TaylorWessing

Datenschutz im Insolvenzverfahren

Herausforderungen im Laufe des Verfahrens

Im Insolvenzverfahren ist es die Aufgabe des Insolvenzverwalters, für den Schutz personenbezogener Daten zu sorgen. Er ist gemäß Art. 4 Nr. 7 DSGVO datenschutzrechtlich verantwortlich. Das gilt nicht nur, wenn personenbezogene Daten für die Zwecke des Insolvenzverfahrens verarbeitet werden, sondern betrifft alle Verarbeitungsvorgänge im schuldnerischen Unternehmen. Ein „Insolvenzprivileg" kennt das Datenschutzrecht dabei nicht.

Angesichts der Gefahr hoher Bußgelder sollten Insolvenzverwalter die datenschutzrechtlichen Auswirkungen ihrer Tätigkeit in den verschiedenen Phasen des Verfahrens berücksichtigen.

Bei allen genannten Punkten gilt:

Ergriffene Datenschutz-Maßnahmen sind zu dokumentieren (Rechenschaftspflicht), u.a zwecks Nachweis der Einhaltung von Datenschutzvorgaben gegenüber den Aufsichtsbehörden. Bei datenschutz-rechtlich kritischen Punkten – z. B. der Übertragung von personenbezogenen Daten im Rahmen eines Asset Deals – ist es ratsam, dies mit einer dokumentierten Prüfung rechtlich abzusichern.

1 Beginn des Insolvenzverfahrens

Bereits vor Eröffnung des Insolvenzverfahrens beginnt – beim starken Insolvenzverwalter – die datenschutzrechtliche Verantwortlichkeit im Zusammenhang mit der Durchführung der vorbereitenden Maßnahmen. Spätestens jedoch die Übernahme der Verwaltungs- und Verfügungsbefugnis nach § 80 Abs. 1 InsO qualifiziert den Insolvenzverwalter als sog. Verantwortlichen im Sinne der DSGVO. Um das Haftungsrisiko einschätzen zu können, sollten sich Insolvenzverwalter zeitnah einen Überblick über die Verarbeitungstätigkeiten im schuldnerischen Unternehmen verschaffen. Vor allem bei hohen Erfolgsaussichten des Sanierungsverfahrens sollte frühestmöglich für umfassende Datenschutz-Compliance gesorgt werden.

Folgende Schritte sind in jedem Fall anzuraten:

1.1 Quick Check

Um den datenschutzrechtlichen Handlungsbedarf einzuschätzen, sollte zuerst untersucht werden, auf welchem Stand sich die gegenwärtige Datenschutz-Compliance des Unternehmens befindet.

Mehr Informationen zum Umfang der Prüfung finden Sie hier:

DSGVO 2021: Alles nur "Papier-Compliance"?

1.2 Risikoanalyse und Nutzenabwägung

Die gegebenenfalls vielen offenen Pflichten können nicht zeitgleich erfüllt werden. Der Insolvenzverwalter muss daher zunächst diejenigen Risiken ermitteln, die den Geschäftsbetrieb bzw. die Betroffenenrechte am stärksten gefährden und die Gefahr hoher Bußgelder mit sich bringen.

1.3 Umsetzung

Ausgehend von den Ergebnissen der vorigen Schritte und unter Berücksichtigung des mit der jeweiligen Maßnahme verbundenen wirtschaftlichen Aufwands sollten die zu treffenden Maßnahmen priorisiert und umgesetzt werden. Datenschutz-Compliance stellt bei der Veräußerung von Unternehmensteilen ein wertvolles Asset dar: Potentielle Erwerber haben ein Interesse daran, keine datenschutzrechtlichen Haftungsrisiken des insolventen Unternehmens zu übernehmen.

2 Datenverarbeitung für die Zwecke des Insolvenzverfahrens

Im Zuge des Insolvenzverfahrens kann es notwendig sein, Daten des schuldnerischen Unternehmens zu durchsuchen, um Anhaltspunkte für Forderungen der Masse zu finden. Eine Rechtfertigung für die Datenverarbeitung ist erforderlich, wenn der Datensatz personenbezogene Daten enthält. Dafür ist bereits ausreichend, lediglich auf E-Mails zuzugreifen, deren Adresse, Absender oder Inhalte Informationen zu natürlichen Personen enthalten (personenbezogene Daten). Bei der Auswertung sollten folgende Aspekte beachtet werden:

2.1 Grundsatz der Datenminimierung (Erforderlichkeit)

So ein Datenzugriff – neben E-Mails können z.B. Rechnungs-/Lieferantendaten, HR-Stammblätter, IT-Protokolle etc. betroffen sein - darf nur in dem für die Zwecke des Insolvenzverfahrens erforderlichen Umfang erfolgen. Bitte beachten: Sollte der Datensatz private Kommunikation von Mitarbeitern enthalten, muss diese im Voraus aussortiert werden.

2.2 Einbeziehung von Dritten

Es ist möglich, Dritte in die Auswertung einzubeziehen. Rechtsanwälte, Steuerberater und Wirtschaftsprüfer sind aufgrund ihrer berufsrechtlichen Unabhängigkeit selbst datenschutzrechtliche Verantwortliche. Eine Übermittlung an sie bedarf daher einer eigenen datenschutzrechtlichen Rechtfertigung. Unterstützende IT-Dienstleister hingegen werden regelmäßig als sog. Auftragsverarbeiter tätig. Abhängig vom Status des Empfängers unterscheiden sich die weiteren datenschutzrechtlichen Anforderungen an eine Übermittlung.

2.3 Informationspflicht gegenüber Betroffenen

Aus Artt. 13 und 14 DSGVO ergibt sich, dass Betroffene über die Verarbeitung ihrer Daten informiert werden müssen. Das gilt auch, wenn Daten für die Zwecke des Insolvenzverfahrens verarbeitet werden. Nur im Einzelfall können Ausnahmetatbestände einschlägig sein, die die Informationspflicht des Insolvenzverwalters einschränken.

3 Veräußerung von Unternehmensteilen

Abhängig von der Art des Unternehmens können Kundendaten wichtige Assets sein, die Erwerber übernehmen möchten. Die Übertragung solcher Daten bedarf als Datenverarbeitung stets einer Rechtfertigung nach Art. 6 Abs. 1 S. 1 DSGVO. Dabei muss nach Ansicht der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz (DSK)) im Grundsatz zwischen verschiedenen Arten von Kundendaten unterschieden werden:

3.1 Daten von Kunden mit laufender Vertragsbeziehung

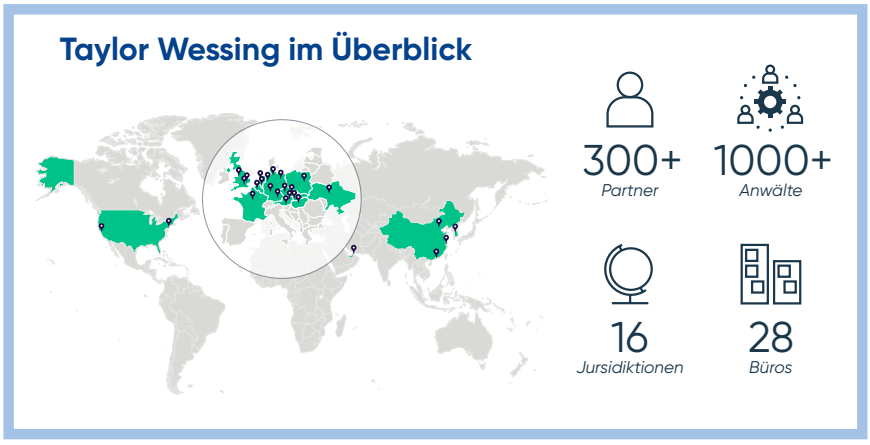
Solche Daten können nach Art. 6 Abs. 1 S. 1 lit. b oder lit. f DSGVO übertragen werden. Für den Übergang des Vertragsverhältnisses selbst ist jeweils eine Zustimmung des Kunden erforderlich. Der DSK zu Folge liegt in der vertragsrechtlichen Zustimmung auch eine „datenschutzrechtliche Zustimmung", welche dann auch die Übermittlung der Daten legitimiert.

3.2 Daten von Kunden mit einer Vertragsbeziehung vor weniger als drei Jahren oder mit einer fortgeschrittenen Vertragsanbahnung

Solche Daten können nach der Ansicht der DSK aufgrund überwiegender Interessen nach Art. 6 Abs. 1 S. 1 lit. f DSGVO übertragen werden. Voraussetzung ist, dass Kunden der Übertragung nicht innerhalb einer zuvor bestimmten Frist widersprechen (sog. Opt-Out-Lösung).

3.3 Daten von Altkunden

Die Daten von Kunden, deren Verträge älter als drei Jahre sind, können nach Ansicht der DSK nur zur Wahrung gesetzlicher Aufbewahrungsfristen übertragen werden. Anderenfalls sind sie zu löschen.



Bei Transaktionen können sich weitere datenschutzrechtliche Fragen stellen. Insbesondere ist zu prüfen, welche personenbezogenen Daten bereits im Rahmen einer Due Dilligence Dritten zugänglich gemacht werden können.

Kontaktieren Sie uns jederzeit gern!

Dr. Axel Frhr. von dem Bussche, LL.M.
Partner, Hamburg
Tel +49 40 36803 129
a.bussche@taylorwessing.com

Dr. Martin Heidrich
Partner, Hamburg
Tel +49 40 36803 133
m.heidrich@taylorwessing.com

Mona Wrobel, LL.M.
Associate, Hamburg
Tel +49 40 36803 164
m.wrobel@taylorwessing.com