Haftung aus Life-Science-Risiken – Teil 2: Vertragsstrafen richtig regeln und rückversichern!

Marcus Hans Rexfort

„… verpflichtet sich der Auftragnehmer, für jeden gesonderten Einzelfall der Zuwiderhandlung, gegen diese Vertraulichkeitsvereinbarung eine Vertragsstrafe an die Gesellschaft zu zahlen. Darüber hinausgehende Schadensersatzansprüche bleiben unberührt.“

Eine Vertragsstrafe steht oftmals gesondert neben dem eigentlichen Vermögensschaden und wird dementsprechend auch separat in Rechnung gestellt. Wichtig bei solchen Vertragsregeln: Ein Versicherer darf nicht daran gehindert werden, seinen „Abwehrschirm“ aufzuspannen, außerdem sollte die Vereinbarung einer Kumulschadenklausel vermieden werden.

Bei einer Datenrechtsverletzung stellt sich weiterhin die Frage nach der Ursache: Wurde beispielsweise eine Cyberattacke ausgeführt, ein Geheimnisverrat oder ein Kommunikationsfehler begangen? Über die Vertragsstrafe und den Vermögensschaden hinaus ergibt sich auch noch ein Reputationsschaden.

Vertraulichkeitsverletzungen – Vertragsstrafen

Vertraulichkeitsverletzungen sind in fast jedem Rahmenvertrag geregelt. Verletzungen der Vertraulichkeit sind gefährlich, weil ein Schadensersatzanspruch entstehen kann, ohne dass tatsächlich ein Vermögensschaden entstanden ist. Sogar existenzgefährdend sind Vertragsklauseln, die kumulierende Strafen nach fortwährender Dauer des Vergehens regeln. Hier wird unterschieden zwischen:

1) dem Vertrauensbruch durch fahrlässiges Verhalten (z. B.: Falscher E-Mail-Adressat),
2) dem Vertrauensbruch mit Vorsatz (z. B.: In geselliger Runde wird zu viel vom Projekt erzählt) und
3) dem Vertrauensbruch durch Wirtschaftskriminalität (Cyberangriff, Datenraub mit Bereicherungsabsicht).

Ein Eigenschaden, der durch fahrlässiges oder mit Vorsatz begangenes Fehlverhalten entstanden ist, kann mit vereinbarten „Sublimit“ in einer Vermögensschadenhaftpflichtdeckung zusätzlich abgesichert werden. Bei diesen in der Wirtschaftskriminalität angesiedelten Delikten wird zwischen *externen* oder *internen Attentätern/Angreifern* unterschieden. Beide Ursachen können durch eine

- Vertrauensschadenversicherung, oder noch besser (zusätzlich) einer
- Cyberpolice abgesichert werden.

Cyber-Risiken/Eigen- und Vermögensschäden

Datenrechtsverletzungen durch Dritte können enorme Schäden bzw. hohe Kosten nach sich ziehen: Etwa durch das Abhandenkommen von Datenträgern, die personenbezogene Daten enthalten.

Entsteht einem Dritten durch die betriebliche Tätigkeit des Versicherungsnehmers (VN) im Rahmen einer Datenrechtsverletzung ein Vermögensschaden und nimmt er diesen dafür in Anspruch, sind folgende Kosten versicherbar: Versicherungsschutz für Vermögensschäden – inklusive eines etwaigen immateriellen Schadens – wegen einer vom Versicherungsnehmer zu verantwortenden Datenrechtsverletzung. Dies gilt auch für alle elektronischen oder nicht elektronischen Störungen wie Phishing oder Social Engineering sowie bei Schäden durch Übertragung von Schadprogrammen.

Untersuchungen durch Regulierungsbehörden sowie Schadensersatzforderungen sind sehr kostspielig. Versichert sind die Kosten für die Verteidigung des VN ohne Deckelung der rechtsanwaltlichen Stundensätze. Übernommen werden auch die Kosten einer forensischen Untersuchung, um genau zu validieren, was vorgefallen ist und wessen Daten in Gefahr waren.

Benötigt der VN Hilfe in der Öffentlichkeitsarbeit und bei der Wiederherstellung seiner Reputation, wird eine darauf spezialisierte Agentur vom Versicherer beauftragt. Fügt ein Hacker den elektronischen Daten des VN Schaden zu oder werden Daten von diesen gestohlen, sind jegliche Kosten für Reparatur, Ersatz oder Wiederherstellung versichert. Wird durch einen Hacker-Angriff der Zugang zu dem Intranet, dem Computersystem, den Programmen des VN oder seinen elektronisch aufbewahrten Daten elektronisch blockiert und dadurch sein

Geschäftsbetrieb unterbrochen, ist ein Ertragsausfallschaden gedeckt.

Der Gesetzgeber hat eine Informationsverpflichtung gem. § 42a Bundesdatenschutzgesetz (BDSG) vorgesehen. Wer feststellt, dass durch einen externen Angriff Dritte Zugriff auf die hausinterne EDV erhalten haben, muss seine Kunden/Patienten umgehend darüber informieren. Diese Informationskosten können sehr teuer werden und sollten deshalb als gesonderte Kostenposition in einer Cyber- oder/und Vertrauensschadenversicherung mit vereinbart und versichert werden.

4- teilige Serie.
Teil 3 in Ausgabe 3/2017 der DZKF
Erscheinungstermin: 28.07.2017

Zum Autor: Marcus H. Rexfort ist Inhaber des Rheinisches Versicherungskontors in Ratingen. Neben der Versicherung von klinischen Studien berät er Auftragsforscher zu deren betrieblichen Risikoabsicherung (www.medizinische-forschung.info).

Website:
www.medizinische-forschung.info

Korrespondenzadresse:
RhVk – Rheinisches Versicherungskontor e. K.,
Josef-Schappe-Str. 21,
40882 Ratingen,
Tel.: + 49 (0) 2102-709077
Fax: 02102-709076,
E-Mail: mail@rhvk.info
Internet: www.rhvk.info

Marcus H. Rexfort