

Industrie 4.0: der rechtliche Schutz von maschinengenerierten Daten

Ein Beitrag von Stefan Hessel

In der Vergangenheit waren die Daten aus Produktionsprozessen eher ein Nebenprodukt mit ungeordnetem wirtschaftlichem Wert. Durch die zunehmende Digitalisierung der Produktionsprozesse im Rahmen der [Industrie 4.0](#) gewinnt die Auswertung von Daten aus den Hard- und Softwareelementen von Maschinen jedoch zunehmend auch wirtschaftlich an Bedeutung. So erlaubt die Analyse der maschinengenerierten Daten einer [Smart Factory](#) beispielsweise die Verbesserung von Produktionsprozessen. Noch interessanter ist die Auswertung maschinengenerierter Daten [über die gesamte Supply Chain](#) oder gar ganze Zweige der Produktion.

Gerade der Handel und Austausch der maschinengenerierten Daten birgt jedoch das hohe Risiko unberechtigter Kenntnisnahme durch Dritte. Das daraus resultierende Schutzinteresse der Unternehmen wirft die Frage nach Schutzmöglichkeiten für die Daten auf. Besonders heikel sind dabei Konstellationen, in denen Unternehmen die Daten – z.B. für die besonders lohnenden unternehmensübergreifenden Analysen – aus ihren eigenen Händen geben. Hier stößt ein Schutz mit technischen Mitteln, etwa durch Verschlüsselung, schnell an seine Grenzen. Nicht viel besser sieht es mit den traditionellen rechtlichen Schutzmöglichkeiten aus. Ein [Eigentumsrecht an Daten besteht nicht](#), Urheberrechte scheitern an der fehlenden persönlich geistigen Schöpfung der Maschinen. Die Daten weisen meist keinen Personenbezug auf, weshalb auch das Datenschutzrecht nicht zur Anwendung kommt.

Dies wäre – unter anderem wegen möglichen [Auskunftsrechten Betroffener](#) – auch wenig wünschenswert. Strafrechtliche Sanktionen setzen in der Regel eine unbefugte Erlangung der Daten voraus, die bei einer ursprünglich „freiwilligen Herausgabe“ fehlt. Durch vertragliche Geheimhaltungsvereinbarungen (z.B. ein NDA) kann zwar ein gewisses Schutzniveau erreicht werden. Das schärfste Schwert der Rechtsordnung, eine strafrechtliche Sanktion, steht in diesem Fall jedoch nicht zur Verfügung. Und auch in einem weiteren Punkt haben Geheimhaltungsvereinbarungen ihre Schwächen: Sie gelten nur zwischen den Parteien, die sie vereinbaren. Verlassen die Daten den Kreis der Vertragspartner und gelangen in die Hände von Dritten, sind diese an die Geheimhaltungsvereinbarung nicht gebunden.

Lösungsmöglichkeiten für die genannten Probleme bietet jedoch das [Geschäftsgeheimnisgesetz \(GeschGehG\)](#). Es ist [vergleichsweise jung und erst am 26.04.2019 in Kraft getreten](#). Inhaltlich regelt das Gesetz die Rechtsfolgen der Erlangung, Nutzung und Offenlegung von Geschäftsgeheimnissen zwischen Privaten. Seine Schutzmechanismen sind anwendbar, sobald ein Geschäftsgeheimnis im Sinne von § 2 Abs. 1 GeschGehG vorliegt. Dies ist der Fall, wenn eine nichtöffentliche Information vorliegt, die von wirtschaftlichem Wert ist und vom rechtmäßigen Inhaber mit angemessenen Maßnahmen zur Geheimhaltung versehen ist. Darüber hinaus muss lediglich ein berechtigtes Interesse an der Geheimhaltung bestehen.

Da eine nichtöffentliche Information nach § 2 Nr. 1 lit. a GeschGehG bereits bei einer Einschränkung der praktischen Zugangsmöglichkeit gegeben sein kann, sind Dreh- und Angelpunkt der Qualifizierung als Geschäftsgeheimnis die angemessenen Maßnahmen zur Geheimhaltung. Diese müssen hinreichend vor unberechtigter Kenntnisnahme schützen, wobei nicht zwingend technische Vorkehrungen erforderlich sind. Auch rechtliche Maßnahmen – etwa die bereits genannten Geheimhaltungsvereinbarungen – können ausreichen. Welche Maßnahmen konkret erforderlich sind, ist durch eine Risikobewertung zu ermitteln.

Aus der Anwendbarkeit des GeschGehG ergeben sich für den Geheimnisinhaber [umfangreiche Rechtsschutzmöglichkeiten](#) – etwa Beseitigungs- und Unterlassungsansprüche sowie Ansprüche auf Schadensersatz. Diese Ansprüche richten sich gegen jeden Rechtsverletzer und im Gegensatz zu Geheimhaltungsvereinbarungen nicht nur gegen Vertragspartner. Wer Geschäftsgeheimnisse verletzt, kann darüber hinaus auch strafrechtlich zur Verantwortung gezogen werden.

Unternehmen kann daher nur nachdrücklich geraten werden, angemessene Schutzmaßnahmen zu etablieren und ein Managementsystem zum Geheimnisschutz einzurichten. Bei richtiger Vorgehensweise bedeutet dies für ein Unternehmen keinen großen Mehraufwand – jedoch einen enormen Nutzen.

Wenn Sie ausführliche Hintergrundinformationen suchen, lesen Sie auch: Hessel/Leffer, [Rechtlicher Schutz maschinengenerierter Daten – Schutz durch das GeschGehG](#), MMR 2020, 647 ff.

[Oktober 2020]



über reuschlaw Legal Consultants

reuschlaw Legal Consultants gehört zu den führenden wirtschaftsberatenden Kanzleien im Produkthaftungsrecht und berät seit 2004 national und international tätige Unternehmen mit Schwerpunkt Produktsicherheitsrecht, Produkthaftungsrecht, Datenschutz & Cybersecurity, Rückrufmanagement, Versicherungsrecht, Compliance Management und Vertragsrecht.

Unternehmenskontakt: Melanie Schaumann | Head of Marketing & Communications | T > +49 30 / 2332895 0 | E melanie.schaumann@reuschlaw.de