Vorsicht, Quishing!

Cyber Insurance Talk | TH Köln

Dr. Florian Höld

11.03.2025

Dr. Florian Höld

Rechtsanwalt | Partner
Fachanwalt für Versicherungsrecht

Theodor-Heuss-Ring 13-15
50668 Köln

Tel.: +49 221 944027-846
E-Mail: florian.hoeld@bld.de

OLG Schleswig weist Berufung gegen 2. deutsches Cyberurteil gem. § 522 ZPO endgültig zurück!

Mit dem 2. Deutschen Cyberurteil des LG Kiel wurde das Anfechtungsrecht des Versicherers gem. § 123 BGB i.V.m. § 22 VVG gestärkt (LG Kiel, Urt. v. 23.05.2024 – 5 O 128/21, r+s 2024, 609 – Dr. Behrad Lalani berichtete beim Cyber Insurance Talk am 03.07.2024).

Schon mit Hinweisbeschluss vom 14.10.2024 (16 U 63/24, BeckRS 2024, 30937) gem. § 522 ZPO wies das OLG Schleswig auf eine Berufung der Klägerin darauf hin, dass das LG Kiel eine Täuschungs-Anfechtung rechtsfehlerfrei angenommen habe (vgl. die Besprechung von *Höld*, r+s 4/2025, 155 sowie in Gen Re PHi – Haftpflicht international Recht & Versicherung 2025, Nr. 1).

Diese Sichtweise hat das OLG Schleswig-Holstein nun nochmals bestätigt und die Berufung durch Beschluss gem. § 522 ZPO vom ***09.01.2025*** (16 U 63/24) endgültig zurückgewiesen.

Es wurde bislang keine Nichtzulassungsbeschwerde zum BGH zugestellt, Entscheidung wohl rechtskräftig.

Agenda

I. „Quishing“ als aktuelle Cyberbetrugsform
II. Bsp.-Fall (angelehnt an LG Koblenz – 14 O 32/24 n.v.)
III. Informationssicherheitsverletzung gem. A1-2 AVB Cyber
IV. LG Hagen, Urt. v. 15.10.2024 – 9 O 258/23, r+s 2025, 28
V. Diskussion & Fazit

„Quishing“ als aktuelle Cyberbetrugsform

WIKIPEDIA
Die freie Enzyklopädie

Hauptseite
Themenportale
Zufälliger Artikel
Spezialseiten

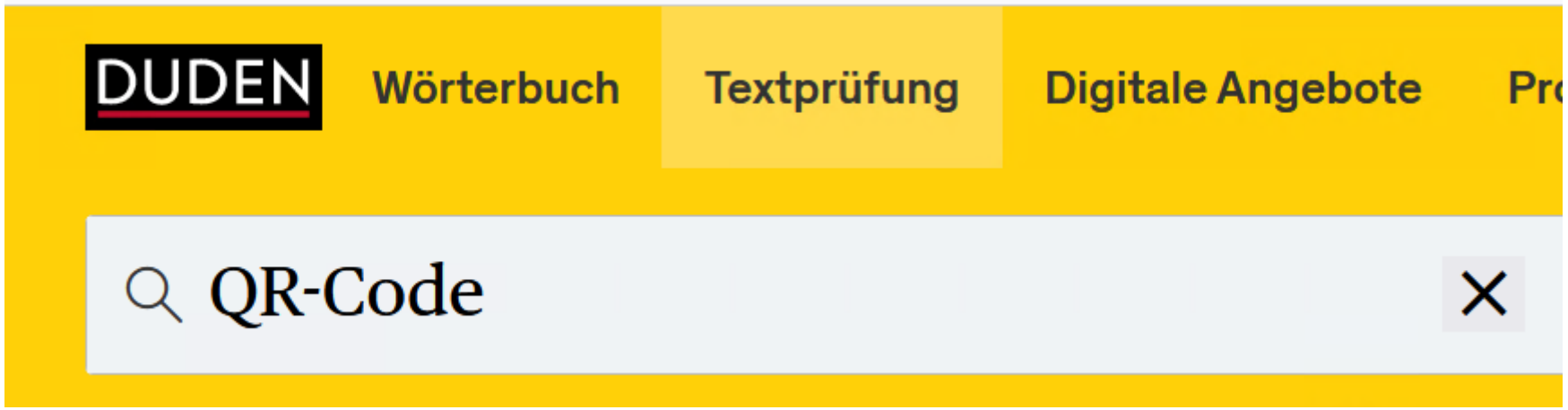
Mitmachen
Artikel verbessern
Neuen Artikel anlegen
Autorenportal
Hilfe
Letzte Änderungen
Kontakt
Spenden

QR-Code

Der **QR-Code** (englisch ***Q**uick **R**esponse*, „schnelle Antwort“, als Markenbegriff „QR Code“) ist ein zweidimensionaler Code, der von dem Tochterunternehmen *Denso Wave* der japanischen Firma Denso im Jahr 1994 entwickelt wurde. Aufgrund einer automatischen Fehlerkorrektur ist dieses Verfahren sehr robust und daher weit verbreitet. Weiterentwicklungen sind der Micro-QR-Code, der Secure-QR-Code (SQRC), der iQR-Code und der Frame-QR-Code.

Die Zeichenkette „https://de.wikipedia.org“ als QR-Code (mit Fehlerkorrektur-Level M)

Inhaltsverzeichnis [Verbergen]



Bedeutung

zweidimensionaler, aus Punkten zu einem Quadrat zusammengesetzter, elektronisch lesbarer Code

SWR

https://www.swr.de › verbraucher › ard-marktcheck › b...

Betrug mit QR-Codes: So funktioniert Quishing

12.11.2024 — Die neue Masche hat bereits einen eigenen Namen: **Quishing**. Der Begriff setzt sich aus Q für QR-Code und Phishing zusammen. Durch Quishing an ...

WIKIPEDIA
Die freie Enzyklopädie

Hauptseite
Themenportale
Zufälliger Artikel
Spezialseiten

Mitmachen
Artikel verbessern
Neuen Artikel anlegen
Autorenportal
Hilfe

Phishing

Unter dem Begriff **Phishing** (Neologismus von *„fishing“*, engl. für „Angeln“) versteht man Versuche, sich über gefälschte Webseiten, E-Mails oder Kurznachrichten als vertrauenswürdiger Kommunikationspartner in einer elektronischen Kommunikation auszugeben. Ziel des Betrugs ist es, z. B. an persönliche Daten eines Internet-Benutzers zu gelangen, etwa ihn zur Ausführung einer schädlichen Aktion wie das Einloggen in einen gefälschten / nachgebauten Webauftritt zu bewegen, um die Zugangsdaten wie das Passwort und den Benutzernamen und gegebenenfalls auch einen 2. Faktor für die 2-Faktor-Identifizierung zu erschleichen. In der Folge werden dann beispielsweise Kontoplünderungen begangen, Bestellungen mit der Unterschlagung von Konsumgütern und der Verkauf dieser an Dritte getätigt, ein weitergehender Identitätsdiebstahl begangen oder eine Schadsoftware installiert. Es handelt sich dabei um eine Form des Social Engineering, bei dem die Gutgläubigkeit des Opfers ausgenutzt wird.[1] Der Begriff ist ein englisches Kunstwort, das sich von *fishing* (Angeln, Fischen) ableitet[2] und bildlich das Angeln nach Passwörtern mit Ködern[3] verdeutlicht. Die Schreibweise mit Ph- entstammt dem Hacker-Jargon (vgl. auch Phreaking).[4][5][6]

POLIZEI DEIN PARTNER
Gewerkschaft der Polizei

PRÄVENTION. FÜR DICH.

Suche nach Informationen, Hilfe, Tipps

Startseite ▸ Themen ▸ Internet / Mobil ▸ Vorsicht, Quishing!

QR-Codes haben eine starke Verbreitung gefunden

Diese Phishing-Variante arbeitet mit Fotos statt Links

Vorsicht, Quishing!

Quick Response (QR)-Codes sind längst ein selbstverständlicher Bestandteil unseres digitalen Alltags. Hinter QR-Codes verbergen sich etwa Speisekarten von Restaurants oder Informationen über Sehenswürdigkeiten. Doch auch bei der Nutzung von QR-Codes ist Vorsicht geboten: Cyberkriminelle setzten sie mitunter für Phishing-Angriffe ein, sowohl in E-Mails und in der Briefpost als auch an öffentlichen Orten wie E-Ladesäulen. So etwas nennt man „Quishing“.


verbraucherzentrale
Beratung
Bildung
Politik
Shop
Marktbeobachtung
Beschwerde einreichen
Menü
Geld & Versicherungen
Digitales
Lebensmittel
Umwelt
Gesundheit & Pflege
Energie
Reise
Verträge
"Quishing": Falsche QR-Codes in Mails, Briefen, ÖPNV und Straßenverkehr
Kriminelle verschicken falsche Bank-Briefe, überkleben QR-Codes an Ladesäulen und auf Parkautomaten, verteilen falsche Strafzettel und hängen Plakate in Bussen und Bahnen auf. Mit QR-Codes wollen sie auf gefälschte Internetseiten locken und Daten oder Geld stehlen.

Bsp.-Fall (angelehnt an LG Koblenz – 14 O 32/24 n.v.)

Sachverhalt:

- Die Kl. betriebt ein Fahrzeugbauunternehmen und stellt u.a. Spezialfahrzeuge für den Motor- und Pferdesport her
- Die Kl. unterhält bei der Bekl. eine Cyberversicherung
- Im Sommer 2022 sprach ein Herr. E. den GF der Kl. darauf an, für einen Kunden aus Aserbaidschan den Kauf 2er Pferdesporttransporter mit Wohnbereich vermitteln zu wollen.
- Nach wochenlangen Verhandlungen und Geschäftskontakten in Türkei, Aserbaidschan, Genf, Barcelona, China, Russland und Tel Aviv unterbreitete die Kl. dem Kunden ein Angebot über 3,8 Mio EUR.
- Der Kunde nahm das Angebot an, es wurden Auftragsbestätigungen ausgestellt.
- Herrn E. wurde eine Vermittlungsprovision i.H.v. 600.000,00 EUR gegen Rechnungsstellung durch ein Unternehmen in der Türkei versprochen.
- Der Vermittler E. verlangte, dass die 600.000,00 EUR *vorab per Bitcoin (Btc.)* zu überweisen seien.
- Die Kl. erklärte, nur dazu bereit gewesen zu sein, die verlangte Provision per Btc. zu transferieren, wenn Zug um Zug ein Teil des Kaufpreises in entsprechender Höhe durch den Kunden gezahlt werde.

Sachverhalt:

- Zur Abwicklung dieser Abrede seien Kl. und Herr E. übereingekommen, „Btc. gegen EURO“ wechselseitig zu überweisen („Überweisungsschaukel“). Die Kl. sollte die Provision in Btc. zahlen, wenn zugleich ein entsprechender Teil des Kaufpreises in EURO an die Kl. gezahlt würde.
- Dazu legte die Kl. zunächst eigens ein Bitcoin Wallet an und transferierte über einen Schweizer Crypto Broker darauf Btc. im Gegenwert von 600.000,00 EUR
- Für die eigentliche „Überweisungsschaukel“ wurde sodann eine Telefonkonferenz zwischen dem GF der Kl. und Herrn E. verabredet und durchgeführt. Parallel zu dieser Konferenz sollten die Transaktionen in Echtzeit über Mobiltelefone durchgeführt werden. Konkret wurde wie folgt vorgegangen:
- Der GF der Kl. führte mit seinem eigenen Mobiltelefon mit Herrn E. und dessen „Bruder“ ein Videotelefonat („WhatsApp“). Die Transaktion der Btc. sollte parallel über das private Mobiltelefon der ebenso anwesenden Tochter des GF abgewickelt werden.
- Der GF loggte sich mit dem Handy seiner Tochter in sein Bitcoin Wallet ein.
- Zunächst wurde 1 Btc. testweise manuell erfolgreich transferiert (= damals ca. 20.000,00 EUR)

Sachverhalt:

- Herr E. reklamierte, dass dieses Vorgehen zu lange dauere und sich der Prozess durch QR-Codes beschleunigen lasse
- Herr E. habe dazu einen Testlauf mit 0,02901 Btc. vorgeschlagen (= ca. 580,00 EUR).
- Die Kl. hätte eingewilligt und diesen Betrag im Wallet als Überweisungsbetrag eingeben.
- Nun forderte Herr E. den GF der Kl. auf, das Handy seiner Tochter mit der geöffneten Wallet an einen QR-Code zu halten, den er Sekunden zuvor per Email an den GF übermittelt hatte.
- Zu diesem Zeitpunkt hätte das Wallet einen Überweisungsbetrag von 0,02901 Btc. angezeigt.
- Nach einem „Wisch“-Befehl durch den GF sei der Betrag „plötzlich“ auf 29,01 Btc. gesprungen und wurde eine Transaktion über 29,01 Btc. (ca. 580.000,00 EUR) tatsächlich durchgeführt.
- Der Überweisungsbetrag sei „automatisch, wie von Geisterhand“ erhöht worden. Angeblich hätte der QR-Code auf dem Mobiltelefon den Befehl ausgelöst, einen Betrag von 29,01 Btc. zu transferieren.
- Zu einer Gegenüberweisung kam es niemals.
- Kl. nimmt daraufhin Bekl. auf Ersatz von 600.000,00 EUR mit der Behauptung in Anspruch, es sei zu einer „unbefugten Nutzung von IT-Systemen“ gekommen.

Sachverhalt:

- Die Bekl. lehnt ab. Die Kl. habe den Betrag (täuschungsbedingt) freiwillig bezahlt. Im Übrigen habe eine IT-Forensikerin festgestellt, dass es keine unautorisierte Überweisung qua QR-Code gab. Die Mobiltelefon der Tochter sei nicht kompromittiert worden.
- Kl. reicht Klage über 600.000,00 EUR beim LG Koblenz ein.

Zu Recht?

AVB:

A1-1.1 Versicherung von Vermögensschäden

Gegenstand der Versicherung sind grundsätzlich Vermögensschäden im Umfang der entsprechenden nachfolgenden Bestimmungen, soweit diese Folge einer unbefugten Nutzung (A507) von IT-Systemen (A206) oder einer Datenschutzverletzung (A097) sind.

A1-2 Unbefugte Nutzung (A507) von IT-Systemen (A206)

Unter einer unbefugten Nutzung (A507) von IT-Systemen (A206) im Sinne dieses Versicherungsvertrages ist jede rechtswidrige und/oder nicht autorisierte Nutzung, einschließlich der Überschreitung der jeweiligen Zugriffsberechtigung von Mitarbeitern des Versicherungsnehmers und/oder mitversicherter Unternehmen (A492), auch dann, wenn der Mitarbeiter lediglich die Möglichkeiten von IT-Systemen (A206) nutzt, obwohl er dazu nicht berechtigt ist, zu verstehen. Als unbefugte Nutzung (A507) im Sinne dieser Bedingungen

AVB:

Ergänzend müssen versicherte *„Zahlungsmittelkonten und Kreditkarten“* tangiert sein und die jeweiligen Voraussetzungen z.B. zu folgenden Klauseln vorliegen:

- *Identitätsdiebstahl*
- *Betrug (nur versichert bei Identitätsdiebstahl)*
- *Elektronische Wallets*

Zudem besteht ein Risikoausschuss für

- *Finanzmarkttransaktionen*

Rechtliche Probleme:

- P1: Ist Mobiltelefon der Tochter versichertes „IT-System“?
- P2: Wurde das Mobiltelefon der Tochter „nicht autorisiert genutzt“? (das war str. , aber eher unplausibel – zumindest das Abscannen des QR-Codes erfolgte willentlich, ebenso das „Wischen“; offenbar wurde sich nur über den Inhalt geirrt.)
- P3: Ist das Wallet versichertes „Zahlungskonto“?
- P4: Liegen die besonderen Klauselvoraussetzungen vor?
- P5: Wurde der etwaige Versicherungsfall grob fahrlässig i.S.v. § 81 Abs. 2 VVG herbeigeführt?
- P6: Greift das Sub-Limit für „Zahlungsmittelkonto im Ausland“?
- P7: Liegt überhaupt ein versicherter „Vermögensschaden“ vor (Stichwort: unfreiwilliger Vermögensschaden)?

GDV Gesamtverband der Versicherer

Unverbindliche Bekanntgabe des Gesamtverbandes der Deutschen Versicherungswirtschaft e.V. (GDV) zur fakultativen Verwendung. Abweichende Vereinbarungen sind möglich.

Allgemeine Versicherungsbedingungen für die Cyberrisiko-Versicherung (AVB Cyber)

Musterbedingungen des GDV
(Stand: Februar 2024)

AVB Cyber

Informationssicherheitsverletzung

Teil A

Abschnitt A1 – Basis-Baustein

A1-1 Gegenstand der Versicherung

Gegenstand der Versicherung sind Vermögensschäden im Umfang der nachfolgenden Bestimmungen, die durch eine Informationssicherheitsverletzung verursacht worden sind.

Informationssicherheitsverletzung

A1-2 Informationssicherheitsverletzung

A1-2.1 Informationssicherheitsverletzung ist eine Beeinträchtigung der

- Verfügbarkeit
- Integrität
- Vertraulichkeit

von elektronischen Daten des Versicherungsnehmers oder von informationsverarbeitenden Systemen, die er zur Ausübung seiner betrieblichen oder beruflichen Tätigkeit – auch mittels Fernzugriff – nutzt.

A1-2.2 Dabei ist es unerheblich, ob sich die elektronischen Daten oder die informationsverarbeitenden Systeme des Versicherungsnehmers in dessen unmittelbarem Verfügungsbereich befinden oder der Versicherungsnehmer sich eines externen Dienstleisters bedient.

Bedient sich der Versicherungsnehmer eines externen Dienstleisters, besteht kein Versicherungsschutz für Schäden, die infolge des Ausfalls, der Unterbrechung oder Störung der Dienstleistung entstehen, soweit sie zu einer Beeinträchtigung der Verfügbarkeit der elektronischen Daten oder informationsverarbeitenden Systeme des Versicherungsnehmers führen.

A1-2.3 Der Begriff „elektronische Daten“ umfasst auch Software und Programme.

Informationssicherheitsverletzung

A1-2.4 Die Informationssicherheitsverletzung muss durch folgende Ereignisse ausgelöst werden:

- Angriffe auf elektronische Daten oder informationsverarbeitende Systeme des Versicherungsnehmers
- unberechtigte Zugriffe auf elektronische Daten des Versicherungsnehmers
- Eingriffe in informationsverarbeitende Systeme des Versicherungsnehmers
- eine Handlung oder Unterlassung, die zu einer Verletzung von datenschutzrechtlichen Vorschriften durch den Versicherungsnehmer führt
- Schadprogramme, die auf elektronische Daten oder informationsverarbeitende Systeme des Versicherungsnehmers wirken.

Prölss/Martin/Klimke, 32. Aufl. 2024, VVG, A1-2-4 AVB Cyber Rn. 26ff.

I. Angriff (A1-2.4 Spiegelstrich 1)

Ein Angriff setzt nach dem Wortsinn mindestens eine **bewusste Handlung** voraus, die auf die Verletzung geschützter Interessen gerichtet ist (HK-VVG/*Pawig-Sander* A1-2 AVB Cyber Rn. 19; *Malek/Schilbach* VersR 2019, 1321, 1324). Vorsätzliches Handeln oder eine vermögensbezogene Schädigungsabsicht sind dagegen keine notwendigen Begriffsmerkmale (zweifelnd HK-VVG/*Pawig-Sander* A1-2 AVB Cyber Rn. 19). Ein Angriff kann sich auch gegen einen **unbestimmten Personenkreis** richten, wie dies etwa bei der ungezielten Verteilung von Schadsoftware zur Erpressung von Lösegeld (sog. Ransomsoftware) der Fall ist (*Malek/Schilbach* VersR 2019, 1321, 1324). 29

II. Zugriff (A1-2.4 Spiegelstrich 2)

Ein Zugriff auf Daten liegt vor, wenn von den Daten Kenntnis genommen wird und/oder die Daten (z. B. durch Anfertigung von Kopien oder durch Weitergabe der Informationen) in irgendeiner Weise genutzt werden (*Malek/Schilbach* VersR 2019, 1321, 1325). Es genügt also eine Beeinträchtigung der Vertraulichkeit von Daten, ihre Verfügbarkeit oder Integrität muss nicht betroffen sein. 30

Unberechtigt ist ein Zugriff, wenn der Zugreifende entweder gar nicht oder jedenfalls im konkreten Fall nicht zur Nutzung der Daten befugt ist, wobei sowohl die interne Befugnis gegenüber dem VN als auch die Befugnis nach datenschutzrechtlichen Vorschriften gegeben sein muss. Erfasst wird also insbes. auch der Fall, dass ein Mitarbeiter des VN unter Überschreitung seiner internen Zuständigkeit Daten zur Kenntnis nimmt und weitergibt (*Malek/Schilbach* VersR 2019, 1321, 1325). Ein Verschulden des Zugreifenden wird nicht vorausgesetzt (**a. A.** HK-VVG/*Pawig-Sander* A1-2 AVB Cyber Rn. 20). 31

III. Eingriff (A1-2.4 Spiegelstrich 3)

Ein Eingriff setzt ein **menschliches Verhalten** voraus, das auf die informationsverarbeitenden Systeme des VN einwirkt und eine Informationssicherheitsverletzung auslöst (*Malek/Schilbach* VersR 2019, 1321, 1325). 32

Nicht erfasst werden daher **Beeinträchtigungen infolge von Naturereignissen** wie etwa unwetterbedingte Stromausfälle (*Malek/Schilbach* VersR 2019, 1321, 1325). Diese Auslegung des Eingriffs entspricht dem herkömmlichen Sprachgebrauch und wird zudem dadurch nahe gelegt, dass alle anderen Fälle des A1-2.4 an menschliches Verhalten anknüpfen. Eine theoretisch denkbare, rein erfolgsbezogene Auslegung (Eingriff = jedes Ereignis, das eine Beeinträchtigung i. S. v. A1-2.1 zur Folge hat) wird ein VN bei verständiger Würdigung schon deshalb nicht in Erwägung ziehen, weil A1-2.4 danach offensichtlich jede Bedeutung genommen würde (*Malek/Schilbach* VersR 2019, 1321, 1325). 33

Nicht erforderlich ist dagegen – wie sich aus dem Vergleich mit Spiegelstrich 1 und Spiegelstrich 2 ergibt – dass es sich um eine mit Schädigungsabsicht vorgenommene oder um eine **unberechtigte Einwirkung** handelt (HK-VVG/*Pawig-Sander* A1-2 AVB Cyber Rn. 22; *Malek/Schilbach* VersR 2019, 1321, 1325 f.; anders wohl *Rudkowski* VersR 2023, 416, 422: zielgerichtetes Verhalten erforderlich). Erfasst werden daher auch **schlichte Bedienungsfehler** durch Mitarbeiter des VN oder externe Dienstleister (gleichgültig ob verschuldet oder nicht), etwa wenn diese zu einem Datenverlust oder einen Systemabsturz führen (HK-VVG/*Pawig-Sander* A1-2 AVB Cyber Rn. 22; *Malek/Schilbach* VersR 2019, 1321, 1325 f.). Vorbehaltlich A1-17 besteht außerdem VersSchutz für einen durch menschliches Verhalten ausgelösten Ausfall von Infrastruktur (Beispiel: plötzlicher Stromausfall führt zu Datenverlust (**a. A.** *Rudkowski* VersR 2023, 416, 422). 34

Ein Eingriff ist auch dann gegeben, wenn die Informationssicherheitsverletzung (z. B. ein Datenverlust) durch die **Installation fehlerhafter Software- oder Hardwarekomponenten** ausgelöst wurde (*Malek/Schilbach* VersR 2019, 1321, 1326; **a. A.** für Softwarekomponenten HK-VVG/*Pawig-Sander* A1-2 AVB Cyber Rn. 22). Die Beeinträchtigung geht in diesem Fall auf die Installation der Komponenten und damit mittelbar auf menschliches Verhalten zurück. Eine „unmittelbare" Einwirkung durch eine Person fordert der Wortlaut nicht und sie ist dem Eingriffsbegriff auch nicht immanent (**a. A.** für Softwarekomponenten HK-VVG/*Pawig-Sander* A1-2 AVB Cyber Rn. 21). Allerdings können bei Softwarefehlern die Ausschlüsse nach A4-1.2 Buchst. f oder A4-2.3 Buchst. f greifen. 35

Prölss/Martin/Klimke, 32. Aufl. 2024, VVG, A1-2-4 AVB Cyber Rn. 26ff.

IV. Verletzung datenschutzrechtlicher Vorschriften (A1-2.4 Spiegelstrich 4)

Spiegelstrich 4 knüpft an die Verletzung datenschutzrechtlicher Vorschriften **durch den VN** an. In Betracht kommen dafür Vorschriften der DS-GVO, aber auch ausländische Vorschriften, da die Klausel insoweit keine Einschränkungen enthält (HK-VVG/*Pawig-Sander* A1-2 AVB Cyber Rn. 23). Ein Beispiel ist die versehentliche oder sonst dem VN zurechenbare Veröffentlichung von personenbezogenen Kundendaten (*Malek/Schilbach* VersR 2019, 1321, 1326). 36

Diese Verletzung muss durch eine **Handlung oder Unterlassung,** d. h. durch ein menschliches Verhalten adäquat verursacht worden sein. Dieser Voraussetzung kommt wohl keine Eingrenzungsfunktion zu, da eine dem VN zurechenbare Verletzung von Datenschutzrecht nur denkbar ist, wenn sie zumindest mittelbar auf menschliches Verhalten (und sei es nur auf das Unterlassen von Schutzmaßnahmen gegen Naturereignisse) zurückgeht. Ein Verhalten des VN selbst ist nicht erforderlich, vielmehr genügt ein Handeln oder Unterlassen von Mitarbeitern oder Dritten (tendenziell **a. A.** HK-VVG/*Pawig-Sander* A1-2 AVB Cyber Rn. 24). **Nicht** vorausgesetzt wird zudem ein **Vertretenmüssen** des VN (**a. A.** HK-VVG/*Pawig-Sander* A1-2 AVB Cyber Rn. 24). Das entspricht auch dem Zweck der CyberVers, die dem VN gerade auch bei schuldlosen Verletzungen (Haftpflicht-)VersSchutz bieten soll. 37

V. Schadprogramme (A1-2.4 Spiegelstrich 5)

Schadprogramm i. S. v. Spiegelstrich 5 ist eine Software, die dazu gedacht ist, unerwünschte Wirkungen bei Dritten hervorzurufen (*Malek/Schilbach* VersR 2019, 1321, 1326). 38

Der Regelung kommt **keine eigenständige Bedeutung** zu, weil Informationssicherheitsverletzungen durch solche Programme bereits von Spiegelstrich 1 oder Spiegelstrich 3 erfasst werden. Als Anwendungsfall für Spiegelstrich 5 werden in der Lit. zwar z. T. Einwirkungen durch sog. Drive-by-downloads angesehen, d. h. die automatisierte Installation von Schadsoftware beim schlichten Betrachten einer Webseite unter Ausnutzung von Sicherheitslücken z. B. von Webbrowsern (*Malek/Schilbach* VersR 2019, 1321, 1326 f.; ähnl. HK-VVG/*Pawig-Sander* A1-2 AVB Cyber Rn. 25: nicht zielgerichtete Angriffe ohne Zwischenschaltung einer Person). Allerdings lässt sich auch dieser Fall unter den Begriff des „Angriffs" subsumieren, da die Wirkung der Schadsoftware letztlich darauf zurückgeht, dass sie von einem Angreifer bewusst in Umlauf gebracht wurde, um bei den – wenn auch zu diesem Zeitpunkt nach Zahl und Identität noch unbestimmten – Betroffenen Schaden anzurichten. Jedenfalls handelt es sich um einen mittelbar durch menschliches Handeln verursachten „Eingriff" i. S. v. Spiegelstrich 2. 39

LG Hagen

LG Hagen, Urt. v. 15.10.2024 – 9 O 258/23, r+s 2025, 28

TATBESTAND:

- VN hat bei VR eine Cyberversicherung abgeschlossen. Dort heißt es u.a.:

3. Informationssicherheitsverletzung

Informationssicherheitsverletzungen im Sinne dieser Bedingungen sind:

3.1. Verletzung datenschutzrechtlicher Bestimmungen nach der Datenschutz-Grundverordnung (DS-GVO), dem Bundesdatenschutzgesetz (BDSG) oder anderen Regelungen zum Datenschutz unzulässige oder unrichtige Erhebungen, Verarbeitungen oder Nutzungen personenbezogener Daten Dritter durch Versicherte; dies gilt auch bei Verletzungen vergleichbarer ausländischer Rechtsnormen.

3.2. Vertraulichkeitsverletzung Verletzungen der Vertraulichkeit Daten Dritter durch den VN, die sich im Verfügungsbereich des VN befinden. Dazu gehören insbesondere Betriebs- und Geschäftsgeheimnisse Dritter.

3.3. Netzwerksicherheitsverletzungen Netzwerke im Sinne dieser Vertragsbedingungen sind Telekommunikations-, Daten- und Rechnernetzwerke des VN. Netzwerksicherheitsverletzungen sind Beeinträchtigungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse des VN.

- Die Kl. steht in einer regelmäßigen Geschäftsbeziehung zu einem polnischen Lieferanten (Lieferant).
- Mit dem Lieferanten kommunizierte die Kl. in der Regel per E-Mail. Kontaktperson der Kl. bei dem Lieferanten war Herr G. F.
- Per E-Mail wurde mit diesem unter anderem die Bezahlung offener Rechnungsbeträge besprochen.
- Herr F. verwendete die E-Mailadresse R. pl.
- Zum Jahreswechsel 2022/2023 hatte die Kl. gegenüber dem Lieferanten aufgrund erfolgter Lieferungen Rechnungen im unteren sechsstelligen Bereich zu begleichen.

LG Hagen, Urt. v. 15.10.2024 – 9 O 258/23, r+s 2025, 28

TATBESTAND:

- Am 25.1.2023 erhielt die Kl. eine E-Mail, mit welcher der vermeintliche Lieferant eine geplante Änderung seiner Bankmitteilung kommunizierte und dies damit begründete, dass die Kontoführungsgebühren der üblichen Bankverbindung zu hoch seien. Dabei verwendete der Absender die E-Mail-Adresse L…plR…pl. Der Domänenteil des Lieferanten „@L…pl." wurde weiterhin verwendet. Die Signatur des Lieferanten und der Name „G. F." wurden ebenfalls weiterhin verwendet.
- Später wurde die Kl. erneut über diese E-Mail kontaktiert und erörterte – wie aus der Kommunikation mit der Lieferantin gewohnt – Bestellungen und offene Rechnungen. Insbesondere wurden der Kl., wie am 25.1.2023 angekündigt, neue Bankdaten mitgeteilt. Zahlungen der Kl. an die Lieferantin sollten danach auf das Konto IBAN N02, X., N03 S., W. erfolgen.
- Auf Grund dieser Nachricht änderte die Kl. die bei ihr für den Lieferanten hinterlegten Kontodaten. Die nun folgenden Rechnungen über insgesamt 85.000 EUR zahlte die Kl. mit insgesamt vier Überweisungen auf das ihr neu mitgeteilte Bankkonto bei der X. in W. …
- Im Nachhinein stellte sich heraus, dass diese E-Mails nicht von dem eigentlichen Lieferanten kamen, sondern Fälschungen waren und auch das Konto, auf welches die Zahlungen geflossen sind, kein Konto des Lieferanten war.
- VN nimmt nun VR auf Zahlung von 85.000,00 EUR in Anspruch.

LG Hagen, Urt. v. 15.10.2024 – 9 O 258/23, r+s 2025, 28

TATBESTAND:

- Denn mit einiger Wahrscheinlichkeit war der Exchange-Server des Lieferanten der Kl. „gehackt“ worden, wodurch es dem unbekannten Absender erst möglich war, die betrügerische E-Mail vom E-Mail-Server des Lieferanten zu verschicken.
- VR lehnt Deckung ab.

Zu Recht?

LG Hagen, Urt. v. 15.10.2024 – 9 O 258/23, r+s 2025, 28

LÖSUNG: *keine* Deckung

Aus den Gründen:

20 Die zulässige Klage ist unbegründet.

21 **I.** Die Kl. hat keinen Anspruch auf Zahlung iHv 85.000 EUR gegen die Bekl. aus dem zwischen den Parteien bestehenden Versicherungsvertrag über eine Cyber-Versicherung in Verbindung mit § 1 VVG.

22 1. Es liegt kein Versicherungsfall vor, weil es an einer Informationssicherheitsverletzung im Sinne des Teil A Ziff. 4 der AVB fehlt. Weder liegt eine Verletzung datenschutzrechtlicher Bestimmungen (Teil A Ziffer 3.1 AVB) noch eine Vertraulichkeitsverletzung (Teil A Ziffer 3.2 AVB) noch eine Netzwerksicherheitsverletzung (Teil A Ziffer 3.3 AVB) vor.

23 a) Eine Verletzung datenschutzrechtlicher Bestimmungen liegt schon deshalb nicht vor, weil die Kl. als VN keinen Verstoß gegen datenschutzrechtliche Bestimmungen begangen hat.

24 Für eine Vertraulichkeitsverletzung im Sinne der AVB fehlt es an einer Verletzung der Vertraulichkeit Daten Dritter durch die Kl.

25 b) Auch eine Netzwerksicherheitsverletzung liegt nicht vor. Dies ergibt die Auslegung der zugrundeliegenden AVB, hier Teil A Ziffer 3.3. der AVB.

LG Hagen, Urt. v. 15.10.2024 – 9 O 258/23, r+s 2025, 28

LÖSUNG: *keine* Deckung

27 Ein solcher VN wird die entsprechende Klausel dahin verstehen, dass es zu einer Verletzung der Sicherheit des Netzwerkes der Kl. gekommen sein muss und eine derartige Verletzung bei dem Empfang von E-Mails, die von einem anderen als dem in den E-Mails angegebenen Absender stammen, nicht gegeben ist. Allein der Umstand, dass aufgrund der unautorisierten Verwendung des E-Mail Exchange Servers des Lieferanten möglicherweise eine nicht zu erkennende Täuschung vorgelegen hat, stellt keinen direkten Angriff auf die Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme der Kl. dar. Die informationstechnischen Systeme – auch das E-Mail System der Kl. – und letztlich auch das Netzwerk der Kl. funktionierten wie vorgesehen. E-Mails konnten auf normale Weise und unverändert empfangen und gesendet werden. Betroffen von dem Cyber-Angriff war lediglich ein Netzwerk eines Dritten.

LG Hagen, Urt. v. 15.10.2024 – 9 O 258/23, r+s 2025, 28

LÖSUNG: *keine* Deckung

28 Berücksichtigt werden müssen bei einer Auslegung der Versicherungsbedingungen weiterhin die – nicht abschließenden – Regelbeispiele aus Teil A Ziff. 3.3.1., in denen es auszugsweise heißt:

Keine Netzwerksicherheitsverletzung liegt vor, wenn

(3) Beeinträchtigungen der oben genannten Art in Netzwerken Dritter stattfinden, die Auswirkungen jedoch auch beim VN auftreten (z. B. man-in-the-middle Angriff bei Zulieferer);

(4) kein Eingriff in das Netzwerk des VN stattgefunden hat (z. B. fake president Angriffe mittels nachgebildeter E-Mail-Adresse).

29 Aus diesen Regelbeispielen kann ein durchschnittlicher und verständiger VN erkennen, dass der vorliegende Fall, der zu den eben genannten Regelbeispielen Ähnlichkeiten aufweist, nicht zu den versicherten Risiken zählt. Voraussetzung des Versicherungsschutzes bleibt eine Netzwerksicherheitsverletzung bei dem VN selbst, die nicht vorliegt. Beeinträchtigungen bei Dritten sind keine Netzwerksicherheitsverletzung bei der Kl. In Abgrenzung zu einem Cyber-Angriff handelt es sich im vorliegenden Fall einer dem „normalen" Betrug nahen Tat.

LG Hagen, Urt. v. 15.10.2024 – 9 O 258/23, r+s 2025, 28

LÖSUNG: *keine* Deckung

30 Auch im Übrigen ist dieses Verständnis der AVB sachgerecht. Denn im vorliegenden Fall ist die Kl. auf eine betrügerische E-Mail hereingefallen. Dieses Risiko ist heute allgegenwärtig und nichts, was notwendigerweise durch eine Cyber-Versicherung abzusichern wäre. Andernfalls wäre jedweder E-Mail-Verkehr mit Spam- oder Phishing-Mails eine Netzwerksicherheitsverletzung bei dem VN. Das versicherte

LG Hagen: Cyber-Versicherung, Begriff der Netzwerksicherheitsverletzung (r+s 2025, 28) 30

Risiko würde sich auf den weltweiten E-Mail-Verkehr ausweiten.

LG Hagen, Urt. v. 15.10.2024 – 9 O 258/23, r+s 2025, 28

LÖSUNG: *keine* Deckung

31 c) Auch liegt kein Versicherungsfall nach der Vertrauensschadenversicherung nach Teil D. Ziff. 1 AVB vor. Der Versicherungsfall ist ergänzend in der Vertrauensschadenversicherung zunächst unter Teil D. Ziff.1 wie folgt definiert:

Versicherungsschutz besteht für den VN wegen eines Versicherungsfalles iSv Teil A Ziffer 4, wenn die Informationssicherheitsverletzung vorsätzlich und rechtswidrig erfolgte und nach den gesetzlichen Bestimmungen über unerlaubte Handlungen zum Schadenersatz verpflichtet und der VN unmittelbar dadurch einen Vermögensschaden erleidet. Es ist dabei unerheblich, ob die Informationssicherheitsverletzung von Mitarbeitern des VN oder von Dritten erfolgte.

32 Weiterhin besteht Versicherungsschutz auch für einen eingetretenen „Täuschungsschaden“ (Teil D. Ziff. 1.2.):

Versicherungsschutz besteht für den mittelbar entstandenen Vermögensschaden, wenn ein Mitarbeiter des VN auf Grund einer Informationssicherheitsverletzung gemäß Teil A Ziffer 3, welche einen Straftatbestand im Sinne des Strafgesetzbuches erfüllt, dazu verleitet wurde, Zahlungen/Überweisungen zu veranlassen.

LG Hagen, Urt. v. 15.10.2024 – 9 O 258/23, r+s 2025, 28

LÖSUNG: *keine* Deckung

33 Zwar umfasst der Versicherungsschutz des Teil D der AVB dem Wortlaut und auch dem Sinn und Zweck nach betrügerische Handlungen die das Vertrauen des VN ausnutzen. Die Vertrauensschadenversicherung bietet – je nach Ausgestaltung – gerade auch Versicherungsschutz für vorsätzliche Eingriffe in informationsverarbeitende Systeme des VN, durch eine Vertrauensperson oder Dritte, und dadurch unmittelbar verursachte Schäden (Schilbach, r+s 2024, 581 Rn. 49, beck-online).

34 Da allerdings immer auch eine Informationssicherheitsverletzung erforderlich ist, ist der Anwendungsbereich der Vertrauensschadenversicherung nicht eröffnet.

LG Hagen, Urt. v. 15.10.2024 – 9 O 258/23, r+s 2025, 28

LÖSUNG: *keine* Deckung

35 2. Entgegen der Auffassung der Kl. sind die streitgegenständlichen AVB in den relevanten Auszügen nicht gem. § 307 BGB unwirksam.

36 a) Zum einen stellen sowohl Teil A. Ziff. 4 AVB, als auch Teil D Ziff. 1.2 Leistungsbeschreibungen des versicherten Risikos dar und unterliegen gem. § 307 Abs. 3 S. 1 BGB nicht der Inhaltskontrolle im Hinblick auf das Kriterium der unangemessenen Benachteiligung. Die Formulierungen in Teil A Ziff. 3 und Teil D Ziff. 1 AVB stellen keine Einschränkungen des zuvor festgelegten Versicherungsumfangs dar, sondern legen erst die vom VR geschuldete Leistung fest (vgl. auch BGH NJW 2023, 208 = r+s 2022, 695).

37 b) Die Leistungsbeschreibungen verstoßen auch nicht gegen das – sich gem. § 307 Abs. 3 S. 2 BGB auch auf das Hauptleistungsversprechen erstreckende (vgl. BGH VersR 2014, 625 r+s 2014, 228) – Transparenzgebot des § 307 Abs. 1 S. 2 BGB.

38 aa) Nach dem Transparenzgebot ist der Verwender allgemeiner Geschäftsbedingungen gehalten, Rechte und Pflichten seines Vertragspartners möglichst klar und durchschaubar darzustellen. Dabei kommt es nicht nur darauf an, dass die Klausel in ihrer Formulierung für den durchschnittlichen VN verständlich ist. Vielmehr gebieten Treu und Glauben, dass die Klausel die wirtschaftlichen Nachteile und Belastungen soweit erkennen lässt, wie dies nach den Umständen gefordert werden kann. Dem VN soll bereits im Zeitpunkt des Vertragsschlusses vor Augen geführt werden, in welchem Umfang er Versicherungsschutz erlangt und welche Umstände seinen Versicherungsschutz gefährden. Nur dann kann er die Entscheidung treffen, ob er den angebotenen Versicherungsschutz nimmt oder nicht (vgl. BGH NJW 2023, 208 = r+s 2022, 695). Maßgebend sind die Verständnismöglichkeiten des typischerweise bei Verträgen der geregelten Art zu erwartenden Durchschnittskunden. Insoweit gilt kein anderer Maßstab als derjenige, der auch bei der Auslegung von Versicherungsbedingungen zu beachten ist (BGH aaO).

39 bb) Nach diesen Grundsätzen sind die Leistungsbeschreibungen der AVB nicht intransparent. Denn für eine Cyber-Versicherung ist typisch und für den Durchschnittskunden erkennbar, dass nur das Risiko der eigenen IT-Systeme geschützt werden soll und nicht weltweite Hacker-Angriffe, die in mittelbarer Weise Auswirkungen gegenüber dem VN haben können. Andernfalls wäre bereits die Teilnahme am E-Mail-Verkehr an sich ein großes Risiko, da niemand vor – auch gut gefälschten – Phishing Mails geschützt ist. Die Versicherungsbedingungen sind insoweit klar und verständlich formuliert, dass im Rahmen der Netzwerksicherheitsverletzung gerade eine Beeinträchtigung der eigenen Netzwerke vorliegen muss.

LG Hagen, Urt. v. 15.10.2024 – 9 O 258/23, r+s 2025, 28

LÖSUNG: *keine* Deckung

BGH: Hausratversicherung, Wirksamkeit der sog. erweiterten Schlüsselklausel r+s 2023, 666

Hausratversicherung, Wirksamkeit der sog. erweiterten Schlüsselklausel

BGB § 307 Abs. 1 Satz 2, Abs. 3 Satz 1; AVB Hausratversicherung (hier: GWW 2014) § 28 Nr. 4 Buchst. a), 4. Spiegelstrich

Die sogenannte "erweiterte Schlüsselklausel" in der Hausratversicherung (hier: § 28 Nr. 4 Buchst. a), 4. Spiegelstrich GWW 2014), wonach ein Einbruchdiebstahl auch dann vorliegt, wenn der Täter in einen Raum eines Gebäudes mittels richtiger Schlüssel eindringt, die er ohne fahrlässiges Verhalten des berechtigten Besitzers durch Diebstahl an sich gebracht hat, unterfällt als primäre Leistungsbeschreibung gemäß § 307 Abs. 3 Satz 1 BGB nicht der Inhaltskontrolle und verstößt auch nicht gegen das Transparenzgebot des § 307 Abs. 1 Satz 2 BGB. (amtl. Leits.)

BGH , Urt. *v.* 5.7.2023 – IV ZR 118/22 (KG)

LG Hagen, Urt. v. 15.10.2024 – 9 O 258/23, r+s 2025, 28

LÖSUNG: *keine* Deckung

BGH: Klauselkontrolle: "unerwartete und schwere" Erkrankung r+s 2022, 695

Klauselkontrolle: "unerwartete und schwere" Erkrankung

UKlaG § 1, § 3 Abs. 1 Nr. 1; BGB § 305 c Abs. 1, § 307 Abs. 1 und 3; VVG §§ 19 ff., § 32 S. 1

1. Die Formulierung "unerwartete und schwere" Erkrankung in den Bestimmungen einer Reiseversicherung (hier: B Reise-Rücktrittsversicherung Nr. 3.1, 3.15, 8 VB-RS 2014 (RRK/UG-D) und B ReiseabbruchVersicherung Nr. 3.1, 7 VB-RS 2014 (RRK/UG-D)) verstößt nicht gegen das Transparenzgebot des § 307 Abs. 1 S. 2 BGB. (amtl. Leits.)

2. Als primäre Leistungsbeschreibung unterfällt die Regelung gemäß § 307 Abs. 3 S. 1 BGB im Übrigen nicht der Inhaltskontrolle. Eine gemäß § 32 S. 1 VVG unwirksame Abweichung von den §§ 19 ff. VVG liegt nicht vor. (amtl. Leits.)

BGH, Urt. v. 19.10.2022 – IV ZR 185/20 (OLG Hamburg)

Anm. von Dr. Dan Schilbach, r+s 2025, 28

So lag der Fall hier. Der bloße Empfang einer betrügerischen (Phishing-)E-Mail begründet nämlich noch keine Netzwerksicherheitsverletzung, und zwar unabhängig davon, ob die E-Mail über eine dem Kl. bekannte und im Regelfall vertrauenswürdige E-Mail-Adresse oder – wie im Regelbeispiel in den AVB explizit genannt – mittels nachgebildeter E-Mail-Adresse verschickt wurde. Anders läge der Fall, wenn der VN auf einen Link oder E-Mail-Anhang einer empfangenen Phishing-E-Mail geklickt und dadurch z. B. Schadsoftware auf den Systemen des VN ausgeführt hätte. In diesem Fall tritt nämlich eine Informationssicherheitsverletzung in Gestalt einer Netzwerksicherheitsverletzung auf den informationstechnischen Systemen des VN selbst ein. Der zugrundeliegende Sachverhalt war indes ein anderer. Mangels Eintritts einer Netzwerksicherheitsverletzung beim VN fehlte es deshalb – wie die Kammer zu Recht angenommen hat – schon an der Grundvoraussetzung für den Versicherungsschutz, nämlich dem Eintritt des versicherten Risikos. Es gibt im Markt vereinzelt Cyber-Bedingungswerke, die Identitätstäuschungen der vorliegenden Art auch unabhängig vom Vorliegen einer Informationssicherheits- bzw. Netzwerksicherheitsverletzung beim VN decken. Im Vordergrund stehen dabei häufig sog. fake-president-Fälle (weitergehend hierzu, Schilbach, in: Dickmann, Cyberversicherung, A1-17.9 Rn. 1 ff.), in denen Angreifer sich mittels technischer Hilfsmittel (z. B. Voice-Cloning-Tools, die auf Künstlicher Intelligenz basieren) als Geschäftsführer ausgeben, um Mitarbeiter des betroffenen Unternehmens zu Überweisungen zu veranlassen (hierzu Rudkowski, VersR 2024, 601, 604).

Diskussion & Fazit

Fazit:

- Ob Cyberbetrug gedeckt ist, richtet sich (wie immer) nach dem konkret individuellen Wording
- Versicherungsschutz kann bestehen, wenn der Cyberversicherungsvertrag (wie oftmals) abseits einer Informationssicherheitsverletzung Identitätstäuschungen versichert (z.B. fake-president-Fälle oder Man-in-the-Middle-Attacken)
- Ob Cyberbetrug eine Informations- bzw. Netzwerksicherheitsverletzung darstellt, hängt im Übrigen von den Einzelfallumständen ab
- Eine bloße Täuschung des VN bzw. ein Betrug als solcher genügt für eine Netzwerksicherheits-verletzung m.E. nicht
- Der Fall des LG Hagen ist m.E. zutreffend entschieden.
- Mit den Urteilsgründen des LG Hagen spricht viel dafür, dass beim Bsp.-Fall „Pferdetransporter“ keine Informationssicherheitsverletzung vorliegt bzw. keine unbefugte Nutzung von IT-Systemen und damit keine Deckung besteht – ein „kompromittierender“ QR-Code konnte jedenfalls nicht bewiesen werden.

Standorte

Köln

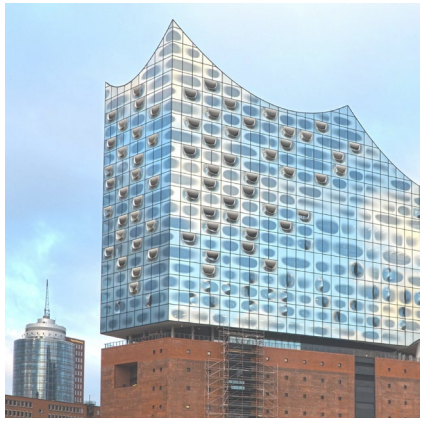
München

Frankfurt

Berlin

Karlsruhe

Dortmund



Hamburg

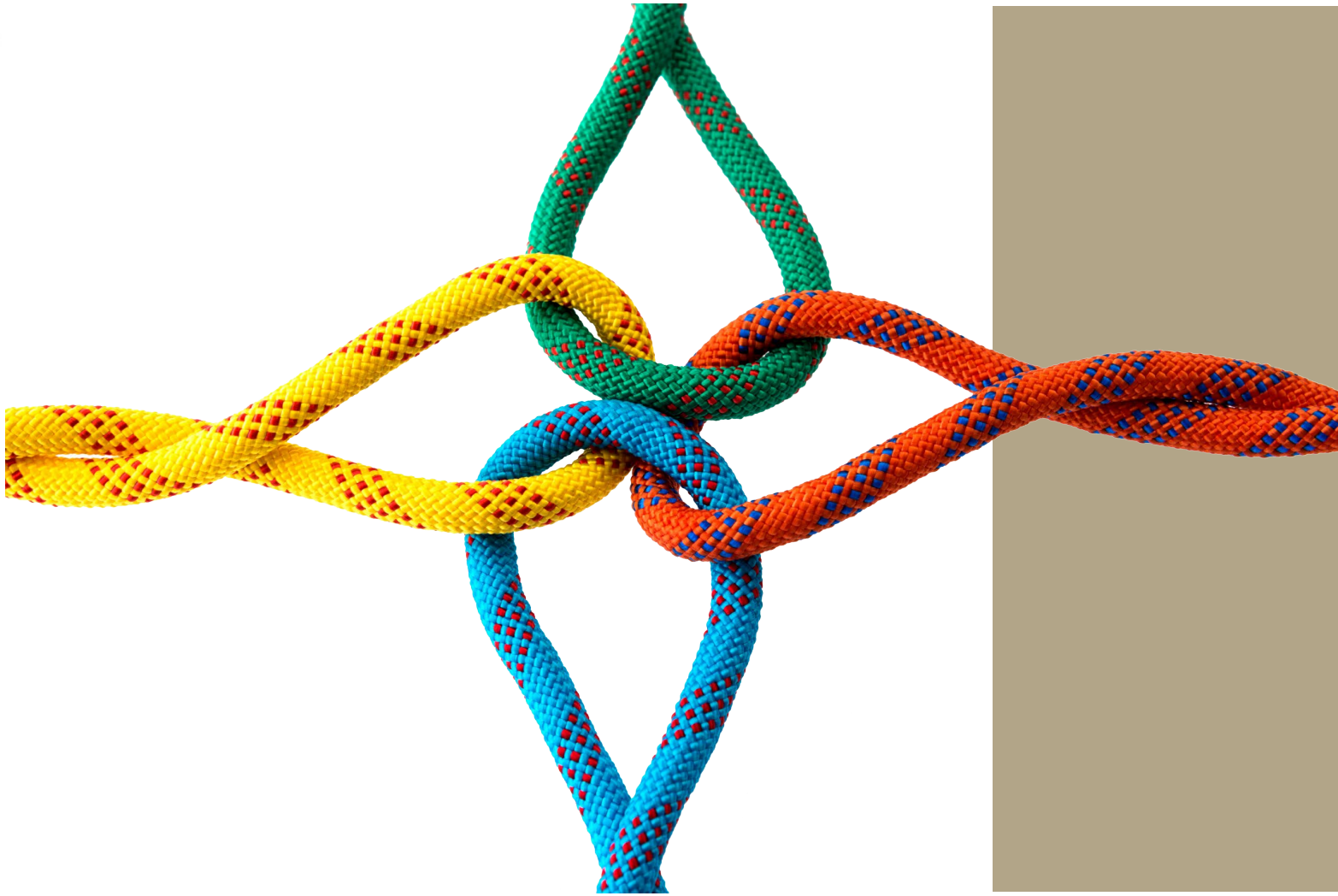
Leipzig

Europe

A core area of our international activity lies in Europe. Over the last decades, we have built up a network of specialised law firms in almost all European jurisdictions, and with whom we work with confidence. We have further intensified this European presence through close cooperation with DAC Beachcroft and thereby strengthened our own European offer.

International

BLD is a founding member of the global law firm group Legalign Global, which includes more than 3,500 lawyers. As a strategic unit within our joint network Legalign Global, we advise on cross-border risks and claims for multinational insurers, brokers and companies. At Legalign Global, we combine knowledge of the respective insurance markets and the legal system and can therefore offer optimal advice and results in claims cases anywhere and at any time. It is also important to mention that because we have separate legal entities, we reduce the potential for conflict and increase the flexibility with which you can commission us.



Rechtliche Hinweise und Haftung

- Alle Inhalte dieses Werkes sind urheberrechtlich geschützt.
  - Das Urheberrecht liegt bei BLD Bach Langheid Dallmayr Rechtsanwälte PartG mbB.
  - Jeder Nachdruck und jede Vervielfältigung – einschließlich Speicherung und Nutzung auf optischen und elektronischen Datenträgern – sowie jede Veränderung und Verwertung, die nicht ausdrücklich vom Urhebergesetz zugelassen sind, bedarf der vorherigen Zustimmung von BLD in Textform.

- Die Inhalte dieser Präsentation dienen nur zur internen Information auf dieser Veranstaltung.
  - Entsprechend darf dieses Werk – auch nicht dem wesentlichen Inhalt nach – nicht an Dritte weitergegeben oder zum Gebrauch bei Dritten verwendet werden, es sei denn, BLD hat dazu seine vorherige Zustimmung in Textform erteilt.

- Diese Präsentation stellt keine rechtliche Beratung dar, sondern ist nur eine allgemeine Darstellung und Erörterung von Rechtsfragen und Rechtsfällen. BLD schließt daher jedwede Haftung für Richtigkeit, Vollständigkeit und Aktualität aus

Legal Disclaimer

- This presentation and all of its contents are protected by copyright.
  - The copyright is owned by BLD Bach Langheod Dallmayr Rechtsanwälte Partnergesellschaft mbB
  - Any reprint or reproduction of this presentation and its content, including storage and transmission via electronic means, and any other modification and use not expressly permitted by the German Copyright Act, requires prior written authorisation from BLD.

- The contents of this presentation are for internal purposes within the context of this meeting only.
  - Accordinglly, this presentation and all of ist content may not be disseminated to, or used by, any third parties, unless BLD has given ist prior written authorisation for suche use or dissemination.

- This presentation does not constitute legal advice, and comprises only a general presentation and discussion of legal questions and cases. BLD excludes any liability in relation to accuracy, completeness and currency of the information contained therein.