Insolvenzverfahren ohne zweckmäßige Datensicherungen sind wie eine Fahrt im „30 Tonner" ohne funktionsfähige Bremsen. Foto: iStockPhoto/captain galaxy

Erfolg, Sicherheit und Transparenz für die Insolvenzverwaltung

Ein Beitrag von THOMAS MÖLLERS

Eine digitale IT-System & Datensicherung ist heute aus **rechtlichen, technischen** und **wirtschaftlichen** Gründen nicht mehr aus Insolvenzen wegzudenken. Insolvenzverfahren ohne zweckmäßige Datensicherungen sind wie eine Fahrt im „30 Tonner" ohne funktionsfähige Bremsen. Das Ergebnis kann dann schnell zu einem schweren „Insolvenzunfall" führen.

Dagegen ist eine Sicherung von Daten ohne die zugehörigen Anwendungen und IT-Systeme ist in etwa so sinnvoll wie der Ritt auf einem toten Pferd. Eine Weisheit der Dakota Indianer sagt dazu: „Wenn du merkst, dass du ein totes Pferd reitest – steige ab!" Daten ohne die zugehörigen Anwendungen und IT-Systeme sind in Insolvenzverfahren praktisch nicht sinnvoll nutzbar!

In der Praxis wird schnell deutlich, dass die üblichen unternehmensinternen Datensicherungen für Insolvenzzwecke meistens völlig unzureichend sind, weil diese die zugehörigen Anwendungen und IT-Systeme nicht mit in die Sicherung einschließen.

Es ist allgemeiner „Common Sense", das größere Mengen an Geld und Gold in einen diebstahlsicheren Tresor gehören. Für die Daten, die gerne als das „neue Geld und Gold des 21. Jahrhundert" bezeichnet werden, gilt das genauso. Insbesondere dann, wenn es sich um größere und für das Insolvenzverfahren relevante Datenbestände handelt, ist eigentlich eine sichere Archivierung in einem zertifizierten Rechenzentrum unumgänglich.

DIE VORTEILE UND DER NUTZEN EINER DIGITALEN DATENSICHERUNG

Datensicherungen sind aus **rechtlicher Perspektive** in Insolvenzverfahren unbedingt erforderlich:

- Einerseits gibt es gerade in der Regelinsolvenz, aber auch in der Eigenverwaltung, gesetzliche Verpflichtungen und das Risiko einer rechtlichen Haftung für die Akteure, wenn sie keine insolvenzgerechten Datensicherungen durchführen.
- Andererseits basieren nahezu alle **rechtlichen Zusammenhänge** im operativen Bereich auf Daten. Jeder Geschäftsvorfall und jeder Vertrag finden sich in irgendeiner Weise und Form in den Daten des insolventen Unternehmens wieder. Für die **Dokumentation** von Sachverhalten sind Daten daher unverzichtbar.
- Daten selbst sind **rechtlicher Bestandteil der Insolvenzmasse.** Jegliche Insolvenzmasse muss gesichert und geschützt werden, daher auch die Daten.
- Daten dienen der Vermehrung von Insolvenzmasse (z.B. durch Anfechtungs- und Haftungsklagen) und sind auch hier als **rechtliche Grundlagen** der Beweise und Indizien unverzichtbar.
- Daten ermöglichen **Rechtfertigungen** und **Exkulpationen.** Auch wenn der BGH kürzlich die Anwendung der sog. „Business Judgement Rule" (BJR) in einer Insolvenz negierte, so ermöglichen doch gerade Daten eine Beurteilung, ob die Gläubigerinteressen bei Entscheidungen des Insolvenzverwalters im Sinne einer **„Insolvency Judgement Rule"** (IJR) eingehalten wurden.

Zwar werden die Rechtsgrundlagen für die Beweiskraft und die Indizienfähigkeit von Daten fortlaufend weiterentwickelt. Aber Daten dienen bereits heute als Grundlage für gerichtsverwertbare Beweise und Indizien und bieten so einen recht sicheren Nachweis vor Gericht.

Dies setzt aber ein ganzheitliches Daten-Management über den gesamten Lebenszyklus voraus – von einer forensischen Erstellung einer Sicherung über die inhaltliche Überprüfung bis hin zu einer langfristig geschützten Archivierung der darin enthaltenen Daten in einer besonders gesicherten Umgebung. Ein solches Verfahren und seine Prozesse müssen ausreichend dokumentiert sein und jederzeit eingehalten werden.

Denn es ist für eine Nutzung der Daten im Insolvenzverfahren die Voraussetzung, dass **revisionssichere** Kopien der betroffenen IT-Systeme und der relevanten Daten erstellt und langfristig archiviert werden. **Revisionssicherheit** bedeutet dabei, dass die IT-Systeme und die Daten:

- dem Verfahren entsprechend ordnungsgemäß gesichert wurden
- in ihrer Verarbeitung im Verfahren entsprechend dokumentiert wurden
- im Zeitpunkt ihrer Sicherung vollständig, richtig und aktuell sind
- vor Veränderung oder Verfälschung geschützt und vor Verlust gesichert sind
- nur durch Berechtigte genutzt werden können
- entsprechend den Aufbewahrungspflichten und der Aufbewahrungsdauer archiviert werden
- jederzeit in ihrer Entstehung und weiteren Verarbeitung und zurück zu ihrer Originalquelle nachvollziehbar und identifizierbar und inhaltlich prüfbar sind.

Auf eine revisionssichere Durchführung der Insolvenz-Datensicherung sollte daher gerade der Insolvenzverwalter im ureigensten Interesse besonderen Wert legen.

Eine digitale IT-System- & Datensicherung lohnt sich aber auch aus **technischen Gründen:**

- Langfristig ist es extrem aufwändig und schwierig, relevante Daten immer wieder neu aus den verfügbaren operativen IT-Systemen und Datenbanken zu extrahieren und in weitere Zielsysteme wie z.B. P_3/P_4 oder DATEV zu exportieren.
- Auch belastet wiederholte Datenextraktion aus den Primärsystemen unnötig die Verfügbarkeit und die Performance der operativen IT-Systeme und des IT-Personals im Insolvenzunternehmen.
- Insolvenzgerechte Datensicherungen führen dazu, dass spätere Änderungen oder Manipulationen der Daten in den operativen Systemen nach der erfolgten Sicherung nicht den Informationsgehalt des Datenbestandes im gesicherten System beeinträchtigen.
- Vor allem Änderungen von Stammdaten führen häufig bei der fehlenden Möglichkeit eine sog. Historisierung und Journalisierung der Daten dazu, dass diese überschrieben werden und somit unwiderruflich verloren gehen.
- Gerade in Situationen, die sog. „Distressed M&A"-Transaktionen erforderlich machen, sind Datensicherungen eine wahre Fundgrube für praktikable Lösungsansätze von schnellen Datenmigrationen in Form von Carve-Outs, Splits oder Merger. Hier können z.B. Prototypen entwickelt und getestet werden, ohne die operativen IT-Systeme und die Organisation zu beeinträchtigen

Last but not least sind es **wirtschaftliche Gründe,** die für eine digitale IT-System- & Datensicherung sprechen:

- Wenn keine insolvenzgerechten Datensicherungen erstellt und in einer separaten geschützten Umgebung archiviert werden, muss ggf. die gesamte bisherige technische IT-Infrastruktur und Umgebung länger als notwendig für den Zugang und den Zugriff auf die Daten genutzt werden.
- Je eher die letzten Insolvenz-Datensicherungen erfolgt sind, desto eher kann die IT-Umgebung des Insolvenzunternehmens aufgelöst und so ein großer Kostenfaktor für das Insolvenzverfahren wirksam für die Insolvenzmasse eliminiert werden.
- Daten dienen als Grundlage für richtige und erfolgreiche Entscheidungen. Erst sie schaffen die notwendige Transparenz und Übersicht. Gleichzeitig können digital gesicherte Unternehmensdaten für Datenanalysen vor wesentlichen Unternehmensentscheidungen und -transaktionen wertvolle Erkenntnisse liefern.
- Unabhängig von einer Rechtsverpflichtung für die Verwendung von Daten für Entscheidungen gibt, lohnt sich die konsequente Datensicherung vor allem für den etwaigen Fall rechtlicher Auseinandersetzungen. Das betrifft gerade diejenigen Daten, die im Zusammenhang mit wichtigen Unternehmensentscheidungen oder -transaktionen stehen.
- Daten selbst können erhebliche Potenziale für die Insolvenzmasse darstellen. Dies können Markt-, Kunden-, Produkt-, Technologiedaten, Intellectual Property, Domains, Know-how oder Rechte in Form von Daten sein. Digitale Datenschätze sind für das Insolvenzunternehmen und Dritte wie Gesellschafter, Wettbewerber, Kunden, Lieferanten und Investoren häufig von einem unschätzbaren Wert. Dieser Sachverhalt wird oft in Insolvenzverfahren unterschätzt.

ZWISCHENFAZIT I

BEGRÜNDUNG: Eine digitale Datensicherung in Insolvenzverfahren ist aus rechtlichen Gründen **notwendig,** aus technischer Perspektive **zweckmäßig** und aus wirtschaftlicher Sicht **sinnvoll.**

RECHTFERTIGUNG: Für die Exkulpation und die Sicherstellung der Revisionsfähigkeit der Arbeit eines Insolvenzverwalters ist die digitale Datensicherung **unverzichtbar.**

UMFANG: Die digitale Datensicherung umfasst notwendigerweise die Sicherung von ganzen **IT-Systemen** zusammen mit den **relevanten Daten** und ihren **Anwendungen.** Eine Sicherung von Daten ohne die zugehörigen Anwendungen und IT-Systeme ist in etwa so sinnvoll wie der Ritt auf einem toten Pferd.

REVISIONSFÄHIGKEIT: Auf eine **revisionssichere** Durchführung der Insolvenz-Datensicherung muss auch der Insolvenzverwalter im ureigensten Interesse besonderen Wert legen. Ansonsten kann es schnell zu einem schweren „Insolvenzunfall" führen.

SICHERHEIT: Daten als das „neue Geld und Gold des 21. Jahrhundert" benötigen einen diebstahlsicheren Tresor – das zertifizierte Rechenzentrum.

DAS VERFAHREN EINER DIGITALEN DATENSICHERUNG IN DER INSOLVENZ

Wie schaut ein Verfahren zur Erstellung einer Digitalen Datensicherung in der Insolvenz aus? Zunächst geht es darum, für eine für Insolvenzzwecke verwendbaren Datensicherung die relevanten Daten zu bestimmen. Der Informatiker spricht vom sog. Scope.

Zu Beginn eines Insolvenzverfahrens ist es meist kaum abzuschätzen, welche Daten und zugehörigen IT-Systeme mit Anwendungen später einmal relevant werden können. Der Jurist spricht hier von einem á priori – á posteriori Problem.

Zu diesem Zweck ist ein **„Numerus Clausus"** von Anwendungen und Handlungsfeldern entwickelt worden, der aus Risikosicht eine gute Abdeckung von Gefährdungen und Vermeidung von zu großen Schadenspotenzialen bietet. Dieser „Numerus Clausus" lässt sich verfahrensspezifisch jederzeit an die Bedürfnisse einer Insolvenz anpassen oder auch erweitern.

Darüber hinaus muss die Sicherheit und Stabilität des **Gesamtverfahrens** zur Datensicherung garantiert, seine Anwendung erlaubt und **ISO 9001 kompatibel** sein. D.h. das Verfahren muss den gesamten Lebenszyklus von Daten umfassen und darf zu keinen prozessualen Lücken oder falsche Reihenfolgen oder Veränderungen oder Verfälschungen von Daten führen.

Die gesicherten Datenbestände müssen jeweils **konsistent** und die gesicherten IT-Systeme untereinander **kohärent** sein. Die Datenqualität muss dabei ermittelt werden. Dafür ist z.B. die IT-Sicherheit nach ISO 27001, ein Qualitäts-Management nach ISO 9001, ein Risiko-Management nach ISO 31000 und ein Projekt-Management nach ISO 21500 notwendig. Ein solches revisionssicheres Verfahren nennt sich **BACKRECVING** und umfasst

- die Bestimmung der relevanten Daten und ihre eigentliche Sicherung (**BACK**UP)
- die notwendige Wiederherstellung (**REC**OVERY) zu Prüfung der Vollständigkeit, Richtigkeit und Wirksamkeit der Sicherung sowie
- die langfristige Archivierung (ARCH**IVING**).

Es sind insbesondere das **ARCHIVING** und das **Projekt-Management,** wo sich heute in der Praxis die „Spreu vom Weizen" trennt. Denn die archivierten IT-Systeme mit den relevanten Daten müssen langzeitig in einer leistungsfähigen IT-Umgebung in einem Rechenzentrum geschützt und speziell gesichert für Auswertungen und Abfragen zeitnah zur Verfügung stehen. Und ohne ein vorschauendes Projekt-Management kann es schnell zu Problemen während der Durchführung und im Ergebnis der Datensicherung können. Die Archivierung muss die IT-Systeme & Daten aus technischer Sicht langzeitfähig und sicher speichern, aus rechtlicher Sicht schützen und aus wirtschaftlicher Perspektive natürlich möglichst kostengünstig betreiben.

Hier helfen sog. Service Level Agreements (SLA), um **risiko- und bedarfsorientiert** die richtigen Leistungs- und Servicemerkmale für die Anforderungen des Insolvenzverfahrens während seines Lebenszyklus wirtschaftlich zu nutzen. So lassen sich z.B. in frühen Phasen eine jederzeitige Online-Nutzung abbilden während in späteren Phasen die IT-Systeme offline eingesetzt werden können. So bleiben die Daten immer angemessen geschützt und belasten gleichzeitig nicht die Insolvenzmasse unnötig.

Die Archivierung muss dabei jederzeit die Bedingungen des Datenschutzes einschließlich der **DSGVO, BDSG und TKG** einhalten sowie den hohen Anforderungen an die Informations- und Datensicherheit entsprechen.

Aktuell genügen nur **ISO/IEC 9001:2015- und ISO/IEC 27001:2013** zertifizierte Rechenzentren diesen Anforderungen und Voraussetzungen des BACKRECIVING.

Ein weiterer Vorteil der Anwendung eines solchen BACKRECIVING Verfahrens und der Nutzung eines solchen ISO/IEC 9001:2015- und ISO/IEC 27001:2013 zertifizierten Rechenzentrums ist: die so gesicherten und archivierten Datenbestände entsprechen den Anforderungen des sog. **EDRM** Rahmenwerks an die Aufbereitung von Daten für das sog. Electronic Discovery, wie z. B. das bekannte eDiscovery Programm **„Relativity"** es voraussetzt.

ZWISCHENFAZIT II

UMFANG: Es ist ein **„Numerus Clausus"** von Anwendungen und Handlungsfeldern für die Ermittlung des Umfangs der Datensicherung entwickelt worden, der aus Risikosicht eine gute Abdeckung von Gefährdungen und Vermeidung von zu großen Schadenspotenzialen bietet. Dieser „Numerus Clausus" lässt sich verfahrensspezifisch jederzeit an die Bedürfnisse einer Insolvenz anpassen und ergänzen.

VERFAHREN: Die Sicherheit und Stabilität des **Gesamtverfahrens** zur Datensicherung müssen garantiert, seine Anwendung erlaubt und **ISO 9001 kompatibel** sein. Die gesicherten Datenbestände müssen jeweils **konsistent** und die gesicherten IT-Systeme untereinander **kohärent** sein. Die Datenqualität muss dabei ermittelt werden. Dafür ist z.B. die IT-Sicherheit nach ISO 27001, ein Qualitäts-Management nach ISO 9001, ein Risiko-Management nach ISO 31000 und ein Projekt-Management nach ISO 21500 notwendig.

LEBENSZYKLUS & PROZESSE: Ein solches revisionssicheres Verfahren über den gesamten Lebenszyklus der relevanten Daten nennt sich **BACKRECVING** und umfasst die Bestimmung der relevanten Daten und ihre eigentliche Sicherung (**BACK**UP), die notwendige Wiederherstellung (**REC**OVERY) zu Prüfung der Vollständigkeit, Richtigkeit und Wirksamkeit der Sicherung sowie die langfristige Archivierung (ARCH**IVING**).

KOMPATIBILITÄT: Erst ein solches **BACKRECVING** Verfahren mit definierten Inhalten und Umfängen sowie designten Prozessen ist **EDRM** konform und **Relativity** kompatibel.

ARCHIVIERUNG & RECHENZENTRUM: Die Archivierung muss jederzeit die Bedingungen des Datenschutzes einschließlich der **DSGVO, BDSG und TKG** einhalten sowie den hohen Anforderungen an die Informations- und Datensicherheit entsprechen. Aktuell genügen nur **ISO/IEC 9001:2015- und ISO/IEC 27001:2013** zertifizierte Rechenzentren diesen Anforderungen und Voraussetzungen des BACKRECIVING.

EMPFEHLUNGEN

Sie sollten eine Datensicherung und ihre Archivierung für Insolvenzzwecke so früh wie möglich beauftragen. Die erste Datensicherung kann bereits in der vorläufigen Insolvenz möglichst unmittelbar nach der Stellung des Insolvenzantrag durch das Unternehmen erfolgen.

Auf eine revisionssichere Durchführung der Insolvenz-Datensicherung sollte gerade Sie als Insolvenzverwalter im ureigensten Interesse besonderen Wert legen.

Lassen Sie dabei komplette IT-Systeme mit zugehörigen Anwendungen und Daten sichern! Die Daten alleine bringen Ihnen meistens keinen Nutzen oder Vorteile.

Bei der Datensicherung sollten sie sicherstellen, dass von Ihrem Dienstleister nur revisionssichere Verfahren wie z.B. das BACKRECIVING verwendet werden.

Denken Sie die Datensicherung vom Ende her. Welche Daten werden für welche Zwecke wie lange noch in welcher Form benötigt? Daher sollten Sie immer grundsätzlich über eine langzeitige Archivierung nachdenken!

Achten Sie darauf, dass die Sicherung und Archivierung der IT-Systeme & Daten auch DSGVO, BDSG, TKG datenschutzkonform ist sowie den hohen Anforderungen an die Daten- und Informationssicherheit gem. ISO 27001 entspricht.

Sie sollten nur ISO 9001 kompatible Verfahren und Dienstleister verwenden, passend zu eigenen Kanzleiorganisation in der Insolvenzverwaltung. Dafür ist auch ein Risiko-Management wie ISO 31000 und ein Projekt-Management wie ISO 21500 durch den Dienstleister notwendig.

Für eine Sicherung und langzeitige Archivierung von IT-Systemen Daten wird ein Projekt-Management auf Seiten der Dienstleister benötigt. Achten Sie darauf, dass der Dienstleister dazu die notwendigen Zertifizierungen im Projekt-Management besitzt.

Verwenden Sie für die Archivierung ausschließlich ISO/IEC 9001:2015- und ISO 27001:2013-zertifizierten Rechenzentren. Die Nutzung nicht-zertifizierter Rechenzentren für die Archivierung selbst kann zu ernsten Problemen führen - sowohl für den Betreiber als auch für Sie als den Auftraggeber.

Der Autor ist Geschäftsführer der INSO Project GmbH (Düsseldorf).