

**R. Sanktionswidrige Schadensbearbeitung trotz Sanktionsklausel**

Denkbar ist es schließlich, dass die Sanktionsklausel vereinbart ist, dann aber dennoch – bemerkt oder unbemerkt – im Schadenfall sanktionswidrig Leistungen erbracht werden. Solcher Leistung fehlt dann der Rechtsgrund. Denn wegen der Sanktionsklausel bezieht sich der Versicherungsvertrag nicht auf den Schadenfall, ohne dass es auf den Verstoß gegen ein gesetzliches Verbot ankäme (dem wegen der Sanktionsklausel ja gerade nicht zuwidergehandelt wurde). Es kommt auch kein Anerkenntnis in Betracht, welches ohnehin nicht deklaratorisch, sondern wegen des fehlenden Rechtsgrundes nur konstitutiv sein könnte. Dieses Anerkenntnis würde zwar, da wegen Individualität vorrangig, nicht an der Sanktionsklausel scheitern, wohl aber an § 134 BGB. 41

Interessant ist die Frage, ob der Versicherer die erbrachte Leistung zurückfordern kann. Dies ist im Falle irrtümlicher Leistung ohne Weiteres zu bejahen, denn schon wegen der Sanktionsklausel fehlt es an einem Rechtsgrund. Mangels Kenntnis des Versicherers im Irrtumsfalle stellt sich auch nicht die Frage des § 814 BGB (Kenntnis der Nichtschuld). Sie stellt sich aber in aller Schärfe, wenn die Leistung in Kenntnis des Sanktionsverstoßes erfolgt. Richtigerweise ist § 814 BGB dann nicht anwendbar. Seine Anwendung würde direkt dem Zweck des Sanktionsgesetzes zuwiderlaufen und die Folge zivilrechtlicher Unwirksamkeit gem. § 134 BGB konterkarieren. Im Übrigen ist anerkannt, dass die Bestimmung schon dann nicht anwendbar ist, wenn der Empfänger wusste, dass er die Leistung nicht behalten darf (zu Einzelheiten s. Schwab in MüKoBGB BGB § 814 Rn. 7 ff.). 42

## 92. Klausel für den Ausschluss von Cyber- und Blackoutschäden sowie den optionalen Wiedereinschluss von Cyberschäden in der Transportversicherung

*Unverbindliche Muster-AVB des GDV (Stand: Oktober 2020)*

### Vorbemerkungen zu Ziff. 1

#### A. Hintergrund

- 1 Mit dieser Klausel hat der GDV im Jahr 2021 erstmals eine Klausel zu Cyber- und Blackoutrisiken zur Verfügung gestellt, die für die Verwendung in allen Bereiche der Transportversicherung gedacht ist. Bislang gab es nur vereinzelte Bedingungswerke, die eine Cyberklausel enthalten (vgl. Ziff. 36 DTV-ADS für die Seeschiffsversicherung). Im April 2017 hatte der GDV bereits die AVB Cyber veröffentlicht. Dabei handelt es sich nicht um einen Ausschluss, sondern um Versicherungsbedingungen für Cyberrisiken. Die hier kommentierte Cyber- und Blackoutklausel greift Formulierungen der AVB Cyber auf.
- 2 Die Blackoutklausel ist älteren Ursprungs, wurde vom GDV bislang aber noch nicht veröffentlicht, was nun gelegentlich der Entwicklung der Cyberklausel erfolgt. Diese Historie erklärt teils unterschiedliche Strukturen der Klauseln, die sich aber nicht wesentlich auf die Wirkungsweise auswirken. Die Klausel verwendet die Begriffe „Cyber“ und „Blackout“ nur in der Klauselbezeichnung und in Überschriften, nicht aber im Text selbst.

#### B. Cyberrisiko

- 3 Soweit es um Cyberrisiken geht, ist es zum einen Zweck der Klausel, das Bewusstsein für Cyberrisiken zu wecken. Dies geht Hand in Hand mit Bemühungen des GDV, durch die Entwicklung von Reports und Factsheets (s. [www.gdv.de/de/the-men/news/materialien-zum-download-43692](http://www.gdv.de/de/the-men/news/materialien-zum-download-43692), zuletzt abgerufen am 25.4.2022) Hilfestellung für die Identifizierung von, Cyberrisiken zu geben, damit die Versicherer dann entscheiden können, in welchem Umfang sie sie versichern wollen. Außerdem geht es darum, die sich aus den Cyberrisiken ergebenden Kumulrisiken zu begrenzen.
- 4 Die Klausel ist einerseits Ausschlussklausel. Bleibt es bei der Vereinbarung allein der Ziff. 1., dann wird damit die sogenannte Nullstellung der Cyberrisiken erreicht: Versicherungen, denen die Klausel hinzugefügt wird, decken keine Cyberrisiken mehr. Die Klausel erlaubt aber zugleich in Alternativen in unterschiedlichem Umfang den Wiedereinschluss des Cyberrisikos mittels bereitstehender Wortlaute. Das Ziel, Silent Cyber zu vermeiden, wird nur mit der zweiten der alternativen Wiedereinschlussklauseln (Ziff. 3.2) erreicht. Die erste Alternative (Ziff. 3.1) stellt die Deckung dem Grunde nach umfassend wieder her, erfasst damit also gerade auch alle „Silent Cyber“-Risiken und führt lediglich Höchsthaftungssummen ein. Ziff. 3.1 dient damit nur der Kumulbegrenzung. Ziff. 3.2 enthält auch diese Kumulbegrenzung, begrenzt aber auch dem Grunde nach.
- 5 Ein Ausschluss ist nur sinnvoll, wenn ohne ihn Deckungsschutz besteht. Die alternativen Wiedereinschlüsse bezwecken nur die teilweise Wiederherstellung des ohne

den Ausschluss bestehenden Deckungsumfangs. Die Deckung wird dadurch nicht erweitert.

### C. Blackout

Der Begriff stammt ursprünglich aus der Medizin und bezeichnet den zeitweiligen Verlust des Sehvermögens oder des Bewusstseins. Von dort wurde er in technische Bereiche übernommen und bezeichnet traditionell einen **Stromausfall**. So verwendet ihn auch die Klausel und ergänzt ihn um den Ausfall von Informationssystemen. Die Blackoutrisiken sind leichter zu greifen als die Cyberrisiken. Hier geht es nicht um die Vermeidung ungewollter Mitversicherung, sondern allein um die Bekämpfung des Kumulrisikos. Die Klausel stellt keinen Wiedereinchluss zur Verfügung.

### D. Klauseln des englischen Marktes

**I. Vorbemerkung.** Während in Deutschland im Transportbereich erst seit kurzem Verbandsempfehlungen zu einem Cyberausschluss gibt, sind solche Klauseln im englischen Markt schon seit langer Zeit verfügbar. Aus der Fülle der bestehenden Klauseln seien nachfolgend zwei Klauseln beispielhaft wiedergegeben.

#### II. Institute Cyber Attack Exclusion Clause (Cl. 380)

Stand: 10.11.2003

- 1.1 Subject only to clause 1.2 below, in no case shall this Insurance cover loss damage liability or expense directly or indirectly caused by or contributed to by or arising from the use or Operation, as a means for inflicting harm, of any Computer, Computer System, Computer Software Programme, malicious code, Computer virus or process or any other electronic System.
- 1.2 Where this clause is endorsed on policies covering risks of war, civil war, revolution, rebellion, insurrection, or civil strife arising therefrom, or any hostile act by or against a belligerent power, or terrorism or any person acting from a political motive, Clause 1.1 shall not operate to exclude losses (which would otherwise be covered) arising from the use of any Computer, Computer System or Computer Software Programme or any other electronic System in the launch and/or guidance System and/or firing mechanism of any weapon or missile.

#### III. Marine Cyber Exclusion (LMA5402)

Stand: 11.11.2019

This clause shall be paramount and shall override anything in this insurance inconsistent therewith.

- 1 In no case shall this insurance cover any loss, damage, liability or expense directly or indirectly caused by, contributed to by or arising from:
  - 1.1 the failure, error or malfunction of any computer, computer system, computer software programme, code, or process or any other electronic system, or
  - 1.2 the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system.

### Ziff. 1

- 1 **Ausschluss Cyberschäden**
  - 1.1 **Soweit nicht im Wege der Individualvereinbarung anders vereinbart, gelten die nachfolgenden Ziffern 1.2 bis 1.4 für den gesamten Versicherungsvertrag einschließlich aller Deckungserweiterungen.**
  - 1.2 **Vom Versicherungsschutz ausgeschlossen sind ohne Rücksicht auf mitwirkende Ursachen Sachschäden, Vermögensschäden, Haftung, Kosten, Aufwendungen oder mittelbare Schäden soweit sie direkt oder indirekt durch eine Informationssicherheitsverletzung verursacht wurden, aus dieser entstanden sind oder diese beigetragen hat.**

**1.3 Informationssicherheitsverletzung ist eine Beeinträchtigung der**

- Verfügbarkeit
- Integrität
- Vertraulichkeit

von elektronischen Daten oder von informationsverarbeitenden Systemen, die der Versicherungsnehmer bzw. der Versicherte zur Ausübung seiner betrieblichen oder beruflichen Tätigkeit nutzt, oder die von in seinem rechtlichen oder wirtschaftlichen Interesse eingeschalteten Dritten, insbesondere Verkehrsträger, Subunternehmer oder sonstige Erfüllungsgehilfen, genutzt werden. Dabei ist es unerheblich, ob sich die elektronischen Daten oder die informationsverarbeitenden Systeme im unmittelbaren Verfügungsbereich des Versicherungsnehmers bzw. des Versicherten oder des eingeschalteten Dritten befinden oder sie sich eines externen Dienstleisters bedienen.

**1.4 Der Begriff „elektronische Daten“ umfasst auch Software und Programme.****A. Individualvereinbarungen**

- 1 Soweit Ziff. 1.1 Individualvereinbarungen anspricht, handelt es sich um eine nicht erforderliche Klarstellung. Bei der Klausel handelt es sich um allgemeine Versicherungsbedingungen. Auch wenn die Klausel sich selbst nicht als abänderbar bezeichnen würde, gehen Individualvereinbarungen vor (§ 305 b BGB).

**B. Andere AVB**

- 2 S. zunächst allgemein zum Rangverhältnis zwischen AVB Armbrüster in Prölss/Martin Einl. Rn. 291. Soweit andere AVB weitergehende Cyberausschlüsse beinhalten, werden diese durch die Klausel nicht verdrängt. So etwa Ziff. 36.1.2 DTV-ADS für die Seeschiffsversicherung, wo der Gebrauch oder Einsatz von jeder Art von Computern, Computersystemen, Computerausdrucken, Prozessabläufen oder irgendeines anderen elektronischen Systems zum Zwecke der Schadenszufügung ausgeschlossen ist, ohne dass es dabei darauf ankommt, dass eine Informationssicherheitsverletzung im Sinne der Klausel gegeben wäre. Im Übrigen setzt sich die Klausel bei einer „Silent Cyber“-Deckung, also der quasi unbemerkten, jedenfalls nicht angesprochenen Mitversicherung von Cyberrisiken, insbesondere in Allgefahrendeckungen, durch. Wo AVB dagegen ausdrücklich Versicherungsschutz für Cyberrisiken gewähren, wird man regelmäßig deren Vorrang annehmen müssen.
- 3 Ebenfalls unberührt bleiben andere Ausschlüsse, die auch im Bereich von Cyberrisiken ihre Bedeutung behalten und häufig den Versicherungsschutz auch ohne Rücksicht auf eine Informationsrechtsverletzung ausschließen. So zB der Ausschluss von Schäden aufgrund Verzögerung der Reise gem. Ziff. 2.5.1.1 DTV-Gü VolleDeck oder aufgrund inneren Verderbs oder natürlicher Beschaffenheit gem. Ziff. 2.5.1.2 DTV-Gü VolleDeck. Diese Ausschlüsse greifen allerdings nur, wenn die dort ausgeschlossenen Gefahren causa proxima waren (dazu → DTV-Gü VolleDeck Ziff. 2.6 Rn. 5). Die Informationspflichtverletzung schließt den Deckungsschutz schon aus, wenn sie nur mitwirkende, untergeordnete Ursache war (causa remota). Darin liegt bei Ursachenkonkurrenzen die besondere Bedeutung der Klausel, weil sie es entbehrlich macht, andere Ausschlüssen als nächste Ursache zu prüfen.
- 4 Der Ausschluss gilt ausdrücklich auch für anderweitige Deckungserweiterungen. Weitgehend bedarf es einer solchen Bestimmung nicht. Die in der Transportversicherung verbandsseitig zur Verfügung gestellten Deckungserweiterungen sehen regelmäßig vor, dass der erweiterte Deckungsschutz nur im Rahmen der sonstigen Vertragsbedingungen gewährt wird. Ist die Klausel Bestandteil des Vertrages, findet sie über eine derartige Bestimmung auch auf den erweiterten Deckungsschutz Anwendung. Nur wenige Deckungserweiterungsklauseln könnten hier problematisch sein, namentlich in der Güterversicherung die Kriegsklausel (vgl. Nr. 132 dieses

Werkes) und die Streik- und Aufruhrklausel (vgl. Nr. 134 dieses Werkes), weil dort die Erweiterung jeweils nur in Abänderung von Ziff. 2.4.1.1 bzw. Ziff. 2.4.1.1 der DTV-Gü VolleDeck erfolgt, was die Auslegung ermöglichen würde, dass sich die genannten Klauseln nur an diesen Vorschriften messen lassen muss. Bei der Streik- und Aufruhrklausel kommt hinzu, dass diese eigene Ausschlüsse enthält, und damit die Augmentation ermöglicht hätte, dass diese Ausschlüsse abschließend sind. Dies ist zwar auch bei anderen Deckungserweiterungen der Fall (zB Güterfolgeschadenklausel, Nr. 141 dieses Werkes; Vermögensschadenklausel, Nr. 142 dieses Werkes). Dort ist aber ein ersatzpflichtiger Güterschaden Voraussetzung, an dem es gerade fehlt, wenn die Klausel den Deckungsschutz der Grundversicherung ausschließt.

### C. Ausschluss

Auch wenn einzelne Schäden, Kosten usw. aufgezählt werden, handelt es sich 5 nicht um einen Ausschluss von Schäden, sondern um einen Gefahrausschluss („durch eine Informationssicherheitsverletzung verursacht“). Einzelne Schäden und sonstige gedeckte Tatbestände werden nur deshalb aufgezählt, weil die Klausel in allen Bereichen der Transportversicherung Anwendung finden soll. Deshalb sollen sich dort angesprochene Schäden auch in der Klausel wiederfinden. Auch wird damit den Gepflogenheiten auf ausländischen Märkten entsprochen (s. die bei Rn. 7 abgedruckten englischen Klauseln). Für einen wirksamen Gefahrausschluss hätte es aber nicht der Bezugnahme auf irgendwelche Schäden oder Kosten bedurft. Insoweit liegt nur eine Klarstellung vor. Ausgereicht hätte der Ausschluss der Gefahr. Deshalb wirkt der Ausschluss auch bei solchen Deckungen, bei denen der gewährte Versicherungsschutz nicht von der Schadensaufzählung der Klausel erfasst wird.

Bedeutungslos ist, wer oder was die Informationspflichtverletzung ausgelöst hat. 6 Entscheidend ist nicht eine zur Informationspflichtverletzung führende Handlung, sondern der Erfolg der Informationspflichtverletzung. Erfasst werden deshalb auch Informationspflichtverletzungen des Versicherungsnehmers oder seiner Repräsentanten, ohne dass die Klausel deshalb zu einer verhüllten Obliegenheit würde.

### D. Definition der Informationspflichtverletzung

Die hier enthaltene Definition lehnt sich eng an die Definition in Ziff. A.1–2 7 AVB Cyber an, ist mit ihr aber nicht identisch. Übernommen ist das Erfordernis der Beeinträchtigung der Verfügbarkeit, der Integrität und der Vertraulichkeit von elektronischen Daten oder informationsverarbeitenden Systemen. Diese wiederum knüpfen eng an das IT-Grundschutz-Kompendium des Bundesamtes für Sicherheit in der Informationstechnik ([https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium\\_Einzeln\\_PDFs\\_2022/ZIP\\_Da tei\\_Edition\\_2022.html](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzeln_PDFs_2022/ZIP_Da tei_Edition_2022.html); zuletzt abgerufen am 25. 4. 2022) an.

### E. Elektronische Daten

Dies sind alle Informationen, die elektronisch gespeichert sind. Speicherort (ei- 8 gene oder fremde Server) und Speichermedium (Festplatten, Sticks; Disketten, CD-ROM) sind ebenso bedeutungslos wie Formate. Nicht dazu gehören Daten in Papierform (Klimke in Pröls/Martin AVB Cyber Ziff. A.1–2 Rn. 4; Pawig-Sander in HK-VVG AVB Cyber Ziff. A.1.2 Rn. 6), wohl aber Papierdokumente, die gescannt und zB als pdf gespeichert sind, und zwar auch dann, wenn Papierversionen solcher elektronischer Daten noch zur Verfügung stehen. Wer die Daten erstellt hat, ist irrelevant. Die in Ziff. 1.4 enthaltene Einbeziehung von Software und Programmen in den Begriff der elektronischen Daten wurde aus Ziff. A.1–2.3 AVB Cyber

übernommen. Damit entfällt das Erfordernis, zwischen Anwendungen, Programmen und damit erzeugten Daten zu unterscheiden. Irrelevant ist auch der Inhalt der Information, so dass Bild-, Text oder Codedateien dazugehören.

## F. Nutzer und Nutzung der Daten

- 9 Wie Ziff. A1–2 AVB Cyber stellt auch die Cyberausschlussklausel hinsichtlich informationsverarbeitender Systeme auf deren **betriebliche oder berufliche** (also nicht notwendig gewerbliche) **Nutzung** ab. Was elektronische Daten angeht, beschränkt Ziff. A.1–2.2 AVB Cyber diese auf die Daten des Versicherungsnehmers. Die Cyberausschlussklausel dagegen stellt auch bei elektronischen Daten allein auf die betriebliche oder berufliche Nutzung ab.
- 10 Werden Daten (zB Programme) **sowohl beruflich als auch privat** genutzt, greift der Ausschluss auch dann ein, wenn die Informationspflichtverletzung konkret während privater Nutzung erfolgt, denn ausschlaggebend ist nicht, zu welchem Zweck der Versicherungsnehmer die Daten im Moment der Verletzung nutzt, sondern ob er sie grundsätzlich auch beruflich oder betrieblich nutzt. Befinden sich auf einem Rechner zB ein privater und ein beruflicher Email-Account und gelangt über den Anhang einer privaten Email Schadsoftware auf den Rechner, unterfällt dies dem Ausschluss. Ebenso wenn ein „Familien-PC“ während der Zeit des **Home Office** benutzt wird, um auf einen Firmenserver zuzugreifen.
- 11 Es kann sich auch um die Nutzung von Daten Dritter (zB Lizenzen oder Datenpools) handeln, die der Versicherungsnehmer nutzen kann. Ob die Nutzung legal oder illegal ist, ist bedeutungslos. Auch Schäden aus einer manipulierten Raubkopie einer Software sind durch die Klausel ausgeschlossen.
- 12 Die Klausel spricht nicht nur den Versicherungsnehmer an, sondern ausdrücklich auch den **Versicherten**. Das ist dem Umstand geschuldet, dass die im Markt verbreiteten Bedingungen Versicherte teils ausdrücklich ansprechen und ihr Verhalten demjenigen des Versicherungsnehmers gleichstellen (zB Ziff. 8.1 DTV-ADS für die Seeschiffsversicherung), andere aber nicht. Durch die Erwähnung der Versicherten ist klargestellt, dass der Ausschluss auch dann wirkt, wenn es sich um Daten des Versicherten handelt.
- 13 Der Kreis der Nutzer geht aber weit über den Versicherungsnehmer hinaus und erfasst auch **Dritte, soweit sie im Interesse des Versicherungsnehmers** tätig sind. Solche Dritten können vom Versicherungsnehmer selbst, aber auch von anderen in seinem Interesse eingeschaltete sein. Typisches Beispiel ist der vom Spediteur des Versicherungsnehmers eingeschaltete Verkehrsträger. Eine Vertragskette zwischen Versicherungsnehmer oder Versichertem zum Dritten ist dabei nicht erforderlich. Es genügt, dass der Dritte im rechtlichen oder wirtschaftlichen Interesse des Versicherungsnehmers oder Versicherten tätig wird. So beim CIF-Verkauf, bei dem die Gefahr mit Sicherung des Gutes auf dem Seeschiff auf den versicherten Käufer übergeht, ohne dass dieser vertragliche Beziehungen zum Verfrachter hat.
- 14 Es muss sich aber in jedem Fall um eine **Nutzung von Daten oder informationsverarbeitenden Systemen** handeln, nicht um die Nutzung von Technik, die mit Daten oder informationsverarbeitenden Systemen betrieben oder gesteuert wird, die durch Informationsrechtsverletzungen manipuliert und damit unbrauchbar wird. Ein Schiff, das für die Navigation ein globales Navigationssatellitensystem verwendet, nutzt die Daten, die dieses System zur Verfügung stellt. Ein Eingriff in das Satellitensystem mit der Folge der Einschränkung der Verfügbarkeit oder der Integrität der Daten löst damit sowohl für Schäden, die daraus am Schiff wie auch den darauf transportierten Gütern entstehen, den Ausschluss aus. Werden dagegen Daten oder informationsverarbeitende Systeme manipuliert, mit denen ein Schleusentor oder eine Hubbrücke gesteuert werden, und öffnen sich dadurch das Schleusentor oder die Brücke in einem Moment, in dem dadurch Schäden für

Schiffe oder LKW und deren Ladung eintreten, dann handelt es sich nicht um die Nutzung von Daten oder informationsverarbeitenden Systemen, sondern um die Nutzung der Schleuse oder der Hubbrücke. Hier greift der Ausschluss nicht ein.

## G. Informationsverarbeitende Systeme

Der Begriff ist weit zu verstehen (ebenso Malek/Schilbach VersR 2019, 1321; Klimke in Prölss/Martin AVB Cyber Ziff. A.1–2 Rn. 8). Er erfasst mindestens das, was die DGSVO in Art. 4 Nr. 2 als Verarbeitung definiert: jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung; auch Systeme zur reinen Speicherung von Daten. Darunter fallen auch alle funktional abgegrenzten technischen Anlagen zum Zwecke der Informationsverarbeitung (Malek/Schilbach VersR 2019, 1321) und zur Speicherung (Fortmann r+s 2019, 429). 15

## H. „Inhaber“ der Systeme

Wer die informationsverarbeitenden Systeme vorhält oder kontrolliert, ist gleichgültig. Es kann sowohl der Versicherungsnehmer oder der Versicherte oder jeder in deren rechtlichen oder wirtschaftlichen Interesse eingeschaltete Dritte sein. 16

## I. Verfügbarkeit, Integrität und Vertraulichkeit der Daten

Die Verfügbarkeit sowie die Integrität und Vertraulichkeit der Daten sind die drei Schutzziele des IT-Grundschutz-Kompodiums. Durch wen, auf welche Weise und ob zu einem bestimmten Zweck die drei Schutzbereiche verletzt wurden, ist bedeutungslos. Dadurch unterscheidet sich die Klausel wesentlich von den bislang üblichen Cyberklauseln, wie etwa Ziff. 36.1.2 DTV-ADS, die für die Seeschiffsversicherung fordert, dass ein Einsatz als Mittel der Schadenszufügung erfolgt. Ähnlich die aus dem englischen Markt bekannte „(CL380), abgedruckt bei – Vor Ziff. 1 Rn. 7, die auf „a means for inflicting harm“ abstellt. Vermittelnd die ebenfalls im englischen Markt entwickelte „Marine Cyber Exclusion“ Clause (LMA5402), die einerseits ohne bestimmte Zwecke auf 17

„failure, error or malfunction of any computer, computer system, computer software programme, code, or process or any other electronic system“

abstellt, alternativ aber auch auf

„the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system“

(s. die bei → Vor Ziff. 1 Rn. 7 abgedruckte englische Klausel).

**I. Verfügbarkeit.** Verfügbarkeit von Daten ist die jederzeitige Möglichkeit auf ihren Zugriff, was zB durch sog. (D)DoS-Attacken verhindert werden kann, in denen nur der Zugang zu den Daten verhindert wird. Dieser Zugang kann auch unabsichtlich beeinträchtigt werden, zB durch die unbeabsichtigte Vergabe eines neuen Passwortes. 18

**II. Integrität der Daten.** Integrität der Daten ist ihr unveränderter Zustand. Dieser ist verletzt, wenn Daten hinzugefügt, weggenommen oder inhaltlich ver-

ändert sind. Dazu gehört insbesondere auch die **Verschlüsselung** von Daten im Rahmen von Cybererpressungen.

- 20 **III. Vertraulichkeit der Daten.** Vertraulichkeit der Daten ist der Schutz vor Zugriff durch Unberechtigte. Die Art und Weise des Zugriffs ist unbeachtlich. Er kann durch eingeschleuste Software erfolgen, die Daten kopiert und versendet, oder durch sog. Phishing-Mails, mit denen Passworte erlangt werden, die den Zugang erlauben, aber auch dadurch, dass Passwörter analog aufbewahrt und in die Hände Dritter gelangen.

## J. Kausalität

- 21 In der Seeversicherung gilt die **causa-proxima-Regel** (→ DTV-Gü VolleDeck Ziff. 2.6 Rn. 5 ff. (Nr. 100 in diesem Werk)). Maßgeblich ist allein die wirksamste, der Ursächlichkeit nach erheblichste Bedingung (zu den verschiedenen von der Rspr. aufgestellten Kriterien siehe Schwampe RdTW 2020, 85). Ist eine versicherte Gefahr causa proxima, dann bleibt eine lediglich als causa remota mitwirkende ausgeschlossene Gefahr unbeachtlich.
- 22 Der BGH (RdTW 2015, 248) hat die causa-proxima-Regel auf die Transportversicherung des VVG ausgeweitet (krit. dazu → DTV-Gü VolleDeck Ziff. 2.6 Rn. 10 ff. (Nr. 100 in diesem Werk)). Die sogenannten Transporthaftpflichtversicherungen sind demgegenüber keine Transportversicherungen (Koller in Prölss/Martin VVG § 130 Rn. 9). Auf sie hat der BGH die causa-proxima-Regel bislang nicht ausgedehnt. Für sie gilt die Adäquanztheorie.
- 23 In der **Adäquanztheorie** setzt sich bei der Konkurrenz versicherter und nicht versicherter Gefahren die nicht versicherte Gefahr durch. Der Versicherungsschutz ist also dort schon bei bloßer Mitursächlichkeit einer nicht versicherten Gefahr ausgeschlossen (BGH VersR 2015, 1156 zur Haftpflichtversicherung; VersR 1990, 297 zur Lebensversicherung; Rolf in Bruck/Möller VVG § 21 Rn. 35; Enge/Schwampe, S. 65; Langheid/Rixecker VVG § 100 Rn. 53; Gräfe/Brügge, in: Veith/Gräfe/Geber PHdB-VersProz § 19 Rn. 544 zur Haftpflichtversicherung; Stoffregen VersR 2018, 577).
- 24 Vor diesem Hintergrund erweist sich die Ziff. 1.2 der Klausel nicht als Abweichung, sondern eher als **Bestätigung der Adäquanztheorie**, denn auch nach der Ziff. 1.1 soll sich der Ausschluss bei bloßer Mitwirkung durchsetzen. Dem Klauseltext lässt sich nicht entnehmen, dass der Ausschluss auch dann greifen soll, wenn der die Informationsrechtsverletzung nicht einmal den Test der Adäquanz besteht, also auch dann die Deckung ausschließen wollte, wenn der eingetretene Schaden nicht adäquat kausal auf der Informationsrechtsverletzung beruht (ebenso Klimke in Prölss/Martin AVB Cyber Ziff. A.1–17 Rn. 17; wohl auch Rudowski VersR 2023, 416). Derartige ließe sich auch wohl kaum durch AGB vereinbaren (§ 309 BGB).
- 25 Von der nicht zwingenden (Schwampe RdTW 2020, 85) causa-proxima-Regel weicht Ziff. 1.2 aber ab und bewirkt, dass selbst bei bloßer untergeordneter Mitverursachung der Informationspflichtverletzung (causa remota) die Deckung beseitigt wird. Vgl. die ähnliche Formulierung in Ziff. 36.1 DTV-ADS zu Cyberangriffen (dazu näher Schwampe Seeschiffsversicherung DTV-ADS Ziff. 36 Rn. 11). Die Klausel spricht nicht nur von „verursachen“, sondern auch von „entstehen aus“ und „beitragen zu“. Erforderlich wäre das nicht. Es ist die Folge der Bemühungen, sich international üblichen Formulierungen bei Cyberausschlüssen anzupassen (→ Rn. 7).