



## Editorial

### Insbüro – Aktuell

u.a. zum Richtlinienentwurf der EU-Kommission für die Harmonisierung des Insolvenzrechts

### Jahresrückblick

Wegweisende Entscheidungen mit Bezug zur Insolvenztabelle in 2022 – Teil 1 (S. 58)  
*zusammengestellt und mit Anmerkungen versehen von Monika Deppe*

### Praxisforum

Rechnerische Umsetzung des BGH-Beschlusses vom 22.07.2021 (Az. IX ZB 85/19) / hälftige Feststellungskostenbeiträge als absolute Höchstgrenze gem. § 1 Abs. 2 Nr. 1 Satz 2 InsVV (S. 62)

*von Dipl.-Rechtspflegerin (FH)/Dipl. Kauffrau Conny Prasser, Moritzburg*

Die Geschäftsführerhaftung und die Folgen der Betriebsunterbrechung nach einer Cyberattacke auf ein Unternehmen (S. 64)

*von Reinald Budke-Homburg, Osnabrück*

Influencer, Youtuber & Co. – Einige Praxistipps zur Massegenerierung und Risikovermeidung (S. 66)

*von Rechtsanwalt/Fachanwalt Insolvenz- u. Sanierungsrecht/Insolvenzverwalter Christian Weiß, Köln*

Aufgaben und Rechte des Treuhänders in der Wohlverhaltensphase (Teil 3) (S. 69)

*von Prof. Dr. Gerhard Pape, Richter am BGH a.D.*

### Der praktische Fall

Bußgelder wegen Verstoß gegen Mitteilungspflichten gegenüber dem Transparenzregister im Insolvenzverfahren (S. 73)

*von Rechtsanwalt Dr. Heinrich von Büнау, Frankfurt am Main*

### Fragezeichen

§ 65a SGB V Bonus für gesundheitsbewusstes Verhalten und Insolvenzbeschlagnahme (S. 77)

### Rechtsprechungsreport

Energiepreispauschale nach nunmehr gesetzlicher Regelung unpfändbar (S. 79)

Berichtigung der als Vorsteuer abgezogenen Einfuhrumsatzsteuer bei Insolvenzanfechtung (S. 82)

Zur Aussonderung beim (einfachen) Eigentumsvorbehalt (S. 83)

Umgang mit selbständiger Tätigkeit und gleichzeitigen Renteneinkünften (S. 85)

### Entscheidungen in Kürze

### Literaturreport

u.a. Energiepreispauschale und das Jahressteuergesetz 2022 – Problem der (Un-)Pfändbarkeit gelöst? (S. 91)

### Veranstaltungsvorschau Insbüro

### Zitat des Monats

## Herausgeber:

Insolvenz Sachbearbeiterin  
Michaela Heyn, Ahlen

(Schriftleitung)

Justizrat

Winfried Bausch, Aachen

Dipl.-Rechtspflegerin

Karina Breiling, Dortmund

Dipl.-Finanzwirt/Oberregierungsrat

Holger Busch, Koblenz

Dipl.-Rechtspflegerin

Monika Deppe, Greven

Richter am Insolvenzgericht

Dr. Thorsten Graeber, Potsdam

Professor Dr. Hugo Grote,

Köln/Remagen

Rechtsanwalt Professor

Dr. Hans Haarmeyer, Bonn

Insolvenz Sachbearbeiter

Horst Harms-Lorscheidt,

Düsseldorf

Dipl.-Wirtschaftsjurist (FH)/

Insolvenzverwalter Tobias

Hartwig, MBA, Braunschweig

Rechtsanwalt Kai Henning,

Dortmund

Dipl.-Rechtspfleger Lars Hosbach,

Fulda

Rechtsanwalt/Insolvenzverwalter

Dr. Norbert Küpper, Verl

Rechtsanwalt/Insolvenzverwalter

Cornelius Nickert, Offenburg

Rechtsanwalt/Insolvenzverwalter

Dr. Andreas Ringstmeier, Köln

Richter am Insolvenzgericht

Ulrich Schmerbach, Göttingen

Rechtsanwalt Professor

Dr. Jens M. Schmittmann, Essen

Dipl.-Rechtspflegerin Sylvia

Wipperfürth, LL.M. (Com.), Alsdorf

gegen Mehrprämie Security-Baseline-Checks oder IT-Prozess-Dialoge zur jährlichen Kontrolle der IT-Systeme. Hierbei wird insbesondere auch die Organisation der Unternehmens-IT untersucht und bewertet. Solch ein Report kann eine intern oder extern für die IT verantwortliche Person auch dabei unterstützen, **Fehler in der IT-Struktur aufzudecken**. Beispielhaft können hier nicht durchgeführte Softwareaktualisierungen, kritische offene Ports, veraltete Verschlüsselungseinstellungen beim Mailserver und weitere Schwachstellen identifiziert werden. Die öffentliche Sichtbarkeit der Unternehmens-IT ist auch für fremde Dritte mit diversen

Tools und Einstellungen möglich, die dieses Wissen für gezielte Angriffsszenarien nutzen können.

## 8. Organisatorische Maßnahmen im Unternehmen mindern den Schadensumfang

Für einen guten IT-Sicherheitsstandard bedarf es nicht immer enormer finanzieller Investitionen.

Richtig ist, dass IT-Sicherheit zukünftig stets ein permanent fortdauernder Prozess im Unternehmen sein muss. Hierfür müssen Ressourcen eingeplant und geschaffen werden. Organisatorische Maßnahmen können dabei helfen, einen Cyberschaden einzugrenzen, wie z.B.:

- Risikoanalyse der Unternehmens-IT,
- Erstellung eines umfangreichen Notfallplans,
- tägliche und funktionsüberprüfte Back-Ups aller Datenprogramme und -Systeme,
- Dokumentation aller Vorsorge- und Schutzmaßnahmen.

Erfahrungsberichte zeigen, dass diese organisatorischen Maßnahmen das Unternehmen zwar nicht vor dem Eintritt eines Cyberschadens schützen. Diese **existenzmindernden Präventionstools** sorgen aber dafür, dass der Cyberschaden an sich und seine **Auswirkung in die Betriebsunterbrechung so gering wie möglich** gehalten werden. Das Unternehmen erleidet dann zwar einen Schaden, rutscht jedoch nicht in eine existenzbedrohende Schieflage mit allen finanziellen und rechtlichen Konsequenzen.

## 9. Die guten Cyberversicherungen

Die gute Cyberversicherung hilft dem Unternehmen dabei, einen Cyberschaden möglichst nicht entstehen zu lassen – durch aktives, dialoggesteuertes Risikomanagement. Die Wahl für die richtige Cyberversicherung kann nachweislich dabei helfen, einen Cyberschaden nicht eintreten zu lassen.

Sollte es dennoch zu einer erfolgreichen Cyberattacke mit monetären Folgen für ein Unternehmen kommen, stehen diverse Leistungsbausteine zur Absicherung der finanziellen Folgen zur Verfügung.

Die Geschäftsleitung sollte sich bei der Auswahl des Versicherers **durch den Umfang der Versicherungsleistungen leiten lassen** und auch eher eine höhere als zu niedrige Versicherungssumme wählen. Die Cyberversicherung reguliert auch Drittschäden, also Haftpflichtansprüche, die beispielhaft durch eine Identitätsübernahme verursacht werden können. Ebenso sollte ein umfangreiches Präventionspaket für Mensch, Technik und Organisation inkludierter Bestandteil in der Versicherungsprämie sein oder zumindest angeboten werden bzw. dazu buchbar sein. Betriebswirtschaftlich muss die Prämie berücksichtigt werden. Diese wiederum kann durch einen erhöhten Selbstbehalt gemindert werden.

## 10. Fassen wir zusammen

Die IT-Sicherheit im Unternehmen liegt in der Verantwortung der Geschäftsleitung und des Insolvenzverwalters. Diese sollte auch im Eigeninteresse der Geschäftsleitung liegen, denn Pflichtverletzungen können schnell auch in die persönliche Haftung führen. Cyberkriminalität ist eine reale Gefahr und der richtige Schutz vor Cyberangriffen ist eine Pflicht, die unbedingt eingehalten werden sollte. Zu den Pflichten einer ordnungsgemäßen Geschäftsführung gehört auch die Organisationspflicht und hierunter fällt u.a. auch die Wahl der richtigen Cyberversicherung. Diese sollte nicht ausschließlich unter betriebswirtschaftlichen Aspekten ausgesucht werden, sondern auch danach, welche Möglichkeit diese bietet, einen Cyberschaden erst gar nicht entstehen zu lassen. Einen Schaden nicht eintreten zu lassen, sollte grds. als Ziel durch die Geschäftsleitung formuliert sein.

## Influencer, Youtuber & Co. – Einige Praxistipps zur Massengenerierung und Risikovermeidung

von Rechtsanwalt/Fachanwalt Insolvenz- u- Sanierungsrecht/Insolvenzverwalter Christian Weiß, Köln

*Im Insolvenzverfahren über das Vermögen natürlicher Personen begegnen einem bekanntlich die unterschiedlichsten (gewerblichen/freiberuflichen) Betätigungsfelder. Vom Haupterwerb über den Nebenerwerb bis hin zu Verkäufen über Portale wie eBay, Etsy und ähnlichem.*

*Zu den eher schon klassischen Möglichkeiten, dem Insolvenzverfahren über das Vermögen einer natürlichen Person Masse zuzuführen, gehört die Realisierung von Ansprüchen bspw. eines Dichters gegenüber der VG Wort auf entsprechende Tantiemen durch das Insolvenzverwalterteam. Auch die Verwertung von Domains zu Gunsten der Insolvenzmasse<sup>1</sup> ist nicht mehr so neu.*

<sup>1</sup> Dazu ausführlich bereits Müller/Obermüller/Weiß, Domainverwertung: Ein moderner Weg der Massengenerierung, ZInsO 2012, 780; Lorenz, Die Verwertung von Urheberrechten, gewerblichen Schutzrechten und Domains, InsbÜO 2018, 417 ff.