CLYDE&CO

Insurance & Reinsurance

Quarterly Update 03/2022 Germany

Contents

Liebe Leserin, lieber Leser,

wir hoffen, dieses Quarterly Update erreicht Sie frisch erholt nach Ihrem Sommerurlaub.

Der Frühsommer brachte mit unseren **Clyde & Co Financial Lines Days** und unserer **European FID&O Roadshow** ein Highlight: endlich wieder in Person und zweimal "full house" in Düsseldorf und München! Sollten Sie verhindert gewesen sein und noch Interesse an den Tagungsunterlagen haben, sprechen Sie uns gerne an. Ebenso freuen wir uns über Anregungen für Themen für das nächste Jahr oder auch unsere anderen Formate, wie zum Beispiel unser Month in Review.

Im Nachgang zu den Financial Lines Days erreichte uns eine weitere schöne Nachricht: Im zweiten Jahr in Folge wurde Clyde & Co als „Kanzlei des Jahres" für Versicherungsrecht ausgezeichnet. Vergeben vom Handelsblatt in Kooperation mit dem US-Verlag Best Lawyers ist diese Auszeichnung ein weiterer Ausdruck unseres Anspruchs, Beratung an der Marktspitze anzubieten. Gleichzeitig wäre eine solche Auszeichnung ohne Ihr Vertrauen nicht möglich. Hierfür sagen wir: Danke!

Mit diesem Quarterly Update 3/2022 geben wir wieder einen Überblick über aktuelle Themen und Entwicklungen in der Versicherungswirtschaft, neue Rechtsprechung und Gesetzesvorhaben, insbesondere:

- Digitales Kaufrecht und das avisierte Gesetz über künstliche Intelligenz – Haftungsfragen in einer vernetzten Welt
- Lösegeldzahlung – die Diskussion nach Cyber-Angriffen nimmt wieder zu
- Schnittstelle Verbraucherschutz und Nachhaltigkeit: Die Neuregelung der Garantieerklärung nach § 479 Abs. 2 BGB
- Verpflichtung zur Abfrage von Nachhaltigkeitspräferenzen
- NIS-2-Richtlinie – Mehr Cybersicherheit durch neue Pflichten und Geldbußen

Und für alle, die mehr wissen möchten: Am **08.11.2022** findet unser **Casualty Day** in Düsseldorf statt. Dabei erwarten Sie interessante Beiträge wie der von Dr. Daniel Kassing zum Thema „*Haftung, Deckung, Regulierung – Europa drückt bei Digitalisierung und KI auf´s Gaspedal*" oder von unserem Kollegen aus dem Londoner Büro Neil Beresford zum Thema „*The Emerging Risk of Plastics Liability – claims arising from the manufacture, use and disposal of plastics A multi-jurisdictional perspective incl. the US, the UK and Europe*".

Wir wünschen Ihnen eine interessante Lektüre. Bleiben Sie weiterhin gesund und zuversichtlich!

Dr. Henning Schaloske

Digitales Kaufrecht und das avisierte Gesetz über künstliche Intelligenz – Haftungsfragen in einer vernetzten Welt

Mit Begriffen wie „Digitalisierung“, „künstliche Intelligenz“, „Internet der Dinge“ (IoT) und „vernetzte Systeme“ sind Anbieter, Nutzer und die Versicherungswirtschaft bereits seit längerer Zeit in Berührung gekommen. Wenn wir von einer vernetzten Welt oder dem Internet der Dinge sprechen, denken wir an eine Ära, in der nahezu alle technischen Geräte um uns herum intelligent und vernetzt sind. Das betrifft eine Vielzahl von Geräten, die miteinander verbunden sind und interagieren. Die Vernetzung bringt dabei Informationen aus allen möglichen Quellen zusammen und verknüpft diese Daten auf unterschiedlichste Art und Weise. So wird dann neues Wissen, künstliche Intelligenz (KI), geschaffen. Dadurch entstehen neue Ideen, neue Dienstleistungen und neue Produkte – und neue Probleme. Denn die Vernetzung und die Autonomie der Systeme bringen einen Rechtsgrundsatz ins Wanken: Ohne Kontrolle keine Haftung.

Aber auch die Legislative ist nicht untätig geblieben und hat bereits einzelne Vorschriften angepasst bzw. neu implementiert. Und in Zukunft stehen, so viel ist sicher, weitere Neuerungen bevor. In diesem Beitrag geben wir einen kurzen Überblick über bereits geltende und bevorstehende Regelungen im Zusammenhang mit dem Einsatz von künstlicher Intelligenz (KI).

Vorauszuschicken ist, dass die nachfolgend skizzierten Änderungen ausschließlich auf Initiativen der EU beruhen. So resultiert die mit Wirkung zum 01.01.2022 erfolgte Implementierung von Regelungen zum Kaufvertrag mit „digitalen Elementen“ in den §§ 475a ff. BGB aus der Umsetzung der europäische Warenverkaufsrichtlinie (RiLi 2019/771). Danach handelt es sich gemäß Definition in § 475a Abs. 2 Satz 1 BGB um „*eine Ware, die in einer Weise digitale Produkte enthält oder mit digitalen Produkten verbunden ist, dass die Ware ihre Funktionen ohne diese digitalen Produkte nicht erfüllen kann*“. Im Wesentlichen werden damit nun IoT-Geräte erfasst, also etwa das Smartphone oder der SmartTV, die ohne die entsprechenden digitalen Elemente nahezu wertlos sind. Voraussetzung für die Anwendung ist indes das Vorliegen eines Verbrauchsgüterkaufs im Sinne von § 474 BGB.

Eine solche Ware mit digitalen Elementen entspricht gemäß § 475b Abs. 4 Nr. 2 BGB den objektiven Anforderungen im Sinne das Sachmängelgewährleistungsrechts nur, „*wenn dem Verbraucher während des Zeitraums, den er aufgrund der Art und des Zwecks der Ware und ihrer digitalen Elemente sowie unter Berücksichtigung der Umstände und der Art des Vertrags erwarten kann, Aktualisierungen bereitgestellt werden, die für den Erhalt der Vertragsmäßigkeit der Ware erforderlich sind, und der Verbraucher über diese Aktualisierungen informiert wird.*“ Damit ist nunmehr das Recht auf Updates im BGB geregelt. Nicht weiter konkretisiert ist indes der Zeitraum, in dem diese Aktualisierungen sichergestellt werden müssen. Nach der Gesetzesbegründung sollen dafür verschiedene Aspekte maßgeblich sein, etwa die Werbung des Verkäufers, die verwendeten Materialien, der Preis sowie die übliche Nutzungs- und Verwendungsdauer der entsprechenden Ware. Der Unternehmer kann der Pflicht sowohl durch ein Update wie auch durch entsprechende Upgrades nachkommen.

Auf europäischer Ebene sind daneben noch die „Regelung der zivilrechtlichen Haftung beim Einsatz künstlicher Intelligenz“ (Entschließung des Europäischen Parlaments vom 20.10.2020 mit Empfehlungen an die Kommission für eine Regelung der zivilrechtlichen Haftung beim Einsatz künstlicher Intelligenz (2020/2014(INL)) und der Vorschlag für ein „Gesetz über künstliche Intelligenz“ (Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates vom 21.04.2021 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung bestimmter Rechtsakte der Union (2021/0106(COD)) hervorzuheben. Während erstere die Neureglung der zivilrechtlichen Haftung in den Blick nimmt, fokussiert sich der zweite Vorschlag auf regulatorische und organisatorische Anforderungen beim Einsatz künstlicher Intelligenz.

Mit Blick auf die Haftung befürwortet das Europäische Parlament in seinem rund 40-seitigen Vorschlag eine Differenzierung zwischen „KI-Systemen mit hohem Risiko“ und „anderen KI-Systemen“. Bei Ersteren soll es eine verschuldensunabhängige Haftung des sog. Frontend-Betreibers sowie dessen Verpflichtung zum Abschluss einer Haftpflichtversicherung geben. Dabei wird ein Hochrisiko definiert als signifikantes Potenzial eines autonom betriebenen KI-Systems, einen Personen- oder Sachschaden zu verursachen. Laut Anhang zu dem Entwurf sollen dazu etwa Geräte und Schutzsysteme in explosionsgefährdeten Bereichen, Aufzüge, Seilbahnen, aber auch biometrische Identifizierung und Kategorisierung von Personen, Verwaltung und Betrieb kritischer Infrastruktur sowie Zugang zu Bildung oder Rechtspflege gehören. Die verschuldensunabhängige Haftung soll durch Haftungshöchstbeträge von EUR 2 Mio. bei Personenschäden und EUR 1 Mio. bei sonstigen Schäden flankiert werden. Dabei hat das Europäische Parlament die Versicherungswirtschaft als eine maßgebliche Säule des Digitalisierungs-Prozesses ausgemacht und an mehreren Stellen in den Erwägungsgründen festgehalten, dass eine Deckung der Haftung als vertrauensbildende Maßnahme unerlässlich ist. Daher soll die EU-Kommission eng mit der Versicherungswirtschaft zusammenarbeiten, um herauszufinden, wie Daten und innovative Modelle genutzt werden können, um Versicherungspolicen zu entwickeln, die eine angemessene Deckung zu einem erschwinglichen Preis bieten.

Die regulatorischen und organisatorischen Anforderungen im Rahmen des rund 120-seitigen Vorschlags für ein „Gesetz über künstliche Intelligenz“ bestehen insbesondere aus der Definition verbotener Praktiken, etwa in Bezug auf „Techniken der unterschwelligen Beeinflussung” des Verhaltens einer Person, um ihr einen Schaden zuzufügen und detaillierten Anforderungen an ein KI-System mit hohem Risiko, wie beispielsweise die Einrichtung eines Risikomanagementsystems, technische Dokumentationen und Aufzeichnungspflichten, Transparenz und Bereitstellung von Informationen für den Nutzer sowie nicht zuletzt einer menschlichen Aufsicht. Darüber hinaus sieht der Vorschlag auch Sanktionsmöglichkeiten, insbesondere in Gestalt von Geldbußen, bei Verstößen gegen die Anforderungen vor. Der Höhe nach sollen Geldbußen von bis zu EUR 30 Mio. oder von bis zu 6 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt werden können. Auch die Verhängung von Geldbußen gegen Organe der Unternehmen soll möglich werden. Das ordentliche Gesetzgebungsverfahren ist mit Blick auf das „Gesetz über künstliche Intelligenz“ eingeleitet und demnächst wird die erste Lesung im Europäischen Parlament stattfinden.

Damit bleiben Regulierungs- und Haftungsfragen rund um KI-Systeme ein Trend der kommenden Jahre, den es auch aus Versicherersicht aufmerksam zu begleiten gilt. Denn mit Pflichtversicherungsvorschlägen bildet gerade die Versicherungswirtschaft aus Sicht der EU eine Säule für die Umsetzung ihrer digitalen Strategie, aus der sich nicht zuletzt auch neue Geschäftschancen ergeben dürften.

Dr. Daniel Kassing, LL.M.

Diskussion um Lösegeldzahlungen nach Cyber-Angriffen nimmt wieder zu

Es ist kein Geheimnis, dass nach Cyber-Angriffen von den betroffenen Unternehmen teilweise auch Lösegelder an die Angreifer gezahlt werden, um die Schlüssel für illegal verschlüsselte Server zu erhalten oder die Veröffentlichung entwendeter Daten zu verhindern. Eine breite öffentliche Debatte über Umfang, Folgen, Strafbarkeit und Versicherbarkeit solcher Lösegeldzahlungen ist in der Vergangenheit jedoch ausgeblieben. Dies könnte sich nun ändern, nachdem einerseits von Seiten der Staatsanwaltschaften die Frage nach einer möglichen Strafbarkeit von Lösegeldzahlungen erneut aufgeworfen wurde und andererseits fast 100 Cybersecurity-Expertinnen und -Experten in einem offenen Brief auf ein geostrategisches Risiko von Lösegeldzahlungen bei Ransomware-Angriffen hingewiesen und ein Verbot der Lösegeldversicherung gefordert haben.

Hintergrund

Ransomware-Angriffe erleben derzeit eine Hochphase und dies nicht nur gefühlt. Das Bundeskriminalamt verzeichnete in dem im Mai 2022 veröffentlichten„ Bundeslagebild Cybercrime 2021“ mit 146.363 allein in Deutschland bekanntgewordenen Delikten einen neuen Höchstwert bei Cyber-Straftaten. Die Dunkelziffer wird deutlich höher eingestuft. Bei den Angriffen werden die betroffenen Organisationen nicht mehr nur mit der Verschlüsselung ihrer IT-Systeme erpresst. Die Angreifer sind bereits seit längerem dazu übergegangen, vor der Verschlüsselung in größerem Umfang Daten aus den angegriffenen Systemen zu exfiltrierten und damit zu drohen, diese zu veröffentlichen. Häufig wird zugleich mit dem Versand der Erpressernachricht bereits eine erste Kostprobe der entwendeten Daten im Darknet zugänglich gemacht, um den Druck auf das Unternehmen zu erhöhen. Teilweise werden Unternehmen auch nur mit der Veröffentlichung entwendeter Daten erpresst, ohne dass es zu einem Verschlüsselungsangriff gekommen ist. Laut einer Studie des Ransomware Recovery First Responders Coveware liegt der internationale Durchschnitt der gezahlten Lösegelder hierbei derzeit bei knapp über USD 200.000. In Einzelfällen können die Lösegelder bei großen Unternehmen auch deutlich höher ausfallen.

Die Praxis zeigt, dass Lösegelder von den angegriffenen Unternehmen nicht leichtfertig gezahlt werden. Im Einzelfällen entscheiden sich die Unternehmen jedoch zu einer Zahlung, , um bestandsgefährdende Betriebsunterbrechungen und/oder das aus der Veröffentlichung wertvollen Know-hows oder sensitiver personenbezogener Daten resultierende Geschäfts- und Haftungsrisiko zu verhindern. Wie immer, wenn man es mit Kriminellen zu tun hat, besteht keine Sicherheit, dass diese sich nach der Lösegeldzahlung auch an ihre Zusage halten und den kryptographischen Schlüssel zur Wiederherstellung der Systeme auch zur Verfügung stellen bzw. von einer Veröffentlichung oder Kommerzialisierung entwendeter Daten im Darknet absehen werden. Aber auch hier zeigt die praktische Erfahrung im Umgang mit Cyber-Angriffen, dass gerade die etablierten Erpressergruppen mit Rücksicht auf das eigene Geschäftsmodell zu ihrem Wort stehen.

Um den finanziellen Schaden einer häufig nicht vermeidbaren Lösegeldzahlung abzufedern, haben Unternehmen daher durchaus ein legitimes Interesse an einem entsprechenden Versicherungsschutz. War der Betrieb einer Lösegeldversicherung in Deutschland lange Zeit unzulässig, hat die BaFin diese strenge Position 1998 aufgegeben und Versicherungen gegen Produkterpressung und Lösegeldforderungen seitdem unter bestimmten Voraussetzungen erlaubt (Rundschreiben 3/1998 (VA)). Seit 2017 ist auch eine Bündelung von Lösegeldversicherungen mit der Versicherung gegen Cyberrisiken erlaubt. Allerdings haben sowohl das Bundeskriminalamt als auch das Bundesamt für die Sicherheit in der Informationstechnik die Empfehlung ausgesprochen, sich im Falle von Erpressungsversuchen grundsätzlich nicht auf Lösegeldzahlungen einzulassen, da diese die Erpresser zur Fortsetzung und Weiterentwicklung der Angriffe motivieren. Hierbei handelte es sich jedoch um rechtlich unverbindliche Aussagen.

Strafrechtliche Relevanz von Lösegeldzahlungen

Seit Beginn des vermehrten Auftretens von Ransomware-Attacken Mitte der 2010er-Jahre wurde in der rechtswissenschaftlichen Literatur immer wieder diskutiert, ob die Zahlung des Lösegelds an die Angreifer als Unterstützung einer kriminellen Vereinigung nach § 129 Abs. 1 S. 2 Strafgesetzbuch (StGB) strafbar ist, weil durch die Zahlung letztlich eine kriminelle Vereinigung „unterstützt“ wird. Über § 129b Abs. 1 S. 1 StGB gilt diese Vorschrift auch für kriminelle Vereinigungen im Ausland. Es ist allerdings bereits fraglich, ob abgenötigte Handlungen der Opfer überhaupt vom kriminalpolitischen Sinn und Zweck dieser sehr weit formulierten Vorschrift erfasst sein sollen. Zudem würde sich immer auch die Frage nach einer eventuellen Rechtfertigung nach § 34 StGB über den rechtfertigenden Notstand oder jedenfalls nach § 35 StGB über den entschuldigenden Notstand stellen. Es wäre zudem paradox, wenn die BaFin die Versicherbarkeit strafbarer Handlungen erlauben würde. Hinzuweisen ist allerdings darauf, dass es hierzu noch keine Rechtsprechung gibt und in der juristischen Strafrechtsliteratur oftmals vertreten wird, dass eine Rechtfertigung auch nicht möglich sei, z.B. weil der Erpresste durch die Zahlung des Lösegelds in andere Rechtsgüter eingreife und sich damit zum Werkzeug eines rechtswidrig handelnden Dritten machen lasse. Aus der Praxis sind uns jedenfalls keine Fälle bekannt, in denen aufgrund einer Lösegeldzahlung im Zusammenhang mit Cyber-Angriffen ein Ermittlungsverfahren eingeleitet oder gar Anklage erhoben wurde. Und das, obwohl Strafverfolgungsbehörden regelmäßig im Rahmen von Strafanzeigen über Cyber-Angriffe und entsprechende Lösegeldzahlungen informiert werden.

Allerdings erschien am 11. Mai 2022 in der Frankfurter Allgemeinen Zeitung unter dem Titel „*Erst erpresst, dann angeklagt*“ ein Artikel in dem der Leiter der Zentral- und Ansprechpartner Cybercrime Nordrhein-Westfalen, immerhin ein Oberstaatsanwalt, dahingehend zitiert wurde, dass durchaus ein Strafbarkeitsrisiko nach § 129 StGB bestehe, da es für den Tatbestand gerade nicht darauf ankomme, dass ein angegriffenes Unternehmen die Absicht habe, die angreifende kriminelle Vereinigung zu unterstützen. Nach §§ 129, 129b StGB würden sich demnach zunächst die Entscheidungsträger im Unternehmen strafbar machen, welche die Lösegeldzahlung veranlassen, da Unternehmen selbst in Deutschland nicht strafrechtlich verfolgt werden können. Würde man jedoch eine betriebsbezogene Straftat durch Leitungspersonen bejahen, könnte gegen das Unternehmen nach § 30 Abs. 1, Abs. 2 S. 1 Nr. 1 Ordnungswidrigkeitengesetz (OWiG) eine Geldbuße von bis zu 10 Millionen Euro festgesetzt werden.

Es bleibt abzuwarten, ob und in welchem Umfang die in dem Artikel dargestellte Auffassung Gehör findet und Staatsanwaltschaften wirklich dazu übergehen werden, nach Lösegeldzahlungen an Cyber-Kriminelle Straf- und Bußgeldverfahren gegen die erpressten Unternehmen und deren Entscheidungsträger einzuleiten. Dies würde die Kooperationsbereitschaft der angegriffenen Unternehmen mit den Strafverfolgungsbehörden sicher nicht fördern. Zugleich würden Lösegeldzahlungen ein persönliches Haftungsrisiko für Entscheidungsträger darstellen und damit auch für D&O-Versicherer von Bedeutung sein. Umgekehrt dürfte der Ausgleich von Lösegeldzahlungen, sofern man diese wie beschreiben als strafbare Handlung ansieht, unter einer Cyberversicherung schwierig werden.

Der F.A.Z.-Artikel zeigt eindrucksvoll, wie schnell eine vermutlich beendete Diskussion wieder aufflammen kann.

Forderung nach Verbot der Lösegeldversicherung im Bereich Cyber

EAuch die Versicherbarkeit von Lösegeldzahlungen könnte zukünftig in Frage gezogen werden. Aufgrund der eindeutigen Positionierung der BaFin sollte man meinen, die Frage sei geklärt. Ende Juni 2022 haben jedoch 93 Cybersecurity-Expertinnen und -Experten aus Wissenschaft und Praxis in einem offenen Brief and „die Bundespolitik“ (abrufbar unter: https://ransomletter.github.io) die Thematik der Lösegeldzahlung bei Ransomware-Angriffen erneut als „Wurzel allen Übels“ problematisiert und darauf verwiesen, dass ein Großteil der Angreifer Russland und anderen sanktionierten Staaten zugeordnet wird. Vor dem Hintergrund dieser geostrategischen Komponente fordern die Unterzeichner des Briefes, neben Maßnahmen zur Verbesserung der IT-Sicherheit in der Breite, Anreize zur Zahlung von Lösegeldern abzuschaffen. Zwar wird nicht die Kriminalisierung der Lösegeldzahlung verlangt, jedoch die Abschaffung der steuerlichen Absetzbarkeit von Ransomware-Lösegeldzahlungen und vor allem die Abschaffung von Versicherungen, die diese Lösegeldzahlungen absichern.

Stattdessen wird gefordert, dass sich Versicherer darauf konzentrieren, die verursachten Umsatzeinbußen und Wiederherstellungsmaßnahmen absichern. Zudem sollen Unternehmen, die durch Ransomware-Angriffe in eine finanzielle Notlage geraten, in angemessener Weise staatlich unterstützt werden, beispielsweise über einen Hilfsfonds. Die Unterstützung sollte jedoch an Bedingungen geknüpft sein, welche sicherstellen, dass die Opfer ihre Pflicht zur eigenständigen Absicherung nicht vernachlässigen. Zudem wird für Unternehmen ab einer bestimmten, nicht näher spezifizierten Größe eine Meldepflicht für Ransomware-Angriffe und Lösegeldzahlungen gefordert.

Der offene Brief ist in den Medien bereits breit diskutiert worden. Eine Reaktion der Politik oder der BaFin steht bislang aus.

Verstärktes Interesse der Datenschutzbehörden

Auch die deutschen Datenschutzbehörden zeigen verstärkt Interesse an Ransomware-Angriffen. So hat das Bayerische Landesamt für Datenschutzaufsicht Ende 2021 bei kleineren und mittleren Unternehmen, kleineren Krankenhäuser, Schulen und Arztpraxen eine Prüfaktion durchgeführt, die darauf ausgerichtet ist, technische und organisatorische Maßnahmen nach Art. 32 Datenschutz-Grundverordnung (DSGVO) mit dem Ziel zu evaluieren, einen Basisschutz gegen Ransomware-Angriffe zu gewährleisten. Die Auswertung der Prüfung steht noch aus.

Die Praxis zeigt zudem, dass Datenschutzbehörden im Nachgang zu Cyber-Angriffen, bei denen personenbezogene Daten, also Informationen über natürliche Personen, betroffen sind, vermehrt danach fragen, ob das meldende Unternehmen ein Erpresserschreiben erhalten hat und wenn ja, mit welchem Inhalt und wie darauf reagiert wurde. Einige Datenschutzbehörden gehen sogar davon aus, dass die Zahlung eines Lösegelds im Rahmen der Pflichtangaben einer Breach Notification nach Art. 33 Abs. 3 lit. d DSGVO offengelegt werden muss. Aus unserer datenschutzrechtlichen Praxis ist uns bekannt, dass einige Datenschutzbehörden die Auffassung vertreten, dass eine Lösegeldzahlung als risikomindernde Maßnahme des betroffenen Unternehmens anzusehen sei. Bei Zahlungen Zwecks Erlangung der Schlüssel zur Wiederherstellung personenbezogener Daten sei das Lösegeld eine „Maßnahme zur Behebung der Verletzung des Schutzes personenbezogener Daten“, erfolgt die Zahlung zur Verhinderung der Veröffentlichung der Daten, sei dies eine „Maßnahme zur Abmilderung ihrer möglichen nachteiligen Auswirkungen“.

Fazit

Die jüngsten Entwicklungen zeigen, dass Lösegeldzahlungen nach Cyber-Angriffen wieder in den Fokus der öffentlichen und rechtspolitischen Debatte rücken könnten. Sofern hier tatsächlich Handlungsbedarf identifiziert wird, bleibt zu hoffen, dass die Problematik im Rahmen einer offen geführten gesetzgeberischen Initiative geführt wird und zu einer zeitnahen Klärung des strafrechtlichen „Graubereichs“ führt. Zu berücksichtigen ist hierbei, dass die angegriffenen Unternehmen und Organisationen in erster Linie Opfer einer Straftat und nicht die Täter sind. Die erneut aufgeflammte Diskussion zeigt allerdings auch, dass mit Lösegeldzahlungen auch unter dem Druck einer vermeintlich existenzbedrohenden Ransomware-Attacke verantwortungsvoll umgegangen werden muss, um den Regelungsdruck und das Strafbarkeitsrisiko nicht unnötig zu erhöhen. Den Forderungen der Erpresser sollte nur als ultima ratio nachgekommen werden. Das bereits geltende Sanktionsrecht verlangt zudem, dass sowohl vor der Zahlung an die Angreifer als auch vor Auszahlung der Versicherungssumme gründlich geprüft werden muss, ob hinter dem Cyber-Angriff nicht eine bereits sanktionierte Organisation oder Einzelperson steckt. Insgesamt ist und bleibt die beste Maßnahme gegen solche Angriffe eine resiliente und regelmäßig überprüfte IT-Sicherheit und die Fähigkeit, die Verfügbarkeit der Systeme nach einem Angriff rasch wiederherzustellen.

Jan Spittka

Dr. Paul Malek

Schnittstelle Verbraucherschutz und Nachhaltigkeit: Die Neuregelung der Garantieerklärung nach § 479 Abs. 2 BGB

Das Ziel, klimaneutral und nachhaltig zu arbeiten und dennoch dem kodifizierten Verbraucherschutz gerecht zu werden, kann sich für Produkthersteller teilweise schwierig gestalten. Beispiel hierfür ist die Neuregelung der Garantieerklärung in § 479 Abs. 2 BGB, die auf den ersten Blick Verbraucherschutz und Nachhaltigkeit nur schwer miteinander vereinbaren lässt, auf den zweiten Blick aber durchaus Möglichkeiten bietet, mit kreativen Lösungsansätzen die vermeintliche Unvereinbarkeit aufzulösen.

Bis zum 01.01.2022 sah § 479 BGB a.F. vor, dass der Verbraucher einseitig vom Unternehmer verlangen kann, dass ihm die Garantieerklärung in Textform ausgehändigt wird. Diese Regelung hatte ihren Ursprung in der Verbrauchsgüterkaufrichtlinie[1]. Ausweislich des Erwägungsgrundes 21 war rechtspolitisches Ziel der Schutz des Verbrauchers vor Irreführung. Um gegenüber dem Verbraucher ausreichend Transparenz zu gewährleisten, sollten die Garantieerklärungen einige grundlegende Informationen enthalten, die der Verbraucher benötigt, um schnell und effektiv seine Rechte geltend machen zu können. Hierzu zählten insbesondere Name und Anschrift des Garantiegebers, das vom Verbraucher einzuhaltende Verfahren für die Geltendmachung der Garantie sowie die Nennung der Ware, auf die sich die Garantie beziehen soll. Zudem sollte verhindert werden, dass der Verbraucher durch die Garantie davon abgehalten wird, seine gesetzlichen Rechte geltend zu machen.[2] Dementsprechend musste die Garantieerklärung ausdrücklich ausweisen, dass die Garantie nicht die gesetzlichen Rechte, d.h. die Gewährleistungsrechte, des Verbrauchers berührt.

Aus diesem Recht des Verbrauchers auf Herausgabe der Garantieerklärung in Textform ist durch die Umsetzung der Warenkaufrichtlinie[3] eine aktive Pflicht des Unternehmers zur Bereitstellung der Garantieerklärung auf einem dauerhaften Datenträger geworden. Mit Wirkung zum 01.01.2022 verpflichtet die neue Regelung in § 479 Abs. 2 BGB n.F. den Hersteller dazu, dem Verbraucher die Garantieerklärungen spätestens zum Zeitpunkt der Lieferung der Ware auf einem dauerhaften Datenträger zur Verfügung zu stellen.[4] Ein Verlangen des Verbrauchers ist somit nicht mehr notwendig.[5] Als dauerhafter Datenträger gilt nach Art. 2 Nr. 11 der Warenkaufrichtlinie *„jedes Medium, das es dem Verbraucher oder dem Verkäufer gestattet, an ihn persönlich gerichtete Informationen derart zu speichern, dass er sie in der Folge für eine für die Zwecke der Informationen angemessene Dauer einsehen kann, und das die unveränderte Wiedergabe der gespeicherten Informationen ermöglicht“*.[6] Der Begriff des „dauerhaften Datenträgers“ ist im deutschen Recht in § 126b BGB definiert und stellt nichts anderes dar, als die nationale Textform. Durch die Neuregelung von § 479 Abs. 2 BGB soll der Verbraucherschutz dadurch gestärkt werden, dass sich der Verbraucher jederzeit seiner Rechte vergewissern kann und er einen Beweis für die Garantie in der Hand hält. Die gesetzlichen Anforderungen an den Inhalt der Garantieerklärung wurde durch die Warenkaufrichtlinie im Ergebnis zwar nicht erweitert, aber durch klarere Vorgaben gesetzlich ausdrücklich konkretisiert.

Durch die nach dem neuen § 479 Abs. 2 BGB nunmehr erforderliche Garantieerklärung auf einem dauerhaften Datenträger hat sich der Pflichtenkreis des Unternehmers indes deutlich erweitert. Kommt der Unternehmer dieser Pflicht nicht nach, kann dies insbesondere zu Schadenersatzansprüchen führen, wenn die Unterlassung dazu führt, dass der Verbraucher seine Rechte nicht rechtzeitig geltend macht.[7] Gemäß § 476 Abs. 1 BGB ist die Regelung in § 479 BGB zudem unabdingbar, weshalb ein Verzicht auf die Pflicht des zur Verfügung Stellens der Garantieerklärung nicht möglich ist.

Diese aus Verbrauchersicht sicherlich begrüßenswerte Pflicht zur proaktiven Transparenz stellt die Hersteller von Produkten, die im stationären Handel veräußert werden, allerdings angesichts der unternehmensseitig nunmehr vermehrt angestrebten Nachhaltigkeit vor Probleme. Denn der Produkthersteller wird eine Lösung wollen, die zum einen die Einhaltung der gesetzlichen Anforderungen gewährleistet, zum anderen aber auch nachhaltig ist. Aus Sicht der Hersteller wäre es am naheliegendsten, dem Verbraucher zeitgleich mit dem Kauf des Produktes eine Garantieerklärung auf einem dauerhaften Datenträger, wie etwa einem Papierausdruck auszuhändigen. Dieser Lösungsansatz erweist sich indes nur dann sicher handhabbar, wenn der Hersteller zugleich Verkäufer ist oder er – bei einem zwischengeschalteten Händler – in der Lieferkette durch entsprechende tatsächliche Vorkehrungen und vertragliche Regelungen sicherstellt, dass die Garantieerklärung an den Endkunden übergeben wird. Ist der Hersteller nicht zugleich der Letztverkäufer, besteht dabei insbesondere die Möglichkeit, die Garantieerklärung der Produktverpackung vor der Veräußerung an den Zwischenhändler als Papierausdruck beizulegen. Allerdings lässt sich auf diesem Weg nicht gewährleisten, dass die Garantieerklärung bei häufigeren Änderungen durch den Hersteller zum Zeitpunkt des Verkaufs durch den Zwischenhändler noch aktuell ist. Hinzukommt, dass diese Lösung für jedes einzelne Produkt neben der Verpackung die Verwendung von weiterem Papier für die Garantieerklärung voraussetzt, was dem Nachhaltigkeitsgedanke diametral entgegensteht. Denn gerade bei kleinteiligeren Waren wird der Aufdruck direkt auf der Verpackung – der im Übrigen dann ebenfalls nicht aktualisiert werden könnte – aufgrund des Umfangs der Garantieerklärung oftmals nicht möglich sein.

Eine die Ressourcen schonendere Möglichkeit wäre es, die Produktverpackung mit einem entsprechenden QR-Code zu versehen. Dieser könnte vom Kunden gescannt werden und ihm dann die jeweils aktuelle Version der Garantieerklärung anzeigen.[8] So könnte der Hersteller seiner Pflicht zur Verfügungsstellung einer Garantieerklärung auf einem nachhaltigeren Weg nachkommen, da unnötige Ausdrucke verhindert würden.

Wie eingangs bereits angesprochen, gilt als dauerhafter Datenträger nach Art. 2 Nr. 11 der Warenkaufrichtlinie *„jedes Medium, das es dem Verbraucher oder dem Verkäufer gestattet, an ihn persönlich gerichtete Informationen derart zu speichern, dass er sie in der Folge für eine für die Zwecke der Informationen angemessene Dauer einsehen kann, und das die unveränderte Wiedergabe der gespeicherten Informationen ermöglicht“*.[9] Vor diesem Hintergrund erscheint die Nutzung eines QR-Codes auf den ersten Blick als ein gangbarer Weg. Auf den zweiten Blick wird aber deutlich, dass eine derartige Abgabe der Garantieerklärung zum einen nicht zu vernachlässigbaren Mehraufwand mit sich bringen würde und zum anderen aufgrund von Rechtsunsicherheiten sowie tatsächlichen Hindernissen auf Seiten der Verbraucher derzeit nicht zu empfehlen sein dürfte. Denn jedem Verbraucher müsste, in einem personalisierten Bereich, auf den nur er über seinen Benutzernamen und Passwort zugreifen kann, die Information im Internet zur Verfügung gestellt werden. Die Organisation wäre dann vom Produkthersteller zu

1. Richtlinie 1999/44/EG des Europäischen Parlaments und des Rates vom 25.05.1999 zu bestimmten Aspekten des Verbrauchsgüterkaufs und der Garantien für Verbrauchsgüter.
2. FraktionsE, BT-Drs. 14/6040, 246.
3. Richtlinie 2019/771 des Europäischen Parlaments und des Rates vom 20.05.2019 über bestimmte vertragsrechtliche Aspekte des Warenkaufs.
4. Regierungsentwurf zur Warenkaufrichtlinie. S. 19: RegE_Warenkaufrichtlinie.pdf;jsessionid=D2B717088BEC3DC0A5421D0E534A003E.1_cid289 (bmj.de).
5. Regierungsentwurf zur Warenkaufrichtlinie S. 19: RegE_Warenkaufrichtlinie.pdf;jsessionid=D2B717088BEC3DC0A5421D0E534A003E.1_cid289 (bmj.de).
6. (EU) 2019/771 des Europäischen Parlaments und des Rates vom 20.05.2019 über bestimmte vertragsrechtliche Aspekte des Warenkaufs.
7. Faust, in: BeckOK BGB, 62 Edit. Stand 01.05.2022, § 479 Rn. 12.
8. Raue: Herstellergarantien als QR-Code? | Stationärer Handel (taylorwessing.com).
9. Richtlinie 2019/771 des Europäischen Parlaments und des Rates vom 20.05.2019 über bestimmte vertragsrechtliche Aspekte des Warenkaufs.

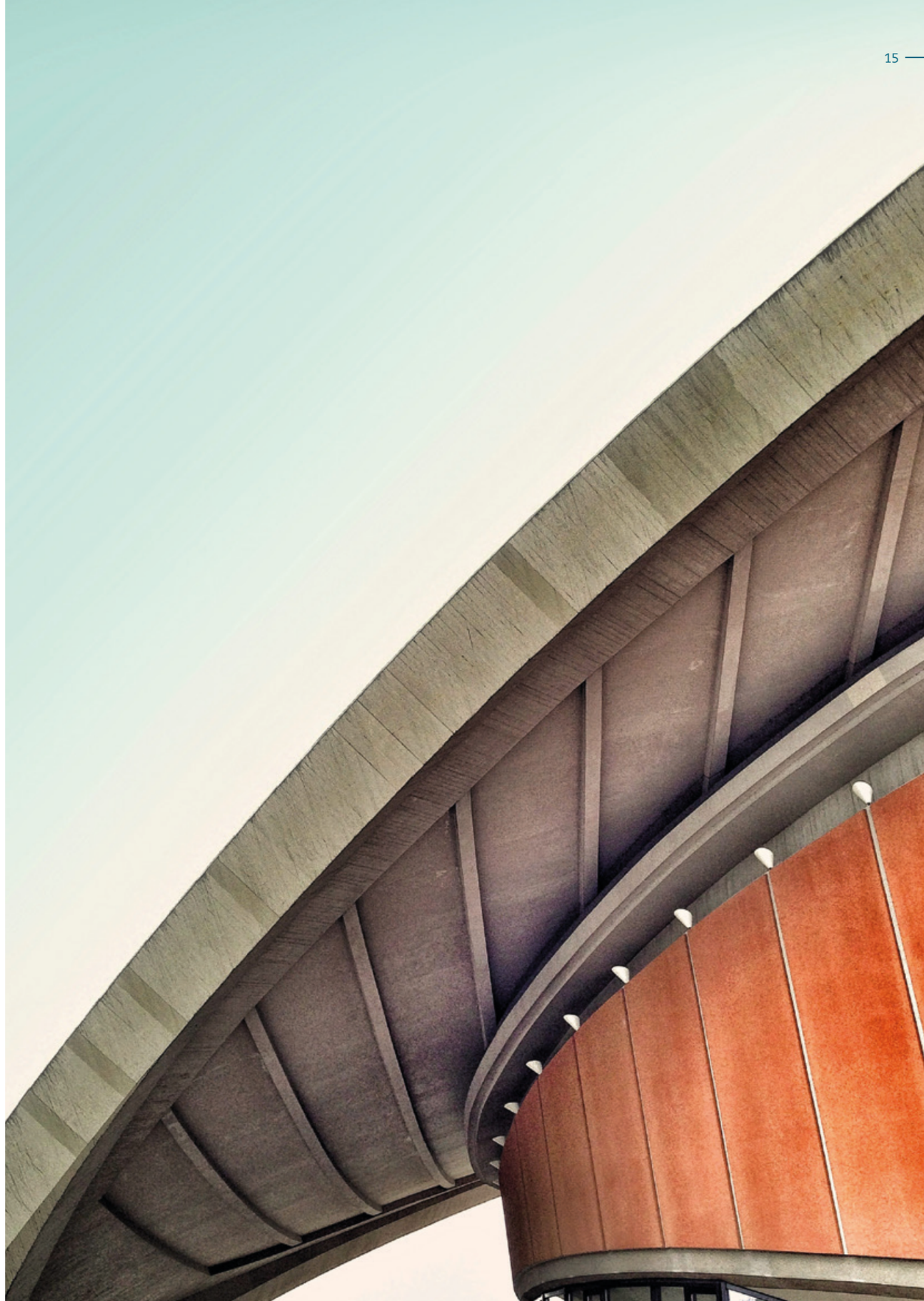
gewährleisten oder an einen Dritten auszulagern. Im Ergebnis wäre ein weitreichender – unter Umständen auch finanzieller – Mehraufwand seitens des Herstellers notwendig, um der gesetzlichen Pflicht nachzukommen. Zudem ist unklar, ob diese Art der zur Verfügungstellung den Ansprüchen des europäischen Gesetzgebers an die Zugänglichkeit der Erklärung genügt. Denn der Wortlaut vom § 479 Abs. 2 BGB n.F. („*zur Verfügung stellen*“) sowie die Definition des „dauerhaften Datenträgers“ („*jedes Medium, das es dem Verbraucher […] gestattet […] Informationen derart zu speichern*“) indizieren, dass dem Verbraucher der Zugang auch technisch möglich sein muss. Wie sich die der Umstand auswirken könnte, dass dem Verbraucher zur Kenntnisnahme des Inhalts eines solchen Datenträgers notwendige Technik nicht zur Verfügung steht, ist bereits im Rahmen von Art. 6 Abs. 3 Verbrauchsgüterkaufrichtlinie [10] und damit auch im Rahmen von § 479 Abs. 2 BGB a.F. diskutiert worden.[11] Teilweise wurde vertreten, dass die Anforderung aus § 479 Abs. 2 BGB a.F. nur dann erfüllt sei, wenn die Mitteilung ohne Hilfsmittel lesbar ist.[12] Bei der Lösung über den QR-Code wäre vor diesem Hintergrund zumindest darüber nachzudenken, ob die Anforderung an die Zugänglichkeit erfüllt ist, wenn wohl noch tatsächliche Zugangsbarrieren für Verbraucher ohne QR-Scanner in Form eines Smartphones oder ohne das grundsätzlich notwendige „Know How“ bestehen.

Dementsprechend ist zu konstatieren, dass wohl derzeit kein Weg an der Papierform vorbeiführt – selbst, wenn diese die vorstehend dargestellten Probleme aufweist. Der europäische Gesetzgeber scheint hier – bewusst oder unbewusst – den Verbraucherschutz deutlich vor dem Ziel der Nachhaltigkeit priorisiert zu haben.

Dr. Isabelle Kilian

Dr. Behrad Lalani

10. Richtlinie 1999/44/EG des Europäischen Parlaments und des Rates vom 25.05.1999 zu bestimmten Aspekten des Verbrauchsgüter.
11. Lorenz, in MüKo BGB, 9. Aufl. 2021, § 479 Rn.8 f.
12. Faust, in BeckOK BGB, 61. Edit., § 479 Rn. 12.



Verpflichtung zur Abfrage von Nachhaltigkeitspräferenzen

Seit dem 02.08.2022 müssen Versicherer und Versicherungsvermittler, die Versicherungsanlageprodukte anbieten, die Nachhaltigkeitspräferenzen ihrer Kunden überprüfen. Diese Pflicht besteht, da Nachhaltigkeitskriterien in den Prozess der Bewertung des Risikoprofils von Investoren aufgenommen wurden. Zurückzuführen ist dies auf zwei EU-Verordnungen[1], die insbesondere die IDD ergänzen und einen Regelungsrahmen zur Abfrage von Nachhaltigkeitspräferenzen enthalten.

Nachhaltigkeitsbezogene Offenlegungspflichten bestehen zwar bereits seit 2021[2]. Nunmehr müssen jedoch die Nachhaltigkeitspräferenzen des betreffenden Kunden im Rahmen der Angemessenheitsprüfung durch den Versicherer oder Vermittler aktiv abgefragt werden. Äußert der Kunde dabei bestimmte Nachhaltigkeitspräferenzen, denen das Versicherungsanlageprodukt nicht entspricht, sind Versicherer und Versicherungsvermittler bei Erfüllung ihrer Beratungspflichten nicht schon deshalb daran gehindert, von einer Empfehlung des Versicherungsanlageprodukts nach § 7c Abs. 1 und Abs. 2 VVG abzusehen. Sie müssen jedoch die Abweichung von den individuellen Nachhaltigkeitspräferenzen erklären, dem Kunden eine Anpassung dieser geäußerten Präferenzen ermöglichen und die Gründe für eine trotz verbleibender Abweichungen ausgesprochene Empfehlung aufzeichnen.[3]

Nachhaltigkeitspräferenz ist danach die Entscheidung eines Kunden oder potenziellen Kunden, ob und, wenn ja, inwieweit eines der folgenden Finanzprodukte in seine Anlage einbezogen werden, sollte:

- ein Versicherungsanlageprodukt, bei dem der Kunde bestimmt, dass ein Mindestanteil in ökologisch nachhaltige Investitionen im Sinne der „Taxonomie-Verordnung“ ((EU) 2020/852) angelegt werden soll;
- ein Versicherungsanlageprodukt, bei dem der Kunde bestimmt, dass ein Mindestanteil in nachhaltige Investitionen (Investition in eine wirtschaftliche Tätigkeit, die zur Erreichung eines Umweltziels oder eines sozialen Ziels beiträgt, ohne andere Nachhaltigkeitsziele erheblich zu beeinträchtigen[4]), angelegt werden soll;
- ein Versicherungsanlageprodukt, bei dem die wichtigsten nachteiligen Auswirkungen auf Nachhaltigkeitsfaktoren berücksichtigt werden.

Bezüglich der Begriffe "erhebliche Beeinträchtigungen“ und "wichtigste nachteilige Auswirkungen auf Nachhaltigkeitsfaktoren" werden technische Regulierungsstandards in der Verordnung (EU) 2022/1288, die ab dem 01.01.2023 gelten soll, detailliert beschrieben. Jeder Finanzmarktteilnehmer muss anhand einer Liste die wichtigsten nachteiligen Auswirkungen erkennen können. Eine Vorlage hierfür findet sich im Anhang I der Verordnung.

Hinweise der DIN-Norm zur konkreten Umsetzung

Auf der Grundlage der oben genannten Grundsätze hat das Deutsche Institut für Normung (**DIN**) Leitlinien veröffentlicht (Anhang B zur DIN-Norm 77230), die dabei helfen, die Anforderungen an die Abfrage zu Nachhaltigkeitspräferenzen zu erfüllen.

Die Leitlinien enthalten sieben Fragen, die sowohl die Bereitschaft des Verbrauchers betreffen, Nachhaltigkeitsziele zu verfolgen, als auch den Wunsch, in seiner Investitionsstrategie Schwerpunkte zu setzen:

- Die erste Frage zielt darauf ab, das allgemeine Interesse des Verbrauchers an Nachhaltigkeit zu überprüfen.
- Die Folgefrage soll klären, ob der Verbraucher in seiner Anlagestrategie bestimmte **Schwerpunkte** setzen möchte. Es kann eine pauschale Schwerpunktsetzung auf ökologische (E) und soziale (S) Themen angeboten werden.
- Der Verbraucher kann auch selbst innerhalb der Themenbereiche E und S bestimmte Schwerpunkte setzen.
- Anschließend ist festzulegen, mit welcher **Intensität** die definierten Ziele verfolgt werden sollen, d. h. ob die Finanzprodukte einen wesentlichen oder einfachen Beitrag zur Erreichung der Ziele leisten sollten.
- Neben der Intensitätsprüfung erfolgt die Festlegung der **Mindestanteile**, mit denen jeder Themenbereich im gewünschten Finanzprodukt vertreten sein soll.
- Zu erfragen ist weiterhin, ob Investitionen ausschließlich in Unternehmen getätigt werden, die bereits nachhaltig agieren oder auch in Unternehmen, die sich in einem **Transformationsprozess** befinden. In diesem Zusammenhang ist zu erläutern, was unter „Transformation“ zu verstehen ist.
- Schließlich gilt zu erörtern, ob und inwieweit der Verbraucher durch die Formulierung von **Ausschlusskriterien** negative Auswirkungen auf Nachhaltigkeitsfaktoren vermeiden möchte. Die Frage muss mindestens fünf Ausschlussthemen vorschlagen und ein Freitextfeld enthalten.

Dr. Andreas Börner

Victor Gontard

1. Delegierte Verordnungen (EU) 2021/1253 und (EU) 2021/1257.
2. Delegierte Verordnung (EU) 2019/2088.
3. Erwägungsgründe (11) bis (14) der Delegierten Verordnung (EU) 2021/1257.
4. Artikel 2 Nummer 17 der Delegierten Verordnung (EU) 2019/2088.

NIS-2-Richtlinie – Mehr Cybersicherheit durch neue Pflichten und Geldbußen

Mit der EU-Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS-Richtlinie; Richtlinie (EU) 2016/1148) aus dem Jahr 2016 wurde ein einheitlicher Rechtsrahmen für den europaweiten Aufbau nationaler Kapazitäten im Bereich der Cybersicherheit inklusive Mindestanforderungen und Meldepflichten für Kritische Infrastrukturen (sog. „KRITIS") festgelegt. In Anbetracht der schnell voranschreitenden Digitalisierung der letzten Jahre soll dieser Rechtsrahmen nun überarbeitet und durch eine neue Richtlinie, die sog. „**NIS-2-Richtlinie**", ersetzt werden.

Hierzu hat sich die NIS-2-Richtlinie selbst drei grundsätzliche Ziele gesetzt, die wie folgt zusammengefasst werden können:

- Erhöhung der Cybersicherheit von Einrichtungen der kritischen Infrastruktur in relevanten Sektoren durch neue Regelungen;
- Reduzierung der Unterschiede in der Cybersicherheit zwischen den verschiedenen Sektoren durch weitere Angleichung;
- Verbesserung der Reaktionsfähigkeit und Zusammenarbeit der unterschiedlichen Akteure (z.B. Einrichtungen und Behörden) bei massiven Cybervorfällen und -krisen.

Der Wortlaut des Entwurfs der EU-Kommission vom 16.12.2020 ist hier abrufbar. Eine Übersichtsseite und ein kurzes Factsheet der EU-Kommission sowie ein Briefing aus Juni 2022 des Wissenschaftlicher Dienstes des EU-Parlaments stehen als offizielle Begleitmaterialen ebenfalls zur Verfügung. In einigen Publikationen wird die NIS-Richtlinie (bzw. deren baldiger Nachfolger) auch „Cybersecurity-Richtlinie" genannt, was im Zusammenspiel mit weiteren aktuellen Gesetzesinitiativen jedoch zu Verwechslungen führen kann.

Nachdem die drei Gesetzgebungsinstitutionen der EU im Trilog am 13.05.2022 eine vorläufige Einigung über den Entwurf erzielten, ist die förmliche Annahme des Gesetzestextes zeitnah – nachdem zunächst noch Ende 2021 angepeilt wurde – geplant. Nach Inkrafttreten haben die Mitgliedstaaten 18 Monate Zeit, um die Richtlinie in nationales Recht umzusetzen. In Deutschland dürfte dies meiner einer erneuten Änderung des im letzten Jahr verabschiedeten IT-Sicherheitsgesetz 2.0 einhergehen, d.h. im Schwerpunkt durch Änderung des BSI-Gesetzes.

Einordnung

Die Überarbeitung der NIS-Richtlinie erfolgt im Rahmen der europäischen Strategie zur „Gestaltung der digitalen Zukunft Europas", bei der die erste von drei Säulen zur „Technologie im Dienste der Menschen" u.a. durch die „Die neue Cybersicherheitsstrategie der EU für die digitale Dekade" konkretisiert wird. Sie zielt darauf ab, die Widerstandsfähigkeit gegenüber Cyberbedrohungen zu stärken und sicherzustellen, dass Bürger und Unternehmen von vertrauenswürdigen digitalen Technologien profitieren.

Dabei soll die NIS-2-Richtlinie bereits bestehende Gesetzesvorhaben im Bereich der Cybersicherheit ergänzen, insbesondere:

- Die eIDAS-Verordnung (Verordnung (EU) 910/2014), die Standards für die elektronische Identifizierung für Transaktionen einführte;
- Die Zahlungsdiensterichtlinie (Richtlinie (EU) 2015/2366; besser bekannt als „PSD2-Richtlinie"), die für Zahlungen u.a. eine Zwei-Faktor-Authentifizierung vorgab;
- Den Rechtsakt zur Cybersicherheit (Verordnung (EU) 2019/881; auch Cybersecurity Act, CSA), der ein europaweites Rahmenwerk zu IT-Sicherheitszertifizierung normierte;
- Die Delegierte Verordnung (EU) 2022/30 vom 12.01.2022 zur Ergänzung der sog. Funkanlagen-Richtlinie (Richtlinie (EU) 2014/53), welche die Sicherheit von 5G-Netzen stärken soll.

Daneben wird die NIS-2-Richtlinie auch weitere Gesetzesvorhaben einbeziehen, insbesondere:

- Das Gesetz zur Cyberwiderstandsfähigkeit (Cyber Resillience Act, CRA), welche durch einen horizontalen Zertifizierungsrahmen die Cybersicherheit vereinheitlichen soll;
- Die Verordnung über digitale Betriebsstabilität (Digital Operational Resilience Act, DORA), mit der sichergestellt werden soll, dass der europäische Finanzsektor in der Lage ist, die Betriebsstabilität im Falle einer schwerwiegenden Störung aufrechtzuerhalten.

Wesentliche Änderungen der NIS-2-Richtlinie

Zur Erreichung der oben genannten Ziele soll mit der NIS-2-Richtlinie insbesondere:

- Die Unterscheidung zwischen „wesentlichen" (essential") und „wichtigen" („important") Einrichtungen eingeführt werden (Art. 1 Abs. 2 lit. b i.V.m. Anhang I und II)

Die Differenzierung zwischen „Betreibern wesentlicher Dienste" und „Anbietern digitaler Dienste" wird aufgegeben und nunmehr anhand des Grades der Kritikalität zwischen „wesentlichen" („essential") und „wichtigen" („important") Einrichtungen unterschieden (vgl. Erwägungsgrund 11). Eine saubere sprachliche Trennung bei Leitlinien zur Cybersicherheit wird im Deutschen also noch wichtiger.

Die neue Einteilung dient insbesondere der Vereinheitlichung und ist von Bedeutung dafür, welche Einrichtungen von den Maßnahmen (s.u.) umfasst werden.

- Der Anwendungsbereich um weitere Sektoren (von 8 um 8 weitere auf 16) verdoppelt werden (Art. 2)

Zu den Sektoren für wesentliche Einrichtungen gehörten bereits Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasser, Digitale Infrastruktur. Neu dazu kommen die Sektoren Abwasser, Öffentliche Verwaltung und Weltraum.

In den Sektoren für wichtige Einrichtungen waren bisher Anbieter digitaler Dienste (also Online-Marktplätze und Suchmaschinenanbieter), die nun um dem Teilsektor der sozialen Netzwerke erweitert werden, enthalten. Neu dazu kommen die Sektoren Post- und Kurierdienste, Abfallbewirtschaftung, Chemie, Lebensmittelwirtschaft und Teile der Industrie (insb. Medizinprodukte, Datenverarbeitungsgeräte, Maschinen- und Fahrzeugbau).

Auch innerhalb der wesentlichen Sektoren gibt es Anpassungen. So sind im Sektor Energie – passend zur „Gaskrise" – die Teilsektoren Fernwärme und Wasserstoff und im Teilsektor Öl nun auch wesentliche Bevorratungsstellen enthalten. Im Sektor Gesundheitswesen kommen – als Folge der Corona-Pandemie – Referenzlaboratorien und Einrichtungen zur Forschung und Produktion von Arzneimitteln hinzu.

Wichtig ist, dass Kleinst- und kleine Unternehmen (weniger als 50 Beschäftigte und unter 10 Mio. € Jahresumsatz) gem. Art. 2 Abs. 1 grundsätzlich vom Anwendungsbereich ausgenommen sind, sofern sie nicht unter eine der Rückausnahmen des Art. 2 Abs. 2 (z.B. bestimmte Netzwerk- oder DNS-Diensteanbieter, oder solche Einrichtungen, bei denen mögliche Störungen weitreichende Auswirkungen für einen Mitgliedsstaat oder bestimmte Sektoren haben) fallen. Hierfür sollen die Mitgliedsstaaten eine Liste der ermittelten Einrichtungen erstellen und diese regelmäßig (min. alle zwei Jahre) überprüfen.

– Die Pflichten für betroffene Einrichtungen umfangreich erweitert werden, u.a. Maßnahmen zur Prävention (Art. 18), eine Risikobewertung der Lieferkette (Art. 19), die Erstmeldung von Vorfällen innerhalb von 24 Stunden (Art. 20)

Nach Art. 17 der NIS-2-Richtlinie sind Leistungsorgane der Einrichtungen für die Umsetzung, Überwachung und bei Nichteinhaltung der Verpflichtungen verantwortlich. Zudem haben sie regelmäßig an spezifischen Schulungen im Bereich der Cybersicherheit teilzunehmen.

In Art. 18 Abs. 1 ist eine allgemeine Anforderung an technische und organisatorische Maßnahmen enthalten, die in Abs. 2 um (allerdings erneut weitgehend unbestimmte) Mindestmaßnahmen konkretisiert wird. Diese umfassen Sicherheitskonzepte, Maßnahmen zur Erkennung von Sicherheitsvorfällen und zur Aufrechterhaltung des Betriebs sowie den Einsatz von Kryptografie und Verschlüsselung. Hinsichtlich der Verschlüsselung wurde der Entwurf zur Richtlinie in der rechtswissenschaftlichen Literatur bereits kritisiert, da zum einen die Grundsätze des Datenschutzes gewahrt werden sollen, andererseits jedoch ein Zugriff für Strafermittlungs- und -verfolgungsbehörden ermöglicht werden soll, was dem Ziel der höchsten Cybersicher widerspreche. Auch sei die wichtige Problematik um sog. „Hackbacks“ zwar aufgegriffen, aber nicht konkretisiert worden.

Gemäß Art. 19 kann die Kooperationsgruppe zudem in Zusammenarbeit mit der Agentur der Europäischen Union für Cybersicherheit (ENISA) Risikobewertungen der Sicherheit der Lieferketten bestimmter Informations- und Kommunikationstechnikdienste (IKT-Dienste) durchführen. Darunterfallende Einrichtungen werden hierfür entsprechende Informationen vorhalten und bereitstellen müssen.

Nach Art. 20 Abs. 4 lit. a müssen Einrichtungen innerhalb von 24 Stunden nach Kenntnisnahme eines erheblichen Sicherheitsvorfall eine erste Meldung an die zuständigen Behörden oder das Computer Security Incident Response Team (CSIRT) übermitteln. Dabei müssen sie angeben, „ob der Sicherheitsvorfall vermutlich auf rechtswidrige oder böswillige Handlungen zurückzuführen ist“, also nicht bloß auf einem technischen oder menschlichen Fehler beruht. Sodann ist spätestens einen Monat nach der Erstmeldung einen Abschlussbericht mit umfangreicheren Informationen zu übermitteln. Hierbei weicht der Entwurf, der als Ziel die Vereinheitlichung von Anforderungen hat, zumindest von der Vorgabe des Art. 33 Abs. 1 DSGVO ab, wonach risikorelevante Verletzungen personenbezogener Daten möglichst binnen 72 Stunden zu melden sind, ansonsten die Verzögerung zu begründen ist. Dies scheint vor dem Hintergrund der NIS-2-Richtlinie jedoch aus drei Gründen geboten: (1) Umfasst diese „nur“ Einrichtungen der kritischen Infrastruktur und nicht jede datenverarbeitende Stelle; (2) ist nicht jeder Vorfall, der zu einem Risiko für betroffene Dritte führt, umfasst, sondern nur solche, die zu „erheblichen materiellen oder immateriellen Verlusten“ für die Einrichtung oder betroffene Dritte führen können. Dies mag sich gegebenenfalls überschneiden, dürfte aber enger auszulegen sein; (3) können notfalls andere Einrichtungen einen potentiellen Ausfall schnellstmöglich ausgleichen und den Erhalt der kritischen Infrastruktur sicherstellen, was bei einer Datenverarbeitung im Sinne der DSGVO regelmäßig nicht notwendig ist.

Gemäß Art. 21 können die Einrichtungen zudem verpflichtet werden, bestimmte IKT-Produkte und -Dienste zertifizieren zu lassen.

– Die Maßnahmen und Befugnisse der nationalen Behörden gestärkt (Art. 28 ff.), u.a. das Bußgeld auf DSGVO-Niveau (10 Mio. € bzw. 2% des weltweiten Jahresumsatzes) gehoben werden (Art. 31 Abs. 4)

Auch die Aufsichtsbefugnisse der nationalen Behörden werden in einzelnen Bereich gestärkt. Am wichtigsten dürfte jedoch die Erhöhung der potenziellen Geldbuße sein, die an Art. 83 Abs. 4 DSGVO angeglichen wird und nun mit einem Höchstbetrag von 10 Mio. € oder 2% des gesamten weltweiten Jahresumsatzes, je nachdem, welcher Betrag höher ist, geahndet werden kann.

– Die Zusammenarbeit der Behörden ausgebaut werden (Art. 12 ff.), insbesondere mit einer Pflicht zum Austausch (Art. 1 Abs. 2), und durch Errichtung eines neuen Netzwerks für massive Cybervorfälle und -krisen („EU-CyCLONe“) (Art. 14)

Auf behördlicher Ebene wird eine neue Pflicht zum Informationsaustausch eingeführt und hierzu die Aufgaben der Kooperationsgruppe und des CSIRT erweitert. Zudem wird ein neues Netzwerk, das sog. „Europäische Netzwerk der Verbindungsorganisationen für Cyberkrisen“ (European Cyber Crises Liaison Organisation Network, EU-CyCLONe) eingerichtet. Dieses setzt sich aus Vertretern der zuständigen Behörden der Mitgliedsstaaten zusammen und hat die Prävention und Koordinierung von Cybersicherheitsvorfällen als Aufgabe.

Fazit

Die NIS-Richtlinie stellte damals einen bedeutenden Meilenstein im Bereich der Cybersicherheit dar, weshalb deren Weiterentwicklung nur konsequent und Anbetracht der rasanten Entwicklungen auch notwendig ist. Der Vorschlag entwickelt viele Aspekte der bisherigen Richtlinie weiter und berücksichtigt – insbesondere bei der Auswahl der (Teil-)Sektoren – Erkenntnisse aktueller Krisen. Einrichtungen und Unternehmen müssen bestehende Prozesse zur Cybersicherheit zwar überarbeiten, können auf diese jedoch in vielen Aspekten aufbauen.

Jan Spittka

Florian Emmerich

Aktuelle Rechtsprechung

BGH: Private Krankenversicherungen können den Schwellenwert für die Prüfung einer Beitragsanpassung mittels § 8b Abs. 1 MB/KK wirksam absenken

Der Bundesgerichtshof entschied am 22.06.2022[1], dass der Schwellenwert für die Prüfung einer Beitragsanpassung von 10 Prozent auf 5 Prozent über § 8b Abs. 1 Musterkrankheitskosten-bedingungen 2009 des Verbandes der privaten Krankenversicherung („MB/KK“) in Verbindung mit einer tariflichen Vereinbarung abgesenkt werden kann. In § 8b Abs. 1 MB/KK lautet es:

> *„Im Rahmen der vertraglichen Leistungszusage können sich die Leistungen des Versicherers z.B. wegen steigender Heilbehandlungskosten, einer häufigeren Inanspruchnahme medizinischer Leistungen oder aufgrund steigender Lebenserwartung ändern. Dementsprechend vergleicht der Versicherer zumindest jährlich für jeden Tarif die erforderlichen mit den in den technischen Berechnungsgrundlagen kalkulierten Versicherungsleistungen und Sterbewahrscheinlichkeiten. Ergibt diese Gegenüberstellung für eine Beobachtungseinheit eines Tarifs eine Abweichung von mehr als dem gesetzlich oder tariflich festgelegten Vomhundertsatz, werden alle Beiträge dieser Beobachtungseinheit vom Versicherer überprüft und, soweit erforderlich, mit Zustimmung des Treuhänders angepasst.“*

Der gesetzliche Vomhundertsatz beträgt grundsätzlich 10 Prozent gem. § 155 Abs. 3 S. 2 Versicherungsaufsichtsgesetz („VAG“). Ein Kläger hatte sich gegen Beitragserhöhungen seines privaten Krankenversicherers gewandt, bei denen der Vergleich der erforderlichen mit den kalkulierten Versicherungsleistungen 10 Prozent nicht überschritt. Er hielt die Beitragsanpassungsklausel § 8b Abs. 1 MB/KK für unwirksam. Dem trat der BGH entgegen. § 8b Abs. 1 MB/KK weiche nicht zum Nachteil des Versicherungsnehmers von den gesetzlichen Vorschriften über die Prämienanpassung ab. Die Klausel enthalte dieselben Voraussetzungen wie § 203 Abs. 2 VVG und erlaube eine Prämienanpassung nur bei einer Veränderung der Rechnungsgrundlagen, die nicht nur als vorübergehend anzusehen ist. Mit der Regelung des § 8b Abs. 1 MB/KK in Verbindung mit den Tarifbedingungen mache der Versicherer allein von der ihm in § 155 Abs. 3 Satz 2 VAG eröffneten Möglichkeit Gebrauch, den Schwellenwert für die Prüfung einer Beitragsanpassung von 10 Prozent auf 5 Prozent abzusenken.

BGH: Haftpflichtversicherer sind hinsichtlich ihrer Versicherungsnehmer im Prozess nicht gem. § 79 Abs. 2 Satz 2 Nr. 2 Var. 3 ZPO vertretungsbefugt.

Der Bundesgerichtshof entschied am 10.03.2022[2], dass eine analoge Ausweitung des Tatbestands des § 79 Abs. 2 Satz 2 Nr. 2 ZPO auf Versicherer nicht in Betracht kommt.

Der Kläger des Verfahrens war von dem Hund der Beklagten gebissen worden. Daraufhin hatte er einen Vollstreckungsbescheid gegen die Beklagte erwirkt. Der Haftpflichtversicherer der Beklagten legte hiergegen für seine Versicherungsnehmerin Einspruch ein. Der Kläger sah in der Einlegung des Einspruchs eine unlautere Handlung gemäß § 3a UWG. Demzufolge handelt unlauter, „*wer einer gesetzlichen Vorschrift zuwiderhandelt, die auch dazu bestimmt ist, im Interesse der Marktteilnehmer das Marktverhalten zu regeln, und der Verstoß geeignet ist, die Interessen von Verbrauchern, sonstigen Marktteilnehmern oder Mitbewerbern spürbar zu beeinträchtigen*”.

Die gesetzliche Vorschrift, gegen die der Haftpflichtversicherer verstoßen habe, sei § 79 Abs.2 ZPO. Das LG verurteilte die Beklagte, es im Rahmen geschäftlicher Handlungen zu unterlassen, ihre Versicherungsnehmer oder mitversicherte Personen in zivilrechtlichen Prozessen zu vertreten. Ausgenommen waren Fälle, in denen die Versicherung Streitgenosse des Verfahrens ist und die Vertretung nicht im Zusammenhang mit einer entgeltlichen Tätigkeit steht.

Das OLG wies die Klage im Berufungsverfahren ab. Der BGH hat die Entscheidung des OLG aufgehoben und die Berufung des Versicherers zurückgewiesen.

Der Versicherer sei gem. § 3 Abs. 1, § 8 Abs. 1 UWG zur Unterlassung verpflichtet. Die Bestimmung des § 79 Abs. 2 ZPO sei eine Marktverhaltensregelung i.S.v. § 3a UWG. Der Versicherer sei kein Streitgenosse gem. § 79 Abs. 2 S. 2 Nr. 2 Var. 3 ZPO. Der Anwendungsbereich des § 79 Abs. 2 Satz 2 Nr. 2 ZPO sei auch nicht über den Wortlaut der Bestimmung hinaus dahingehend zu erweitern, dass dem Streitgenossen ein Versicherungsunternehmen gleichsteht, dem ein Recht zur Nebenintervention (§§ 66, 68 ZPO) zusteht. Eine analoge Anwendung des Begriffs des Streitgenossen auf den Nebeninterventionsberechtigten scheide aus, weil es an einer planwidrigen Regelungslücke fehle. Es liege zudem keine vergleichbare Interessenlage vor. Im Verhältnis des Haftpflichtversicherers zu seinem Versicherungsnehmer fehle es an der Voraussetzung der Unentgeltlichkeit, die für alle in § 79 Abs. 2 Satz 2 Nr. 2 ZPO aufgeführten Personen gilt und damit prägend für diesen Ausnahmetatbestand sei. Entgegen der Annahme des Berufungsgerichts gebiete es auch die Berufsausübungsfreiheit gem. Art. 12 Abs. 1 GG nicht, der Beklagten eine Vertretungsbefugnis gem. § 79 Abs. 2 Satz 2 Nr. 2 ZPO zuzubilligen.

OLG München: Anleger können sich bei Klagen gegen Wirtschaftsprüfer von der Wirecard AG zum Nachweis der Kausalität zwischen dem Bestätigungsvermerk und dem Kaufentschluss auf den Anscheinsbeweis stützen. Obiter dictum zum Musterverfahren nach dem Kapitalmarktmusterverfahrensgesetz („KapMuG“).

Das OLG München verhielt sich am 13.12.2021[3] in einem anlegerfreundlichen Hinweisbeschluss zu den Anforderungen eines Schadensersatzanspruches aufgrund einer vorsätzlich sittenwidrigen Schädigung (§ 826 BGB) wegen einer „gewissenlosen“ Abschlussprüfung der Wirtschaftsprüfer der Wirecard AG.

Gegenstand des Beschlusses war die Frage nach dem Nachweis der Kausalität zwischen einem fehlerhaften Bestätigungsvermerk (§ 322 HGB) und dem Schaden der Anleger. Erwirbt ein Anleger Aktien nach der Veröffentlichung eines Unternehmensberichts, wird der Kausalzusammenhang zwischen einem Unternehmensbericht und dem Kaufentschluss der Anleger nach der Rechtsprechung des BGH vermutet (Anscheinsbeweis). Hierfür muss der Anleger den Unternehmensbericht nicht tatsächlich gelesen haben. Es genügt bereits, dass der Bericht die Einschätzung des Wertpapiers in Fachkreisen allein durch seine Veröffentlichung mitbestimmt und damit eine Anlagestimmung erzeugt.

Diese Rechtsprechung des BGH zum Unternehmensbericht überträgt das OLG München auf den uneingeschränkten Bestätigungsvermerk. Nach § 325 HGB haben Kapitalgesellschaften u.a. folgende Unterlagen offenzulegen: den festgestellten oder gebilligten Jahresabschluss, den Lagebericht und den Bestätigungsvermerk. Bei dem Bestätigungsvermerk handelt es sich um ein zur Veröffentlichung bestimmtes, unternehmensexternes Informationsinstrument. Weil der Bestätigungsvermerk den positiven Jahresabschluss als zutreffend bestätigt, bestimmt er die Einschätzung eines Wertpapiers in Fachkreisen zumindest mit. Die so erzeugte Anlagestimmung dauert in der Regel bis zur Veröffentlichung des nächsten Jahresabschlusses an. Andere Faktoren können jedoch dazwischentreten und für die Einschätzung des Wertpapiers bestimmend werden. Dem Kläger kommt nach der Einschätzung des Senats ein Erfahrungssatz aufgrund des gewöhnlichen Laufs der Dinge dahingehend zugute, dass der Bestätigungsvermerk seine Anlageentscheidung zumindest mittelbar mitbeeinflusst hat. Es erscheine äußerst unwahrscheinlich, dass ein durchschnittlicher Anleger Aktien erwerbe, wenn ein Insolvenzverfahren droht und im Zeitpunkt des Erwerbs in keiner Weise absehbar war, ob das Problem behoben werden kann. Der Kläger kann also mit Hilfe des Anscheinsbeweises darlegen, dass er die streitgegenständlichen Aktien nicht gekauft hätte, wenn der Wirtschaftsprüfer einen uneingeschränkten Bestätigungsvermerk nicht erteilt hätte.

1. BGH, Urt. v. 22.06.2022 – IV ZR 253/20.

2. BGH, Urt. v. 10.03.2022 – I ZR 70/21.

3. OLG München, Beschluss v. 13.12.2021 – 3 U 6014/21.

Dabei weicht das OLG München von der Linie des OLG Stuttgart ab. Dieses war der Auffassung, dass ein solcher Erfahrungssatz als Dauerkausalität auf unabsehbare Zeit jedem beliebigen späteren Aktienerwerber zu einem Schadensersatzanspruch verhelfen würde. § 826 BGB solle aber keinen allgemeinen Schutz des enttäuschten Anlagevertrauens gewährleisten. Das OLG München hingegen sieht keinen Grund, den Anspruch bereits auf Ebene der Kausalität einzuschränken. Das bestimmende Element des § 826 BGB sei die vorsätzliche sittenwidrige Schädigung.

Die Prüfung der vorsätzlichen sittenwidrigen Schädigung wiederum verlaufe zweistufig. In einem ersten Schritt müsse geklärt werden, ob und in welchen Punkten die Bestätigung objektive Fehler enthält. In einem zweiten Schritt werde geprüft, ob der Wirtschaftsprüfer seine Aufgabe nachlässig erledigt hat, zum Beispiel durch unzureichende Ermittlungen oder durch Angaben ins Blaue hinein, und ob er dabei eine Rücksichtslosigkeit an den Tag gelegt hat, die angesichts der Bedeutung des Bestätigungsvermerks für die Entscheidung Dritter als gewissenlos erscheint. Dies gelte in den Dieselfällen ebenso wie bei der unrichtigen Ausstellung des Bestätigungsvermerks. Ob die vorsätzliche sittenwidrige Schädigung im Verschweigen einer unzulässigen Abschalteinrichtung durch den Hersteller oder in der „gewissenlosen" Abschlussprüfung durch einen Wirtschaftsprüfer besteht, mache keinen Unterschied.

In einem Obiter dictum äußerte sich der Senat noch zu den Anforderungen für die Einleitung eines Musterverfahrens nach dem Kapitalmarktmusterverfahrensgesetz („KapMuG"). Bislang ungeklärt ist,[4] ob das KapMuG für Ansprüche anwendbar ist, die auf einen unrichtigen Bestätigungsvermerk des Wirtschaftsprüfers gestützt werden. Während unterschiedliche Kammern am LG München I den sachlichen Anwendungsbereich des KapMuG als nicht eröffnet angesehen haben, tendieren verschiedene Senate der Oberlandesgerichte Stuttgart und München dazu, den Bestätigungsvermerk des Wirtschaftsprüfers als öffentliche Kapitalmarktinformation im Sinne von § 1 Abs. 2 KapMuG zu qualifizieren und damit den Weg für ein Musterverfahren nach dem KapMuG zu öffnen. Die 3. Kammer des LG München I hat ein KapMuG-Verfahren gegen Markus Braun als früheren Vorstandsvorsitzenden von Wirecard am Bayerischen Obersten Landgericht eröffnet und den Bestätigungsvermerk des Wirtschaftsprüfers als Beihilfetat qualifiziert.

Nach dem OLG München dürfte der Bestätigungsvermerk eine öffentliche Kapitalmarktinformation darstellen, weil es sich um ein unternehmensexternes Informationsinstrument handelt. Der Bestätigungsvermerk enthält in der Zusammenschau mit dem Lagebericht und dem Jahresabschluss Informationen, die für eine Vielzahl von Anlegern bestimmt sind. Jahresabschlüsse und Lageberichte werden zudem in § 1 Abs. 2 Ziff. 5 KapMuG als Musterbeispiel für öffentliche Kapitalmarktinformationen genannt. Der Wirtschaftsprüfer dürfe auch Musterbeklagter sein. Anspruchsgegner könne jeder sein, gegen den ein schlüssiger Schadensersatzanspruch wegen falscher, irreführender oder unterlassener öffentlicher Kapitalmarktinformation geltend gemacht wird.

OLG Dresden: Für einen Schadensersatzanspruch aufgrund eines Verstoßes gegen die DSGVO ist das Überschreiten der Bagatellgrenze eine Anspruchsvoraussetzung.

Das OLG Dresden bestätigte am 30.11.2021,[5] dass eine Überschreitung der Bagatellschwelle bei der Rechtsgutsverletzung eine (ungeschriebene) Voraussetzung für einen Schadensersatzanspruch unter der DSGVO darstellt.

Der Kläger ist ein Autohändler und verlangt von zwei Beklagten gesamtschuldnerisch die Zahlung von Schadensersatz wegen der Verletzung seiner Rechte aus der DSGVO in Höhe von EUR 21.000. Der Beklagte 1 organisiert Oldtimer-Ausfahrten. Der Beklagte 2 ist Geschäftsführer und hatte für den Beklagten 1 eine Recherche durchgeführt. Dabei gewann der Beklagte 2 Erkenntnisse über ein strafrechtlich relevantes Verhalten des Klägers. Der Beklagte 2 unterrichtete den Vorstand der Beklagten 1 hierüber, welcher daraufhin dem Kläger eine Mitgliedschaft bei der Beklagten 1 versagte. Das LG sprach dem Kläger Schadensersatz in Höhe von EUR 5.000 zu. Der Kläger verfolgte im Rahmen seiner Berufung die Zahlung der ursprünglich verlangten EUR 21.000 weiter. Die Berufung hatte keinen Erfolg.

Der Anspruch auf Schadensersatz ist in Art. 82 Abs. 1 DSGVO iVm Art. 4 Nr. 7 DSGVO geregelt. Voraussetzung ist, dass der Verantwortliche gegen die DSGVO verstößt.

Nicht jede Datenschutzrechtsverletzung führt jedoch automatisch zu einem ersatzfähigen Schaden. Der Verantwortliche muss das Rechtsgut des Klägers vielmehr in einem Maße verletzen, dass keine bloße Bagatelle mehr vorliegt. Entgegen der Auffassung der Beklagten überschritt die Weitergabe der Rechercheergebnisse diese Bagatellschwelle. Bei der Beurteilung der Schwere der Rechtsgutsverletzung berücksichtigte das OLG, dass dem Kläger die Mitgliedschaft versagt wurde und er deshalb die Möglichkeit verlor, als Autohändler durch die Mitorganisation der Oldtimer-Ausfahrten auf sich aufmerksam zu machen. Des Weiteren habe der Kläger damit rechnen müssen, dass die über ihn eingeholten Daten auch weiteren Personen außer dem Vorstand der Beklagten 1 bekannt gemacht wurden. Dies stelle eine nicht völlig unerhebliche Beeinträchtigung dar und überschreite damit die Bagatellgrenze.

Für die Beurteilung der Höhe des Schadens ist Erwägungsgrund Nr. 146 S. 3 DSGVO zu berücksichtigen. Danach soll der Begriff des Schadens im Lichte der Rechtsprechung des Gerichtshofs weit ausgelegt werden. Den Zielen der DSGVO ist in vollem Umfang zu entsprechen. Nach dem Effektivitätsprinzip (*effet utile*) sei daher auch die Annahme einer abschreckenden Schadenshöhe nicht ausgeschlossen. Dies bedeute aber nicht, dass die Geldentschädigung zwingend „Strafcharakter" haben müsse. Lediglich müsse der Höhe des Anspruchs auf der Basis des Effektivitätsprinzips eine abschreckende Wirkung zukommen. Bei den weitergegebenen Daten handelte es sich um besonders sensible Daten (Strafrechtsbezug). Dennoch lag ein einmaliger Verstoß vor, sodass das OLG München die ausgeurteilte Summe von EUR 5.000 für angemessen hielt.

AG München: Die Corona-Pandemie ist keine Naturkatastrophe im herkömmlichen Sinne. Es fehlt ihr an der für Naturkatastrophen typischen, unmittelbaren physischen Auswirkung.

Das AG München entschied am 20.05.2021,[6] dass die Corona-Pandemie im Sinne der nachfolgenden Klausel einer Reiseabbruchsversicherung keine Naturkatastrophe darstellt:

> *„§ 4 Was erstatten wir bei einer Naturkatastrophe? Wenn Sie wegen einer Naturkatastrophe am Urlaubsort (zum Beispiel Lawinen, Erdbeben) die Reise nicht planmäßig beenden können: Wir übernehmen die notwendigen Mehrkosten für Unterkunft, Verpflegung und Rückreise."*

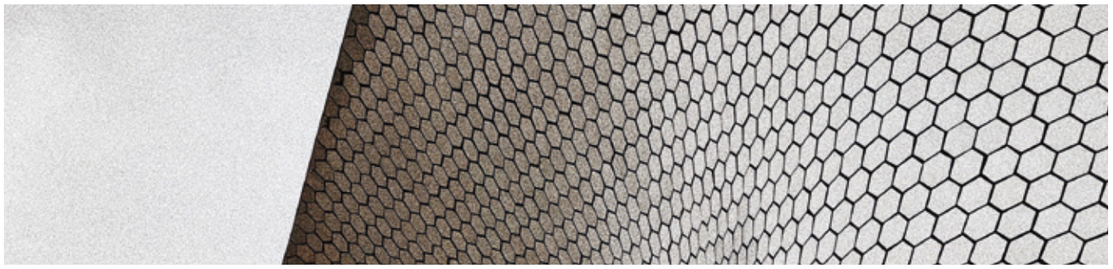
Der Kläger hatte eine Reise nach Sri Lanka gebucht und angetreten. Der Rückflug wurde aufgrund von Reisebeschränkungen gegen die Verbreitung von SARS-CoV-2 annulliert. Daraufhin buchte der Kläger einen eigenen Rückflug. Er nimmt die Beklagte nun aus § 4 seiner Reiseabbruchsversicherung in Anspruch. Die Beklagte verweigert die Zahlung u.a. deswegen, weil kein versichertes Ereignis vorliege. Das AG München wies die Klage ab.

Die Corona-Pandemie unterscheide sich von einer Naturkatastrophe im Sinne der Versicherungsklausel dadurch, dass eine Naturkatastrophe nach dem klassischen Verständnis unmittelbare physische Auswirkungen auf die Umwelt habe. Zudem trete eine Naturkatastrophe nur zeitlich und lokal begrenzt auf. Naturkatastrophen im allgemeinen Sprachgebrauch, wie Erdbeben, Sturmfluten, Lawinen und Wirbelstürme, hätten gemeinsam, dass die zerstörerische Kraft direkt aus dem Naturereignis selbst folge. Bei Auswirkungen durch staatliche Maßnahmen hingegen liege begrifflich keine Naturkatastrophe vor. Die Auswirkungen staatlicher Maßnahmen träten zum einen nur mittelbar auf. Zum anderen würden sich die Maßnahmen lokal unterscheiden, je nachdem, welches Land welche Maßnahmen verhängt. Eine Naturkatastrophe hingegen habe an jedem Ort, an dem sie auftreten könnte, die gleichen Auswirkungen. Darüber hinaus charakterisiere eine Naturkatastrophe, dass sie allein aus einer zentralen, lokal auftretenden Gefahrenquelle rührt, wie zum Beispiel bei einem Vulkanausbruch. Die Gefahren der Corona-Pandemie seien jedoch aufgrund der Ausbreitung dezentral und lokal nicht begrenzbar. Schließlich bestünde die Gefahrenquelle einer Naturkatastrophe typischerweise nur für einen begrenzten Zeitraum von maximal einigen Wochen. Lediglich die Nachwirkungen könnten über längere Zeiträume bestehen. Zwar ist auch die Corona-Pandemie grundsätzlich ein zeitlich vorübergehendes Ereignis. Jedoch bestünde die Gefahr durch das Coronavirus um ein Vielfaches länger als bei klassischen Naturkatastrophen.

4. Möllers, Bestätigungsvermerk des Wirtschaftsprüfers und KapMuG, BKR 2022, 339, 341.

5. OLG Dresden, Urt. v. 30.11.2021 – 4 U 1158/21.

6. AG München, Urt. v. 20.05.2021 – 275 C 23753/20.



Aktuelle Entwicklungen

BaFin stellt VAIT Novelle vor

Die Aufsichtsbehörden reagieren mit neuen Regulationen auf weiter steigende IT-Risiken.

Am 03.03.2022 hat die BaFin ihre versicherungsaufsichtsrechtlichen Anforderungen an die IT („VAIT“) veröffentlicht. Die BaFin hat damit die Leitlinie der Europäischen Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung („EIOPA“) zu Sicherheit und Governance im Bereich der Informations- und Kommunikationstechnologien (IKT) umgesetzt. Im Vergleich zur vorherigen Fassung deckt die überarbeitete Version der VAIT zwei zusätzliche Themenbereiche ab:

die operative Informationssicherheit und das IT-Notfallmanagement. Zudem konkretisiert sie Anforderungen an das Informationsrisiko- und Informationssicherheitsmanagement sowie an das Berechtigungsmanagement und an IT-Ausgliederungen.

Aus Sicht der BaFin entwickelt sich auch das Thema fragmentierte Wertschöpfungsketten sehr dynamisch. Die Aus- und Weiterverlagerungen sind schwer kontrollier- und steuerbar und stellen eine Herausforderung sowohl für die Versicherer als auch für die Aufsicht dar. Die BaFin möchte deshalb in allen Sparten des Finanzsektors mehr Daten erheben, um Risiken zu überwachen, die sich aus den Aus- und Weiterverlagerungen ergeben. Deswegen hat sie für alle Sektoren ein einheitliches elektronisches Meldeverfahren implementiert. So soll die Ausgliederungslandschaft analysiert und mögliche Risiken adäquat adressiert werden.

Die Änderungen an die VAIT wurden auch mit Blick auf den Digital Operational Resilience Act („DORA“) der EU vorgenommen. Diesen legte die Kommission im September 2020 vor. Der Rechtsakt soll die IT-Sicherheit von Finanzunternehmen wie Banken, Versicherungsunternehmen und Wertpapierfirmen stärken. Im Mai 2022 haben Rat und Parlament eine Einigung über den Vorschlag erzielt. Die Finalisierung durch das Europäische Parlament wird im September 2022 erwartet.

Regulierung von Nachhaltigkeitsrisiken und Pflichtversicherung für Elementarschäden

Neben den IT-Risiken bleibt die Regulierung von Nachhaltigkeitsrisiken weiterhin im Fokus der BaFin. Nachhaltigkeitsrisiken werden den inhaltlichen Schwerpunkt der Jahreskonferenz der Versicherungsaufsicht am 02.11.2022 darstellen. Die Vorsitzende von EIOPA sprach bereits im Juni über die Integration der Grundsätze der Nachhaltigkeit in Solvency II, IORP II und die IDD sowie in die technischen Standards für die SFDR. Sie wird auf der Konferenz die europäische Perspektive auf Nachhaltigkeitsaspekte darlegen.

Dazu gehört auch die EU-Richtlinie zur Nachhaltigkeitsberichterstattung (Corporate Sustainability Reporting Directive, „CSRD“). Über ihren Text erzielten der Rat der Europäischen Union und das Europäische Parlament am 21.06.2022 eine Einigung. Die Richtlinie wird zu einer besseren Datengrundlage für die bereits bestehenden Offenlegungspflichten über wesentliche Auswirkungen von Investitionsentscheidungen auf Nachhaltigkeitsfaktoren unter der EU Offenlegungsverordnung führen. Sie erweitert den Umfang an Nachhaltigkeitsinformationen, welche die Unternehmen in ihren Lageberichten bereitstellen müssen. Die Anwendung der Richtlinie erfolgt in drei Stufen: Für Unternehmen, die bereits der Vorgängerrichtlinie zur nichtfinanziellen Unternehmensberichterstattung (Non Financial Reporting Directive, “NFRD”) unterliegen, gilt die Verordnung für am oder nach dem 01.01.2024 beginnende Geschäftsjahre. Große Unternehmen, die derzeit nicht unter die NFRD fallen, müssen die Verordnung für am oder nach dem 01.01.2025 beginnende Geschäftsjahre anwenden. Kapitalmarktorientierte kleine und mittelständische Unternehmen, bestimmte kleine und nicht-komplexe Kreditinstitute sowie Versicherungs-Captives sind für am oder nach dem 01.01.2026 beginnende Geschäftsjahre von der neuen Richtlinie betroffen.

Auch auf nationaler Ebene rückte die Flutkatastrophe im vergangenen Sommer die Folgen des Klimawandels mit ihren verheerenden Schäden erneut in das Bewusstsein der Bevölkerung. Der Sachverständigenrat für Verbraucherfragen beim BMUV (SVRV), der Verbraucherzentrale Bundesverband (vzbv) und der Gesamtverband der Deutschen Versicherungswirtschaft (GDV) legten ausgearbeitete Vorschläge zur Erhöhung der Versicherungsdichte bei Elementarschäden vor. Die Prämien sollen risikoadjustiert, also nicht nach dem Solidarprinzip bemessen sein. Die Bundesländer hingegen haben sich nach der Konferenz der Regierungschefinnen und Regierungschefs der Länder am 02.06.2022 für die Einführung einer Pflichtversicherung für Elementarschäden für alle Gebäudebesitzer ausgesprochen.

Gesetz für einen besseren Schutz hinweisgebender Personen

Am 27.07.2022 hat das Bundeskabinett den Regierungsentwurf für ein neues Hinweisgeberschutzgesetz beschlossen. Mit dem Gesetz soll die Richtlinie EU 2019/1937 (Hinweisgeberschutzrichtlinie (HinSch-RL) oder EU-Whistleblower-Richtlinie) in nationales Recht umgesetzt werden. Dies hätte schon zum 17.12.2021 geschehen müssen. Die EU-Kommission hatte deshalb bereits ein Vertragsverletzungsverfahren gegen Deutschland eingeleitet. Ziel des Gesetzes ist es nun, den Schutz hinweisgebender Personen vor Benachteiligungen zu gewährleisten, die ihnen wegen ihrer Meldung drohen und sie davor abschrecken könnten.

Der Entwurf sieht folgende zentrale Regelungselemente vor:

- Der persönliche Anwendungsbereich (§ 1 HinSchG) umfasst alle Personen, die in ihrem beruflichen Umfeld Informationen über Verstöße erlangt haben.

- Der sachliche Anwendungsbereich (§ 2 HinSchG) umfasst u.a. Informationen über Verstöße, die straf- oder bußgeldbewehrt sind, soweit eine verletzte Bußgeldvorschrift dem Schutz von Leben, Leib, Gesundheit oder dem Schutz der Rechte von Beschäftigten oder ihrer Vertretungsorgane dient, sowie Informationen über sonstige Verstöße gegen Rechtsvorschriften des Bundes und der Länder sowie unmittelbar geltende Rechtsakte der Europäischen Union und der Europäischen Atomgemeinschaft.

- Für hinweisgebende Personen werden mit internen und externen Meldekanälen zwei gleichwertig nebeneinanderstehende Meldewege vorgesehen, zwischen denen sie frei wählen können (§§ 7 bis 31 HinSchG).

- Es werden die Voraussetzungen festgelegt, unter denen eine hinweisgebende Person Informationen über Verstöße öffentlich zugänglich machen darf (§ 32 HinSchG). Dies ist u.a. der Fall, wenn die hinweisgebende Person eine externe Meldung erstattet hat und keine Rückmeldung erhalten hat, oder trotz Rückmeldung keine geeigneten Folgemaßnahmen ergriffen wurden. Auch wenn ein hinreichender Grund zur Annahme besteht, dass der Verstoß wegen eines Notfalls, der Gefahr irreversibler Schäden oder vergleichbarer Umstände eine unmittelbare oder offenkundige Gefährdung des öffentlichen Interesses darstellen kann, darf die Information öffentlich zugänglich gemacht werden, sowie wenn im Fall einer externen Meldung Repressalien zu befürchten sind oder Beweismittel unterdrückt oder vernichtet werden könnten.

- Sofern hinweisgebende Personen die Anforderungen des HinSchG an eine Meldung oder Offenlegung einhalten, werden sie umfangreich vor Repressalien wie Kündigung oder sonstigen Benachteiligungen geschützt (§§ 33 bis 39 HinSchG).

Insight

UKRAINE

Aktuelle Beiträge zu den relevanten rechtlichen Themen im Rahmen der Russland-Ukraine-Krise sowie weitere aktuelle Informationen finden Sie auf unserer **Ukraine Crisis Hub** auf unserer Homepage unter

https://www.clydeco.com/en/insights/crisis-in-ukraine-and-russia

COVID-19

Aktuelle Nachrichten und relevante Entwicklungen im Zusammenhang mit COVID-19 können Sie unserem **Coronavirus Information Hub** entnehmen unter **www.clydeco.com/en/coronavirus.**

CLYDE & CO INTERNATIONAL

Auch international gibt es einiges zu berichten: Wir freuen uns verkünden zu können, dass wir nun auch ein festes Office in Chile eingerichtet haben. Die neue Kanzlei wird 11 lokale Partner und ein Team von 40 Anwälten mit Fachkenntnissen in den Bereichen Gesellschafts- und Transaktionsrecht, Litigation, Steuern, Arbeit und Projekte sowie Bauwesen haben. Das Büro in Santiago wird als regionales Drehkreuz dienen, um sich mit anderen Märkten zu verbinden und das Wachstum in Lateinamerika zu konsolidieren.

Ferner ist Clyde & Co im Juli mit der britisch-irischen Anwaltskanzlei BLM fusioniert, wodurch die Kanzlei die Position als führender Rechtsberater im Versicherungssektor gestärkt hat.

Mehr Informationen finden Sie unter

https://www.clydeco.com/en/insights/2022/08/clyde-co-opens-in-chile-to-drive-growth-in-latin-a

TEAM

"Wir freuen uns, dass uns ein „Rückkehrer" wieder unterstützt. Dr. Ciya Aslan verstärkt seit dem Juli 2022 als Associate unsere Versicherungspraxis.

Zudem verstärkt uns ab August 2022 im Bereich Datenschutz, e-Privacy und Cybersecurity Florian Emmerich als Associate. Er verstärkt somit sowohl unsere Corporate Insurance & Regulatory wie auch unsere Cyber Practices.

VORTRÄGE UND WEBINARE

- Dr. Henning Schaloske zu: „A global snapshot: Claims trends & topics“, bei Swiss RE / Munich RE, Mai 2022
- Dr. Paul Malek zu: „Silent Cyber“, Junges Haftpflichtforum Köln, Juni 2022
- Dr. Henning Schaloske zu: „Menschenrechte und neue Haftungsrisiken für Unternehmen und Geschäftsleiter“, AXA XL Financial Lines, Juli 2022
- Dr. Henning Schaloske zu: „ESG und Supply Chain“, AIG Connect, Juni 2022
- Dr. Henning Schaloske zu: „Ukrainekrieg – Kriegsausschluss, Ransomware & more“ Euroforum Cyber; Juni 2022
- Dr. Paul Malek zu: „Haftpflichtrisiken nach Cyber-Attacken“, Euroforum Cyber, September 2022

480

Partners

2,400

Lawyers

3,200

Legal professionals

5,000

Total staff

60+

Offices worldwide*

www.clydeco.com

*Includes associated offices Clyde & Co LLP is a limited liability partnership registered in England and Wales. Authorised and regulated by the Solicitors Regulation Authority.

2533150 - 10 - 2022