Börsen-Zeitung
Zeitung für die Finanzmärkte
Ausgabe 200 vom 17.10.2020, Seite 9

RECHT UND KAPITALMARKT

Daten als Haftungs- und Litigation-Risiko

Auf welche Streitigkeiten sich Unternehmen und Manager jetzt einstellen müssen

Von Martin Strauch und Carolin Marx *)

Börsen-Zeitung, 17.10.2020

Smartes Fahren boomt. Connected Cars sind dabei auf die Fahrzeug- und Nutzungsdaten angewiesen und sammeln wertvolle Daten über Fahrer und Verkehr. Nicht nur in der Automobilbranche entstehen große Datenmengen, längst sind Daten wesentlicher Bestandteil des Geschäfts sowohl im Tech-Bereich als auch in klassischen Industrien. Doch neben neuen Geschäftsfeldern und -chancen öffnen sich für Unternehmen ebenso viele juristische Flanken.

Vielerorts mangelt es noch an Prozessen, die die Haftung im Umgang mit Daten vermeiden und im Fall der Fälle managen. Was sind die riskantesten Fallstricke für Unternehmen und Manager, die zu einer Haftung führen? Mit welchen Strategien kann diesen effizient begegnet werden? Welche Streitgebiete sind besonders risikoträchtig?

Die Datenschutz-Grundverordnung (DS-GVO) erscheint wegen des hohen Bußgeldrahmens vielen Unternehmen als Damoklesschwert. Hinzu kommen Schadensersatzansprüche von Verbrauchern und Regressansprüche von Unternehmen etwa gegen Zulieferer oder (IT-)Dienstleister. Regress kann auch für Bußgelder oder Schadensersatzzahlungen an Verbraucher genommen werden. Manager trifft ein Haftungsrisiko, wenn sie kein ausreichendes Datenschutz-Compliance-System eingeführt haben. Auslöser einer solchen Haftung kann etwa eine unzureichende Aufklärung der Kunden über die Nutzung und Verarbeitung ihrer personenbezogenen Daten sein.

Das Litigation-Risiko aus einer solchen Verletzung mag auf den ersten Blick nicht besonders groß sein. Denn es scheint am Schaden zu fehlen und der Aufwand für die Verfolgung des Anspruchs scheint zu hoch.

Dem begegnet die DS-GVO, indem sie auch „immaterielle Schäden“ ersatzfähig macht. Wie hoch diese bei reinen Datenschutzverletzungen sind, lässt sich nicht pauschal beantworten. Insbesondere deutsche Gerichte verlangen bisher eine konkrete Darlegung der Beeinträchtigung durch den Datenschutzverstoß. Wenn überhaupt wurden bisher drei- und vierstellige Summen pro Verstoß zugesprochen.

Solche kleinen Einzelschäden können schnell ein großes Risiko bedeuten, wenn hunderttausenden oder Millionen Daten von Kunden betroffen sind – etwa bei vernetzten Produkten oder Online-Angeboten. Zudem machen es Verbraucherverbände und spezialisierte Kanzleien den Verbrauchern immer leichter, sich online in sozialen Netzwerken für eine Anspruchsverfolgung zu registrieren. Sie bündeln viele kleine Ansprüche, womit sich die Verfolgung als großer Anspruch lohnt. Daneben soll bald die „EU-Verbandsklage“ auch grenzüberschreitende Klagen durch Verbraucherverbände ermöglichen. Dann könnten Schadensersatzansprüche für Datenschutzverstöße in verschiedenen Mitgliedsstaaten durch ein Produkt oder Internetangebot in einem Verfahren gebündelt werden.

Cyberangriffe

Um diesem Risiko und einer nachgelagerten Haftung von Managern möglichst effizient zu begegnen, sollten Unternehmen nicht nur weiterhin auf eine wirksame Datenschutz-Compliance setzen und ihre entsprechenden Regeln und Prozesse regelmäßig überarbeiten und dokumentieren. Sie sollten auch bereit sein, alle relevanten Informationen für eine Verteidigung gegen Ansprüche insbesondere von Kunden oder Kunden von Kunden vorzubereiten. Bei drohenden Offenlegungspflichten interner Unterlagen sollte auch das Thema „Legal Privilege“ nicht vergessen werden.

Cyberangriffe vereinen die Risiken wegen Datenschutzverstößen mit erheblichen weiteren Schäden etwa durch Betriebsausfälle. Insbesondere bei „Ransomware“-Attaken können erhebliche Schäden entstehen. Dabei werden Daten mit einer Schadsoftware gesperrt oder verschlüsselt und nur gegen eine Lösegeldzahlung wieder freigegeben. Auch hier sind (Massen-)Klagen von Kunden und Verbrauchern denkbar. Auch reine B2B-Klagen sind zu erwarten, insbesondere zum Regress gegen Zulieferer, Dienstleister und das Management.

Insofern brauchen Unternehmen einen guten „Incident-Response-Plan“, der nicht nur technische Maßnahmen, sondern auch die rechtlichen Pflichten, wie zum Beispiel Informations- und Ad-hoc-Pflichten, umfasst. Häufig übersehen wird aber, dass darin auch bereits die Dokumentation zur Abwehr und Geltendmachung von Schadensersatz- und Regressansprüchen vorgesehen sein sollte.

Fahrzeug- und Nutzerdaten eines vernetzten Produkts, beispielsweise eines Autos, haben einen beträchtlichen Wert für die Weiterentwicklung des Produkts und andere Neuentwicklungen. Unternehmen schützen diese teils fast unbemerkt in allgemeinen Geschäftsbedingungen oder Rahmenvereinbarungen.

Litigation-Risiken entstehen etwa, wenn der Fahrzeughersteller die Daten an Zulieferer weitergibt. Es besteht dann kein gesetzlicher Schutz gegen die Benutzung der Daten für die (Weiter-)Entwicklung von Zulieferteilen für andere Hersteller. Deshalb wir dies vertraglich geregelt.

Umfassende Auditierungsrechte und Berichtspflichten erleichtern insofern den Beweis einer Pflichtverletzung im Umgang mit den überlassenen Daten. Außerdem sollte der Zulieferer Prozesse zur Erkennung und Einhaltung des vereinbarten Datennutzungsrahmens implementieren. Je nach Verhandlungsposition können dabei auf beiden Seiten einheitliche Einkaufs- oder Lieferbedingungen zum Umgang mit solchen Daten sehr hilfreich sein.

Kartellrechtliche Fragen

Daten und Datenmengen können den entscheidenden Wettbewerbsvorteil bringen. Doch wo Wettbewerb herrscht – oder herrschen sollte – ist das Kartellrecht nicht weit. Dabei geht es nicht nur um Kartelle, bei denen sich Wettbewerber rechtswidrig miteinander absprechen. Im Kontext von Daten rückt vielmehr der kartellrechtswidrige Missbrauch einer marktbeherrschenden Stellung in den Fokus. In diesem Kontext sind vermehrt zivilrechtliche Auseinandersetzungen zu verzeichnen und weiter zu erwarten. Auch für Manger ergeben sich Risiken einer persönlichen Haftung insbesondere für Kartellbußgelder.

Das bedeutet gleichzeitig, dass Unternehmen und Manager ihren Blick weiten müssen: Die Bußgelder der Kartellbehörden waren mit ihren

teils schwindelerregenden Höhen längst im Risikokatalog von Unternehmen angekommen. Wer mit Daten hantiert, sollte allerdings im Blick behalten, dass finanzielle Risiken oder Chancen auch und gerade in zivilgerichtlichen Streitigkeiten schlummern können. Das kann – je nach Seite im Gerichtssaal – extrem unbequem oder extrem lukrativ sein: Denn in kartellrechtlichen Streitigkeiten gibt es die im deutschen Recht weitgehend einmalige Chance, an Beweisunterlagen und Informationen des Gegners zu gelangen. Die „deutsche Discovery" macht kartellrechtliche Streitigkeiten daher gerade im Kontext von Daten zum scharfen Schwert.

Dass Daten die wettbewerbsrelevante Größe der Stunde sind, meint auch das Bundeswirtschaftsministerium. Zum gerade veröffentlichten Gesetzesentwurf zur Reformierung des deutschen Kartellrechts heißt es:

„Daten haben eine immer stärkere Bedeutung als Wertschöpfungsfaktor. Infolge starker Netzwerkeffekte sowie großer Skalen- und Verbundvorteile lassen sich vor allem in der Plattformökonomie Marktkonzentrations- und Monopolisierungstendenzen beobachten. Dadurch steigt die Marktmacht der Plattformbetreiber, die Nutzerdaten sammeln und auswerten und Anbietern den Zugang zu Kundengruppen erschweren können."

Der Gesetzgeber gibt damit die Richtung vor. Das öffnet Tür und Tor für zivilrechtliche Auseinandersetzungen. Als potenzieller Kläger ist dafür die Sicherung der digitalen Marktgegebenheiten entscheidend. Die Schnelllebigkeit der digitalisierten Welt bedeutet, dass Beweissicherung früher denn je zu beginnen hat. Wer sich hingegen als Inhaber von Daten potenziellen Klagen ausgesetzt sieht, ist ebenfalls gut beraten, die eigenen Entscheidungen früh und genau zu dokumentieren sowie sachliche Gründe für die eigenen Handlungen, Programmierungen und Datenverwaltung zu fixieren.

.....

*) Dr. Martin Strauch ist Counsel und Carolin Marx Senior Associate von Hogan Lovells in München.