Trusted Cloud

Kompetenzzentrum Trusted Cloud

Leitfaden – Haftungsrisiken beim Cloud Computing

Nr. 10

Arbeitsgruppe „Rechtsrahmen des Cloud Computing“

Cloud Computing kann in Deutschland nur wirtschaftlich erfolgreich sein, wenn die rechtlichen Rahmenbedingungen eine effiziente Nutzung von Cloud-Diensten ermöglichen. Ein innovationsfreundlicher Rechtsrahmen ist daher von besonderer Bedeutung. Für die rechtlichen Aspekte von Cloud Computing hat das Bundesministerium für Wirtschaft und Energie (BMWi) daher innerhalb des Kompetenzzentrums Trusted Cloud eine eigene Arbeitsgruppe einrichten lassen.

In der Arbeitsgruppe „Rechtsrahmen des Cloud Computing“ erarbeiten Experten aus Wirtschaft, Anwaltschaft und Wissenschaft sowie Vertreter aus Datenschutzbehörden gemeinsam mit Projektbeteiligten aus dem Trusted-Cloud-Programm Lösungsvorschläge für rechtliche Herausforderungen. Sie wird geleitet von Prof. Dr. Georg Borges. Themenschwerpunkte sind u. a. Datenschutz, Vertragsgestaltung, Urheberrecht sowie Haftungsfragen und Strafbarkeitsrisiken. Darüber hinaus wird ein Pilotprojekt zur datenschutzrechtlichen Zertifizierung von Cloud-Diensten durchgeführt, das Impulse für die rechtssichere Nutzung von Cloud Computing und die Gewährleistung eines hohen Datenschutzniveaus setzen soll.

Inhaltsverzeichnis

Vorwort **6**

1 Einführung **7**

2 Haftung des Cloud-Anbieters für die eigene Leistung **8**
2.1 Leistungsstörungen im Rahmen vertraglicher Leistungspflichten 8
2.2 Beeinträchtigung von Verfügbarkeiten aufgrund des Ausfalls von Unterlieferanten (§ 278 BGB) und Konnektivitätsausfällen 10

3 Konsequenzen bei Datenpannen (insbesondere Verlust, Veränderung, unbefugter Zugriff) **11**
3.1 Zivilrechtliche Haftung 11
3.2 Straftaten und Ordnungswidrigkeiten 12
3.3 Mitteilungspflichten bei Datenpannen 13

4 Vertragliche Haftungsbeschränkungen **15**
4.1 Dem AGB-Recht unterfallende Standardverträge 15
4.2 Individuell ausgehandelte Cloud-Verträge 17

5 Haftung für rechtswidrige Anwenderinhalte und regulatorische Verstöße **19**
5.1 Haftung für rechtswidrige Anwenderinhalte 19
5.2 Mithaftung für regulatorische Verstöße 21

6 Haftung des Cloud-Anwenders **23**
6.1 Vertragliche Haftung gegenüber dem Cloud-Anbieter 23
6.2 Haftung für rechtswidrige Inhalte 25
6.3 Haftung für Verstöße gegen das Datenschutzrecht 26
6.4 Haftung für Verstöße gegen Spezialgesetze 27

7 Zusammenfassung **28**

Autoren **30**

Vorwort

Cloud Computing bietet wesentliche Vorteile für die Datenverarbeitung, nicht zuletzt in kleinen und mittelgroßen Unternehmen. Daher überrascht es nicht, dass sich weltweit ein Trend zur Nutzung von Cloud Computing entwickelt hat, das auch die technisch-organisatorische Grundlage neuer Entwicklungen, wie „Industrie 4.0“, darstellt.

Mit dem Einsatz von Cloud Computing können, nicht anders als bei klassischem IT-Outsourcing, Haftungsrisiken für Anbieter wie Anwender von Cloud-Diensten einhergehen. Da Cloud Computing eine recht neue Form der IT-Dienstleistung ist, besteht in der Praxis derzeit oft noch Unsicherheit über den Umfang der Risiken und die Strategien zu ihrer Vermeidung.

Der vorliegende Leitfaden soll Anbieter und Anwender von Cloud-Diensten darin unterstützen, relevante Haftungsrisiken zu erkennen und diese, soweit möglich, zu vermeiden oder durch adäquate Vertragsregeln angemessen zwischen den Beteiligten zu verteilen. Er richtet sich insbesondere an Entscheider sowie Mitglieder von Rechtsabteilungen in Unternehmen, die Cloud Computing anbieten oder nutzen möchten.

Der Leitfaden befindet sich auf dem Stand März 2015 und wurde im Rahmen der Arbeitsgruppe „Rechtsrahmen des Cloud Computing“ im Kompetenzzentrum Trusted Cloud erarbeitet. Die von Prof. Dr. Georg Borges geleitete Arbeitsgruppe ist Bestandteil des Technologieprogramms „Trusted Cloud“ des Bundesministeriums für Wirtschaft und Energie (BMWi). Weitere Informationen finden Sie unter www.trusted-cloud.de.

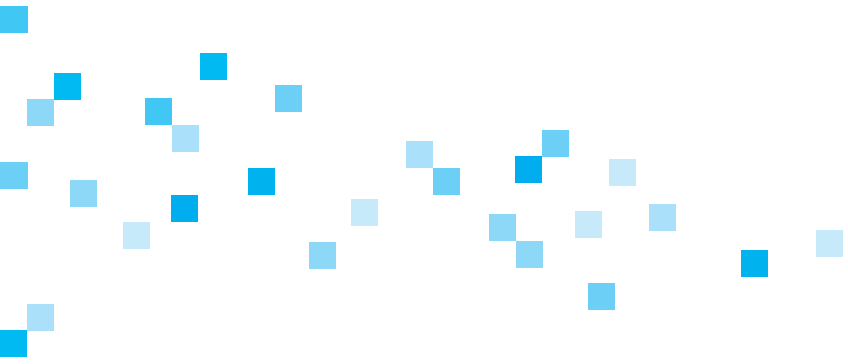
Die Autoren hoffen, dass der Leitfaden eine schnelle Orientierung ermöglicht und Unterstützung bei der Bereitstellung und Inanspruchnahme von Cloud-Diensten bietet.

Dr. Marc Hilber, LL.M. (Illinois)

Leiter der Task Force „Vertrag & Lizenzen“
der AG „Rechtsrahmen des Cloud Computing“

Prof. Dr. Georg Borges

Leiter der AG „Rechtsrahmen
des Cloud Computing“



1 Einführung

1 Eine der wichtigsten Fragen des Cloud Computing betrifft die damit verbundenen Haftungsrisiken. Cloud-Anwender, Cloud-Anbieter und Unterauftragnehmer sehen sich Haftungsrisiken ausgesetzt, die vor Vertragsschluss bewertet und beim Business-Case berücksichtigt werden müssen. Haftung bedeutet in diesem Zusammenhang die Verantwortlichkeit für den Schaden eines anderen. Erleidet also der Cloud-Anwender einen Schaden, stellt sich für ihn die Frage, ob er Ersatz für diesen vom Cloud-Anbieter oder von einem Unterauftragnehmer verlangen kann. Entsteht umgekehrt ein Schaden beim Cloud-Anbieter oder bei einem seiner Unterauftragnehmer, fragt dieser sich ebenso, ob er vom Anwender Ersatz verlangen kann.

Der vorliegende Leitfaden stellt wesentliche Haftungsaspekte aus Sicht des Cloud-Anwenders und des Cloud-Anbieters dar. Der Darstellung der Haftungsrisiken liegen vornehmlich sog. Business-Clouds zugrunde, bei denen der Cloud-Anwender keine Privatperson ist, sondern die Cloud zu Geschäftszwecken nutzt.

2 Im Vordergrund steht die Haftung des Cloud-Anbieters gegenüber dem Cloud-Anwender. Für die Haftung des Cloud-Anbieters ist in erster Linie relevant, ob er die Cloud-Leistung vertragsgerecht erbracht hat oder nicht. Daher werden Haftungsansprüche des Cloud-Anwenders gegen den Cloud-Anbieter wegen Fehlern in seiner Leistung (siehe Ziffer 2), insbesondere wegen Datenverlusten (siehe Ziffer 3), erörtert. Eine große Bedeutung haben vertragliche Haftungsausschlüsse bzw. -grenzen (siehe Ziffer 4). Zudem stellt sich die Frage, ob der Cloud-Anbieter aufgrund einer Verletzung von Rechten Dritter durch vom Cloud-Anwender eingestellte Inhalte oder aufgrund von regulatorischen Verstößen haftet (siehe Ziffer 5).

3 Auch die Haftung des Cloud-Anwenders ist zu bedenken. So kann sich die Konstellation ergeben, dass der Cloud-Anwender seinerseits pflichtwidrig handelt oder in sonstiger Weise eine Haftung gegenüber dem Cloud-Anbieter begründet, etwa durch das Einstellen rechtswidriger Inhalte in die Cloud. Auch hier stellt sich die Frage, ob er ggf. durch eine vertragliche Haftungsbeschränkung geschützt werden sollte (siehe Ziffer 6). Die Zusammenfassung der wesentlichen Aspekte (siehe Ziffer 7) bietet dem eiligen Leser einen Einstieg in die verschiedenen Kapitel des Leitfadens.

Der Leitfaden soll in erster Linie eine Orientierungshilfe für die Praxis bieten. Daher wird die Darstellung der Rechtsfragen durch Hinweise zur praktischen Gestaltung („Praxishinweis“) ergänzt.

2 Haftung des Cloud-Anbieters für die eigene Leistung

2.1 Leistungsstörungen im Rahmen vertraglicher Leistungspflichten

4 Für die vertragliche Haftung des Cloud-Anbieters ist der Ausgangspunkt das gesetzliche Leitbild des zugrunde liegenden Vertragstypus. In Fortführung der ASP-Entscheidung des Bundesgerichtshofs (BGH) vom 15.11.2006[1] wird man Cloud-Angebote im Bereich Infrastructure as a Service (IaaS), Platform as a Service (PaaS) und Software as a Service (SaaS)[2] grundsätzlich als typengemischte Verträge mit überwiegend mietvertraglichen Elementen einordnen können.[3] Das schließt nicht aus, dass einzelne Vertragsbestandteile oder bestimmte Cloud-Modelle aufgrund ihrer Natur anders zu bewerten sein können.

5 Der gesetzliche Haftungsrahmen für Schäden aus Schlechtleistung und sonstiger Vertragsverletzung ist – außer durch die allgemeinen Haftungsregeln – damit nach deutschem Recht primär durch das Mietvertragsrecht bestimmt.[4]

6 Die vertraglich geschuldete Leistung unterscheidet sich je nach Art des Cloud-Angebots, ist aber typischerweise durch die Bereitstellung von Software-Funktionalitäten (beim SaaS) oder Infrastruktur-Dienstleistungen (beim PaaS und IaaS) und der damit verbundenen hohen Verfügbarkeiten (zum Teil ausdrücklich oder jedenfalls aufgrund von Service-Level-Agreements [SLA]) charakterisiert. Das ist auch dringend empfehlenswert, da für die spezifischen Cloud-Leistungen bedarfsgerechte Regelungen erforderlich sind und das Mietrecht des BGB, das grundsätzlich von einer ständigen Verfügbarkeit der Mietsache ausgeht, dies nicht abbildet. Bei der Gestaltung der SLA ist aber darauf zu achten, dass die Verfügbarkeit der Cloud-Services angemessen gestaltet wird und Einschränkungen damit im Einklang mit dem AGB-Recht bleiben (insbesondere § 307 BGB). Denn wenn Cloud-Verträge mehrfach und standardisiert verwendet werden, ist das AGB-Recht auch im kaufmännischen Verkehr zu beachten (siehe nachfolgend Ziffer 4).

7 **Praxishinweis**
Die Beschreibung des Inhalts und insbesondere der Verfügbarkeiten eines Cloud-Dienstes bildet die maßgebliche Grundlage für den vertraglichen Haftungsrahmen. Nur eine präzise Darstellung der geschuldeten Leistungskomponenten ermöglicht eine passende Zuordnung zu vertraglichen Anspruchsgrundlagen.

8 Bleibt die tatsächliche Leistung hinter der vertraglich geschuldeten zurück (einschließlich etwaiger Unterbrechungen der Verfügbarkeit des Cloud-Dienstes), ist dies grundsätzlich als Sachmangel einzuordnen (§ 536 Abs. 1 BGB).

1 BGH, Urteil vom 15.11.2006 – XII 120/04, abgedruckt in NJW 2007, 2394.
2 Zu den verschiedenen Service-Modellen des Cloud Computing siehe z. B. die Ausführungen des Bundesamtes für Sicherheit in der Informationstechnik unter https://www.bsi.bund.de/DE/Themen/CloudComputing/Grundlagen/Grundlagen_node.html (zuletzt aufgerufen am 17.03.2015).
3 Kompetenzzentrum Trusted Cloud: Leitfaden – Vertragsgestaltung beim Cloud Computing (Stand: März 2014), S. 17 (abrufbar unter: http://www.trusted-cloud.de/media/content/140317_Vertragsleitfaden_gesamt_RZ_Ansicht.pdf, letzter Abruf 17.03.2015).
4 Bei grenzüberschreitenden Sachverhalten kommt man gemäß Art. 3 der VO (EG) 593/2008 („Rom I-Verordnung") jedenfalls dann zur Anwendung deutschen Rechts, wenn sich die Vertragsparteien durch vertragliche Rechtswahl geeinigt haben.

9 Ein Rechtsmangel liegt dagegen vor, wenn der Gebrauch der Mietsache dem Cloud-Anwender durch das „Recht eines Dritten ganz oder zum Teil entzogen“ wird (§ 536 Abs. 3 BGB). Dies ist z. B. bei Unterlassungsansprüchen eines Dritten wegen Schutzrechtsverletzung gegen den Cloud-Anwender der Fall. Der Cloud-Anbieter haftet ebenfalls, wenn wegen der Verletzung von Rechten Dritter ein Unterlassungsanspruch gegen ihn geltend gemacht wird und er daher die geschuldete Leistung nicht erbringen kann.[5]

10 **Praxishinweis**
Die für den Cloud-Dienst eingesetzten Software-Komponenten müssen für die beabsichtigte Nutzung ausreichend lizensiert sein, d. h., der Cloud-Anbieter verfügt über umfassende Nutzungsrechte an den eingesetzten Programmen, die den jeweiligen Geschäftszweck ggf. bis hin zur Bereitstellung zur gewerblichen Nutzung durch Dritte abdecken. Die zugehörigen Nutzungsbedingungen auch etwaiger Open-Source-Software sollten im Hinblick auf etwaige Einschränkungen überprüft werden, um einen späteren Rechtsmangel und damit Schadensersatzanspruch des Cloud-Anwenders zu vermeiden.

11 Das mietvertragliche Gewährleistungsrecht sieht für Sach- und Rechtsmängel Ansprüche auf Mietminderung (§ 536 BGB) und bei anfänglichen Mängeln verschuldensunabhängigen Schadensersatz (§ 536a Abs. 1 BGB) vor.

12 **Praxishinweis**
Wenn der Cloud-Dienstleister die Möglichkeit einer mietrechtlichen Minderung der Vergütung auch bei unverschuldeter Nicht- oder Schlechtleistung transparenter regeln möchte, kann er entsprechende Service-Levels mit Pönalen (Service-Credits) bereits vertraglich vorsehen. Allerdings dürfen diese Regelungen gerade in allgemeinen Geschäftsbedingungen nicht dazu führen, dass die mietvertraglichen Rechte des Cloud-Anwenders bei einem Leistungsausfall damit faktisch ausgehebelt werden, sondern sie sollten eine angemessene Kompensation in Relation zur Vergütung und zum Risiko darstellen.

13 Daneben kommen im Falle des Datenverlusts und unbefugter Datenveränderungen auch konkurrierende deliktische Ansprüche nach Maßgabe der §§ 823 ff. BGB in Betracht (dazu noch näher unten Ziffer 3).[6] In vielen Fällen handelt es sich dabei nicht um eine die mietvertragliche Hauptleistung betreffende Leistungsstörung, sondern lediglich um eine Verletzung vertraglicher Nebenpflichten, bei denen nach deutschem Recht Schadensersatz gemäß § 280 Abs. 1, § 241 Abs. 2 BGB zu leisten ist.

5 Da die urheberrechtlich relevanten Handlungen (Vervielfältigung der Software auf den Systemen des Anbieters und Zurverfügungstellung der Software an die Cloud-Kunden) in erster Linie dem Cloud-Anbieter zuzurechnen sind, ist die Inanspruchnahme des Cloud-Anbieters die wahrscheinlichere Variante. Siehe zu den urheberrechtlichen Aspekten des SaaS Kompetenzzentrum Trusted Cloud: Arbeitspapier – Lizenzierungsbedarf beim Cloud Computing (Stand: November 2012), abrufbar unter: http://www.trusted-cloud.de/media/content/140228_Arbeitspapier_Lizenzen_gesamt_RZ.pdf.

6 Auch hier gilt, dass deutsches Deliktsrecht grundsätzlich anwendbar ist, wenn der Schaden auf dem Gebiet der Bundesrepublik Deutschland eintritt, Art. 4 Abs. 1 VO (EG) 864/2007 („Rom II-Verordnung“). Allerdings kann der Cloud-Vertrag auch dazu führen, dass im Rahmen einer akzessorischen Anknüpfung nach Art. 4 Abs. 3 Rom II-Verordnung das auf den Vertrag anwendbare Recht auch für die unerlaubte Handlung gilt.

14 Soweit die gestörte Leistung aufgrund ihres Charakters und Inhalts einem anderen Vertragstypus als dem Mietrecht zuzuordnen ist, richtet sich die Haftung des Cloud-Anbieters nach den entsprechenden Regelungen dieses Vertragstypus. In Betracht kommt insbesondere die Anwendung von Werkvertragsrecht auf Business Process as a Service (BPaaS). In diesen Fällen stellt der Cloud-Anbieter keine Software oder andere Ressourcen zur Nutzung durch den Kunden zur Verfügung, sondern er stellt selbst Ergebnisse zur Verfügung (unter Nutzung von Software). Da in der Praxis IaaS, PaaS und SaaS überwiegen, die alle wohl dem Mietrecht unterfallen, wird nachfolgend dem Gebot der Kürze und Übersichtlichkeit folgend die Rechtslage ausschließlich anhand des Mietrechts dargestellt.

2.2 Beeinträchtigung von Verfügbarkeiten aufgrund des Ausfalls von Unterlieferanten (§ 278 BGB) und Konnektivitätsausfällen

15 Soweit sich der Cloud-Anbieter zur Erfüllung seiner vertraglichen Verpflichtungen der Hilfe Dritter bedient (etwa zur Bereitstellung von Rechen- und Speicherkapazität, Räumlichkeiten und dergleichen), haftet der Cloud-Anbieter für das Verschulden seiner Erfüllungsgehilfen ebenso wie für eigenes Verschulden (§ 278 BGB). Für Konnektivitätsausfälle, die auf Fehler des von ihm eingeschalteten Dienstleisters zurückgehen, ist der Cloud-Anbieter also regelmäßig im Rahmen der von ihm ggf. versprochenen Verfügbarkeiten ebenfalls verantwortlich. Ein über die Minderung hinausgehender Schadensersatzanspruch setzt jedoch Verschulden des Dienstleisters voraus, sofern die Beeinträchtigung nach Vertragsschluss entsteht. Für vor Vertragsschluss vorhandene Mängel haftet der Dienstleister sogar verschuldensunabhängig gem. § 536a Abs. 1 1. Alt. BGB. Selbstverständlich richtet sich der Haftungsrahmen aber immer nach dem Inhalt der geschuldeten Leistung.[7] Wenn der Gegenstand der Leistung eines Cloud-Dienstes sich auf die einwandfreie Anbindung seiner angebotenen Server- und Rechenkapazitäten an das Internet beschränkt, liegen etwaige jenseits dieser Anbindung auftretende Konnektivitätsausfälle außerhalb der vertraglich geschuldeten Leistung und damit auch außerhalb eines vertraglichen Haftungstatbestands. Entsprechend definieren Cloud-Anbieter typischerweise ihren Leistungsumfang dahingehend, dass sie für Ausfälle der Netzinfrastruktur nicht verantwortlich gemacht werden können. Dies erscheint im Regelfall auch sachgerecht für eine kalkulierbare Begrenzung der Risikosphäre des Cloud-Anbieters.[8]

16 **Praxishinweis**

Cloud-Anbieter und Cloud-Anwender sollten vertraglich regeln, wer für die Netzanbindung an das Rechenzentrum des Cloud-Anbieters verantwortlich ist und wer welche Risiken bei Kommunikationsausfällen trägt. So kann etwa die Verfügbarkeit eines Cloud-Services aus der Sicht des Cloud-Anwenders „end-to-end“ eine hohe Bedeutung haben und sich in den erwarteten Service-Levels widerspiegeln. Umgekehrt wird aber der Cloud-Anbieter nur eine Verfügbarkeit der eigenen IT-Umgebung sicherstellen können. Bei kritischen Anbindungen ist es daher ratsam, als Teil einer Notfallplanung alternative Anbindungswege bei dem Ausfall der Hauptverbindung vertraglich vorzusehen.

7 Kompetenzzentrum Trusted Cloud: Leitfaden – Vertragsgestaltung beim Cloud Computing (Stand: März 2014), S. 14 (abrufbar unter: http://www.trusted-cloud.de/media/content/140317_Vertragsleitfaden_gesamt_RZ_Ansicht.pdf, letzter Abruf 17.03.2015).

8 Ein allgemeiner Konnektivitätsausfall dürfte ein außerhalb der vertraglich geschuldeten Leistung liegender Fall höherer Gewalt sein.

3 Konsequenzen bei Datenpannen (insbesondere Verlust, Veränderung, unbefugter Zugriff)

17 Die Daten des Cloud-Anwenders werden beim Cloud-Anbieter, der mit der Verarbeitung dieser Daten beauftragt ist, gespeichert (zumindest vorübergehend). Insbesondere bei unzureichender Sicherung durch den Cloud-Anbieter können diese Daten gelöscht, verändert oder sogar unbefugten Dritten zugänglich werden, etwa durch einen Hacker-Angriff. Damit stellt sich die Frage, wer für derartige Schäden haftet.

18 Die Haftung für Datenpannen richtet sich nach den allgemeinen zivilrechtlichen Bestimmungen (siehe Ziffer 3.1). Strafrechtliche Folgen sind nach deutschem Recht im Bereich fahrlässiger Pflichtverstöße ausgeschlossen; der Rahmen für Ordnungswidrigkeiten ist dagegen u. a. im Rahmen des Datenschutzrechts durchaus eröffnet (siehe Ziffer 3.2). Ferner bestehen bei Datenpannen Mitteilungspflichten, deren Verletzung auch zu einer Haftung führen kann (siehe dazu Ziffer 3.3).

3.1 Zivilrechtliche Haftung

3.1.1 Vertragliche Haftung und Sorgfaltsmaßstab

19 Kommt es zum Verlust von Daten in der Cloud, ergeben sich etwaige Schadensersatzansprüche aus der Verletzung einer vertraglichen Hauptpflicht oder Nebenpflicht (§ 280 Abs. 1, § 241 Abs. 2 BGB). Zur Bestimmung vertraglicher Nebenpflichten ebenso wie hinsichtlich der Frage pflichtgemäßer Sorgfalt (und somit der Frage des Vertretenmüssens und der Einstandspflicht des Cloud-Anbieters) können technische Standards und Normen zur IT-Sicherheit wie z. B. der BSI-Grundschutz oder der internationale Standard ISO/IEC 27001 – jedenfalls, soweit sie vertraglich einbezogen sind – eine wichtige Rolle spielen.[9] Aber auch aus dem Gedanken der Verkehrssicherungspflicht und allgemeiner vertraglicher Schutzpflichten lassen sich Sorgfaltsmaßstäbe herleiten. Mit zunehmender Sensitivität und Schutzbedürftigkeit der vom Cloud-Anwender eingebrachten Daten dürften die Haftungsmaßstäbe an den Cloud-Anbieter steigen – soweit ihm die Art der zu verarbeitenden Daten (wie etwa aus der abzuschließenden Auftragsdatenverarbeitungsvereinbarung für ihn ersichtlich) bekannt ist oder bekannt sein müsste.

9 Dabei ist klar, dass technische Standards als solche keinen Rechtsnormcharakter haben. Durch vertragliche Inbezugnahme oder auch im Rahmen der Produkthaftung können sie allerdings mittelbar als wertvolle Orientierungspunkte zur Bestimmung der pflichtgemäßen Sorgfalt herangezogen werden.

20 **Praxishinweis**
Cloud-Anbieter und Cloud-Anwender sollten möglichst konkret die benötigten Sicherheitsstandards im Vorfeld identifizieren und anschließend im Cloud-Vertrag vereinbaren bzw. aus verschiedenen standardisierten Leistungspaketen des Cloud-Anbieters die tatsächlich benötigten Standards auswählen. Bei kritischen Daten und einem Bedarf an hoher Verfügbarkeit ist darauf besonders zu achten. Hierbei kommt es nicht nur auf die abstrakte Zusicherung eines Standards (wie z. B. ISO-27001-Compliance) an, sondern auf klare Regelungen zur konkreten Umsetzung dieser Standards sowie zusätzlich auf eine entsprechende Überprüfung bzw. Zertifizierung. Auf diese Weise kann ein Cloud-Anbieter die geschuldeten Pflichten konkretisieren, während der Cloud-Anwender das angebotene Sicherheitsniveau besser einschätzen kann.

21 ### 3.1.2 Deliktische Haftung

Neben vertraglichen Ansprüchen kommen deliktische Ansprüche gemäß §§ 823 ff. BGB in Betracht. Aus ihnen kann der Cloud-Anwender möglicherweise sogar direkt gegen einen Erfüllungsgehilfen des Cloud-Anbieters vorgehen. Zudem kann es sein, dass Schäden im Rahmen deliktischer Ansprüche geltend gemacht werden, ohne dass vertraglich vereinbarte Haftungsbeschränkungen dem entgegenstehen.

22 Ob der Verlust oder die unbefugte Veränderung von Daten einen Eingriff in das Recht des Eigentümers bzw. ein sonstiges Recht im Sinne des § 823 Abs. 1 BGB oder ein sonstiges Schutzrecht nach § 823 Abs. 2 BGB darstellen, ist in der Rechtsprechung noch nicht geklärt. Grundsätzlich stellen elektronische Daten keinen körperlichen Gegenstand dar, sind also keine Sache gemäß § 90 BGB, an der Eigentumsrechte bestehen können. Eine durch den Verlust von Daten bedingte Eigentumsverletzung liegt nach der Rechtsprechung zwar dann vor, wenn der Eigentümer mit seiner Sache nicht mehr nach Belieben (§ 903 BGB) verfahren und die in seiner Sache gespeicherten Daten nicht mehr auslesen oder verändern kann. Allerdings ist der Cloud-Anwender nicht Eigentümer der in der Cloud eingesetzten Hardware-Ressourcen. Daher ist zweifelhaft, ob die Rechtsprechung dem Cloud-Anwender einen Anspruch aus § 823 Abs. 1 BGB zuerkennen würde.

23 Daneben können deliktische Schadensersatzansprüche aus der Verletzung von Schutzgesetzen im Sinne des § 823 Abs. 2 BGB (etwa bei vorsätzlicher Normverletzung gemäß §§ 303a, 303b StGB [dazu sogleich]) sowie Schadensersatzansprüche gemäß § 7 BDSG (bei schuldhaft herbeigeführtem Datenverlust) bestehen.

3.2 Straftaten und Ordnungswidrigkeiten

24 Strafrechtliche Folgen aus der Verletzung der Strafnormen zur Datenveränderung und Computersabotage (§§ 303a, 303b StGB) können sich für die beim Cloud-Anbieter für die Datensicherheit Verantwortlichen in der Geschäftsleitung bzw. in leitender Position im Falle des vorsätzlichen Verstoßes ergeben, dürften aber in der Regel geringe praktische Bedeutung haben.

25 Anders verhält es sich bei fahrlässigen Verstößen gegen die Katalogbestimmungen des § 43 BDSG im Zusammenhang mit einer Verarbeitung personenbezogener Daten, da im Rahmen der für Cloud-Dienste maßgeblichen Auftragsdatenverarbeitung grundsätzlich der Anwender verantwortliche Stelle bleibt. Hier können den Anwender nach derzeitiger Rechtslage Bußgelder bis zu 300.000 EUR im Einzelfall (oder höher, wenn der vom Täter gezogene wirtschaftliche Vorteil darüber liegt) treffen und der Verstoß kann als Ordnungswidrigkeit geahndet werden (§ 43 Abs. 3 BDSG). Bei bloß fahrlässigem Handeln gilt nach § 17 Abs. 2 OWiG der hälftige Höchstbetrag, also 150.000 EUR im Einzelfall. Eine Ordnungswidrigkeit des Cloud-Anbieters kommt allgemein nur gemäß § 43 Abs. 2 Nr. 1 BDSG in Betracht, wenn er über das vertraglich zulässige Maß hinaus fahrlässig oder vorsätzlich personenbezogene Daten unbefugt verarbeitet.[10] Der Cloud-Anbieter haftet zudem auch vertraglich, wenn er vertragswidrig die Ursache für ein dem Anwender auferlegtes Bußgeld setzt.

26 Werden personenbezogene Daten unbefugt gegen Entgelt oder in der Absicht verarbeitet, sich oder einen anderen zu bereichern, ist die Tat strafbar. Bei gewerblich angebotenen Cloud-Lösungen, die erhaltene Daten nicht ausschließlich zum vereinbarten Zweck verarbeiten, ist ein möglicher Strafbarkeitszusammenhang daher nicht von vornherein ausgeschlossen (§ 44 BDSG).

3.3 Mitteilungspflichten bei Datenpannen

27 Für den Fall eines Datenverlusts oder Datenlecks, bei dem besondere Kategorien personenbezogener Daten unrechtmäßig übermittelt werden oder Dritten in sonstiger Weise unrechtmäßig zur Kenntnis gelangen, hat die verantwortliche Stelle die Aufsichtsbehörden und Betroffenen zu informieren (§ 42a BDSG bzw. § 83a SGB X, § 15a TMG oder § 93 Abs. 3 TKG bei Sozial-, Telemedien- oder Telekommunikationsdaten sowie vergleichbare Regelungen, z. B. im Bank- und Versicherungsaufsichtsrecht). Die Informationspflichten gelten für spezifische Datenkategorien (nämlich die besonderen Arten i. S. des § 3 Abs. 9 BDSG, Daten, die einem Berufsgeheimnis unterliegen [u. a. gemäß § 203 StGB], Daten über Straftaten und Ordnungswidrigkeiten und den Verdacht solcher Taten sowie Bankkonto- und Kreditkontodaten; siehe § 42a Abs. 1 BDSG). Die Informationspflichten greifen, sofern „schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen“, und erfordern regelmäßig unverzügliches Handeln und eine Information über die Art der unrechtmäßigen Kenntniserlangung und Empfehlungen zur Minderung möglicher nachteiliger Folgen.

28 Wenn die Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig gemacht wird, liegt eine Ordnungswidrigkeit nach § 43 Abs. 2 Nr. 7 BDSG vor; weist der Cloud-Anbieter den Cloud-Anwender nicht auf eine bei ihm aufgetretene Datenpanne hin und kann daher der Cloud-Anwender seine Mitteilungspflicht nicht erfüllen, kommt eine Haftung des Cloud-Anbieters in Betracht, wenn gegen den Cloud-Anwender als verantwortliche Stelle ein Bußgeld verhängt wird (vgl. Ziffer 3.2).

10 Cloud Computing ist regelmäßig als Auftragsdatenverarbeitung einzuordnen. Daher ist grundsätzlich der Cloud-Anwender die datenschutzrechtlich verantwortliche Stelle. Der Cloud-Anbieter kann aber ausnahmsweise zum einen im Rahmen einer sog. Funktionsübertragung als verantwortliche Stelle anzusehen sein, wenn er die Daten nicht nach Vertrag und Kundenweisung verarbeitet, sondern im eigenen Ermessen. Zum anderen wird vertreten, dass der Cloud-Anbieter auch dann als verantwortliche Stelle anzusehen ist, wenn er (fahrlässig oder vorsätzlich) personenbezogene Daten über die Vorgaben des Cloud-Anwenders hinaus verarbeitet. In diesen Fällen ist der Cloud-Anbieter selbst unmittelbarer Adressat datenschutzrechtlicher Bestimmungen und haftet entsprechend.

29 Während der Cloud-Anbieter in der Regel nicht unmittelbarer Normadressat des BDSG ist (Ausnahme z. B. § 9 BDSG), entspricht es jedoch der vertraglichen „best practice“, dass Cloud-Anbieter bereits in ihren Vertragsbedingungen vertragliche Verpflichtungen gegenüber dem Cloud-Anwender zur unverzüglichen Benachrichtigung und Mitwirkung an der Aufklärung von auftretenden Datenpannen aufnehmen (und damit die Mitteilungspflichten aus § 11 Abs. 2 Nr. 8 BDSG über eigene Verstöße hinaus erweitern), um dem Cloud-Anwender eine gesetzeskonforme Nutzung des Cloud-Dienstes zu ermöglichen.

30 **Praxishinweis**
Die vertragliche Ausgestaltung von Mitteilungspflichten des Cloud-Anbieters im Falle von Datenpannen entspricht der „best practice“ und sollte in keiner Vereinbarung einer Auftragsdatenvereinbarung (ADV) fehlen. Darüber hinaus hat auch der Cloud-Dienstleister ein Interesse an einer rechtzeitigen Information über etwaige Datenpannen, da sich ansonsten ein möglicher Schaden wie auch ein etwaiger Verschuldensanteil bei einer verspäteten Meldung erhöhen kann.

31 Liegt im Einzelfall keine wirksame Auftragsdatenverarbeitung vor oder hält der Cloud-Anbieter Dienste vor, die sich etwa im Rahmen von ausgelagerten Geschäftsprozessen nicht ohne Weiteres als Auftragsdatenverarbeitung abbilden lassen, kann es auch dazu kommen, dass der Cloud-Anbieter selbst Normadressat des § 42a BDSG ist.[11] Im Bereich des hier diskutierten Cloud Computing stehen Leistungen im Fokus, die gegenüber einem Unternehmer erbracht werden. In dieser Konstellation geht es vorwiegend um Mitarbeiter- oder Kundendaten, die der Cloud-Anwender durch den Anbieter in der Cloud verarbeiten lässt. In diesen Fällen ist der Cloud-Anwender in der Regel die verantwortliche Stelle, während der Cloud-Anbieter Auftragsdatenverarbeiter ist.

32 Dem Cloud-Anbieter können auch Informationspflichten nach dem Telemedienrecht (§ 15a TMG) obliegen. Dies gilt jedenfalls, soweit Cloud-basierte Lösungen dazu dienen, Dritten Informationen zukommen zu lassen. Im Übrigen ist in der Literatur sehr umstritten, ob vom Cloud-Anwender wie eigene Ressourcen genutzte Cloud-Dienste auch Informationspflichten nach Telemedienrecht (§ 15a TMG) begründen; eine diesbezügliche Rechtsprechung liegt bisher nicht vor. Soweit ein SaaS-Dienst lediglich die Online-Bereitstellung eines bestimmten Software-Tools vorsieht und kein darüber hinausgehender Informations- und Kommunikationszweck gegenüber Dritten besteht oder dieser vollständig in den Hintergrund tritt (z. B. bei reinen „Office“-Anwendungen wie etwa Textverarbeitungs-, Tabellenkalkulations- und Datenbanksoftware oder Software zur Verarbeitung von Mitarbeiter- oder Kundendatenbanken), ist die Anwendbarkeit des § 15a TMG wohl nicht überzeugend, da kein sachlicher Bezug der Leistung des Cloud-Anbieters zu den Informationen besteht. Im Anwendungsbereich des § 15a TMG gilt, dass der Cloud-Anbieter, soweit ein unrechtmäßiger Zugriff auf Bestands- und Nutzungsdaten (§§ 14, 15 TMG) erfolgt ist, selbst entsprechenden Informationspflichten nachzukommen hat. § 42a BSDG findet dann über §15a TMG entsprechende Anwendung.

11 Sofern der Cloud-Anbieter Leistungen auch gegenüber Endverbrauchern erbringt, ist er ebenfalls verantwortliche Stelle. Nutzt eine Privatperson (für rein private Zwecke) einen Cloud-Dienst, z. B. einen Speicher- oder E-Mail-Dienst, ist der Cloud-Anbieter verantwortliche Stelle, die personenbezogene Daten beim Betroffenen erhebt.

4 Vertragliche Haftungsbeschränkungen

33 Die Vorenthaltung von Verfügbarkeiten, ein fehlerhafter oder unvollständiger Datenzugriff, aber auch der Verlust oder die Unauffindbarkeit von Daten, die unterbliebene oder fehlerhafte Ausführung damit verbundener Rechenoperationen oder auch Datenverluste aufgrund von Eingriffen Dritter (durch die Ausnutzung von Sicherheitslücken und Hacking) begründen Ansprüche auf Ersatz jedes „adäquatkausal" verursachten Schadens, sofern dem Cloud-Anbieter ein vertraglicher (oder gesetzlicher) Pflichtenverstoß zur Last fällt. Dabei gilt grundsätzlich, dass jeder Schaden – einschließlich aller mittelbaren und Folgeschäden – in unbegrenzter Höhe zu ersetzen ist, sofern die Parteien nichts Abweichendes vereinbart haben. Daher besteht ein legitimes Interesse, die Haftung des Cloud-Anbieters zu beschränken, zumal bei sog. mehrmandantenfähigen („multitenancy") Architekturen der Public Cloud ein Systemfehler in der Regel alle oder zumindest zahlreiche Cloud-Anwender betrifft und daher aus Sicht des Cloud-Anbieters ein existenzgefährdendes Risiko bestehen kann. Nach deutschem Vertragsrecht ist zu unterscheiden zwischen Haftungsklauseln in Standardverträgen (die dem AGB-Recht unterfallen) und solchen in individuell ausgehandelten Verträgen.

4.1 Dem AGB-Recht unterfallende Standardverträge

34 Geht man davon aus, dass Cloud-Anbieter ihr Geschäftsmodell im Wesentlichen – ob in der Private Cloud oder in der Public Cloud – auf Standardisierung und Skalierbarkeit stützen, kommt der Ausgestaltung und Durchsetzung standardisierter Vertragsbedingungen ein sehr hoher Stellenwert zu. Damit steht die Industrie – und mittelbar auch der Markt der Cloud-Anwender – vor den Herausforderungen des AGB-Rechts und dem relativ starren Rahmen, den die Rechtsprechung auch für unternehmerische Rechtsbeziehungen (dem B2B-Verkehr) setzt. Dies gilt für eine mittelbare Haftungsbeschränkung durch eine eingeschränkte Leistungsbeschreibung ebenso wie für eine unmittelbare Beschränkung der Haftung:

35 - Eine Beschränkung bis hin zum Ausschluss vertraglicher Haftung könnte durch eine Einschränkung der zugesicherten Leistung selbst stattfinden. Standardbedingungen von Cloud-Anbietern, die lediglich Leistungen in der jeweils aktuell bereitstehenden Form („as is") anbieten und damit faktisch keinerlei Leistungsinhalte vertraglich zusichern wollen, sind jedoch AGB-rechtlich kaum möglich, da keine ausreichende Transparenz der geschuldeten Leistung besteht und der eine klar vereinbarte Vergütung schuldende Leistungsempfänger unangemessen benachteiligt wird.[12] Schließlich dürften unklare Leistungsvereinbarungen auch für Cloud-Anwender nicht akzeptabel sein, deren Geschäft oder zumindest deren relevante Prozesse von diesen Cloud-Services abhängen und eine ausreichende Zuverlässigkeit erfordern.

12 Näher dazu Kompetenzzentrum Trusted Cloud: Leitfaden – Vertragsgestaltung beim Cloud Computing (Stand: März 2014), S. 14 (abrufbar unter: http://www.trusted-cloud.de/media/content/140317_Vertragsleitfaden_gesamt_RZ_Ansicht.pdf, letzter Abruf 17.03.2015).

36 ■ Nach bisher unumstrittener AGB-Rechtsprechung kann der Cloud-Anbieter seine Haftung (jenseits der unbeschränkten Haftung für Vorsatz und grobe Fahrlässigkeit) für die (einfache) fahrlässige Verletzung sog. „Kardinalpflichten“ (Vertragspflichten, die für die Rechtsbeziehung von wesentlicher Bedeutung sind und auf deren Einhaltung der Vertragspartner in besonderer Weise vertrauen kann) lediglich auf den „typischerweise vorhersehbaren Schaden“ begrenzen. Mit dem unbestimmten Rechtsbegriff des „typischerweise vorhersehbaren Schadens“ hat sich die Rechtsprechung einen weiten Ermessensspielraum geschaffen, nach einer Einzelfallbetrachtung über die Ersatzfähigkeit auch weitreichender Schäden zu entscheiden.

37 Gerichtsentscheidungen zu vertraglichen Haftungsfragen im IT-Bereich sind eine Seltenheit. Damit steht nach derzeitigem AGB-Recht ein nach deutschem Vertragsrecht bestehender Haftungsrahmen im Raum, der weit von dem industrieüblichen internationalen Standard entfernt ist. So regelt die angelsächsisch geprägte Vertragskultur der IT-Branche außerhalb des AGB-Rechts (aber auch häufig genug im Rahmen von – dann nach deutschem Vertragsrecht[13] ggf. nicht durchsetzbaren – AGB-Klauseln) üblicherweise Haftungsausschlüsse für bestimmte indirekte bzw. Folgeschäden (wie z. B. entgangenen Gewinn, Folgeschäden an anderweitigen Rechtsgütern des Anwenders, Vermögensschäden). Ebenso häufig sind darüber hinaus Haftungsobergrenzen („Caps“) mit Blick auf den Umfang ersatzpflichtiger Schäden bei (zumindest leicht) fahrlässigen Verletzungen. Damit erzielen die Anbieter eine Risikobegrenzung, um die bei IT-Leistungen vorhandenen Schadenspotentiale kaufmännisch angemessen abzusichern. Dies kann auch im Interesse der Cloud-Anwender liegen, um eine Verteuerung der Cloud-Leistung zu vermeiden.

38 **Rechtspolitischer Hinweis**
Rechtspolitisch ist eine Modifizierung des deutschen AGB-Rechts sehr zu wünschen, sodass in Formularverträgen dem Industriestandard gemäße, angemessene Haftungsbeschränkungen im unternehmerischen Verkehr möglich sind.

39 Die öffentliche Hand hat dieses Erfordernis schon seit langem erkannt und hat in ihren eigenen IT-Einkaufsbedingungen (den diversen EVB-IT für unterschiedliche Vertragstypen[14]) entsprechende vorformulierte Haftungsausschlüsse und Haftungsobergrenzen eingeführt. Auch dies verdeutlicht, dass der gesetzliche Haftungsrahmen nach dem AGB-Recht einschließlich der Beschränkung auf den „typischerweise vorhersehbaren Schaden“ nach den Marktgepflogenheiten zu weit gesetzt ist.

40 Während IT-Anbieter im klassischen IT-Projektgeschäft durch abweichende, individuell ausgehandelte Haftungsregelungen kaufmännisch angemessene Begrenzungen erzielen können (dazu sogleich Ziffer 4.2), steckt der Cloud-Anbieter in dem Dilemma, seine standardisierte Leistung jenseits des Industriestandards nur mit einem nicht begrenzten Haftungsrisiko anbieten zu können. Folglich muss der Cloud-Anwender mit einem Risikozuschlag rechnen, der den Anreiz der mit Standardisierung und Skalierbarkeit verbundenen Kostenersparnis womöglich zu einem beachtlichen Anteil wieder zunichtemacht (s. o. Rz. 23). Der vertraglichen Ausgestaltung der Haftungsregelungen in den allgemeinen Geschäftsbedingungen des Cloud-Anbieters sind damit enge Grenzen gesetzt.

13 Gilt für den Vertrag ausländisches Recht, sind diese Haftungsausschlüsse in der Regel auch wirksam. Welches Recht auf den Cloud-Vertrag Anwendung findet, können die Parteien wählen. Von dieser Möglichkeit sollten die Parteien angesichts der sonst bestehenden Unsicherheiten Gebrauch machen. Näher dazu Kompetenzzentrum Trusted Cloud: Leitfaden – Vertragsgestaltung beim Cloud Computing (Stand: März 2014), S. 12 (abrufbar unter: http://www.trusted-cloud.de/media/content/140317_Vertragsleitfaden_gesamt_RZ_Ansicht.pdf, letzter Abruf 17.03.2015).

14 Eigene IT EVB für Cloud-Lösungen gibt es bisher nicht; insoweit müssen sich die öffentliche Hand und Cloud-Anbieter in vielen Fällen mit einer für den Einzelfall modifizierten Fassung der EVB-IT Überlassung Typ B behelfen.

41 **Praxishinweis**
Eine Schadensersatzpflicht für Vorsatz, grobe Fahrlässigkeit oder Körperverletzungen kann nicht beschränkt werden. Bei einfacher fahrlässiger Verletzung von Vertragspflichten können nur sonstige Pflichten, die keine Kardinalspflichten sind, eingeschränkt oder ausgeschlossen werden. Vertragspflichten, die für die Rechtsbeziehung von wesentlicher Bedeutung sind und auf deren Einhaltung der Vertragspartner in besonderer Weise vertrauen kann („Kardinalspflichten"), können nur auf den typischerweise vorhersehbaren Schaden beschränkt werden. Da es keine geltungserhaltende Reduktion einer unwirksamen Haftungsklausel gibt, sollte der Cloud-Anbieter hier keine unwirksamen Haftungsgrenzen vorsehen, da er sonst vollumfassend haftet.[15]

42 Das Cloud-Dilemma akzentuiert das – durchaus allgemein anerkannte – Grundproblem, dass das deutsche AGB-Recht für den unternehmerischen Verkehr einer Lockerung und Flexibilisierung bedarf, um eine näher am Industriestandard ausgerichtete Risikobalance zu ermöglichen. Die seit Jahren laufende Diskussion zur Lockerung der strengen AGB-rechtlichen Regelungen zu Haftungsbeschränkungen im unternehmerischen Verkehr stellt jedoch in zeitlicher Hinsicht keine kurzfristigen Lösungen in Aussicht.[16]

4.2 Individuell ausgehandelte Cloud-Verträge

43 Im Einzelfall können spezielle Cloud-Services wie etwa mit IT-Outsourcing verwandte Private-Cloud-Infrastrukturen für Unternehmen jedoch auch durchaus auf der Basis von Individualverträgen vereinbart werden und damit zugehörige Haftungsregelungen den engmaschigen Beschränkungen des AGB-Rechts entgehen, soweit die Klauseln tatsächlich ausgehandelt wurden. Die Beschränkung der Haftung ist dann etwa mit typischen Regelungen in IT-Auslagerungsverträgen zu vergleichen. Während auch hier Ansprüche aus vorsätzlicher Schädigung, bei Telekommunikationsdienstleistungen (§ 7 Abs. 2 TKV), nach Produkthaftungsgesetz, aus ausdrücklich erklärten Garantien oder der Verletzung von Leben, Körper und Gesundheit nicht eingeschränkt werden können, ist es den Parteien darüber hinaus bis zur Grenze einer krassen Benachteiligung einer Seite aufgrund einer sittenwidrigen Regelung (§ 138 BGB) möglich, Haftungsregelungen frei zu vereinbaren.

15 Es wäre lediglich noch (entsprechend dem BGH-Urteil vom 17.10.2013 – I ZR 226/12) denkbar, in einer separaten Klausel den vorhersehbaren Schaden für leichte Fahrlässigkeit summarisch zu vereinbaren, soweit die angebotene Leistung eine vernünftige Einschätzung des möglichen Schadens ermöglicht.

16 Dies ist insbesondere mit Blick auf eine Ausrichtung an der „good commercial practice", also unter Berücksichtigung der industrieüblichen Gepflogenheiten einer Branche, inzwischen deutlich ausgesprochen und gefordert worden (siehe z. B. Beschlüsse des 69. Deutschen Juristentags 2012, S. 5, www.djt-net.de/beschluesse/beschluessee; Schreiben des Mittelstandverbunds ZGV an das BMJ vom 21. März 2012, www.mittelstandsverbund.de; Zustimmung des VDMA, www.vdma.org/article/-/articleview/643207; Zustimmung des ZVEI, www.zvei.org). Entsprechend empfiehlt es sich mit Blick auf Cloud-Dienste, das notwendigerweise standardisierte und im Kern gerade nicht auf Individualabreden ausgerichtete Geschäftsmodell zu betonen und entsprechende Lösungsvorschläge in die Diskussion zur AGB-Reform für den unternehmerischen Verkehr einzubringen. Der vom 69. Deutschen Juristentag beschlossene Reformansatz, die AGB-Kontrolle im B2B-Bereich auf die „good commercial practice" auszurichten, könnte hierfür den passenden Rahmen bieten.

44 In der Praxis werden individualvertragliche Haftungsregelungen hierbei die Interessen des Cloud-Anbieters an einer weitreichenden Risikobegrenzung mit dem Erfordernis des Cloud-Anwenders an einen sicheren und zuverlässigen Service, für den der Anbieter auch einzustehen hat, ausbalancieren müssen. Entsprechend sind betragsmäßige Haftungshöchstgrenzen zumindest für einfache Fahrlässigkeit durchaus üblich und orientieren sich oft anteilig an Jahres- oder Gesamtkosten des Cloud-Services, während eine Haftungsbeschränkung von grob fahrlässig verursachten Schäden von Cloud-Anwendern aufgrund der erwarteten Sorgfalt bei der Leistungserbringung nur bei unkritischen Anwendungen mit geringem Schadenspotential akzeptiert werden dürfte. Während Cloud-Anwender in der Regel auch keinem Ausschluss von Folgeschäden bzw. mittelbaren Schäden zustimmen wollen, da hiermit praktisch keine relevanten Schadensfälle bei einer Beeinträchtigung des Cloud-Services übrig bleiben, ist der Ausschluss bestimmter Schadensarten wie entgangener Gewinn häufiger anzutreffen. Auch ist ein Cloud-Anbieter bei einer verbleibenden Haftung für Datenverluste gut beraten, wenn er einen derartigen Anspruch durch eine Verpflichtung des Cloud-Anwenders auf regelmäßige Datensicherung praktisch einschränkt. Schließlich ist neben Mitverschuldensregelungen auch eine Anrechnung etwaiger Ansprüche wegen Pönalen, Vertragsstrafen oder Zahlungen aufgrund einer Verletzung von vereinbarten Service-Levels („Service-Level-Credits“) auf einen Schadensersatzanspruch mit gleicher Ursache ebenso üblich wie ein Ausschluss von Ansprüchen bei höherer Gewalt außerhalb des Verantwortungsbereichs des Cloud-Anbieters („Force majeure“).

45 **Praxishinweis**

Im Rahmen individuell ausgehandelter Verträge sind Haftungsausschlüsse für bestimmte Schadensarten (z. B. Vermögensschäden) sowie Haftungsobergrenzen (als Nominalbeträge oder Prozentsätze des Vertragsvolumens) für (einfache) Fahrlässigkeit durchaus üblich, während die sonstige Haftung für Vorsatz sowie Schäden an Leben, Körper, Gesundheit oder sonstige gesetzlich nicht begrenzbare Schadensfälle (z. B. nach Produkthaftungsgesetz) unbeschränkt bleibt. Damit würde man beispielsweise die Haftung des Cloud-Anbieters bei (leicht) fahrlässig verursachten Schäden ausschließen und im Zusammenhang mit dem Cloud-Service pro Vertragsjahr auf einen prozentualen Betrag der jährlichen Gesamtvergütung oder einen Eurobetrag beschränken und etwa eine Haftung für Schäden aufgrund eines entgangenen Umsatzes oder Gewinns ausschließen.[17]

46 Darüber hinaus könnte ein Ersatz für Datenverlust dadurch beschränkt werden, dass der Cloud-Anwender industrieübliche Sicherungskopien der eigenen Daten anlegen muss und bei einer Verletzung dieser Pflicht für entstehende Datenverluste nicht gehaftet wird. Außerdem könnten etwaige Service-Credits auf Haftungsansprüche angerechnet werden.

17 Soweit die in der Cloud verarbeiteten Daten einer besonderen Vertraulichkeit oder Sensitivität unterliegen und der Cloud-Anwender einen erhöhten Sorgfaltsmaßstab erwartet, wäre eine pauschale Haftungsbegrenzung ggf. unangemessen. Der Cloud-Anbieter könnte in diesem Fall auf eine Ausnahme von einer Haftungsbeschränkung bei einer Verletzung von Sorgfaltspflichten im Zusammenhang mit der Vertraulichkeit der Daten vertraglich verpflichtet werden.

5 Haftung für rechtswidrige Anwenderinhalte und regulatorische Verstöße

47 Der Cloud-Anbieter kann ferner möglicherweise für vom Cloud-Anwender eingestellte rechtswidrige Inhalte und für Verstöße gegen regulatorische Anforderungen, wie sie sich z. B. aus dem Außenwirtschaftsgesetz oder der Regulierung des Finanzwesens ergeben, haften.

5.1 Haftung für rechtswidrige Anwenderinhalte

48 Da der Cloud-Anbieter Daten des Cloud-Anwenders verarbeitet und speichert, stellt sich die Frage, wie der Cloud-Anbieter haftet, wenn diese Daten Rechte Dritter, insbesondere Urheberrechte oder sonstige Immaterialgüterrechte, verletzen. Neben urheber- und markenrechtlichen Ansprüchen kommen dabei etwa Schadensersatz- und Unterlassungsansprüche nach UWG in Betracht.

5.1.1 Haftung des Cloud-Anbieters als Störer

49 So können z. B. Urheberrechte Dritter verletzt werden, wenn der Cloud-Anwender urheberrechtlich geschützte Werke mittels des Cloud-Dienstes verarbeitet, z. B. sogar der Öffentlichkeit zugänglich macht.[18] Der Cloud-Anbieter kommt in diesen Fällen als Teilnehmer oder Täter einer vorsätzlichen unerlaubten Handlung des Cloud-Anwenders gemäß § 97 Abs. 1 und 2 UrhG, § 823 Abs. 1 und § 830 BGB nur in Betracht, sofern er konkrete Kenntnis von solchen Vorgängen hat. Denkbar ist zudem eine Schadensersatzhaftung des Anbieters aus fahrlässiger Verletzung der Urheberrechte Dritter (nach § 97 Abs. 2 UrhG) oder eine Inanspruchnahme auf Unterlassung (als Störer gemäß §§ 1004, 823 BGB analog bzw. § 97 Abs. 1 UrhG).

50 Voraussetzung für eine Haftung des Cloud-Anbieters auf Schadensersatz als (Mit-)Störer ist, dass dieser schuldhaft adäquatkausal zu einer fremden Urheberrechtsverletzung beigetragen hat. Ein Anspruch auf Beseitigung und Unterlassung der Rechtsverletzung besteht dabei auch ohne ein schuldhaftes Handeln.[19] Dafür kann z. B. auch die Unterstützung der Handlung des Cloud-Anwenders genügen, sofern der Cloud-Anbieter die rechtliche Möglichkeit zur Verhinderung dieser Handlung hatte.

51 Rein faktische Voraussetzung einer derartigen Inanspruchnahme des Anbieters durch Dritte ist aber stets, dass der Dritte überhaupt Kenntnis davon hat, dass die rechtswidrigen Inhalte beim Cloud-Anbieter verarbeitet werden. Dies ist naturgemäß der Fall, sofern es sich bei dem Cloud-Dienst um eine öffentlich zugängliche Plattform handelt, auf der Inhalte veröffentlicht werden können. Setzt der Cloud-Anwender, wie typischerweise beim IaaS, PaaS oder SaaS, die Cloud-Lösung wie eine interne Ressource ein, wird der Dritte, dessen Rechte verletzt werden, in der Regel keine Kenntnis davon erlangen und daher seine Ansprüche ohnehin nur gegen den Cloud-Anwender richten.

18 In Betracht kommen insbesondere das Hochladen, Streamen oder anderweitige Verbreiten (§§ 17, 69c Nr. 3 UrhG), das öffentliche Zugänglichmachen (§§19a, 69c Nr. 4 UrhG) oder Vervielfältigen (§§ 16, 69c Nr. 3 UrhG).

19 Zum Störerbegriff etwa: BGH NJW 2007, 432.

52 Jedenfalls hat der BGH klargestellt, dass sich die Störerhaftung nicht über Gebühr auf Dritte, wie z. B. den Cloud-Anbieter, erstrecken darf. Ihm dürfen keine Anforderungen auferlegt werden, die seine Tätigkeit unverhältnismäßig erschweren.[20]

53 Die rechtswidrigen Inhalte sind vom Cloud-Anbieter nach Kenntniserlangung zu sperren oder zu entfernen. Hat der Cloud-Anbieter Kenntnis von einer Rechtsverletzung, hat er die objektiv zumutbaren Vorsorgemaßnahmen einschließlich geeigneter technischer Vorkehrungen zu treffen, um weitere gleichartige Rechtsverletzungen zu verhindern. Die technische und organisatorische Umsetzung (einschließlich geeigneter technischer Filter) stellt für Cloud-Anbieter, die eine öffentliche Plattform betreiben, eine erhebliche Herausforderung dar, um diese in einem wirtschaftlich verhältnismäßigen Umfang und in zuverlässiger Weise zu vollziehen.

5.1.2 Haftungsprivilegierung nach §§ 7 ff. TMG?

54 Gemäß §§ 7 ff. TMG sind zivilrechtliche Schadensersatzansprüche und eine strafrechtliche „Verantwortlichkeit“ allerdings eingeschränkt, soweit es sich bei der vom Cloud-Anbieter angebotenen Leistung um einen Telemediendienst handelt (dazu oben Ziffer 3.3).

55 Die eingeschränkte Haftung des Diensteanbieters nach §§ 7 ff. TMG setzt voraus, dass aus Sicht des Anbieters fremde Informationen vorliegen. Fraglich ist daher, ob der Cloud-Anbieter sich die Informationen des Cloud-Anwenders „zu eigen gemacht“ hat. Dies ist dann der Fall, wenn der Diensteanbieter die Inhalte vor dem Einstellen auf seiner Plattform auf Vollständigkeit und Richtigkeit überprüft.[21] Die Abgrenzung von fremden gegenüber eigenen Informationen ist damit für eine Vielzahl von Cloud-Diensten unproblematisch. Bei anderen Diensten wie etwa „Flickr“ oder „Instagram“ oder Streaming-Angeboten kommt es dagegen auf die konkrete Aufbereitung und den Prozess des Einstellens der Inhalte an.

56 Grundsätzlich hat der Cloud-Anbieter keine präventiven Prüfpflichten und muss nur dann eingreifen, wenn er konkrete Kenntnis von den eine Rechtsverletzung begründenden Umständen hat.[22] Sonst verstößt er gegen eine zumutbare Verhaltenspflicht, womit zugleich das Hosting-Privileg des § 10 TMG entfällt.

57 **Praxishinweis**
Es bietet sich damit gerade für Cloud-Anbieter mit öffentlich zugänglichen Cloud-Dienstleistungen an, für Dritte eine einfache Möglichkeit zur Meldung einer Rechtsverletzung etwa auf der zugehörigen Website vorzusehen. Eingehende Beschwerden sollten jedoch auch zur Vermeidung einer eigenen Haftung gewissenhaft weiterverfolgt werden. Umgekehrt empfiehlt es sich, den Cloud-Anwender in den Nutzungsbedingungen zur ausschließlichen Verarbeitung rechtmäßiger Inhalte zu verpflichten und sich bei einer (vermuteten) Verletzung dieser Pflicht ein Recht zur Suspendierung oder Kündigung auszubedingen.

20 Die Frage, ob der Diensteanbieter als Störer (mit)haftet, ist im Rahmen einer Einzelfallbetrachtung zu beantworten. Dabei sind folgende Kriterien anzuwenden: (1.) Funktion und Aufgabenstellung des als Störer in Anspruch genommenen Diensteanbieters, (2.) die Eigenverantwortung des unmittelbar die Rechte anderer verletzenden Dritten und (3.) die Frage, ob der Störer offensichtlich und unschwer die Verletzung erkennen oder dies erst nach eingehender rechtlicher Überprüfung identifizieren kann (zu diesen Aspekten: BGH, Urteil vom 17.5.2001 – ZR 251/99 [ambiente.de], abgedruckt in CR 2001, 850, 851). Eine umfassende Prüfung der von Cloud-Anwendern eingestellten Inhalte oder gar eine Vorabkontrolle sind nicht geboten (hierzu: BGH, Urteil vom 12.7.2007 – I ZR 18/04, abgedruckt in GRUR 2007, 890, 894). Ein Unterlassungsanspruch des Schutzrechtsinhabers besteht dann, wenn der Cloud-Anbieter konkrete Hinweise auf entsprechend rechtswidrige Inhalte hat.

21 Statt vieler: BGH, Urteil vom 12.7.2007 – I ZR 18/04, abgedruckt in GRUR 2007, 890, 894 f.

22 BGH GRUR 2011, 1038, 1040 – Stiftparfüm.

5.2 Mithaftung für regulatorische Verstöße

58 Eine weitere Frage ist, ob der Cloud-Anbieter für etwaige regulatorische Verstöße des Cloud-Anwenders nach öffentlich-rechtlichen Vorschriften haftet – beispielsweise wenn dieser den Cloud-Dienst in einer Weise nutzt, die ein Vorgehen nach besonderem oder allgemeinem Gefahrenabwehrrecht oder anderen öffentlich-rechtlichen Eingriffstatbeständen erforderlich macht. Angesichts der Vielzahl möglicher Eingriffstatbestände sind allgemeine Aussagen nur schwer zu treffen. Bei einer Nutzung des Cloud-Angebots, von der eine konkrete Gefahr für rechtlich geschützte Güter ausgeht oder die rechtswidrigen Zwecken dient (Beispiel: Cloud-basierte Kommunikationsforen, in denen Verstöße gegen die Anti-Terror-Gesetzgebung festgestellt werden), kann ein behördliches Vorgehen gegen den Cloud-Anbieter (etwa durch Anordnung der Schließung des Nutzungszugangs) in Extremfällen im Rahmen der Gefahrenabwehr den Anforderungen an die Erforderlichkeit und Verhältnismäßigkeit entsprechen: Oft wird der eigentliche Störer, etwa wenn unter falscher Identität agierend oder im Ausland belegen, nicht greifbar sein. Eine solche öffentlich-rechtlich begründete Verantwortlichkeit des Cloud-Anbieters setzt jedoch voraus, dass dieser Störer im öffentlich-rechtlichen Sinne ist.

5.2.1 Polizeirechtliche Störer-Haftung des Cloud-Anbieters?

59 Als Verhaltensstörer gilt dabei im Allgemeinen der, der die unmittelbare Ursache für eine Gefahr im polizeirechtlichen Sinne setzt; nach einer engeren Auffassung ist es derjenige, der diese Gefahr in rechtswidriger Weise setzt. Störer ist demnach derjenige, der durch seine Nutzung des Cloud-Angebots die letzte Ursache für die betreffende Gefahr setzt, also der Cloud-Anwender, nicht der Cloud-Anbieter.

60 Eine Haftung des Cloud-Anbieters als Zustandsstörer hängt davon ab, dass er die tatsächliche Sachherrschaft über eine Gefahrenquelle im polizeirechtlichen Sinne hat. Ob der Cloud-Anbieter diese Sachherrschaft hinsichtlich der vom Cloud-Anwender eingestellten Inhalte schon aufgrund seiner tatsächlichen (Mit-)Herrschaft über die zugrunde liegende Rechnerinfrastruktur hat, ist bislang offen. Wenn die Gefahr aber von einer vom Cloud-Anwender bestimmten Nutzung ausgeht – und gerade nicht auf bestimmte Eigenschaften der bei einer Gefahrenbetrachtung an sich neutralen Sache zurückzuführen ist, kann der Cloud-Anbieter lediglich nach den Grundsätzen der Verantwortlichkeit von Nichtstörern in Anspruch genommen werden. Diese greift aber nur subsidiär und bei erheblicher Gefahr, die nicht durch eine Inanspruchnahme des unmittelbaren (Verhaltens-)Störers abgewehrt werden kann. Möglicherweise kommt dies in Betracht, wenn der eigentliche Störer nicht identifizierbar oder außerhalb des Zugriffsbereichs deutscher Behörden agiert.

5.2.2 Spezialgesetzliche Eingriffstatbestände[23]

61 Gerade bei grenzüberschreitender Inanspruchnahme von Cloud-Diensten können Eingriffe auf Grundlage der Dual-Use-Verordnung (Verordnung [EG] Nr. 428/2009] oder des Außenwirtschaftsgesetzes (AWG) nicht von vornherein ausgeschlossen werden. § 6 AWG ermöglicht es bei einer Gefahr im Außenwirtschaftsverkehr (gemäß § 1 AWG umfasst

23 Sonstige Haftungskonstellationen im Zusammenhang mit Spezialgesetzen, z. B. steuerrechtlich relevante Fragestellungen wie etwa zum Zugriff auf Buchungsunterlagen des Cloud-Nutzers auf Cloud-Datenspeichern im Ausland oder zu Cloud-Rechenzentren als möglichen Betriebsstätten, können hier nicht im Einzelnen ausgeführt werden.

dieser Güter-, Dienstleistungs-, Kapital-, Zahlungs- und sonstigen Wirtschaftsverkehr mit dem Ausland), im Einzelfall Beschränkungen durch Verwaltungsakt anzuordnen. Anordnungen können insbesondere getroffen werden, um wesentliche Sicherheitsinteressen der Bundesrepublik Deutschland zu wahren oder eine erhebliche Störung der auswärtigen Beziehungen der Bundesrepublik Deutschland zu verhüten (§ 4 Abs. 1 AWG). Angesichts der Bandbreite möglicher Cloud-Dienste erscheint ein Vorgehen nach dieser Vorschrift nicht ausgeschlossen. Vor allem wenn der Cloud-Anbieter vom Anwender in die Cloud eingestellte außenwirtschaftsrechtlich relevante Daten über nationale Grenzen hinweg verschiebt, liegt ein Verstoß gegen das Außenwirtschaftsrecht nahe, für den der Anbieter – bei einem Vertragsverstoß – haften kann.

62 **Praxishinweis**
Ein Cloud-Anbieter sollte deshalb grundsätzlich sicherstellen, dass die typischerweise in seiner Cloud verarbeiteten Daten keinen besonderen, etwa territorialen Restriktionen unterliegen. In erster Linie obliegt es allerdings dem Cloud-Anwender, den Cloud-Anbieter vertraglich so zu verpflichten, dass er seinen eigenen, z. B. außenwirtschaftsrechtlichen Pflichten genügen kann. Gerade bei einer Nutzung ausländischer Cloud-Angebote hat ein Cloud-Anwender, der lokalen Restriktionen unterliegt, besondere Sorgfalt bei der Prüfung einer Eignung des Cloud-Angebots für die eigenen Zwecke zu beachten.

63 Als weiteres Beispiel für eine Eingriffsgrundlage aus dem Bereich regulierter Sektoren kann § 37 Abs. 1 S. 4 des Gesetzes über das Kreditwesen (KWG) dienen. Im Falle verbotener oder nicht genehmigter Bankgeschäfte des Cloud-Anwenders kann die zuständige Aufsichtsbehörde Verfügungen auch direkt gegenüber den in die Abwicklung der unzulässigen Geschäfte einbezogenen Unternehmen, Personen oder Verantwortlichen in den betreffenden Unternehmen erlassen. Hierunter fallen alle Unternehmen und Personen, die zum Betrieb der unerlaubten Geschäfte beitragen, in diesem Umfang insbesondere auch Internetprovider und sonstige Dritte wie etwa ein Cloud-Anbieter, der einen Service im Zusammenhang mit Bankgeschäften anbietet. In diesem Zusammenhang wird ein Cloud-Anwender aus dem Finanzsektor auch auf einer unbeschränkten, vertraglichen Haftung des Cloud-Anbieters für die Verletzung regulatorischer Pflichten des Cloud-Anwenders aufgrund eines Fehlverhaltens oder einer Schlechtleistung des Cloud-Anbieters bestehen.

64 **Praxishinweis**
Sollte ein Cloud-Anbieter Dienstleistungen für den Finanzsektor anbieten, so hat er sich mit den besonderen aufsichtsrechtlichen Anforderungen dieser Branche auseinanderzusetzen. Finanzinstitute erwarten üblicherweise, dass branchenspezifische Anforderungen wie aufsichtsrechtliche Rundschreiben (z. B. zu den MaRisk[24]) auch von Cloud-Anbietern beachtet werden, die zumindest auslagerungsähnliche Services anbieten.

24 BaFin-Rundschreiben 10/2012 (BA) „Mindestanforderungen an das Risikomanagement – MaRisk“ vom 14.12.2012, siehe http://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/rs_1210_marisk_ba.html?nn=2818068 (letzter Abruf 22.03.2015).

6 Haftung des Cloud-Anwenders

6.1 Vertragliche Haftung gegenüber dem Cloud-Anbieter

6.1.1 Verletzung von Mitwirkungs- und Nebenpflichten

65 Während die vertragliche Hauptleistung naturgemäß beim Cloud-Anbieter liegt, sind dem Cloud-Anwender typischerweise vertragliche Mitwirkungs- und Nebenpflichten auferlegt. Grundsätzlich ist der Cloud-Anwender verpflichtet, alle in seiner Sphäre liegenden Handlungen vorzunehmen, die erforderlich sind, um den Cloud-Anbieter in die Lage zu versetzen, seine Leistungen zu erbringen, sowie sich so zu verhalten, dass die Systeme des Cloud-Anbieters nicht beeinträchtigt werden. Diese Pflichten beziehen sich insbesondere auf die von ihm in die Cloud eingestellten Daten und Inhalte, erstrecken sich z. B. aber auch auf die Verwaltung der Login-Daten durch den Cloud-Anwender und den Betrieb der eigenen IT-Schnittstellen.

66 Die Mitwirkungs- und Nebenpflichten bezwecken im Hinblick auf eingestellte Inhalte, den Cloud-Anbieter gegen eine von ihm nicht kontrollierbare Inanspruchnahme Dritter aus (i) Schutzrechtsverletzungen (insbesondere Marken- und Urheberrechtsverletzungen), (ii) Verletzungen gegen regulatorische Verstöße (aus den Cloud-Anwender betreffender Regulierung) oder (iii) auch Datenschutzverstöße abzusichern. Diese Haftungsszenarien werden in den Vertragsbedingungen der Cloud-Anbieter zum Teil ausdrücklich angesprochen, zum Teil können sie aber auch als begleitende Schutzpflichten nach allgemeinen Grundsätzen gemäß §§ 241, 242, 280 BGB bestehen bzw. daraus hergeleitet werden. Mit anderen Worten: Wenn es nach der Art des Cloud-Dienstes in weitgehendem Umfang in das Belieben des Cloud-Anwenders gestellt ist, welche Daten und Informationen er in die Cloud stellt, so muss er – im Sinne einer interessengerechten Risikoverteilung – auch das Risiko einer damit verbundenen Rechtsverletzung tragen.

67 Dies gilt jedenfalls gemäß § 280 BGB, wenn der Cloud-Anwender zumindest fahrlässig gehandelt hat, er also bei Wahrung der im Verkehr üblichen Sorgfalt die Rechtsverletzung hätte erkennen und diese – durch Nichteinstellung der betreffenden Daten oder Inhalte – hätte vermeiden können.

68 Auch wenn der Cloud-Anbieter grundsätzlich selbst dafür verantwortlich bleibt, eine mehrmandantenfähige Umgebung vorzuhalten und die jeweiligen Daten voneinander getrennt zu verarbeiten, ist darüber hinaus eine Haftung des Cloud-Anwenders für fehlerhafte Systemnutzung oder eigene Schadsoftware möglich, die eine Betriebsstörung der Cloud verursachen und damit Schadensersatzansprüche anderer Cloud-Anwender gegenüber dem Cloud-Anbieter begründen.

6.1.2 Schutzrechtsverletzungen

69 Das Einstellen von urheberrechtlich geschützten Inhalten Dritter in das System des Cloud-Anbieters kann eine unzulässige Verbreitungs- und Vervielfältigungshandlung im Sinne des § 97 i. V. m. §§ 16, 17 UrhG darstellen. Für diese haftet der Cloud-Anwender unmittelbar auf Schadensersatz und Unterlassung gegenüber dem Inhaber der verletzten Rechte. Entsprechendes gilt bei der Verletzung fremder Markenrechte gemäß § 14 Abs. 2 und 6 MarkenG. Im Rahmen von IaaS-Lösungen und der unzulässigen Nutzung proprietärer Software oder Open Source Software durch den Cloud-Anwender auf der bereitgestellten Infrastruktur kommt zusätzlich eine Haftung gemäß § 97 UrhG i. V. m. § 69c UrhG in Betracht. Zusätzlich ist ein Regressanspruch des Cloud-Anbieters gegen den Cloud-Anwender wegen der Verletzung vertraglicher Nebenpflichten in engen Grenzen denkbar; dies ist zumindest in den Grenzen eines Mitverschuldens (§ 254 BGB) möglich, wenn der Cloud-Anbieter nach Kenntniserlangung von den rechtswidrigen Inhalten diese nicht unverzüglich entfernt und damit seine Haftungsprivilegierung nach § 10 S. 1 Nr. 2 TMG entfällt.

6.1.3 Verstöße des Cloud-Anwenders gegen eigene regulatorische Pflichten

70 Sollte der Cloud-Anwender gegen regulatorische Pflichten verstoßen und dadurch eine Nutzung des Cloud-Dienstes nicht mehr möglich sein, könnten auch Schadensersatzansprüche des Cloud-Anbieters denkbar sein. Verfügt etwa eine Regulierungsbehörde, dass der Dienst nicht in der Form angeboten bzw. genutzt werden darf, kann dem Cloud-Anbieter ein Schadensersatzanspruch gegenüber dem Cloud-Anwender zustehen.

71 Die regulatorischen Rahmenbedingungen für den Cloud-Anwender können sich auch nachträglich ändern und ihm die Nutzung des Cloud-Dienstes verwehren. Soweit der Cloud-Dienst branchenspezifisch angeboten wird (z. B. eine SaaS-Lösung im Bankenumfeld), kann es durchaus sein, dass der Cloud-Anbieter gewisse regulatorische Anpassungen selbst vornehmen muss bzw. der Cloud-Anwender erwarten kann, dass diese in dem Cloud-Dienst rechtzeitig umgesetzt werden und mithin der Cloud-Anwender – zwar im Außenverhältnis gegenüber der Regulierungsstelle, nicht aber im Innenverhältnis gegenüber dem Cloud-Anbieter – haftbar ist. Hier kommt es im Zweifel auf die Natur des geschuldeten Cloud-Dienstes und der zugrunde liegenden vertraglichen Bestimmungen an.

72 **Praxishinweis**
Entsprechend ist beiden Parteien zu raten, sich im Vorfeld auf eine angemessene Risikoverteilung zu einigen und tragfähige Regelung über ein Vertragsanpassungsverfahren (Change-Procedure) zu verständigen. Um das Risiko des Cloud-Anwenders aufgrund neuer aufsichtsrechtlicher Regelungen zu beschränken, kann er einerseits den Cloud-Anbieter auf die Einhaltung auch künftiger regulatorischer Anforderungen verpflichten; andererseits hat er aber auch die kommerziellen Folgen einer Anpassung des Services im Interesse beider Seiten zu regeln. Darüber hinaus ist es empfehlenswert, den Cloud-Anbieter zu verpflichten, sich über allgemeine regulatorische Entwicklungen zu informieren, während der Cloud-Anwender spezielle Anforderungen selbst kommunizieren sollte.

6.1.4 Haftungsbeschränkung zugunsten des Cloud-Anwenders

73 Auch der Cloud-Anwender sieht sich also einem möglicherweise schwer kalkulierbaren Schadensersatzrisiko ausgesetzt. Damit stellt sich die Frage, ob der Cloud-Anwender – jedenfalls soweit es um seine verschuldensabhängige Haftung nach §§ 241, 242, 280 BGB oder auch aus unerlaubter Handlung (gegenüber dem Cloud-Anbieter) geht – ebenfalls eine vertragliche Haftungsbeschränkung vereinbaren sollte. Die von Cloud-Anbietern regelmäßig vorgelegten AGB enthalten solche Regelungen typischerweise nicht. In individuell ausgehandelten Verträgen über Cloud-Dienste kommt es in der Praxis zu einer Vielzahl von Gestaltungen, in denen die Parteien die wechselseitige Risikobalance nach entsprechender Risikobewertung und ausgiebiger Verhandlung einvernehmlich festlegen.

74 **Praxishinweis**
Auch ein Cloud-Anwender sollte die Möglichkeit von Schadensersatzansprüchen des Cloud-Anbieters berücksichtigen. Eine vertragliche Haftungsbeschränkung zugunsten des Cloud-Anwenders kann im Einzelfall daher zweckmäßig und geboten sein. Hierbei bietet es sich an, gerade in einzelvertraglichen Regelungen eine wechselseitige Haftungsbeschränkung der Parteien zu vereinbaren.

75 6.2 Haftung für rechtswidrige Inhalte

Der Cloud-Anwender haftet nach allgemeinen Grundsätzen für die Rechtskonformität von Daten und Inhalten, die er nutzt und ggf. im Rahmen der Nutzung eines Cloud-Dienstes dem Cloud-Anbieter überantwortet. Die Überlegungen zu einer etwaigen Haftung des Cloud-Anbieters für rechtswidrige Inhalte Dritter (s. o. Ziffer 5.1) stehen ggf. neben, aber nicht an Stelle der Haftung des Cloud-Anwenders.

76 **Praxishinweis**
Der Cloud-Anwender bleibt grundsätzlich für die eigenen Daten in der Cloud verantwortlich und muss sich rechtswidrige Inhalte anrechnen lassen. Soweit dieses Haftungsrisiko gegenüber Dritten besteht, kann es vertraglich nicht beschränkt werden. Der Cloud-Anwender sollte etwa die Berechtigung zur Verarbeitung der Daten in einem Cloud-Service oder die Lizenzbedingungen einer in diesem Zusammenhang eingesetzten Software vorab prüfen.

6.3 Haftung für Verstöße gegen das Datenschutzrecht

77 Der Cloud-Anwender unterliegt als verantwortliche Stelle in vollem Umfang der datenschutzrechtlichen Verantwortung und Haftung. Mit Blick auf die gemäß § 11 BDSG abzuschließende Vereinbarung einer Auftragsdatenvereinbarung (ADV) treffen ihn bereits vor Nutzung des Cloud-Dienstes umfangreiche Auswahl-, Prüf- und Sorgfaltspflichten, denen sodann während der Laufzeit des Cloud-Nutzungsverhältnisses entsprechende Überwachungs- und Audit-Pflichten nachfolgen.[25] Bei der Inanspruchnahme von Cloud-Diensten hat der Cloud-Anwender dabei besonders sorgfältig zu prüfen, ob (i) personenbezogene Daten ggf. im Rahmen der vom Cloud-Anbieter bereitgestellten Infrastruktur (einschließlich der von ihm eingesetzten unternehmenszugehörigen oder externen Subunternehmer) außerhalb der EU und des EWR verarbeitet werden und (ii) besondere Arten personenbezogener Daten (§ 3 Abs. 9 BDSG) betroffen sein könnten, bei denen – je nach Lesart der zuständigen Datenschutzbehörde – ein grundsätzliches Hindernis für die Auslagerung der Datenverarbeitung bestehen könnte. Dabei hat der Cloud-Anwender möglicherweise zusätzlich zu prüfen – und im Zweifel mit den Datenschutzbehörden in geeigneter Form abzustimmen –, ob er lediglich anonymisierte oder verschlüsselte Daten in die Cloud einstellen sollte. Verletzt der Cloud-Anwender diese Sorgfaltspflichten, handelt er ordnungswidrig gemäß § 43 Abs. 1 Nr. 2b BDSG – und zwar unabhängig davon, ob er einen Cloud-Nutzungsvertrag nach Maßgabe des § 11 BDSG abschließt oder welche Haftungsbeschränkung gegenüber dem Cloud-Anbieter vereinbart wird.

78 **Praxishinweis**
Der Cloud-Anwender hat vorab eine sorgfältige Datenschutzanalyse durchzuführen. Bei einer weisungsgebundenen Verarbeitung personenbezogener Daten in der Cloud ist eine ausreichende Auftragsdatenverarbeitungsvereinbarung abzuschließen. Insbesondere die Zulässigkeit eines internationalen Datentransfers in Länder außerhalb von EU und EWR (inkl. zusätzlich erforderlicher Vertragsdokumentation wie etwa EU-Standardvertragsklauseln) und der Übermittlungen von etwaigen betroffenen besonderen Arten personenbezogener Daten (§ 3 Abs. 9 BDSG) sowie Möglichkeiten der Anonymisierung, Pseudonymisierung und/oder Verschlüsselung von Daten zur technischen Umsetzung oder gar Vermeidung datenschutzrechtlicher Anforderungen sind genau zu prüfen. Hierbei kommt es gerade nicht auf die Kosten oder die Komplexität des Cloud-Services oder das gewählte Vertragsrecht an, sondern auf die Qualität der betroffenen Daten sowie die Lokalität der Cloud-Server, die zwingend anzuwendendes Datenschutzrecht begründen.

79 Parallel dazu kann der Cloud-Anwender auch dem Sonderproblem des Offenbarens von Geheimnissen i. S. des § 203 StGB ausgesetzt sein, die ihm ggf. als besonders verpflichtetem Berufsträger (Arzt, Rechtsanwalt etc.) oder auch als Institution (z. B. als Krankenversicherung oder Betreiber eines Krankenhauses) anvertraut worden sind. Es besteht in der Fachliteratur weitgehend Einigkeit, dass hier dringender Handlungsbedarf besteht unangebrachte Strafbarkeitsrisiken durch eine gesetzgeberische Lösung abzubauen sind.[26]

25 Siehe dazu umfassend Thesenpapier – Datenschutzrechtliche Lösungen für Cloud Computing der AG Trusted Cloud (http://www.trusted-cloud.de/media/content/140228_Thesenpapier_Datenschutz_gesamt_RZ.pdf; letzter Abruf 17.03.2015).
26 Siehe Thesenpapier – Schweigepflicht bei der Auslagerung von IT-Dienstleistungen der AG Trusted Cloud, S. 17 (http://www.trusted-cloud.de/media/content/150129_Thesenpapier_Schweigepflicht_gesamt_RZ_Ansicht_EZ.pdf; letzter Abruf 17.03.2015).

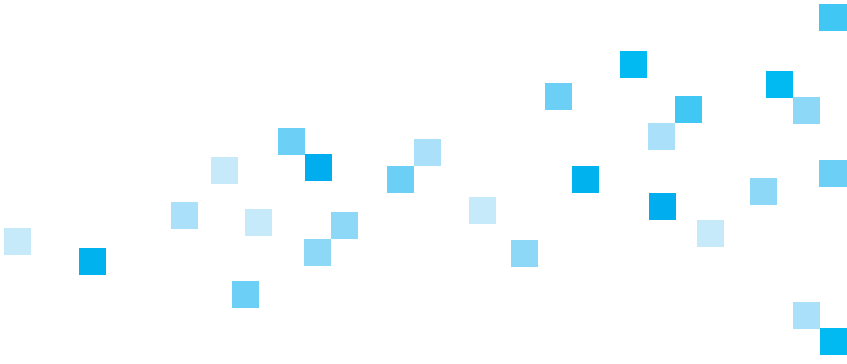
80 **Rechtspolitischer Hinweis**
Das zumindest theoretische Risiko einer Strafbarkeit für Träger von Berufsgeheimnissen, die im Rahmen ihrer ordentlichen Tätigkeit Cloud-Dienste nutzen möchten, bedarf der gesetzgeberischen Abhilfe.

6.4 Haftung für Verstöße gegen Spezialgesetze

81 So wie bereits oben angesprochen gibt es eine Fülle spezialgesetzlicher Regulierungen und Vorschriften, die grundsätzlich die Auslagerung von Dienstleistungen – und damit auch die Nutzung von Cloud-Diensten betreffen (s. o. Ziffer 6.1.3).

82 **Praxishinweis**
Der Cloud-Anwender muss als Adressat der betreffenden regulatorischen Anforderungen vorab und während der Nutzung von Cloud-Diensten sicherstellen, dass er die regulatorischen Voraussetzungen erfüllt, und dies ggf. auch mit den entsprechenden Regulierungsbehörden abklären. Hierbei finden damit oftmals auch auf Cloud-Dienste „klassische" Regelungen zu Auslagerungen (Outsourcing) und damit ein entsprechender Prüfungs- und Dokumentationsbedarf Anwendung. Dies bedeutet, dass etwa Finanzinstitute vertragliche Regelungen gemäß § 25b KWG i. V. m. dem MaRisk-Rundschreiben umsetzen müssen, um eine eigene Compliance mit regulatorischen Vorgaben sicherzustellen.

83 Nach welchen rechtlichen Normen der Cloud-Anwender in Anspruch genommen werden kann, hängt auch hier vom Einzelfall ab. Beauftragt etwa der Cloud-Anwender einen (traditionellen) IT-Dienstleister, der wiederum seine Infrastruktur im Rahmen einer IaaS-Lösung temporär oder dauerhaft auf ein nachgelagertes Subunternehmen auslagert, dürfte es in der Regel bei einer primären (gefahrenabwehrrechtlichen oder regulatorischen) Verantwortlichkeit des Cloud-Anwenders bleiben. Unterliegt der Cloud-Anbieter dagegen aufgrund des Zuschnitts seines Angebotes selbst spezialgesetzlichen regulatorischen Anforderungen, dürfte eine Haftung des Cloud-Anwenders daneben regelmäßig nicht in Betracht kommen.



7 Zusammenfassung

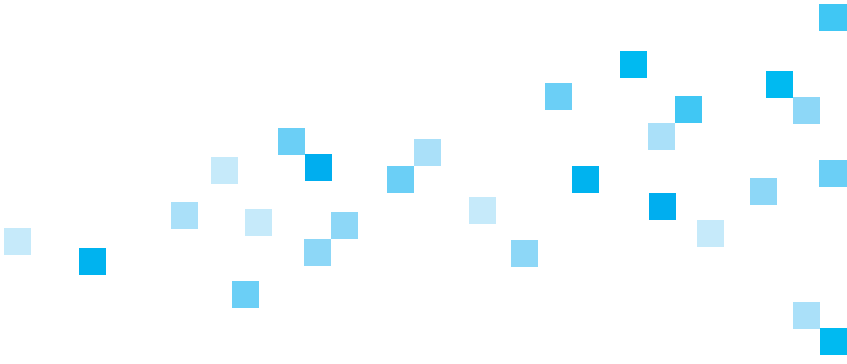
84 Erbringt der Cloud-Anbieter seine Leistung vertragsgerecht, kann das Haftungsrisiko gegenüber dem Cloud-Anwender (also dem Kunden) minimiert werden. Bei Vertragsverletzungen besteht ein vertraglicher Schadensersatzanspruch außerhalb von ausdrücklichen Garantien nur bei Verschulden des Cloud-Anbieters, das z. B. bei allgemeinen, d. h. unverschuldeten Konnektivitätsausfällen nicht vorliegt, und bezüglich Beeinträchtigungen, die schon bei Vertragsschluss vorliegen (§ 536a Abs. 1 1. Alt. BGB). Allerdings kann der Kunde daneben auch bei unverschuldeter Nicht- oder Schlechtleistung die Vergütung mindern (Ziffer 2).

85 Bei durch den Cloud-Anbieter bzw. seine Erfüllungsgehilfen verschuldeten Datenverlusten kann neben dem vertraglichen auch ein gesetzlicher Schadensersatzanspruch aus unerlaubter Handlung – ggf. auch direkt gegenüber einem Subunternehmer des Cloud-Anbieters – bestehen (Ziffer 3).

86 Einer Haftung entgegenstehen können insbesondere vertragliche Haftungsausschlüsse bzw. -grenzen (Ziffer 4). Während in Standardverträgen, die nicht deutschem Recht unterliegen, häufig entsprechend dem Industriestandard weitgehende Haftungseinschränkungen wirksam vereinbart werden können, sind Haftungsbeschränkungen nach deutschem AGB-Recht nur in sehr engem Maße zulässig und daher häufig unwirksam, sofern sie in Standardverträgen enthalten sind. Eine Weiterentwicklung des AGB-rechtlich zulässigen Haftungsrahmens sollte für B2B-Verträge in Ausrichtung auf industrieübliche, vertragstypische Risikoübernahmen und die „good commercial practice“ im Rahmen der Weiterentwicklung des AGB-Rechts diskutiert und vorangebracht werden (Ziffer 4.1). Individualverträge bieten dagegen bereits jetzt flexiblere Möglichkeiten, werden jedoch auch von den Parteien auf der Basis des jeweiligen Risikoprofils zu verhandeln sein (Ziffer 4.2).

87 Schließlich besteht für Cloud-Anbieter das Risiko, für Inhalte zu haften, die Cloud-Anwender in die Cloud einstellen (Ziffer 5). Dieses Risiko besteht insbesondere, wenn die Cloud-Lösung dazu dient, von den Anwendern eingestellte Inhalte Dritten bzw. der Öffentlichkeit zugänglich zu machen. Denn dann ist wahrscheinlich, dass Unterlassungs- und Schadensersatzansprüche auch gegen den Cloud-Anbieter geltend gemacht werden. Diese bestehen in der Regel aber nur, sofern der Cloud-Anbieter trotz Kenntnis von den rechtswidrigen Inhalte untätig bleibt (Ziffer 5.1). Ein weiteres Risiko des Anbieters besteht darin, dass er für regulatorische Vorgaben wie Außenwirtschaftsrecht oder Kreditwesengesetz, die sich aus dem Geschäftsgegenstand des Kunden ergeben, (mit)haftet. Diese Haftung besteht aber in der Regel nur, wenn der Verstoß gegen die – den Kunden treffenden – regulatorischen Anforderungen zugleich einen Verstoß gegen vertragliche Pflichten darstellt (Ziffer 5.2).

88 Der Cloud-Anwender haftet im Außenverhältnis unmittelbar für Schutzrechtsverletzungen, Datenschutzverstöße und regulatorische Verstöße (Ziffer 6). Sie können im Einzelfall vertragliche Regressansprüche des Cloud-Anbieters gegen den Cloud-Anwender auslösen (Ziffer 6.1). Haftungsbeschränkungen, die zugunsten des Cloud-Anwenders greifen, sind in der Regel nicht in den AGB des Cloud-Anbieters vorgesehen. Sie können aber im Wege einer individualvertraglichen Lösung durchaus sinnvoll und geboten sein (Ziffer 6.1.2). Darüber hinaus ist der Cloud-Anwender gut beraten, Daten oder Software vor einer Verarbeitung in der Cloud sorgfältig auf eine entsprechende Eignung bzw. Zulässigkeit für die geplante Verarbeitung zu überprüfen, um eine etwaige Inanspruchnahme durch Dritte oder den Cloud-Anbieter zu vermeiden (Ziffer 6.2). Soweit personenbezogene Daten verarbeitet werden, trifft den Cloud-Anwender als verantwortliche Stelle die datenschutzrechtliche Verantwortlichkeit (Ziffer 6.3).



Autoren

Prof. Dr. Georg Borges, Kompetenzzentrum Trusted Cloud, Universität des Saarlandes

Mathias Cellarius, SAP SE

Dr. Alexander Duisberg, Bird & Bird LLP

Günther Eble, Kommunale Informationsverarbeitung Baden-Franken

Alexander Glaus, Deutsche Bank AG

Björn Hajek, Infineon Technologies AG

Dr. Marc Hilber, Oppenhoff & Partner

Rudi Kramer, DATEV eG

Thomas Kranig, Bayerisches Landesamt für Datenschutzaufsicht

Johannes Landvogt,
Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Dr. Jan Geert Meents, DLA Piper UK LLP

Stephan Sädtler, Universität Passau

Gunther Schiefer, Karlsruher Institut für Technologie

Dr. Joseph Walenta, Deutsches Herzzentrum Berlin

Impressum

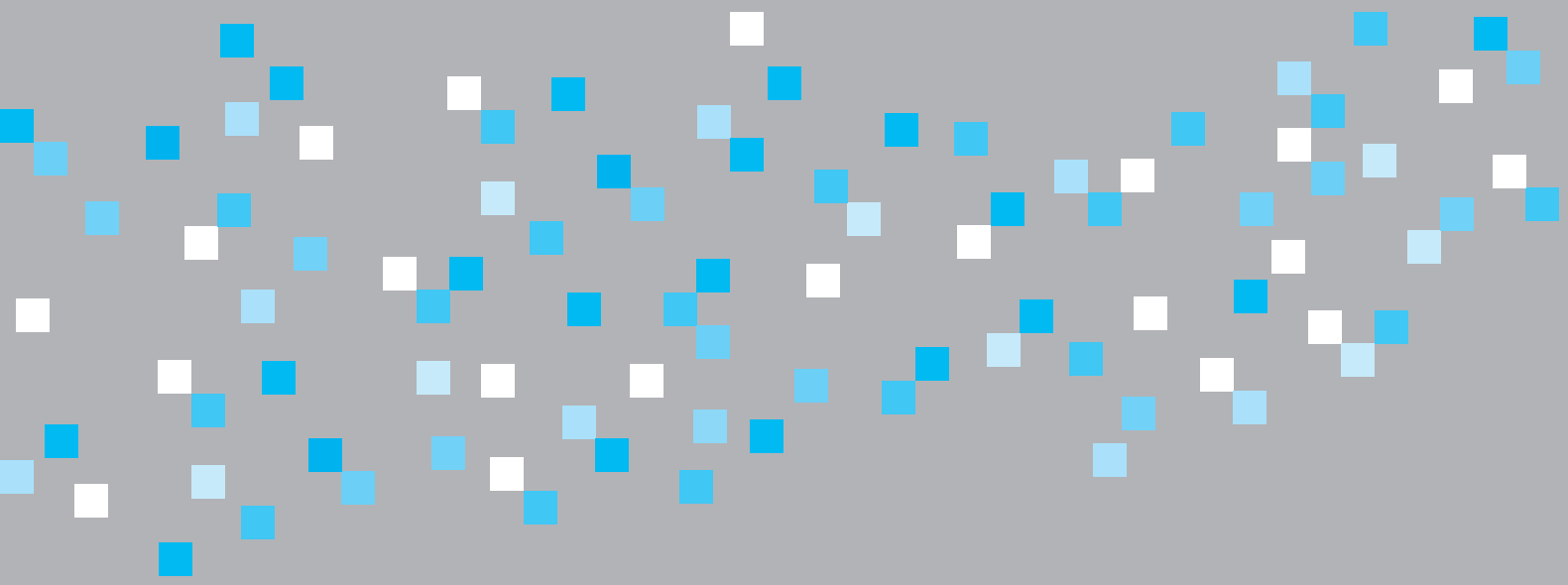
Herausgeber
Kompetenzzentrum Trusted Cloud
Arbeitsgruppe „Rechtsrahmen des Cloud Computing“
E-Mail: kompetenzzentrum@trusted-cloud.de
www.trusted-cloud.de

Im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi)

Gestaltung
A&B One Kommunikationsagentur, Berlin

Druck
DCM Druck Center Meckenheim

Stand: April 2015



www.trusted-cloud.de