutlich, dass der Verarbeitungsbegriff nicht auf die gezielte Übermittlung beschränkt bleibt, sondern dass bereits die Einblicksmöglichkeit Dritter zur Verarbeitung führt.

Historische Entwicklung

Um das System des Datenschutzrechts und seine Wirkungsweise zu verstehen, ist ein Blick auf die Geschichte des Datenschutzes hilfreich. Das weltweit erste Datenschutzgesetz wurde 1970 in Hessen verabschiedet. Weitere Bundesländer folgten, und 1977 erließ auch der Bund ein Datenschutzgesetz, das Bundesdatenschutzgesetz. Das Bundesdatenschutz-

gesetz regelte die Verwendung personenbezogener Daten durch die Bundesverwaltung (öffentliche Stellen des Bunds) und in der gesamten Privatwirtschaft (den sogenannten nicht öffentliche Stellen). Außerdem legte es die Stellung des Bundesbeauftragten für Datenschutz als Aufsichtsbehörde für die öffentlichen Stellen des Bunds fest. Die Landesdatenschutzgesetze regelten die Datenverarbeitung durch die Landesbehörden und sonstige unter Aufsicht des Lands stehende juristische Personen (öffentliche Stellen). Für den gesamten nicht öffentlichen Bereich wurde die Aufsicht an die Länder delegiert. Die Landesdatenschutzgesetze regeln deshalb auch die Umsetzung der Datenschutzaufsicht für den nicht öffentlichen Bereich. Die Europäische Datenschutzrichtlinie[47] forderte in Art. 28 Abs. 1 die völlige Unabhängigkeit der Aufsichtsbehörden. In den meisten Fällen erfolgt die Zuweisung an den jeweiligen Landesdatenschutzbeauftragten.

Begleitet wurde die Datenschutzgesetzgebung durch die Rechtsprechung des Bundesverfassungsgerichts. Hervorzuheben sind hier die Mikrozensus-Entscheidung vom 16.7.1969[48], in der ein unantastbarer Bereich privater Lebensgestaltung des einzelnen Bürgers postuliert wurde. Dieser ist der Einwirkung der öffentlichen Gewalt entzogen. In der Lebach-Entscheidung vom 5.6.1973[49] traf das Bundesverfassungsgericht eine grundlegende Abwägung zwischen dem Recht der Presse auf Berichterstattung über ein Strafverfahren und dem Persönlichkeitsrecht des Straftäters und beschränkte die namentliche Berichterstattung auf das zeitliche Umfeld des Verfahrens und der Tat.

Bis heute prägende Bedeutung hat vor allem das Volkszählungsurteil vom 15.12.1983,[50] in dem mit dem *Recht auf informationelle Selbstbestimmung* eine Ausprägung des allgemeinen Persönlichkeitsrechts geschaffen wurde. Das Recht auf informationelle Selbstbestimmung ist bis heute aus deutscher Sicht das grundrechtliche Fundament des Datenschutzes. Das Bundesverfassungsgericht hatte die Auswirkungen eines unzureichenden Selbstbestimmungsrechts über personenbezogene Daten als Ausgangspunkt genommen und festgestellt, dass

> *»[eine Gesellschaftsordnung ...], in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß, [mit dem Recht auf informationelle Selbstbestimmung nicht vereinbar wäre]. [...] Hieraus folgt: Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. [...]Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.«*

Die meisten Landesverfassungen haben die informationelle Selbstbestimmung in ihren Grundrechtskatalog aufgenommen. Auch Art. 8 der Charta der Grundrechte der Europäi-

47 Richtlinie 95/46/EG des Europäischen Parlaments und des Rats vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutzrichtlinie)

48 BVerfGE 27, 1

49 BVerfGE 35, 202

50 BVerfGE 65, 1

schen Union enthält seit dem Jahr 2000 eine Grundrechtsbestimmung zum Datenschutz. Für die Datenschutz-Grundverordnung als Europäisches Recht stellt das Grundrecht auf Schutz personenbezogener Daten aus Artikel 8 das verfassungsrechtliche Fundament dar. Die dortige Regelung einer Beschränkung der Verarbeitung personenbezogener Daten auf solche mit einer gesetzlich geregelten Erlaubnisgrundlage oder auf Grundlage einer Einwilligung, die dort festgelegte Zweckbindung, das individuelle Auskunftsrecht und die dort verankerte Überwachung durch unabhängige Stellen werden hierin begründet. Bemerkenswert ist, dass diese im Gegensatz zum Recht auf informationelle Selbstbestimmung nicht als Freiheitsrecht, sondern als Recht auf staatlichen Schutz formuliert ist. Dennoch spielt die Selbstbestimmungsmöglichkeit des Einzelnen auch in der Datenschutz-Grundverordnung eine große Rolle, was an den gestärkten Betroffenen- und Transparenzrechten deutlich wird.

Einen weiteren Meilenstein stellte die Europäische Datenschutzrichtlinie (RL 95/46/EG) vom 24.10.1995 dar. Durch die Richtlinie wurde das Datenschutzrecht unter Übernahme der Grundlinien des deutschen Rechts europaweit harmonisiert. Mit der Datenschutzrichtlinie für elektronische Kommunikation folgten 2002 – überarbeitet 2009 – speziellere Datenschutzvorgaben auf EU-Ebene.[51] Die Europäische Datenschutzrichtlinie wurde durch die Datenschutz-Grundverordnung zum 25.05.2018 aufgehoben.[52] Die Datenschutzrichtlinie für elektronische Kommunikation gilt dagegen noch fort. Sie soll durch die »E-Privacy-Verordnung« ersetzt werden, deren Verabschiedung jedoch noch aussteht.

Die Datenschutz-Grundverordnung trat am 25.05.2016 in Kraft und gilt als Verordnung unmittelbar ohne weiteren Umsetzungsakt in allen Mitgliedstaaten. Das BDSG alter Fassung wurde mit Geltung der Grundverordnung zum 25.05.2018 aufgehoben und durch ein neues Bundesdatenschutzgesetz im Rahmen des Datenschutz-Anpassungs- und Umsetzungsgesetzes EU ersetzt.[53] Diesem ersten Anpassungsgesetz, das neben dem Neuerlass des BDSG zahlreiche weitere erste Anpassungen nationaler Gesetze enthalten hat, wird vermutlich bald eine weiteres Anpassungsgesetz für weitere Gesetze folgen, deren Verweise oder Inhalte an das neue Recht anzupassen sind.[54]

Das neue Bundesdatenschutzgesetz enthält nur noch eine Reihe von Konkretisierungen der Grundverordnung, die den Mitgliedstaaten überlassene Regelung des Beschäftigtendatenschutzes und ansonsten Umsetzungsbestimmungen u. a. zum Aufbau der Datenschutz-

51 RL 2002/58/EG des Europäischen Parlaments und des Rats vom 12.07.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation; geändert durch RL 2009/136/EG des Europäischen Parlaments und des Rats vom 25.11.2009 zur Änderung der Richtlinie 2002/22/EG […], der Richtlinie 2002/58/EG […] und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz.

52 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rats vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), abrufbar unter *https://eur-lex.europa.eu*.

53 Gesetz zur Anpassung des Datenschutzrechts an die Verordnung 2016/679/EU und zur Umsetzung der Richtlinie 2016/680/EU (Datenschutz-Anpassungs- und –Umsetzungsgesetz EU – DSAnpUG-EU), BGBl I vom 5.7.2017, S. 2097.

54 Entwurf eines Zweiten Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU – 2. DSAnpUG-EU).

aufsicht. Durch die neue Grundverordnung, die zwar keine grundsätzlichen Unterschiede bezüglich des Datenschutzaufbaus mit sich bringt, aber dennoch vollständig neues Recht darstellt, befindet sich das Datenschutzrecht derzeit und auch auf absehbare Zeit hinaus stark in Bewegung. Bei einigen Regelungen des neuen Bundesdatenschutzes ist so bereits umstritten, ob sie sich noch im von der DSGVO zugelassenen Rahmen bewegen oder aber diesen sprengen und dadurch unanwendbar werden.[55] Viele Stellungnahmen, Orientierungen und Entscheidungen der Aufsichtsbehörden und viele bisherigen Auffassungen befinden sich in Anpassung an das neue Recht oder bedürfen der Anpassung an das neue Recht. Von den Änderungen sind auch die Anforderungen an die IT-Sicherheit betroffen.

Grundsätze und Mechanismen des Datenschutzrechts

Das Grundrecht auf informationelle Selbstbestimmung macht deutlich, dass die Verwendung personenbezogener Daten zu Eingriffen in die Grundrechte des Betroffenen führt. Hieraus leitet sich ein tragendes Grundprinzip des Datenschutzrechts ab: Ein Erheben, Verarbeiten oder Nutzen von personenbezogenen Daten darf nur auf Grundlage einer rechtlichen Erlaubnisnorm stattfinden und ist ansonsten verboten. Dieser Grundsatz wird auch als *Verbot mit Erlaubnisvorbehalt* bezeichnet. Als Bestandteil des Art. 8 Abs. 2 der Charta der Grundrechte und konkretisiert durch Art. 6 Abs. 1 DSGVO besteht dieser Grundsatz auch weiterhin. Der Grundsatz darf jedoch nicht darüber hinwegtäuschen, dass die Datenschutz-Grundverordnung sehr weite allgemeine Erlaubnisnormen enthält, vor allem die Verarbeitung auf Grundlage des berechtigten Interesses, Art. 6 Abs. 1 f) DSGVO. Die speziellen Regelungen des Bundesdatenschutzgesetzes etwa zur Verarbeitung zu Werbezwecken existieren nicht mehr. Stattdessen enthält Art. 6 Abs. 1 DSGVO die wesentlichen Erlaubnisnormen:

- Die Verarbeitung kann auf die Einwilligung des Betroffenen gestützt werden (Art. 6 Abs. 1 a) DSGVO).
- Die Verarbeitung von personenbezogenen Daten ist für die Begründung, Durchführung oder Beendigung eines Vertrags oder eines vorvertraglichen Rechtsverhältnisses erforderlich (Art. 6 Abs. 1 b) DSGVO). Ein wichtiger Unterfall ist hier das Beschäftigtenverhältnis, bei dem die Verarbeitung jedoch auf § 26 BDSG nF gestützt wird.
- Die Datenverarbeitung wird durch rechtliche Verpflichtungen des Verantwortlichen erforderlich (Art. 6 Abs. 1 c) DSGVO).
- Die Verarbeitung ist zum Schutz lebenswichtiger Interessen erforderlich (Art. 6 Abs. 1 d) DSGVO).
- Schließlich besteht ein Auffangtatbestand mit der Erlaubnis, personenbezogene Daten zur Wahrung berechtigter Interessen der verantwortlichen Stelle zu verwenden. In diesem Fall ist jedoch eine Abwägung mit anzunehmenden bzw. offensichtlich überwiegenden schutzwürdigen Interessen der Betroffenen durchzuführen (Art. 6 Abs. 1 f) DSGVO.

55 So z. B. bei der Videoüberwachung gem. § 4 BDSG, BVerG, Urteil v. 27.03.2019, 6 C 2.18, Rn. 47, *https://www.bverwg.de/270319U6C2.18.0.*

Die oben genannten rechtlichen Verpflichtungen finden sich in einer Unzahl von Spezialgesetzen, von den Sozialgesetzbüchern bis hin zu öffentlich-rechtlichen Gesetzen wie den Melde- oder Polizeigesetzen. Ausführlichere Datenschutzregeln in nationalen Gesetzen werden jedoch je nach Regelungsinhalt durch die Datenschutz-Grundverordnung verdrängt, soweit diese keine Öffnungsklausel enthält und den Regelungsgegenstand grundsätzlich umfasst.

Neben dem fortbestehenden Verbot mit Erlaubnisvorbehalt und den Erlaubnistatbeständen des Art. 6 Abs. 1 DSGVO sieht die DSGVO ergänzend die Grundsätze der Verarbeitung nach Treu und Glauben und der Verarbeitung in einer für den Betroffenen nachvollziehbaren Weise vor, d. h., dass bei der Prüfung der Rechtmäßigkeit und der Anwendung der Erlaubnisse aus Art. 6 Abs. 1 DSGVO auch die Perspektive des Betroffenen zu berücksichtigen ist.

Neben diesem die Struktur des Datenschutzrechts prägenden ersten Grundprinzip stehen weitere Grundprinzipien, die in Art. 5 Abs. 1 DSGVO niedergelegt sind: die Zweckbindung, die Datenminimierung und Speicherbegrenzung, das Transparenzgebot, das sich ebenfalls aus der Nachvollziehbarkeit für den Betroffenen ableitet, die Richtigkeit der verarbeiteten personenbezogenen Daten und deren Integrität und Vertraulichkeit in Form der angemessenen Sicherheit durch technische und organisatorische Maßnahmen.

Die **Zweckbindung** personenbezogener Daten ist auch eine wesentliche Forderung des Volkszählungsurteils. Die Datenschutz-Grundverordnung hat dieses Kernprinzip im Grundsatz nicht angetastet. Grundsätzlich dürfen personenbezogene Daten nur für den vorab festzulegenden Zweck verwendet werden, für den sie erhoben oder übermittelt worden sind. Der Zweck muss dabei nach einer der oben genannten Alternativen rechtlich zulässig sein. Ist später eine Verwendung der Daten für andere Zwecke beabsichtigt, bedarf es einer neuen Rechtsgrundlage oder einer Abwägung nach den Kriterien des Art. 6 Abs. 4 DSGVO, der dem Verantwortlichen in einem engen Rahmen die Verarbeitung zu einem nicht ursprünglich vorgesehenen Zweck gestattet.

Eine weitere Grenze der Datenverwendung wird durch das **Erforderlichkeitsprinzip** gezogen. In der Datenschutz-Grundverordnung wird dieses zusammenfassende Prinzip durch die Grundsätze der Datenminimierung und der Speicherbegrenzung repräsentiert. Der Wortlaut von Art. 5 Abs. 1 c) DSGVO (Datenminimierung) lautet: » Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.« Damit wird das Erforderlichkeitsprinzip deutlicher formuliert, als es bislang im Bundesdatenschutzgesetz der Fall war, das die Erforderlichkeit vor allem in den Erlaubnistatsbeständen des § 28 Abs. 1 BDSG ausformuliert und durch die Zielvorgabe, die Datenverarbeitung so weit wie möglich zu minimieren (Datensparsamkeit), in § 3a BDSG aF ergänzt hat. Die verantwortliche Stelle darf demnach nur die personenbezogenen Daten erheben und verarbeiten, die für den festgelegten Zweck benötigt werden. Die Erforderlichkeit begrenzt auch die Dauer der Verarbeitung. Ist der Zweck erfüllt und bestehen keine Aufbewahrungspflichten mehr (etwa steuerlicher Natur oder aufgrund gesetzlicher Dokumentationspflichten), sind die personenbezogenen Daten zu löschen oder zu anonymisieren. Dieser Aspekt des Erforderlichkeitsprinzips wird in der DSGVO als Speicherbegrenzung (Art. 5 Abs. 1 e) DSGVO gesondert hervorgehoben. Für die Umsetzung der IT-Sicherheit hat dieses Prinzip besondere Bedeutung, wie im Folgenden noch dargestellt wird, denn es begrenzt bspw. auch die Dauer, über die

Sicherheitsprotokollierungen aufbewahrt werden dürfen, und zwingt, den Auswertungszeitraum zu begründen.

Schließlich gilt das Grundprinzip der **Transparenz**. Der Betroffene soll einschätzen können, was Dritte über ihn wissen (so verkürzt das Volkszählungsurteil). Die Erwägungsgründe der Datenschutz-Grundverordnung lauten hierzu: »Der Grundsatz der Transparenz setzt voraus, dass alle Informationen und Mitteilungen zur Verarbeitung dieser personenbezogenen Daten leicht zugänglich und in klarer und einfacher Sprache abgefasst sind. …« (ErwG 39 S. 3 f.). Dieser Grundsatz wird durch die deutlich verschärften Art. 12 ff. DSGVO konkretisiert. Angesichts der steigenden Komplexität vieler Datenverarbeitungen stellt die Umsetzung dieses Grundsatzes und die Anforderung der Verständlichkeit eine wesentliche Herausforderung bei der DSGVO-Umsetzung dar. Ergänzend dienen individuelle Auskunftsansprüche gegen verantwortliche Stellen (Art. 15 DSGVO) und Benachrichtigungspflichten (bspw. in Art. 19, 21 DSGVO oder Art. 34 DSGVO im Fall von Datenschutzvorfällen) der Transparenz.

Der Grundsatz der **Richtigkeit** der Daten (Art. 5 Abs. 1 d) DSGVO) ist als solcher ebenfalls nicht neu, wird aber durch die Datenschutz-Grundverordnung erstmals als Grundsatz betont. Er bezieht sich auf die Verpflichtung zur Aktualität und zur selbstständigen Berichtigung von, bezogen auf den Zweck, unrichtigen personenbezogenen Daten. Die Verpflichtung zur fortlaufenden Kontrolle wird auf die Erforderlichkeit und auf angemessene Maßnahmen begrenzt. Konkretisiert wird der Grundsatz vor allem durch das Betroffenenrecht auf Berichtigung, Art. 16 DSGVO, oder Löschung, Art. 17 DSGVO, die allerdings eine aktive Rolle des Betroffenen vorsehen.

Für die Informationssicherheit besonders bedeutsam sind die Hervorhebung von **Integrität und Vertraulichkeit** sowie die **Gewährleistung einer angemessenen Sicherheit** der personenbezogenen Daten als Grundsatz in Art. 5 Abs. 1 f) DSGVO. § 9 BDSG aF hat hier zwar ebenfalls bereits eine umfassende Regelung dargestellt, durch die Aufzählung als Grundsatz erfahren die Datensicherheit und die Verpflichtung zu technischen und organisatorischen Maßnahmen jedoch eine deutliche gesetzliche Aufwertung. Die Konkretisierung erfolgt durch Art. 24, 32 DSGVO sowie durch die Pflicht zu Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO, sogenanntes privacy by design und privacy by default).

Für die Praxis zusätzlich bedeutsam ist die in Art. 5 Abs. 2 DSGVO geregelte Nachweis- oder **Rechenschaftspflicht**, die dem Verantwortlichen auferlegt, seine Maßnahmen zur Einhaltung der Anforderungen aus der Datenschutz-Grundverordnung nachweisen zu können. Hieraus ergibt sich eine umfassende Dokumentationspflicht, die zwar in Bezug auf ihre Wahrnehmung nicht näher ausgestaltet ist, jedoch absehbar einen höheren Dokumentationsaufwand für die Verantwortlichen erzeugt. Diese Nachweispflicht umfasst auch die ergriffenen technischen und organisatorischen Maßnahmen sowie die Begründung ihrer Auswahl in Bezug auf die Einschätzung der bestehenden Risiken. Somit wird insbesondere auch der Bereich der Informationssicherheit durch diesen Grundsatz berührt.

Der Datenschutzbeauftragte

Der Datenschutzbeauftragte wird durch die Datenschutz-Grundverordnung weiterhin vorgesehen, die Ausgestaltung der Bestellpflicht bleibt nach Art. 37 Abs. 4 DSGVO den Mitgliedstaaten überlassen. Der Datenschutzbeauftragte hat die Aufgabe, die Rechtskonformität der im Unternehmen stattfindenden Verwendung personenbezogener Daten

zu überwachen. Er berät die Geschäftsführung in Datenschutzfragen, sensibilisiert die Beschäftigten in Datenschutzfragen und wirkt bei der datenschutzkonformen, datensparsamen Gestaltung neuer Verfahren der automatisierten Datenverarbeitung mit. Der Datenschutzbeauftragte ist in seiner Tätigkeit weisungsfrei und zur Verschwiegenheit verpflichtet (Art. 37 ff. DSGVO, §§ 5 f., 38 BDSG nF). Er ist dem Leiter der verantwortlichen Stelle unmittelbar zu unterstellen und genießt dank §§ 38 Abs. 2, 6 Abs. 4 BDSG nF nach deutschem Recht auch weiterhin Kündigungsschutz.

Die Pflicht zur schriftlichen Bestellung des Datenschutzbeauftragten knüpft in Deutschland für nicht öffentliche Stellen nach wie vor an die Beschäftigtenzahl an. Die Pflicht besteht, sobald mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten befasst sind oder sobald eine verantwortliche Stelle personenbezogene Daten in einer besondere Risiken für die Betroffenen begründenden Art und Weise verarbeitet.

Damit der Datenschutzbeauftragte seine Aufgaben wahrnehmen kann, muss die verantwortliche Stelle ihn ausreichend mit Ressourcen ausstatten. Sie muss ihm ein Verzeichnis der Verfahren zur Verfügung stellen, in denen personenbezogene Daten verwendet werden. Der Datenschutzbeauftragte muss auch so in die Prozesse der Stelle eingebunden sein, dass er geeignet auf die Einhaltung von Datenschutzvorschriften hinwirken kann. Beispielsweise muss er dazu rechtzeitig in Prozesse zur Systementwicklung eingebunden werden. Sinnvoll ist in der Regel auch, dass der Datenschutzbeauftragte an der Beantwortung von Auskunftsersuchen beteiligt wird.

Während der Informationssicherheitsbeauftragte lediglich in verschiedenen Standards, z. B. dem BSI-Grundschutz (Kapitel 6), Erwähnung findet, hat der betriebliche Datenschutzbeauftragte mit den Art. 37 ff. DSGVO eine gesetzliche Arbeitsgrundlage. Zwischen dem betrieblichen Datenschutzbeauftragten und dem Informationssicherheitsbeauftragten kann Personalunion bestehen[56], vorausgesetzt die Gestaltung der Funktionen bedingt nicht, dass der Betreffende in einer der beiden Funktionen seine eigene Tätigkeit in der jeweils anderen Funktion zu überwachen hat. Wie im weiteren Verlauf des Kapitels gezeigt wird, bestehen aber durchaus Zielkonflikte zwischen Maßnahmen für Datenschutz und Informationssicherheit. Daher scheint eine Rollentrennung grundsätzlich geboten.

Auftrags(daten)verarbeitung

Die Datenverarbeitung erfolgt heute zunehmend nicht mehr allein durch die verantwortliche Stelle. Vielfach werden Verarbeitungsprozesse an Dritte als Dienstleister ausgelagert. Innerhalb von Konzernen werden häufig Tochtergesellschaften mit der zentralen IT-Betreuung und -Bereitstellung, der Personalverwaltung, Buchhaltung oder Marketingaktivitäten für die gesamte Konzerngruppe beauftragt. Der aktuelle Trend zur Auslagerung von IT-Aufgaben wird durch die Public-Cloud markiert. Eine solche Verlagerung von Infrastruktur- bis hin zu Software-as-a-Service-Angeboten betrifft häufig auch die Verarbeitung personenbezogener Daten. Die Daten sollen aber bei ausgelagerter Verarbeitung genauso geschützt werden, wie dies bei der verantwortlichen Stelle gefordert ist.

Das Datenschutzrecht hat diesem Umstand durch die Regelung der Auftrags(daten) verarbeitung bereits in dem BDSG und der Datenschutz-Richtlinie Rechnung getragen

56 LArbG Hamm, Beschluss v. 8.4.2011, 13 TaBV 92/10 (DuD 2011, 737).

(s. § 11 BDSG aF). Die Datenschutz-Grundverordnung hat dieses Institut als solches erhalten (Art. 28 DSGVO).[57] Die DSGVO-Regelungen nehmen den Auftragsverarbeiter jedoch stärker in die Pflicht. Er hat unabhängig vom Auftraggeber und seinem Auftrag, Datenschutzpflichten zu erfüllen (bspw. eigenes Verarbeitungsverzeichnis, eigene Pflichten und Verantwortung bei der Unterbeauftragung). Bei der Auftragsverarbeitung bleibt der Auftraggeber Verantwortlicher für den gesamten Verarbeitungsprozess – auch für die beim Auftragnehmer verarbeiteten Daten. Voraussetzung hierfür ist, dass der Auftragnehmer die Daten nicht für eigene Zwecke verarbeitet und einer engen Weisungsbindung des Auftraggebers unterliegt. Die Rechte des Betroffenen, bspw. auf Auskunft, Berichtigung oder Löschung, richten sich weiter gegen den Auftraggeber und Verantwortlichen. Der Auftragsverarbeiter gilt nicht als Dritter, sondern als Teil der verantwortlichen Stelle (Art. 4 Nr. 10 DSGVO). Im Gegensatz zum früheren Bundesdatenschutzgesetz gilt dies umfassend und nicht nur für Auftragsverarbeiter innerhalb der EU. Nach der in Deutschland vorherrschenden Auffassung benötigt die verantwortliche Stelle keine weitere Rechtsgrundlage, um die personenbezogenen Daten an den Auftragsdatenverarbeiter weiterzugeben.[58]

Art. 28 Abs. 3 DSGVO gibt nicht länger die Schriftform vor, setzt aber weiter den Abschluss eines Vertrags oder gleichwertigen Rechtsinstruments voraus und stellt zum bisherigen § 11 BDSG aF weitgehend identische inhaltliche Regelungsanforderungen für diesen Vertrag auf. Dazu gehören unter anderem Umfang, Art und Zweck der beabsichtigten Datenverarbeitung, das Weisungsrecht des Auftraggebers, die Verpflichtung, bearbeitende Personen zur Vertraulichkeit zu verpflichten, die Umsetzung der Betroffenenrechte, Unterauftragsverhältnisse, Nachweis-, Kontroll- und Besichtigungsrechte des Auftraggebers und die Abwicklung bei Vertragsende. Gegenstand des Vertrags hat wie bisher die Verpflichtung des Auftragverarbeiters zum Ergreifen angemessener technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO zu sein, genauso wie die vertragsgemäße Unterstützung des Verantwortlichen bei dessen Einhaltung der Verpflichtung zu Umsetzung technischer und organisatorischer Maßnahmen sowie zur Behandlung von Datenschutzvorfällen.

Der Anwendungsbereich der Auftragsdatenverarbeitung schließt auch in der DSGVO **Wartungsdienstleister** ein. Eine diesbezügliche Gesetzesfiktion, die den Wartungsdienstleister grundsätzlich zum Auftragsverarbeiter erklärt[59], enthält die Datenschutz-Grundverordnung zwar nicht mehr. Da der Verarbeitungsbegriff der Datenschutz-Grundverordnung jedoch sehr weit gefasst ist und mit der Offenlegung auch den Einblick des Wartungsdienstleisters erfasst, tritt hier keine Änderung ein. Die Grenze, ab der Einblicksmöglichkeiten von Dienstleistern (bspw. Reinigungsdiensten) zur Auftragsverarbeitung führen, ist wie bisher eine Auslegungsfrage. Ein mögliches Kriterium kann hier darstellen, ob der Einblick planmäßiger und erforderlicher Bestandteil der Dienstleistung ist. Unter Wartungsdienstleistungen fallen Fernwartungen und auch sämtliche Formen der Systembetreuung vor Ort. Auch wenn hierbei Daten nur beiläufig zu Kenntnis genommen und nicht aktiv

57 Die Übersetzung der Verordnung hat jedoch neben anderen auch den Begriff »Auftragsdatenverarbeitung« trotz identischem Wortlaut anderer Sprachfassungen im Deutschen in Auftragsverarbeitung verkürzt.

58 Nach Art. 4 Nr. 9 DSGVO setzt der Empfängerbegriff die Eigenschaft des Dritten nicht mehr voraus, sodass sich der Begründungsweg insoweit verändert, die Entwicklung bleibt im Zuge der Vereinheitlichung der Rechtsauslegung zu beobachten.

59 So zuvor § 11 Abs. 5 BDSG aF.

verarbeitet werden, bestehen Gefährdungen und sind datenschutzrechtliche Schutzmaßnahmen umzusetzen.

Im Auftragsverarbeitungsvertrag sind für die Tätigkeiten vor Ort technisch-organisatorische Maßnahmen zu vereinbaren, die für die Systeme in der Hand des Dienstleisters gelten, mit denen ein Zugriff erfolgt. Solche Vereinbarungen, bspw. zum Zugangs- und Zugriffsschutz, beziehen sich dann u. a. auf Notebooks oder Datenspeicher, die der Dienstleister für seine Arbeiten mitbringt.

Selbstverständlich müssen aber auch von der verantwortlichen Stelle Sicherheitsmaßnahmen gegenüber den Wartungstechnikern ergriffen werden. Der Zugriff auf Bestände mit personenbezogenen Daten ist nach Möglichkeit zu entziehen oder mindestens nach dem Need-to-know-Prinzip zu begrenzen. Werden Remote-Zugriffe verwendet, ist festzulegen, mit welchen Systemen über welche Schnittstellen zugegriffen wird und wie der Transfer geschützt wird. Besondere Bedeutung hat die Kontrolle und Nachvollziehbarkeit der Remote-Zugriffe. Regelmäßig ist eine Freigabe durch den Auftraggeber pro Zugriff und eine möglichst revisionssichere Protokollierung der Tätigkeit, wenigstens aber eine Vereinbarung zur Dokumentation der Zugriffe zu fordern. Die Darstellung erfolgt derzeit in der Praxis noch immer häufig nach dem Katalog der ehemaligen Anlage des Bundesdatenschutzgesetzes aF zu § 9 BDSG, als den dort aufgezählten »Kontrollen«, die den Schutzzielen des Art. 32 DSGVO (s.u.) zugeordnet werden. Aus dem Wortlaut heraus ist es nicht mehr abzuleiten, dass eine solche Liste Vertragsinhalt zu werden hat. Zu regeln ist lediglich die diesbezügliche Verpflichtung des Auftragsverarbeiters, Maßnahmen zu ergreifen. Diese zu dokumentieren, ist eine eigenständige Verpflichtung aus Art. 5 Abs. 2 (Rechenschaftspflicht) und Art. 32 DSGVO. Um als Verantwortlicher jedoch seine DSGVO-Erfüllung bei der Auftragsverarbeitung nachweisen zu können, ist eine Aufnahme wesentlicher Maßnahmen in den Vertrag dennoch wie bislang zu empfehlen.

Grenzen der Auftrags(daten)verarbeitung

Eine Grenze findet die Anwendung der Auftragsdatenverarbeitung, wenn Teile der Verarbeitung durch den Dienstleister für dessen eigene Interessen stattfinden, bspw. bei konzernweiten Auswertungen der von den Tochtergesellschaften weitergegebenen personenbezogenen Daten. In diesem Fall findet neben der Auftragsdatenverarbeitung eine Übermittlung statt. Die Übermittlung darf aber nur erfolgen, wenn sie datenschutzrechtlich zulässig ist, bspw. als im Rahmen der Arbeitsaufgaben des betroffenen Mitarbeiters erforderliche Übermittlung. Kritisch ist eine Auftragsdatenverarbeitung zu bewerten, wenn Träger von Berufsgeheimnissen dadurch geschützte Informationen Dritten offenbaren (§ 203 StGB). Hier hat sich die Rechtslage durch die Ergänzung des § 203 StGB in dessen Absätzen 3 und 4 ebenfalls im Jahr 2018 geändert. Existierte hier zuvor ein erhebliches Rechtsrisiko und wenigstens eine ausgeprägte Grauzone bei der Auslagerung, sind nun Voraussetzung für die Beauftragung von Dienstleistern mit möglichem Einblick geregelt und ist diese nun rechtskonform möglich. Der Dienstleister wird durch die Gesetzesänderung jedoch in die Strafbarkeit nach § 203 StGB mit einbezogen, das Zeugnisverweigerungsrecht und damit auch die Abwehr von Beschlagnahmungen von Daten werden auch auf ihn erstreckt.

Besondere Probleme wirft die Beauftragung von Dienstleistern außerhalb der Europäischen Gemeinschaften und außerhalb der Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum auf. Der Auftraggeber oder der Verantwortliche einer Übermittlung hat hier zunächst ein angemessenes Datenschutzniveau sicherzustellen.

Nach einem Beschluss der Europäischen Kommission können hierzu sogenannte Standardvertragsklauseln genutzt werden.[60] Teil der hierbei eingegangenen Verpflichtungen ist die Benennung von Unterauftragnehmern und die Weitergabe der vereinbarten Datenschutzpflichten auch an diese. Die Möglichkeiten rechtskonformer Vereinbarungen und der datenschutzkonformen Gestaltung stoßen bei Public-Cloud-Diensten in den meisten Fällen an ihre Grenzen, da hier sowohl die klare Benennung der beteiligten Unterauftragnehmer als auch die Lokalisierung der Daten Schwierigkeiten bereitet.[61]

3.2.2 Grundlagen zur Informationssicherheit im Datenschutzrecht

Aus dem Datenschutzrecht resultieren verschiedene Pflichten zur Gewährleistung von Informationssicherheit bezüglich personenbezogener Daten. Sicherheitsmaßnahmen sind grundsätzlich zu treffen, damit die Grundsätze der Zweckbindung, der Integrität und Vertraulichkeit sowie der Transparenz umgesetzt werden: Wären Daten nicht gegen die Verwendung durch Unberechtigte geschützt, könnten sie für beliebige Zwecke und damit unrechtmäßig verwendet werden. Außerdem könnte die verantwortliche Stelle nicht mehr nachvollziehen, wofür die Daten verwendet werden, und damit dem Betroffenen auch nicht mehr korrekt Auskunft erteilen.

Eine direkte gesetzliche Pflicht, die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um eine gesetzeskonforme Datenverwendung sicherzustellen, ergibt sich aus Art. 24 Abs. 1 und 32 DSGVO. Ergänzend ist mit Art. 25 DSGVO, dem Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, noch die Verpflichtung hinzugetreten, nachvollziehbar bereits bei der Gestaltung und Planung von Verarbeitungen Risikofolgen abzuschätzen und zur Umsetzung der DSGVO geeignete technische und organisatorische Maßnahmen zu ergreifen.

Zu ergreifen sind die jeweiligen Maßnahmen allerdings nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Anhaltspunkte zur Angemessenheit von Maßnahmen können die technischen Standards zur Informationssicherheit geben. Der Verhältnismäßigkeitsvorbehalt bedeutet zudem nicht, dass die

---

60 Es werden drei verschiedene Fassungen der Vertragsklauseln angeboten.
Für das Verhältnis **Auftraggeber zu Auftragnehmer**: Beschluss der Kommission vom 5.2.2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragnehmer in Drittländern nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rats, abrufbar unter *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:DE:PDF*
Für die **Übermittlung an einen Dritten als eigene verantwortliche Stelle**: Entscheidung der Kommission vom 15.6.2001 hinsichtlich Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer nach der Richtlinie 95/46/EG, abrufbar unter *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:181:0019:0031:DE:PDF*
Alternativ für die **Übermittlung an einen Dritten als eigene verantwortliche Stelle**: Entscheidung der Kommission vom 27.12.2004 zur Änderung der Entscheidung 2201/497/EG bezüglich der Einführung alternativer Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer, abrufbar unter *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0074:0084:DE:PDF*.

Ähnlich wie der bezüglich der USA durch den EuGH als unzureichend erkannte ehemalige Safe-Harbor-Schutz, sind jedoch auch die Standardvertragsklauseln wie auch der privacy shield als Safe-Harbor-Nachfolger derzeit Gegenstand anhängiger EuGH-Prüfungen.

61 Vertiefend siehe dazu auch [Bed 2013] oder [Bren 2013].

verantwortliche Stelle auf die Maßnahmen bei geringem Schutzbedarf gänzlich verzichten kann: Unter Vorbehalt steht vorrangig das »Wie« der Maßnahmen, nicht das »Ob«. Auf der anderen Seite ist der Maßstab des Art. 32 DSGVO die Berücksichtigung der generellen Verarbeitungszwecke und -umstände, des Verarbeitungsumfangs und der unterschiedlichen Eintrittswahrscheinlichkeit sowie der Schwere des Risikos für die Betroffenen. Auch hier gilt, dass die Vorschrift zusammen mit der Rechenschaftspflicht zu lesen ist. Somit hat der Verantwortliche sich dokumentiert mit den möglichen Risiken seiner Datenverarbeitung für die Betroffenen und einer Einschätzung des Schutzbedarfs auseinanderzusetzen. Die Vorgängerregelung des § 9 BDSG zu technischen und organisatorischen Maßnahmen ist nicht mehr in Kraft. Für die Praxis spielt sie dennoch bezüglich der Darstellung und der inhaltlichen Anforderungen an die Maßnahmen eine Rolle. Die zugehörige Anlage führte acht Anforderungen (Kontrollen) an die interne Organisation auf. Wie oben dargestellt bilden diese nach wie vor für die Praxis ein Grundgerüst für die Darstellung der technischen und organisatorischen Maßnahmen. Dies gilt vor allem für die im Rahmen der Auftragsverarbeitung erforderliche Darstellung der getroffenen Maßnahmen oder für die nach Art. 30 Abs. 1 g) DSGVO erforderliche Darstellung der technischen und organisatorischen Maßnahmen im Rahmen des Verzeichnisses der Verarbeitungstätigkeiten. Ein solches Verzeichnis über die einzelnen Verarbeitungsverfahren haben Unternehmen über einer Mitarbeiterschwelle von 250 Beschäftigten zu führen. Es ist jedoch darüber hinaus sinnvoll, ein solches Verzeichnis auch mit Blick auf die Rechenschaftspflicht und den Nachweis der Rechtmäßigkeitsprüfung der einzelnen Verarbeitungen zu führen.

Anforderungen an Informationssicherheit im Datenschutzrecht

Die konkreten, inhaltlichen Vorgaben aus dem Datenschutzrecht an die Informationssicherheit waren bis Mai 2018 vor allem dem Anhang zu § 9 BDSG aF zu entnehmen. Die verantwortliche Stelle sollten Maßnahmen zur

- Zutrittskontrolle,
- Zugangskontrolle,
- Zugriffskontrolle,
- Weitergabekontrolle,
- Eingabekontrolle,
- Auftragskontrolle,
- Verfügbarkeitskontrolle und
- Zweckbindung durch Datentrennung

ergreifen. Dem vorangestellt war die Anforderung, die interne Organisation datenschutzgerecht zu gestalten. Die Kontrollaufgaben der Liste waren in eine übergreifende Organisation des Datenschutzes einzubetten, die bspw. Arbeitsanweisungen, Verfahrensregelungen, Kommunikationswege und Schulungen umfassen sollte.

Art. 32 DSGVO als neuer Maßstab greift auf keinen solchen Katalog zurück. Im Gegenzug stellt er die individuelle Abwägung des Verantwortlichen und deren Nachvollziehbarkeit in den Vordergrund. Unter dem Gesichtspunkt der Maßnahmen beschränkt sich die DSGVO darauf, einige Maßnahmenarten und Mittel exemplarisch hervorzuheben. Dies betrifft die Pseudonymisierung und Verschlüsselung sowie den Verfügbarkeitsschutz im Sinne einer schnellen Wiederherstellbarkeit von Daten nach Zwischenfällen. Im Übrigen

haben sich die Maßnahmen daran zu orientieren, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Verarbeitungssysteme und Dienste sicherzustellen. Es wird damit also auf die klassischen Informationssicherheitsziele Bezug genommen.

Als Ergänzung fordert Art. 32 DSGVO ein Verfahren zur regelmäßigen Evaluierung der getroffenen Maßnahmen. Hinsichtlich der tatsächlich zu erfüllenden Anforderungen ist die Datenschutz-Grundverordnung damit deutlich weniger konkret gestaltet worden. Aus diesem Grund bietet sich weiterhin die Orientierung an den bisherigen Anforderungsinhalten an, die durch § 9 BDSG aF und seine Anlage etabliert wurden.

Die Kontrollpflichten im Einzelnen

Die **Zutrittskontrolle** soll Unbefugten den »physischen« Zutritt zu den Datenverarbeitungsanlagen verwehren. Da zu den Datenverarbeitungsanlagen nicht nur die Server des Unternehmens gehören, sondern auch die einzelnen Clients und Terminals, ist nicht nur für den Zutrittsschutz des Serverraumes zu sorgen, sondern auch sicherzustellen, dass Rechnerarbeitsplätze innerhalb der verantwortlichen Stelle nicht durch Unbefugte erreicht werden können. Ein weiterer Aspekt der Zutrittskontrolle ist die Einblicksverhinderung, sodass Unbefugten oder Dritten nicht die Beobachtung der Bildschirme von Rechnerarbeitsplätzen möglich ist.

Die **Zugangskontrolle** soll der Verhinderung der unbefugten Nutzung der Datenverarbeitungsanlagen dienen. Im Rahmen der Zugangskontrolle ist der Zugang zu Arbeitsplatzrechnern, Mobilgeräten und Datenträgern an die Identifikation zugelassener Nutzer zu knüpfen.

Teil der Sicherheitsanforderungen ist es, den Zugriff auf personenbezogene Daten auf denjenigen Personenkreis einer verantwortlichen Stelle zu beschränken, dessen Aufgaben den Zugriff erforderlich machen. So muss bspw. in praktisch jeder verantwortlichen Stelle der Zugriff auf die Daten der Personalverwaltung so beschränkt werden, dass er nur den Mitarbeitern der Personalabteilung möglich ist. Die **Zugriffskontrolle** dient dazu, Berechtigungen und Berechtigungsgrenzen zu definieren, umzusetzen und zu kontrollieren.

Besonderes Augenmerk gebührt hierbei der Archivierung personenbezogener Daten, etwa zur Erfüllung von Aufbewahrungs- und Dokumentationspflichten, bspw. nach den Regeln der AO. Nach § 35 Abs. 3 BDSG sind diese Daten, nachdem sie für ihre anderen Verarbeitungszwecke nicht mehr erforderlich sind und nur noch aufbewahrt werden müssen, zu sperren. Die Sperrung bedeutet, dass die weitere Verwendung nur noch für solche Personen möglich sein darf, die Aufgaben mit Archivbeständen erfüllen, sie also z. B. steuerlich prüfen.

Zur Zugriffskontrolle gehört auch der allgemeine Schutz vor unbefugten Lesen, Kopieren, Ändern oder Entfernen der personenbezogenen Daten, also bspw. der Schutz vor Hackern.

Die **Weitergabekontrolle** hat zum einen den Schutz der Daten bei jeder Form des Datentransports vor unbefugten Zugriffen zu gewährleisten, sowohl intern als auch an Dritte oder Auftragnehmer. Zum anderen ist sicherzustellen, dass jederzeit geprüft werden kann, an welche Stellen Übermittlungen vorgesehen sind. Die Weitergabekontrolle ist nicht auf die automatisierte Datenverarbeitung beschränkt, sondern fordert auch den Schutz anderer Medien, bspw. Papierakten. Vor allem bezüglich des internen Austauschs personenbezogener Daten ergeben sich zwangsläufig Überschneidungen mit Zielen und Maßnahmen der Zugriffskontrolle, da hier lediglich der Ausgangspunkt unterschiedlich ist:

Für die Zugriffskontrolle steht die Authentifizierung und Berechtigung im Vordergrund, für die Weitergabekontrolle der Schutz bei Transport und Übertragung.

Die **Eingabekontrolle** soll die Nachvollziehbarkeit der Eingabe, Veränderung oder Entfernung personenbezogener Daten in den Datenverarbeitungssystemen gewährleisten. Sie bedingt damit eine Protokollierung der Änderungen an personenbezogenen Daten. Diese Protokolleinträge enthalten in der Regel nicht nur personenbezogene Daten der Betroffenen, deren Daten geändert werden, sondern auch über die Benutzer, die Aktionen durchgeführt oder Ereignisse ausgelöst haben. Handelt es sich dabei um Beschäftigte einer verantwortlichen Stelle, sind solche Daten häufig zur Überwachung von Mitarbeitern oder zu Leistungskontrollen geeignet. Damit unterliegen die Aufzeichnungen der Mitbestimmung (§ 87 Abs. 1 BetrVG[62]). Gleichzeitig sind auch die einschlägigen Datenschutzvorschriften anzuwenden. Dies gilt insbesondere für den Grundsatz der Zweckbindung, Datenminimierung und Speicherbegrenzung.

Für Protokolle ist daher in besonderem Maße Datensparsamkeit und eine kurzfristige Auswertung geboten. Die Kriterien der Auswertung ergeben sich aus den vor der Aufzeichnung bestimmten Zwecken. Aus den zulässigen Auswertungszielen ergeben sich der notwendige Umfang der Protokollierung, der Rhythmus der Auswertung und die Speicherdauer für Protokolldaten ohne Auffälligkeiten. Ein Aufzeichnen ohne solche Vorgaben ist in der Regel als Vorratsdatenspeicherung zu qualifizieren und nach BDSG nicht zulässig. Der Umfang der Protokolldaten muss auch verhältnismäßig zum Auswertungsziel sein. Daher sind eine umfassende Protokollierung oder eine lange Speicherdauer mit der Begründung, man wolle Unregelmäßigkeiten aufklären können, kritisch zu hinterfragen. In der Regel bietet es sich an, den Umfang der Protokollierung mit dem betrieblichen Datenschutzbeauftragten und der Beschäftigtenvertretung abzustimmen und zu dokumentieren.

Die **Auftragskontrolle** folgt als Pflicht bereits direkt aus Art. 28 DSGVO. Dieser erfordert auch, dass die personenbezogenen Daten beim Auftragnehmer nur den Anweisungen entsprechend verarbeitet werden können. Es ist also sicherzustellen, dass die Weisungsbindung sowohl technisch als auch organisatorisch abgesichert ist.

Die **Verfügbarkeitskontrolle** beinhaltet die Forderung, eine angemessene Datensicherung sicherzustellen, um die Daten gegen eine zufällige Zerstörung oder gegen Verlust zu schützen.

Ziele der **zweckorientierten Datentrennung** sind im Falle der Auftragsdatenverarbeitung die Trennung von Daten verschiedener Auftraggeber bei einem Auftragnehmer. Nur dadurch können Weisungen jeweils unabhängig von den Weisungen anderer Auftraggeber umgesetzt werden. Außerdem müssen Einblicke der Auftraggeber in die jeweils anderen Datenbestände wirksam verhindert werden. Die Forderung ist aber auch auf die interne Verarbeitung anzuwenden. Sie fordert die Trennung von Daten verschiedener interner Verfahren, die unterschiedlichen Zwecken dienen und daher u. a. auch unterschiedlichen Berechtigungen unterliegen. Maßnahmen zu dieser Forderung sind gegebenenfalls auch beim Auftragnehmer zu realisieren.

62 Entsprechend in den jeweiligen Personalvertretungsgesetzen des Bundes und der Länder, siehe auch Abschnitt 3.7.3.

Zusammengefasst bildeten die Vorgaben des Anhangs zu § 9 BDSG aF die wohl am weitesten ins Detail gehende gesetzliche Regelung zu Informationssicherheitspflichten. Es handelt sich dabei aber nicht um eine abschließende Liste, mit der sämtlichen Pflichten Rechnung getragen wird. Spezifische Aspekte der Datenverarbeitung, bspw. besondere Risiken, können weitere Maßnahmen außerhalb des Katalogs erfordern. So könnten bspw. auf die Mitarbeiter gerichtete Sicherheitsmaßnahmen notwendig oder der Verzicht auf Auftragsdatenverarbeitung angebracht sein. Die Forderungen im Anhang bestimmen auch keine tatsächlich zu ergreifenden Maßnahmen und deren Angemessenheit. Hierfür ist auf die gängigen technischen Standards oder Best-Practice-Lösungen der Informationssicherheit zurückzugreifen.

Neben den technischen und organisatorischen Maßnahmen hat zudem die Meldung und Aufklärung von Datenschutzvorfällen durch Art. 33 DSGVO an Bedeutung gewonnen. Dieser regelt eine innerhalb von 72 Stunden zu erfüllende Meldepflicht an die Aufsichtsbehörde, soweit die Verletzung des Schutzes der personenbezogenen Daten ein hohes Risiko für den Betroffenen zur Folge hat. Zu melden sind eine Beschreibung des Ereignisses, insbesondere der betroffenen personenbezogenen Daten, die Zahl der Betroffenen und die der Datensätze. Die wahrscheinlichen Folgen sind darzustellen, ebenso die ergriffenen und vorgeschlagenen Maßnahmen zur Schadensbegrenzung. Durch die enge Meldefrist von 72 Stunden bleibt dem Verantwortlichen wenig Zeit zur Vorfallsanalyse, geregelte Melde- und Analyseprozesse sind hier praktisch zwingend erforderlich.

Durchsetzung von Informationssicherheit im Datenschutzrecht

Zur Durchsetzung der im Datenschutzrecht geforderten angemessenen Informationssicherheit hat der Gesetzgeber, inzwischen mit der Datenschutz-Grundverordnung die Europäische Union, eine Reihe von Druckmitteln und Sanktionen vorgesehen.
Insgesamt ist der Katalog der Bußgeldtatbestände gegenüber dem Bundesdatenschutzgesetz erheblich erweitert worden. Die Verletzung der Pflicht zu technischen und organisatorischen Maßnahmen ist ebenso erfasst wie eine unzureichende Berücksichtigung der Gestaltungsmöglichkeiten im Einführungsstadium der Verarbeitung. Auch eine mangelnde Datenschutzdokumentation stellt einen Bußgeldtatbestand dar, ebenso wie das Versäumnis, einen Vorfall zu melden.

Die Sanktionshöhe ist desgleichen erheblich verschärft. Im Gegensatz zu 50.000 Euro Bußgeldrahmen des BDSG für einfache Verstöße und 300.000 Euro für schwere Verstöße setzt die Datenschutz-Grundverordnung in Art. 83 DSGVO Rahmen von 10.000.000 Euro oder 2 % des weltweit erzielten Jahresumsatzes für Verstöße an, für schwere Verstöße erfolgt nochmals eine Verdoppelung.

Eine unbefugte Offenbarung oder Übermittlung, etwa durch unzureichende Schutzmaßnahmen, fällt ebenso unter die zweite Kategorie wie die Nicht-Befolgung von Anweisungen der Aufsichtsbehörde.

Art. 84 DSGVO gibt den Mitgliedstaaten zudem vor, auch nicht bußgeldbewehrte Verstöße innerstaatlich mit wirksamen, verhältnismäßigen und abschreckenden Sanktionen zu belegen. Hierunter fällt etwa der Straftatbestand des § 42 BDSG nF, der Freiheitsstrafen bis zu drei Jahren bei unbefugten Übermittlungen oder anderweitigen gewerbsmäßigen unbefugten Offenlegungen und bis zu zwei Jahren bei dem Erschleichen von Daten, unberechtigter Verarbeitung gegen Entgelt vorsieht.

Die Aufsichtsbehörden haben außerdem die Möglichkeit, **Vor-Ort-Kontrollen** der verantwortlichen Stellen vorzunehmen und Anordnungen zur Beseitigung festgestellter Verstöße oder von Mängeln bei den technischen und organisatorischen Maßnahmen zu erlassen (Art. 58 DSGVO). Werden die Anordnungen nicht in angemessener Zeit befolgt, kann die Aufsichtsbehörde den Betrieb der mängelbehafteten Verfahren untersagen und z. B. IT-Anwendungen stilllegen lassen.

Dem Betroffenen steht zudem ein eigener **Schadensersatzanspruch** zu, falls ihm Schäden aus einer unzulässigen Datenverwendung entstehen, die auf einer Sorgfaltspflichtverletzung der verantwortlichen Stelle beruht (Art. 82 DSGVO).

3.3 Telekommunikationsrecht

Das Telekommunikationsrecht hat neben der Wettbewerbsregulierung das Ziel, die Nutzerinteressen und das Fernmeldegeheimnis zu schützen (§§ 1, 2 Abs. 2 TKG[63]). Gegenstand des Telekommunikationsrechts ist die Telekommunikation, d. h. der technische Vorgang des Aussendens, Übermittelns, Vermittelns und Empfangens von Nachrichten in Form von elektromagnetischen oder optischen Signalen mittels technischer Einrichtungen (§ 3 Nr. 22, 23 TKG). Zentraler Ansatzpunkt sind außerdem Telekommunikationsdienste: Dabei handelt es sich um in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen. Mittels dieser Dienstdefinition wird die Abgrenzung zu den Telemediendiensten erreicht (zu letzteren siehe Abschnitt 3.4.1).

Für die Informationssicherheit ist das Telekommunikationsrecht von Interesse, weil ähnlich wie für die Banken auch für die Telekommunikationsprovider als Betreiber einer kritischen Infrastruktur besondere Sicherheitsvorgaben in Teil 7 Abschnitt 3 »Öffentliche Sicherheit« des TKG geschaffen wurden. Schutzgüter sind neben der informationellen Selbstbestimmung und der flächendeckenden Verfügbarkeit von Telekommunikation vor allem die Wahrung des ebenfalls grundrechtlich (Art. 10 Abs. 1 GG) geschützten Fernmeldegeheimnisses (§ 88 TKG), also der Vertraulichkeit der Kommunikation und ihrer Umstände. Teile der vorgegebenen Maßnahmen können als Orientierung auch für andere Infrastrukturen herangezogen werden, etwa die Anforderungen an den Inhalt eines Sicherheitskonzepts. Weitere Vorgaben sind praktisch inhaltsgleich zu den entsprechenden Regelungen des Datenschutzrechts, etwa die Definition der Maßnahmenangemessenheit (§ 109 Abs. 2 S. 4 TKG, § 9 BDSG). Auch diese Definition kann damit als übertragbar auch für Informations- und Kommunikationsinfrastrukturen gelten, für die Informationssicherheit nicht gesondert gesetzlich geregelt ist.

Das Thema Telekommunikationsrecht setzt aber auch spezifische rechtliche Grenzen für Sicherheitsmaßnahmen. Die aus dem Telekommunikationsverhalten entstehenden Daten, u. a. auch Standortdaten, bieten besonders umfangreiche Möglichkeiten zur Profilbildung. Betriebliche Sicherheitsmaßnahmen unter Rückgriff auf TK-Daten, vor allem bei einer erlaubten privaten Nutzung, können daher besonders leicht rechtliche Grenzen überschreiten. Diese Aspekte werden im Abschnitt 3.9.2 behandelt.

63 Telekommunikationsgesetz