CB-BEITRAG

Prof. Dr. Beatrix Weber, MLE, und Heinrich Buschermöhle

Rechtssicherheit durch Technische Sicherheit: IT-Compliance als dauerhafter Prozess

Technische Sicherheit erzeugt mehr Rechtssicherheit, wenn sie Haftung und Schäden vermindern oder zu vermeiden hilft. Bei Verstößen gegen Recht und Gesetz drohen erhebliche Bußgelder und ggf. ein Image-Verlust. IT-Compliance als Einhaltung von Recht und Gesetz von und durch IT ist vom technisch Machbaren und wirtschaftlich Vertretbaren abhängig. Technische Sicherheit kann dann mehr Rechtssicherheit erzeugen, wenn für Konzeption und Implementierung der technischen und organisatorischen Maßnahmen die gesetzlichen Anforderungen berücksichtigt, Risiken eingeschätzt und diese beweisbar dokumentiert werden. Hierfür ist ein strukturierter und dauerhafter IT-Compliance Prozess erforderlich.

I. IT-Compliance

1. Begriff

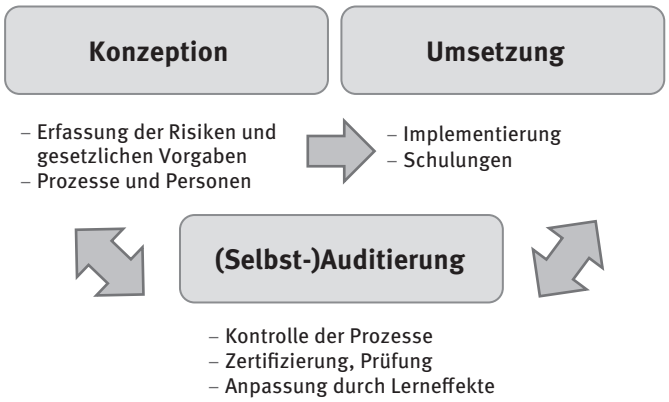
IT-Compliance ist Bestandteil von Compliance, d. h. der Einhaltung von Recht und Gesetz, von organisationsinternen Normen und von ethischen Richtlinien und Werten. *Aufgabe von Compliance* ist die Identifizierung und Bewertung der relevanten rechtlichen Grundlagen sowie möglicher Änderungen und die Bewertung der Risiken bei Nichteinhaltung der rechtlichen Vorgaben. Dabei kann zum einen Compliance *durch* IT, d. h. die Umsetzung von Compliance-Systemen, -Anwendungen oder -Maßnahmen mit Hilfe von IT oder die Compliance *von* IT-Systemen und -Prozessen selbst, d. h. deren originäre Risiken, betrachtet werden.[1]

IT-Compliance umfasst u. a. die Themen Datenschutz, Nutzung von Hard- und Software, Systemen und Anwendungen durch Mitarbeiter wie E-Mail und Internetzugang, IT-Sicherheit, und die Bereiche Beschaffung Prozesse, Finanzen/Steuern, Vertrieb, u. a. Kundendaten, Dokumentenmanagement mit Bezug auf IT-Strukturen. Aufgrund der Querschnittsfunktion der IT im Unternehmen betrifft IT-Compliance nahezu alle Unternehmensbereiche und erfolgt am besten in einer Matrixorganisation.

2. IT-Compliance als Teil des Risikomanagements

Compliance soll als Bestandteil des *Risikomanagements* zur Vermeidung von Haftung für das Unternehmen, seine Organe und Mitarbeiter dienen. Haftung und Schäden materieller und immaterieller Art sollen vermieden oder jedenfalls durch die präventive Erfüllung von Organisationspflichten verringert werden. Eine ausdrückliche Rechtspflicht zu Compliance besteht für die Bereiche der Bank-, Finanz- und Versicherungsdienstleistungen gem. § 25 a KWG, § 33 WpHG, § 29 VAG.[2] Für sonstige Unternehmen wird die Pflicht zu Compliance überwiegend aus §§ 76 Abs. 1, 91 Abs. 2, 93 AktG und § 43 GmbHG abgeleitet. Die Unternehmensleitung hat geeignete Maßnahmen zu treffen, damit Risiken früh erkannt und möglichst abgewendet werden. Darunter fällt auch die Pflicht, für IT-Compliance zu sorgen.[3]

Abbildung 1: IT-Compliance als Teil des Risikomanagements



IT-Compliance ist ohne *IT-Sicherheit* nicht gestaltbar. Der Zugriff auf Daten oder die Integrität von Systemen kann nur geschützt werden, wenn die entsprechenden Sicherheitslösungen dies ermöglichen. Zum Teil wird schon eine „Akzentverschiebung" vom Datenschutz hin zur Datensicherheit postuliert.[4] Auch § 2 Abs. 2 BSIG[5] definiert IT-Sicherheit *in* und *bei* der Anwendung von IT-Systemen:

„Sicherheit in der Informationstechnik im Sinne dieses Gesetzes bedeutet die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit,

1 Schon *Taeger*, in: Taeger/Rath (Hrsg.), IT-Compliance als Risikomanagement-Instrument, 2007, S. 3; *Rath*, in: Taeger/Rath (Hrsg.), IT-Compliance als Risikomanagement-Instrument, 2007, S. 7, 10.

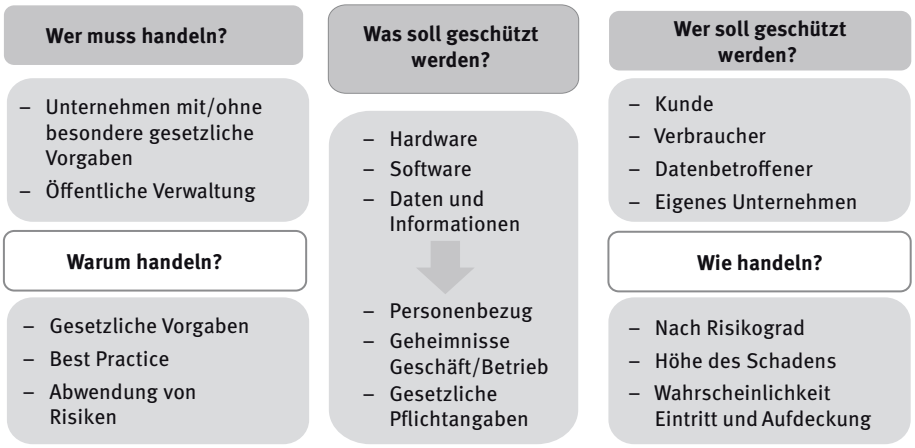
2 § 12 WpDVerOV, § 5 a FinAV.

3 § 91 Abs. 2 AktG; s. dazu im Ganzen *Weber*, in: Schmola/Rapp, Compliance, Governance und Risikomanagement im Krankenhaus, 2016, S. 3–24.

4 *Duisberg*, in: Peters/Kersten/Wolfenstetter, Innovativer Datenschutz, 2012, S. 244, 260.

5 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz).

Abbildung 2: Implementierung IT-Compliance



Unversehrtheit oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen

1. in informationstechnischen Systemen, Komponenten oder Prozessen oder

2. bei der Anwendung von informationstechnischen Systemen, Komponenten oder Prozessen."

So werden z. B. bei der Verarbeitung großer Datenmengen, Big Data bzw. Smart Data, Cloud-Lösungen externer Dienstleister eingesetzt, die zu vermehrtem Angriffspotential bei den externen Speichern sowie den Kommunikationswegen führen. Hier sollen Lösungen zu Verschlüsselung[6] und Zertifizierung[7] eine Hilfe bieten.

Mit dem IT-SicherheitG[8] und der Datenschutzgrundverordnung wird die Verpflichtung zu Compliance nunmehr in Einzelgesetzen geregelt. Betreiber *sog. Kritischer Infrastrukturen* müssen gem. § 8a des *IT-SicherheitsG* angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritschen Infrastrukturen maßgeblich sind. *Anbieter von Telemediendiensten* haben gem. § 13 Abs. 7 TMG ebenso durch technische und organisatorische Vorkehrungen sicherzustellen, dass kein unerlaubter Zugriff auf die für ihre Telemedien genutzten technischen Einrichtungen möglich ist und diese sowohl gegen Verletzungen des Schutzes der personenbezogenen Daten als auch gegen Störungen bzw. Angriffe von außen gesichert sind.

Technischer Bezugspunkt ist in beiden Fällen der *„Stand der Technik"*. Angemessen sind die Vorkehrungen für die Kritischen Infrastrukturen, wenn der Aufwand im Vergleich zu den Folgen eines Ausfalls oder einer Beeinträchtigung nicht unverhältnismäßig ist. Ziel des IT-Sicherheitsgesetzes ist die Schaffung branchenübergreifender Mindeststandards in Bezug auf die Kritischen Infrastrukturen, d. h. für Einrichtungen, Anlagen oder Teile davon in den Sektoren Energie, Informationstechnik, Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen, die von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.[9] Mindestens alle zwei Jahre ist die Erfüllung der organisatorischen und technischen Vorkehrungen nachzuweisen, insbesondere durch Sicherheitsaudits, Prüfungen oder Zertifizierungen.[10] Das IT-Sicherheitsgesetz stellt damit eine gesetzliche Normierung von präventiven Maßnahmen im Bereich der IT-Compliance dar, verknüpft mit technischen Standards, die allerdings nur für die beschriebenen Sektoren gelten. Die Maßnahmen nach dem IT-Sicherheitsgesetz für Telemediendienste sind in ihrer Umsetzung hinsichtlich der relevanten Komponenten und Systeme weiter konkretisierungsbedürftig.[11]

Die *Europäische Datenschutzgrundverordnung*[12] zielt auf den Aufbau von Compliance-Strukturen im Datenschutzbereich. So sind die Verantwortlichen gehalten, eine *interne Strategie* festzulegen und auf dieser Basis geeignete technische und organisatorische Maßnahmen zu ergreifen, die die Grundsätze von „privacy by design" und „privacy by default" bei der Entwicklung und Gestaltung von Diensten, Produkten und Anwendungen unter Verarbeitung von personenbezogenen Daten berücksichtigen. Hierbei sind der Stand der Technik, die Implementierungskosten, Art, Umfang und Zweck der Verarbeitung sowie die Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken abzuwägen, Art. 25 Abs. 1 und ErwGr. 78 DGVO. Für die Sicherheit der Verarbeitung sind die *Risiken zu ermitteln* und *Maßnahmen* zur Eindämmung wie z. B. die Verschlüsselung zu treffen und ein *Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung* aufzubauen. Auch hier wird die Angemessenheit des Schutzniveaus mit Blick auf den Stand der Technik und die Implementierungskosten beurteilt, Art. 32 Abs. 1, ErwGr. 83 DSGVO.

Damit ist eine Tendenz erkennbar, Einzelfall- und anwendungsbezogene Rechtspflichten im Bereich der Informationstechnologien zur Verpflichtung des Aufbaus von präventiven Prozess- und Systemstrukturen, d. h. zu Compliance Systemen, weiterzuentwickeln.

6 Zum Ganzen *Müller-Quade/Huber/Nilges*, DuD 2015, 531 ff.

7 Trusted Cloud Datenschutzprofil, AG „Rechtsrahmen des Cloudcomputing" im Rahmen des Technologieprogramms „Trusted Cloud" des BMWi, Stand: 1.8.2016, abrufbar unter www.trusted-cloud.de/artikel/trusted-cloud-datenschutzprofil (Abruf: 11.8.2016).

8 Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme.

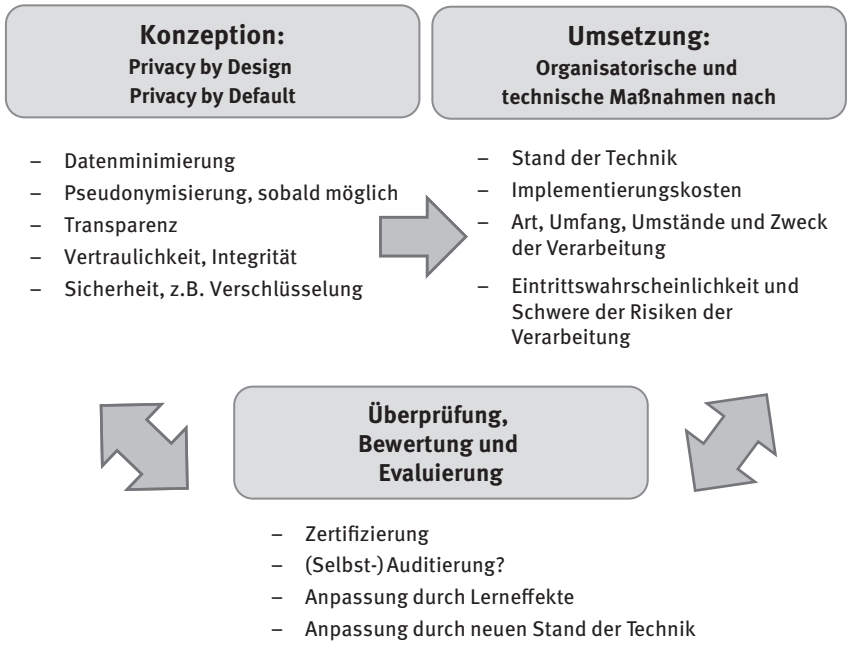
9 § 2 Abs. 10 IT-SicherheitsG.

10 § 8a Abs. 3 IT-SicherheitsG.

11 TeleTrust – Bundesverband IT-Sicherheit e. V., Handreichung zum Stand der Technik i. S. d. IT-Sicherheitsgesetzes, S. 12, abrufbar unter www.teletrust.de/publikationen/broschueren/stand-der-technik/(Abruf: 11.8.2016).

12 DSGVO, VO (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der RL 95/46/EG, ABIEU L 119/1, vom 4.5.2016.

Abbildung 3: Datenschutz-Compliance, Art. 25 und 32 DSGVO



II. Strukturierter IT-Compliance-Prozess

1. Konzeption: Erfassung des Rechtsrahmens

a) Gesetze

IT-Compliance ist von einer Vielzahl von Gesetzen geprägt, die auf ihre Anwendbarkeit hin in jedem Einzelfall geprüft werden müssen.[13] Nur ganz auszugsweise seien IT-SicherheitsG, DSGVO, BDSG, TMG, TKG, BetrVG, UWG, StGB, StPO, BSIG, HGB,[14] AO, KonTraG genannt. Dazu kommen noch Abkommen wie das bisherige Safe Harbour und nunmehr Privacy Shield Abkommen im Bereich der Datenübertragung in die USA. Die Identifizierung und Bewertung des relevanten Rechtsrahmens sowie möglicher Änderungen und die Bewertung der Risiken bei Nichteinhaltung der rechtlichen Vorgaben wird damit im Bereich der IT-Compliance immer komplexer.

b) Branchenstandards, Soft Law

In der IT-Praxis spielt für IT-Compliance die *Rechtsprechung* und das sog. Soft Law, d. h. *branchenübliche Normen und Standards*, eine entscheidende Rolle. Das liegt zum einen daran, dass alle Bereiche der Informationstechnologien einem schnellen Wandel unterworfen sind und zum anderen, dass unbestimmte Rechtsbegriffe in den einschlägigen Gesetzen wie die „erforderlichen technischen und organisatorischen Maßnahmen" ausgefüllt werden müssen. Standards bilden „anerkannte Regeln der Technik ab". Aus ihnen lässt sich ggf. etwas zum in vielen Gesetzen geforderten, höher angesiedelten „Stand der Technik" und zur Beurteilung der Einhaltung der Sorgfaltspflichten für mögliche Haftungstatbestände ableiten.[15]

DIN-Normen sind keine Rechtsnormen, sondern private technische Regeln mit Empfehlungscharakter. Es besteht eine widerlegliche Vermutung, dass DIN- und vergleichbare kodifizierte technische Normen die „allgemein anerkannten Regeln der Technik" widergeben. Diese Vermutung ist jedoch widerlegbar. Insbesondere veraltete DIN-Normen können hinter den anerkannten Regeln der Technik zurückbleiben.[16] Sonstige Branchenstandards können allerdings den Stellenwert sog. „antizipierter Sachverständigengutachten" genießen.[17]

Für die IT-Compliance seien beispielhaft die folgenden Normen, Branchenstandards und Referenzmodelle genannt, ohne dass diese eine abschließende Aufzählung darstellt:[18]

- *ISO 2000*: IT Service Management (ITSM)
- *ISO 27000 Reihe:* IT-Sicherheit
- *ITIL:* IT Infrastructure Library, Sammlung von Best Practices Methoden, Prozessen und Praktiken
- *COBIT:* Control Objectives for Information and related Technology des IT Governance Institutes: IT als Prozesse
- *BSI*-Grundschutzkatalog
- *IDW PS 330:* Abschlussprüfung bei Einsatz von Informationstechnologie
- *BITKOM*-Kompass der IT-Sicherheitsstandards
- *Aktuell für einen Einzelbereich: EU*-Commission: Final Draft Code of Conduct on privacy for mobile health applications[19]

c) Unternehmensinterne Regelungen

Unternehmensinterne Regelungen können aufgrund des Direktionsrechts des Arbeitsgebers gesetzt werden, soweit sie die vertraglich geschuldete Leistung betreffen. Soweit eine Mitbestimmungspflicht besteht, z. B. gem. § 87 Abs. 1 Nr. 6 BetrVG für den Einsatz von

13 Über 25 000 im weitesten Sinne relevant, Schätzung *Rath*, in: Taeger/Rath (Hrsg.), IT-Compliance als Risikomanagement-Instrument, 2007, und in: Wecker/Ohl (Hrsg.), Compliance in der Unternehmerpraxis, 3. Aufl. 2013, S. 131.

14 Für die Archivierung: GoBS: Grundsätze ordnungsgemäßer DVgestützter Buchführungssysteme; GDPdU: Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen.

15 Im Einzelnen s. unten II. 2.

16 BGH, 14.5.1998 – VII ZR 184/97, BB 1998, 1604 NJW 1998, 2814 f.; *Seibel*, NJW 2013, 3000, 3001.

17 *Scherer/Fruth*, CCZ 2015, 9, 13; *Vieweg*, NJW 1982, 2473f m. w. N.

18 Weitere bei *Rath/Sponholz*, in: Behringer (Hrsg.), Compliance kompakt, 3. Aufl. 2013, S. 297 f.; *Rath*, in: Taeger/Rath (Hrsg.), IT-Compliance als Risikomanagement-Instrument, 2007, S. 20.

19 Finaler Entwurf, der Art. 29 Gruppe vorlegt, Stand 7.6.2016.

technischen Überwachungseinrichtungen, bietet sich eine Betriebsvereinbarung an. Ergänzend können einzelvertragliche Regelungen getroffen werden, die sich allerdings in großen Unternehmen für Belegschaft im Bestand nicht anbieten. Üblich ist die Umsetzung in den folgenden Regelungen:

- Arbeits-/Tarifvertrag
- Arbeitsordnung
- Richtlinien zu Datenschutz/-sicherheit und/oder IT-Richtlinien
- Code of Conduct
- Social Media Guidelines
- Richtlinien zu BYOD (Bring Your Own Device)

2. Implementierung von organisatorischen und technischen Maßnahmen

a) Stand der Technik

Der Verstoß gegen die Organisations- und Überwachungspflichten setzt i. d. R. Pflichtwidrigkeit voraus. Eine Pflichtwidrigkeit kann jedenfalls im Bereich der IT-Compliance dann vorliegen, wenn gegen Gesetze verstoßen wird, die bestimmte organisatorische und technische Maßnahmen auf der Grundlage einer Generalklausel, oft des „Stands der Technik", vorschreiben.

„Stand der Technik"[20] ist der „Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen und Betriebsweisen, der nach herrschender Auffassung führender Fachleute das Erreichen des gesetzlich vorgegebenen Zieles gesichert erscheinen lässt. Verfahren, Einrichtungen und Betriebsweisen oder vergleichbare Verfahren müssen sich in der Praxis bewährt haben oder sollten – wenn dies noch nicht der Fall ist – möglichst im Betrieb mit Erfolg erprobt worden sein."[21] Dem entspricht weitgehend die Formulierung *„die besten verfügbaren Techniken"*. Der Stand der Technik ist damit zwischen den „allgemein anerkannten Regeln der Technik" und dem „Stand von Wissenschaft und Technik" angesiedelt.[22] Die allgemeine Anerkennung und praktische Bewährung ist allein für den Stand der Technik nicht ausschlaggebend. Es ist zu ermitteln, was *technisch notwendig, geeignet, angemessen und vermeidbar* ist.[23] Teilweise wird sogar vertreten, dass für den Stand der Technik die allgemeine Anerkennung und praktische Bewährung nicht erforderlich sei, da technische Verfahren erst am Ende eines längeren Prozesses anerkannt seien. Mit dem Stand der Technik werde ausdrücklich auf die Anerkennung verzichtet, um der Dynamik technischer Neuentwicklungen besser gerecht werden zu können.[24]

Zahlreiche Gesetze beziehen sich auf den Stand der Technik, siehe nur § 8a Abs. 1 und 2 IT-SicherheitsG und § 13 Abs. 7 TMG. Die *Einhaltung von Recht und Gesetz*, d. h. der erforderlichen Sorgfaltspflichten und präventiven Maßnahmen, um eine Haftung auszuschließen, hängt dann maßgeblich von der Einhaltung der technischen Vorgaben ab. Tatsächlich ist IT-Compliance damit *rechtlich* zumeist nur nach dem Rahmen geprägt, in der konkreten Anwendung von den *technischen* Gegebenheiten und dem aktuellen Stand der Technik abhängig. Auch eine Auflistung von technischen und organisatorischen Maßnahmen durch den Gesetzgeber kann immer nur einen momentanen Stand abbilden, nicht abschließend sein, und damit keine „Garantien" i. S. e. Rechtssicherheit erzeugen.[25]

Die Frage, ob *„Compliance die Technik beherrscht"*[26] oder „die Technik das Recht" ist theoretisch klar zu formulieren, in der Anwendung aber durchaus differenziert. So gibt der Gesetzgeber in den Bereichen Datenschutz und Datensicherheit über Art. 2 Abs. 1, Art. 1 Abs. 1 GG und das BDSG einen Rahmen vor, in dem sich bestimmte Wertentscheidungen widerspiegeln.[27] Grundsätzliche Wertekonflikte wie bei der Ausgestaltung des Rechts auf informationelle Selbstbestimmung als Schutzrecht und „Recht auf ein analoges Leben"[28] oder als „Recht der digitalen Souveränität"[29] oder des „Rechts auf Ökonomisierung der eigenen Daten", die sich im Widerstreit zwischen den Prinzipien der Datensparsamkeit und Zweckbindung vs. Smart Data-Anwendungen als Innovationsmotor und Technologien zu mehr Nachhaltigkeit und Effizienz äußern, sind in der Auslegung des GG[30] und dann auf der Ebene des Gesetzgebers zu lösen. Compliance, die Einhaltung von Recht und Gesetz, setzt darunter an. Die konkreten Systeme, Anwendungen, Protokolle und Formate schließlich sind Teil der Implementierung entsprechender Maßnahmen, müssen sich in der Praxis entwickeln und so zum Stand der Technik beitragen.[31] Auch die Risikoanalyse als Kernstück von IT-Compliance wird durch diese vom Gesetzgeber getroffenen Wertentscheidungen begrenzt. Konkrete Kriterien für die Risikoentscheidungen in der Praxis sind hier weiter zu erarbeiten.[32]

Rechtstechnisch gesehen, wird bei der sog. einstufigen Vermutung die technische Regel, bei deren Einhaltung die Erfüllung der Norm widerleglich vermutet wird, im Gesetz selbst bezeichnet. Bei der sog. zweistufigen Vermutung wird in der Norm eine Institution mit der Befugnis ausgestattet, die technische Regel zu setzen.[33] Die Verwendung von Generalklauseln sichert zwar die laufende mögliche Anpassung an die technische Entwicklung, verlagert aber die verbindliche Konkretisierung auf die administrativen oder standardsetzenden Institutionen bzw. die Rechtsprechung.[34] Für die Unternehmen als

---

20 Zum Begriff „Stand der Technik" bei der Produkthaftung für Software *Taeger*, Außervertragliche Haftung für fehlerhafte Computerprogramme, 1995, S. 236 ff.

21 BMJV, Handbuch der Rechtsförmlichkeit, Rn. 256, abrufbar unter http://hdr.bmj.de/page_b.4.html (Abruf: 11.8.2016).

22 BMJV, Handbuch der Rechtsförmlichkeit, Rn. 256, abrufbar unter http://hdr.bmj.de/page_b.4.html (Abruf: 11.8.2016).

23 BVerfG, 8.8.1978 – 2 BvL 8/77, NJW 1979, 359, 362, Kalkar-Entscheidung „Schneller Brüter".

24 *Seibel*, NJW 2013, 3000, 3003 m. w. N.

25 These 4.5., Smart Data Begleitforschung, FZI: Smart Data – Smart Privacy: Impulse für eine interdisziplinär rechtlich-technische Evaluation, Technical Report des BMWi-Technologieprogramms „Smart Data – Innovation aus Daten", 2015, S. 15. Prof. *Weber* ist Mitglied der Begleitforschung Recht im BMWi.

26 *Scherer/Fruth*, CCZ 2015, 9, 16.

27 BMWi: Grünbuch Digitale Plattformen, Mai 2016, S. 54, abrufbar unter www.bmwi.de/BMWi/Redaktion/PDF/G/gruenbuch-digitale-plattformen,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf (Abruf: 11.8.2016); IT-Gipfel 2015: Leitplanken digitaler Souveränität, abrufbar unter www.bmwi.de/BMWi/Redaktion/PDF/IT-Gipfel/it-gipfel-2015-leitplanken-digitaler-souveraenitaet,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf (Abruf: 11.8.2016).

28 *Heiko Maas*, Infoveranstaltung des BMJV, Berlin 21.7.2016, abrufbar unter www.bmjv.de/SharedDocs/Artikel/DE/2016/07202016 _360grad_ InternetDerDinge.html (Abruf: 11.8.2016).

29 BMWi, Digitale Strategie 2015, S. 33, abrufbar unter www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/digitale-strategie-2025,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf (Abruf: 11.8.2016); Grünbuch Digitale Plattformen (Fn. 27), S. 56.

30 Volkszählungsurteil, BVerfG, 15.12.1983 – 1 BvR 209/83, 1 BvR 484/83, 1 BvR 440/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83, BVerfGE 65, 1, Rn. 169 f., 172; Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme, BVerfG, 27.2.2008 – 1 BvR 370/07, 1 BvR 595/07, NJW 2008, 822.

31 S. dazu *Raabe*, in: Smart Data Begleitforschung, FZI, Smart Data – Smart Privacy? 2015, S. 5.

32 Smart Data Begleitforschung, FZI, Smart Data – Smart Privacy? 2015, S. 14.

33 BMJV, Handbuch der Rechtsförmlichkeit, Stand 1.8.2016, Rn. 259 f., abrufbar unter http://hdr.bmj.de/page_b.4.html (Abruf: 11.8.2016).

34 BVerfG, 8.8.1978 – 2 BvL 8/77, NJW 1979, 359, 362, Kalkar-Entscheidung „Schneller Brüter".

Rechtsanwender entsteht damit eine laufende Unsicherheit, die auch eine permanente Überprüfung erfordert, ob die getroffenen technischen Maßnahmen und Prozesse dem Stand der Technik entsprechen oder branchenüblich sind.

Praxisbeispiel: Start up Projekt „wdd" als Motor für den Stand der Technik

Start ups rücken immer mehr als Innovationstreiber in den Blickpunkt. Nur knapp ein Fünftel der Start ups sieht in ihren Produkten und Diensten kein Innovationspotential.[35] Start ups bieten auch eine gute Plattform, um technische Maßnahmen zu erproben, die den Stand der Technik weiterentwickeln oder sogar ein Best Practice Beispiel setzen können. Ein Beispiel ist die Web Defacement Monitoring Solution, mit der automatisiert unerwünschte Veränderungen von Webseiten erkannt werden können, die IT-Verantwortlichen benachrichtigt und Compliance-Reports erstellt werden können.[36]

b) Weitere Faktoren

Neben dem Stand der Technik können weitere Faktoren wie die Kosten der Implementierung, Art, Umfang und Umstände und die Eintrittswahrscheinlichkeit sowie die Schwere der Risiken zu berücksichtigen sein, z. B. gem. Art. 25 Abs. 1, 32 Abs. 1, ErwGr 83 DSGVO.

Die *wirtschaftliche Zumutbarkeit* ist im Rahmen einer Verhältnismäßigkeitsprüfung zu berücksichtigen. Maßnahmen sind angemessen, wenn der erforderliche Aufwand für organisatorische und technische Maßnahmen nicht außer Verhältnis zu den Folgen der Nichtbeachtung ist. Die Beurteilung nach *Art, Umfang, Umstände und Zweck der Verarbeitung* der Daten setzt dem Stand der Technik nichttechnische Kriterien entgegen, die in die Abwägung einfließen. Mit Würdigung der *Eintrittswahrscheinlichkeit und Schwere der Risiken* werden typische Compliance-Elemente aufgenommen.[37]

3. Evaluierung

Nach Konzeptionierung und Implementierung ist dritter Baustein von Compliance-Management-Systemen die Evaluierung der getroffenen Maßnahmen. Dies kann im Wege der Zertifizierung oder der Auditierung, ggf. durch Dritte, geschehen. Die Wahl einer Evaluierungsmethode ist bisher gesetzlich nicht allgemein vorgeschrieben. Geprüft wird i. d. R. nicht, ob ein Unternehmen Recht und Gesetz einhält, sondern ob das vorgefundene Compliance-Management-System angemessen und wirksam mit Blick auf die angestrebten Compliance-Ziele und -Risiken ist. Im Sinne eines fortlaufenden Prozesses sind Anpassungen des Compliance-Management-Systems aufgrund der Erkenntnisse und Lerneffekte, aber auch aufgrund von Veränderungen des rechtlichen Umfelds oder des Stands der Technik vorzunehmen.[38]

Für Compliance allgemein existieren derzeit die folgenden Prüfstandards:

- *ISO 19600:* Compliance Management Systeme
- *ISO 26000:* Corporate Social Responsibility
- *Zertifizierung Hamburger Compliance Modell*
- *Zertifizierung TÜV*
- *IDW PS 980:* Freiwilliger Prüfstandard zu Compliance Management Systemen

Diese können künftig durch Prüf- oder Zertifizierungssysteme in Einzelbereichen ergänzt werden.[39]

III. Fazit: Rechtssicherheit durch Technik als dauerhafter Prozess

Technische Sicherheit kann Rechtssicherheit erzeugen, wenn die organisatorischen und technischen Maßnahmen in einem strukturierten Compliance-Prozess erfolgen. Dazu ist die Erfassung der technischen, rechtlichen, finanziellen und sonstigen Risiken nach Umfang und Eintrittswahrscheinlichkeit erforderlich. Welche Maßnahmen zur Abwendung dieser Risiken getroffen werden sollten, ist nur durch Erfassung des rechtlichen Rahmens, des Stands der Technik und in Abwägung mit den Kosten und ggf. sonstigen Faktoren zu beurteilen. Datenschutzgrundverordnung und IT-SicherheitG sowie die weiter zu erwartenden Verordnungen und technischen Standards bieten nur Anhaltspunkte. Um Rechtssicherheit für das einzelne Unternehmen anzustreben, ist die Dokumentation der Sachverhalte, der einschlägigen Gesetze und Standards, des Stands der Technik und die Implementierung sowie regelmäßige Überprüfung der getroffenen technischen und organisatorischen Maßnahmen erforderlich. Ob die getroffenen Maßnahmen den rechtlichen Anforderung an Sorgfaltspflichten entsprechen und damit haftungsvermeidend wirken können, wird sich im Einzelnen erst durch Setzung technischer Standards und in der Anwendung durch die Rechtsprechung zeigen.

AUTOREN

Prof. Dr. Beatrix Weber, *MLE, ist Professorin für Gewerblichen Rechtsschutz und IT-Recht und Leiterin der Stabsstelle Compliance an der Hochschule für Angewandte Wissenschaften Hof sowie der Forschungsgruppe „Recht in Nachhaltigkeit, Compliance und IT" am Institut für Informationssysteme. Schwerpunkte: Rechtsfragen der Digitalisierung, Industrie 4.0, Datenschutz, Law Process Modeling und Compliance. Die Einführung von CMS hat sie in Konzernunternehmen, KMU und in der Hochschule begleitet.*

Heinrich Buschermöhle *engagiert sich seit Juli 2015 als Geschäftsführer der Blue Eye Solutions GmbH, ein Spin Off der]init[AG, im Bereich IT-Compliance und Cybercrime mit einer Lösung zur effizienten Erkennung von unerwünschten und ungewollten Veränderungen auf Webseiten. Bei der]init[AG betreut er als Mitgründer Betriebsprojekte im eigenen BSI zertifizierten Rechenzentrum.*

35 European Startup Monitor 2015, abrufbar unter http://europeanstartupmonitor.com/fileadmin/country_report/country_report_ germany. pdf (Abruf: 11.8.2016).

36 wdd wurde 2015 als Tool für IT-Compliance in einem gemeinsamen Projekt der Blue Eyes Solution und des Instituts für Informationssysteme, iisys, der Hochschule Hof, Forschungsgruppe Recht in Nachhaltigkeit, Compliance und IT, entwickelt: www.web-defacement-detector.de (Abruf: 11.8.2016).

37 S. oben: IT-Compliance als Teil des Risikomanagements.

38 Zum Ganzen *Weber*, in: Schmola/Rapp, Compliance, Governance und Risikomanagement im Krankenhaus, 2016, S. 3–24.

39 Art. 42 i. V. m. 25 Abs. 3 DSGVO.