



Editorial

Insbüro – Aktuell

Jahresrückblick

Wegweisende Entscheidungen zur Insolvenztabelle in 2020 (S. 106)
von *Dipl.-Rechtspflegerin Monika Deppe, Greven*

Praxisforum

Die Änderungen der InsVV ab dem 01.01.2021: Was hat sich geändert, verbessert oder verschlechtert? (S. 110)
von *Richter am Amtsgericht Dr. Thorsten Graeber, Potsdam*

„Im Insolvenzverfahren auf Reisen“: Einige Akronyme und datenschutzrechtliche Anregungen (S. 113)
von *Rechtsanwalt und Insolvenzverwalter Christian Weiß, Köln und dem Datenschutzberater Rolf Ament, Kirchheim*

Zur Auskunftspflicht des Insolvenzverwalters gegenüber den GmbH-Gesellschaftern aus § 51a Abs. 1 GmbHG (S. 115)
von *Stadtrechtsdirektor a. D. Markus Geißler, Freiburg i. Br.*

Insbüro – Dokumentation

Tagungsbericht – 40. Verbraucherinsolvenzveranstaltung: „Online aber praxisnah“ (S. 120)

Der praktische Fall

Gutschrift von Einkommen auf dem P-Konto nach Ablauf der Abtretungsfrist (S. 122)
von *Wirtschaftsjuristin LL.M. Julia Messing, Lüdenscheid*

Fragezeichen

Wirkung des Pfändungsschutzes auf dem P-Konto bei übertragenem Guthaben aus der Zeit vor Insolvenzeröffnung (S. 125)

Rechtsprechungsreport

Prozesskostenhilfe für Insolvenzverwalter (S. 126)

Umfang der Restschuldbefreiung (S. 128)

Entstehung und Begründung eines Rückforderungsanspruches zwecks insolvenzrechtlicher Einordnung (S. 130)

Entscheidungen in Kürze

Gehaltsabrechnung des Monats

Sonderzahlung, PRP-2 und RSU – Die Abrechnung hat es in sich (S. 137)

Literaturreport

Veranstaltungsvorschau Insbüro

Zitat des Monats

Beilagen in diesem Heft

Teil-Synopse zum SanInsFoG

Herausgeber:

Professor Dr. Hugo Grote,
Köln/Remagen

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

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

„Im Insolvenzverfahren auf Reisen“: Einige Akronyme und datenschutzrechtliche Anregungen

von Rechtsanwalt und Insolvenzverwalter Christian Weiß, Köln und dem Datenschutzberater Rolf Ament, Kirchheim¹

Schwerpunkt dieses Beitrages ist weniger die abschließende rechtliche Einordnung des Datenschutzes auf Reisen, sondern vielmehr soll der Beitrag den Lesern² einige datenschutzrechtliche Anregungen³ geben, wenn Sie oder der Insolvenzverwalter – wie so oft – außerhalb der Kanzlei unterwegs sind – sei es zu dem nächsten insolventen Betrieb, sei es z.B. zu einer Fortbildung –, und zwar aus der Praxis der Autoren für die Praxis der Insolvenzsachbearbeitung. Denn es darf nicht vergessen werden: Das datenschutzrechtliche Grundsatzanforderungs des (exkulperierenden) Nachweises, dass die Datenschutzgrundsätze eingehalten wurden – vermutlich denkt man beim „Datenschutz“ zunächst an Digitales, also EDV mit Hard-/Software-Bezug Datensicherheit – beginnt – auch auf Reisen – jedoch bereits im analogen Bereich und betrifft auch das Verhalten der Menschen an sich.

I. Ganz analog: Die Akten im Auto

Natürlich nimmt man für das Erstgespräch in dem insolventen Betrieb auch die Handakte der Kanzlei mit in das Auto. Hier gilt es, bei ganz lapidaren Dingen, wie z.B. dem **Halt an der Tankstelle**, für Datensicherheit Sorge zu tragen. Ein weiteres simples, aber in der Praxis nicht seltenes Beispiel ist, das Dokumente mit personenbezogenen Daten, z.B. eine Gehaltsabrechnung oder ein Kontoauszug, nur lose in der Akte befindlich sind und **beim Verlassen des Autos** unter Mitnahme der Handakte unbemerkt **aus der Akte fallen**. Hier ist also vor Verlassen der Kanzlei/spätestens des Autos dahingehend Sorge zu tragen, dass derartiges nicht geschieht. Sofern Sie im Rahmen oder in Ausführung des Insolvenzmandates personenbezogene Daten mit sich führen, sind diese gegen unbefugte Zugriffe zu schützen – sei es durch „nichtöffentliches Liegenlassen“ im Auto oder noch besser durch einen entsprechenden Koffer/„Käfig“ im Auto und letztlich, indem diese Akten möglichst rasch wieder in die sicheren Kanzleiräume gebracht werden.

Die Anforderungen des Datenschutzes betreffen sowohl das Homeoffice als auch das Auto. Im Homeoffice gibt es einen Mix von Maßnahmen, aus dem jeder bedarfsgerecht das Richtige für seine Organisation auswählen sollte. Datensicherheit durch **abschließbare Schränke** sind ein Muss, damit Akten während der Abwesenheit vor Zugriff und Einsicht Dritter sowie einem evtl. Missbrauch der Daten optimal geschützt sind. Um die DSGVO professionell und präzise umzusetzen, ist die sog. **Clean Desktop Police**⁴ im Homeoffice ebenso essenziell wie am Schreibtisch in der Kanzlei. Wer im Außendienst unterwegs ist, sollte i.S.d. Datenminimierung zudem exakt planen, was unterwegs überhaupt benötigt wird. Je weniger man dabei hat desto weniger kann verloren gehen. Die Organisation des mitgeführten Aktenkoffers ist gleichzeitig ein Extraplus für die Arbeitseffizienz. Wer einen **Mietwagen** für seine Dienstreise nutzt, hat noch eine Besonderheit zu berücksichtigen: Wenn sich dienstliche Smartphones mit der **Freisprecheinrichtung** des Fahrzeuges verbinden, ist der Datenschutz nicht unbedingt gewährleistet: Denn durch die Konnektivität werden Daten im **Medienspeicher** des Mietwagens abgelegt – und verbleiben dort ggf.

auch. Achtung!

II. Handy, Notebook und Co.

Die Mobilität in einer Insolvenzverwalterkanzlei macht die Nutzung von Handys, Notebooks und Co. geradezu unerlässlich. Oftmals wird ein (privates) Handy für beide Belange genutzt; mitunter aber auch zwei Endgeräte. Wie dem auch sei, im Grundsätzlichen gilt: Der Insolvenzverwalter als datenschutzrechtlich Verantwortlicher⁵ sollte optimalerweise in Abstimmung mit der Kanzlei-IT oder/und dem Datenschutzbeauftragten⁶ Vorkehrungen treffen, damit die Verarbeitung personenbezogener Daten auch auf diesen externen Geräten auf einem entsprechenden und aktuellen Schutzniveau erfolgt. Daneben sind auch **datenschutzrechtliche Regelungen** für die Nutzung von Geräten **Bestandteil der technischen und organisatorischen Maßnahmen** (TOM). Dies kann insbesondere der sichere Passwortschutz vor unberechtigtem Zugriff bis hin zu Fernaktivierung/-Löschung bei Verlust von Handy oder Notebook sein. Daneben ist eine Regelung zur App-/Software-Verwendung auf derartigen Geräten denkbar und auch sinnvoll. Im Bereich mobiler Endgeräte gibt es sichere und unterstützende Arbeits-

- 1 Christian Weiß ist Rechtsanwalt/Fachanwalt f. Insolvenzrecht/Insolvenzverwalter und seit geraumer Zeit spezialisiert in der Schnittmenge aus Insolvenz-/Datenschutzrecht tätig. Rolf Ament weist eine Expertise als externer Datenschutzberater auch für Insolvenzkanzleien auf.
- 2 Bitte im Folgenden natürlich immer m/w/d zu verstehen, letztlich auch um allen Beteiligten wenigstens hier die Diskussion um eine „gendergerechte“ Darstellung zu ersparen.
- 3 Zu einem der Klassiker im Insolvenzverfahren mit Datenschutzbezug äußerst lesenswert Reisener, Der datenschutzrechtlich konforme Verkauf von Kundendaten, InsbÜO 2020, 393 (Heft 10/2020).
- 4 Clean Desktop Police = Prinzip des aufgeräumten Schreibtisches.
- 5 Zu den unterschiedlichen Stadien eines Insolvenz-/Sanierungsverfahrens und damit korrespondierenden Unterschieden datenschutzrechtlicher Verantwortlichkeiten vertiefend Weiß/Reisener, Datenschutz in der Insolvenzkanzlei, 2. Aufl., Rn. 498 ff. m.w.N.
- 6 Zur Einbindung des Datenschutzbeauftragten z.B. bei der Datenschutz-Folgeabschätzung nach Art. 35 DSGVO: Ferik, in: Schwartmann/Jaspers/Thüsing/Kugelman, Heidelberger Kommentar DS-GVO/BDSC, 2. Aufl., Art. 35 Rn. 11.

mittel, z.B. in Form von „Containerlösungen“⁷ für Handys und Notebooks. Wertvolle Unterstützung in Sachen Sicherheit kann in diesem Zusammenhang nämlich ein **Mobile Device Management (MDM)** bieten. Es schafft für die mobilen Endgeräte, die im Rahmen der Tätigkeit als Insolvenzverwalter eingesetzt werden, ein **individuell konfigurierbares Sicherheitskonzept**. Mithilfe einer Konsole kann der jeweilige Administrator die Devices zentral einrichten und verwalten. Vorgefertigte Profile können einfach auf neue mobile Endgeräte übertragen werden – der administrative Aufwand lässt sich somit ebenfalls erfreulich reduzieren. Auch Zugriffe der Benutzer können individuell geregelt werden. Das betrifft bspw. die Auswahl der Apps, die dem Benutzer zur Verfügung stehen sollen – oder eben aus Datenschutzgründen auch nicht. Mit einem **professionellen Berechtigungsmanagement** kann diese für die individuellen Anforderungsprofile angepasst werden. Zudem ist es auch möglich, die Geräteeinstellungen – bspw. Kamera, Passwörter, Verschlüsselung und andere datenschutzrelevante Elemente – effektiv einzustellen. Das MDM⁸ ist auch beim Smartphoneverlust – einem Supergau in Sachen Datenschutz – wertvoll: Es ermöglicht das Finden, Sperren und Löschen verlorener Geräte.

III. Exkurs: WhatsApp und andere Messenger-Dienste

Nicht nur seit Inkrafttreten der DSGVO⁹/des BDSG¹⁰ 2018 sind derartige Dienste wie WhatsApp und andere Messenger-Dienste nicht mehr hinwegzudenken – auch aus der beruflichen Praxis. Die **Datenschutzrisiken** sind **immanent und eklatant**,¹¹ aber in den Griff zu bekommen. Beginnen wir mit einigen im Zusammenhang gängiger Akronyme zu den möglichen Besitz- bzw. Eigentums- und Wartungskonstellationen¹² bei Endgeräten wie Handys betreffend, aus deren – nachfolgend nur kurz angerissenen (Gefahren-)Verteilungen – sich natürlich bereits an sich auch Datenschutzrisiken ergeben können:

- **COBO** (corporate owned business only) bedeutet im übertragenen Sinne, dass ein der Kanzlei gehörendes Handy zur Verfügung gestellt wird – und zwar nur für den Geschäftsgebrauch;¹³
- **CYOD** (choose your own device) bedeutet hingegen, dass ein Diensthandy gewählt wird, das der Kanzlei gehört und von ihr gewartet wird, aber auch privat gebraucht werden darf. In die Richtung gehend auch:
- **COPE** (corporate owned personally enabled) bedeutet, dass die Kanzlei das Gerät für den jeweiligen Nutzer erwirbt, der es dann auch privat nutzen darf. Konfiguration und Wartung liegen in der Sphäre der Kanzlei.
- **BYOD** (bring your own device) dürfte datenschutzrechtlich¹⁴ am Heikelsten sein; wird hier doch das Privathandy des Insolvenzverwalters bzw. Insolvenzfachbearbeiters auch für geschäftliche Zwecke verwendet.

Unabhängig von Vorstehendem stellt sich bei der Verwendung von Messenger-Diensten¹⁵ auf Handys jedenfalls immer die Frage der Datenschutzkonformität eben der Verwendung: Aufgrund des Verbotes mit Erlaubnisvorbehalt bedarf bekanntlich jede Verarbeitung personenbezogener Daten der Legitimation. Am Beispiel von WhatsApp für den Zugriff von Facebook auf das Adressbuch des Nutzers¹⁶ sei dies erläutert:

Über Apps, wie z.B. „WhatsBox“¹⁷, lassen sich hier abstellend auf die zuvor kurz erläuterten, hinter den Akronymen liegenden **Nutzungskonzepte** datenschutzkonforme Lösungen und vor allem die erforderliche Nachweisbarkeit möglichst **DSGVO-konformen Verhaltens** in dem Bereich für die Insolvenzverwalterkanzlei – nicht nur auf Reisen – herbeiführen.¹⁸ Die Nutzung eines Handys für die Tätigkeiten als Insolvenzverwalter und der Einsatz von WhatsApp schließen sich nicht aus. Voraussetzung ist dann aber die Nutzung einer modernen Container-Lösung, die bedarfsgerecht und somit maßgeschneidert eingesetzt wird. Bei einer **Container-App** wie beispielweise „SecurePIM“ ist es möglich, dass sämtliche dienstlichen Daten in der zusätzlichen App so abgelegt werden, dass **keine andere App Zugriff** darauf hat. So werden sämtliche Kontakte, Dokumente, Chatnachrichten, eMails etc. in dieser Container-App auf dem Gerät sicher gespeichert. Bei einer möglichen Übertragung werden sie verschlüsselt und sind somit datenschutzkonform. Eine Alternative kann es sein, gleich auf einen anderen Messenger wechseln. Es gibt durchaus Anbieter, die von vornherein die datenschutzrechtlichen Anforderungen erfüllen. Die Versionen für Unternehmen sind kostenpflichtig. Voraussetzung ist es zudem, dass der Kommunikationspartner denselben Messenger nutzt; woran in der Praxis einige Produkte bereits scheitern.

7 Exemplarisch und ohne Aussage zur Qualität und Güte z.B.: Whatsbox der SRT GmbH.

8 MDM = Mobile Device Management.

9 DSGVO = Datenschutzgrundverordnung.

10 BDSG = Bundesdatenschutzgesetz.

11 Dazu bspw. *Jaspers/Schwartzmann/Mühlenbeck*, in: *Schwartzmann/Jaspers/Thüsing/Kugelman*, *Heidelberger Kommentar DS-GVO/BDSG*, 2. Aufl., Art. 9 Rn. 150.

12 Eine anschauliche Übersicht/Gegenüberstellung findet sich z.B. bei <https://www.lanline.de/it-management/byod-cyod-cope-was-steckt-dahinter.10774.html> (22.10.2020).

13 Mithin ein klassisches Diensthandy.

14 Arbeitsrechtliche und sonstige Problematiken sollen hier im Rahmen dieses Beitrages nicht beleuchtet werden.

15 Siehe hierzu z.B. den Überblick <https://www.giga.de/apps/whatsapp-fuer-android/specials/whatsapp-alternativen-7-messenger-ios-android/> (22.10.2020).

16 Das daneben vermutlich vorhandene „Profiling“, die Datenübertragung in die USA, unverschlüsselte backups von Facebook stellen weitere datenschutzrechtliche No-Gos dar, die hier nur der Vollständigkeit halber erwähnt werden.

17 <https://sr-t.it/de/service/whatsbox-de/> (22.10.2020).

18 Ebenfalls der Vollständigkeit halber: Bei WhatsApp Business stellt sich die datenschutzrechtliche Einordnung z.B. aufgrund von Belehrungsmöglichkeiten i.S.v. Art. 13 f. DSGVO, Verträge zur Auftragsverarbeitung grds. „datenschutzkonformer“ dar. Die Verwendung einer „Containerlösung“ sollte von der Insolvenzkanzlei aber auch hier jedenfalls in Erwägung gezogen werden.

IV. Wir reisen mit dem Zug

Statt mit dem Auto zur Fortbildung zu fahren, kann ja auch der Zug genommen werden. Die Zeit kann man wunderbar nutzen – auch zum Arbeiten, z.B. um E-Mails zu empfangen oder zu senden. Die meisten Zuggesellschaften bieten heute kostenloses W-Lan zur Nutzung an. Gerade diese Art der Datenübertragung birgt aber eine Missbrauchsgefahr und auch sonstige Probleme bei der Datensicherheit – insbesondere bei offenen Netzwerken. Der Insolvenzverwalter/-Sachbearbeiter sollte also unbedingt drauf achten, sich **nur** in ein **verschlüsseltes Netzwerk** einzuwählen, das optimalerweise wiederum Sicherheitsmechanismen nach dem aktuellen Stand der Technik vorhält. Vorstehendes gilt sinngemäß für das W-Lan eines Hotels, das wir während der Fortbildung nutzen, um in Pausen oder am Feierabend noch online zu sein. Die Cloud ist dann ggf. die perfekte Option, mit der man **Sicherheitslücken einer „fremden“ WLAN-Verbindung** begegnen kann. Das gilt beim Virenschutz für die mobilen Geräte – bspw. Handy und Tablet –, wenn sich aus dem sicheren Firmen-WLAN ausgeloggt wird. Es ist der Idealfall, wenn in diesem Moment der gesamte Datenverkehr sofort verschlüsselt (VPN) und an eine **Cloud Firewall** umgeleitet wird. Dadurch kann kompetent sichergestellt werden, dass die Kommunikation und das „Surfen“ auch in offenen und unsicheren WLANs sicher bleiben. Ein zusätzlicher Mobile Antivirus unterbindet zusätzlich Zugriffe durch gefährliche Webseiten und Schadcodes. Durch ein eingesetztes MDM¹⁹ lassen sich demnach viele Sicherheitslücken lückenlos und intelligent schließen. Aber auch der **Faktor Mensch** sollte in Datenschutz und Datensicherheit unbedingt integriert werden: Denken Sie bitte auch daran, unterwegs Ihre mobilen Geräte vor der Einsicht neugieriger Platznachbarn zu schützen. Sogenannte **Sichtschutzfolien** arbeiten effizient und unkompliziert. Gerade für Smartphones bieten

Powerfolien nicht nur einen perfekten Sichtschutz, sondern schützen Ihr Smartphone auch vor Glasbruch oder anderen Risiken.

V. Fazit

Vorstehende Ausführungen können und wollen bei weitem nicht abschließend sein, aber den Leser für die Thematik „Im Insolvenzverfahren auf Reisen“ sensibilisieren – vom Corona-Homeoffice²⁰ ganz zu schweigen. Im Bereich der Insolvenzverwaltung sind Datenschutz und Datensicherheit auch außerhalb der Kanzlei ein unerlässliches Thema. Sicherheitslücken können wie skizziert unterschiedlich generiert werden: Durch nicht zugriffsgeschützte Akten, durch die ungesicherte Nutzung von W-LANs, durch den Einsatz von Messenger-Diensten und natürlich durch die Weitergabe von relevanten Daten. Das BDSG und die DSGVO begegnen Verstößen gegen die datenschutzrechtlichen Regelungen mit unangenehmen Sanktionen. Zudem wird die Professionalität in Verruf gebracht, wenn Datenschutzverstöße einer Insolvenzkanzlei bekannt werden, zumal die datenschutzmäßigen Risiken – wie aufgezeigt – in der Praxis weitestgehend unnötig sind. Für **soliden Schutz** gibt es **materielle und digitale Unterstützung**. Experten können wertvolle Dienste leisten, damit nachweislich alles für einen sinnvollen Datenschutz getan wurde.

In dem Sinne viel Spaß und Erfolg bei den nächsten und möglichst datenschutzkonformen Reisen in Insolvenzverfahren!

19 MDM = Mobile Device Management, Quelle: Fa. Securepoint GmbH.

20 Vgl. *Kremer*, in: Schwartmann/Jaspers/Thüsing/Kugelmann, Heidelberger Kommentar DS-GVO/BDSG, 2. Aufl., Art. 24 Rn. 20 mit weiteren Beispielen und Nachweisen.

Zur Auskunftspflicht des Insolvenzverwalters gegenüber den GmbH-Gesellschaftern aus § 51a Abs. 1 GmbHG

von Stadtrechtsdirektor a. D. Markus Geißler, Freiburg i. Br.

Nach § 51a Abs. 1 GmbHG hat der Geschäftsführer den GmbH-Gesellschaftern auf Verlangen Auskunft zu erteilen über sämtliche Angelegenheiten der Gesellschaft. In der Insolvenz der GmbH geht diese Informationspflicht jedoch nicht in ihrer originären Qualität auf den Insolvenzverwalter über. Für das Verständnis der damit einhergehenden Fragen skizziert der folgende Beitrag zunächst den thematischen Gehalt des § 51a Abs. 1 GmbHG mit seinen tatbestandlichen Besonderheiten (II.). Als dann (III., IV.) werden die maßgeblichen Kriterien herausgearbeitet, welche den Auskunftsanspruch der Gesellschafter gegenüber dem Insolvenzverwalter begrenzen. Daran anschließend findet sich der Vorschlag eines Musterschreibens, in welchem der Insolvenzverwalter das Auskunftsersuchen eines Gesellschafters (tlw. abschlägig) beantwortet (V.). Nicht wegen einer besonderen Wichtigkeit, sondern eher der Vollständigkeit halber geht der Beitrag abschließend noch der Frage nach, ob ein zur Auskunft verpflichtender Vollstreckungstitel, den ein Gesellschafter gegen die GmbH bereits erstritten hat, gem. § 727 ZPO gegen den Insolvenzverwalter umgeschrieben werden könnte. Denn dies würde ja ein zweites gerichtliches Streitverfahren (§ 51b GmbHG) gegen einen zur Auskunft nicht bereiten Insolvenzverwalter erübrigen.