PLATTFORM INDUSTRIE 4.0

ERGEBNISPAPIER

Schutz von Geschäftsgeheimnissen im Kontext von Industrie 4.0

Impressum

Herausgeber
Bundesministerium für Wirtschaft und Energie (BMWi)
Öffentlichkeitsarbeit
11019 Berlin
www.bmwi.de

Redaktionelle Verantwortung
Plattform Industrie 4.0
Bülowstraße 78
10783 Berlin

Stand
November 2021

Diese Broschüre wird ausschließlich als Download angeboten.

Gestaltung
PRpetuum GmbH, 80801 München

Bildnachweis
adobe stock
Funtap / S. 10
Irina Shi / S. 21
Jackie Niam / S. 18
Maksim Kabakou / S. 13
sdecoret / S. 5

iStock
Traitov / Titel

Zentraler Bestellservice für Publikationen der Bundesregierung:
E-Mail: publikationen@bundesregierung.de
Telefon: 030 182722721
Bestellfax: 030 18102722721

Inhalt

Einführung

Neue Gefahren – neues Gesetz – neue Herausforderungen

Die Produktionsverfahren und Geschäftsmodelle der Industrie 4.0 leben von der intelligenten Vernetzung produzierender Unternehmen, deren Produktionsanlagen sowie externer Dienstleister, die Dienste der Datenverarbeitung sowie -analyse anbieten. Der stete Austausch von Informationen ermöglicht eine flexible und kundenzentrierte Produktion, ressourcenschonendes Wirtschaften sowie die ständige Weiterentwicklung von bestehenden Technologien zugunsten von Innovation und Wettbewerb.

So ermöglicht z. B. der Fernzugriff auf Produktionsanlagen (sog. „Remote Access") eine örtlich unabhängige Steuerung von Produktionsanlagen und -prozessen. Die Zustandsüberwachung in Echtzeit (sog. „Condition Monitoring") und globale, proaktive Fernwartung (sog. „Predictive Maintenance") von Maschinen verhindern kostenintensive Ausfallzeiten. Die Auswertung von generierten Sensorendatenmassen zur Ermittlung von Produktionsdefiziten mittels Data Analytics Services trägt zur Weiterentwicklung und Verbesserung von Produktionsanlagen und -prozessen bei. Auf Datenaustauschplattformen findet ein unternehmensübergreifender Datenaustausch zwischen unterschiedlichen Akteuren statt, und zwar nicht nur bilateral von einem Hersteller zu einem oder mehreren Betreibern und umgekehrt, sondern auch mit externen Dienstleistern, die als Datenaggregatoren oder Diensteanbieter tätig sind.

Die Vernetzung trägt somit zur Optimierung von Wertschöpfungsprozessen, der Steigerung des Effizienzniveaus und der Entwicklung neuer datenbasierter Geschäftsmodelle bei.

Die Vernetzung von Menschen, Maschinen und Produkten birgt aber auch die Gefahr der unbefugten Erlangung, Offenlegung oder Nutzung von Geschäftsgeheimnissen in sich. Denn Unternehmen gewähren ihren Geschäftspartnern durch den dynamischen Austausch von Daten in Industrie 4.0-Umgebungen gewollt oder ungewollt tiefe Einblicke in ihr technisches Know-how sowie in ihre geschäftliche bzw. operative Tätigkeit. So kann z. B. ein Maschinenhersteller, der einem Maschinenbetreiber gegenüber Fernwartungsdienste erbringt, anhand der ihm übermittelten Zustandsdaten Rückschlüsse auf dessen Auslastung ziehen. Industrie 4.0-Anwendungen und -prozesse bieten darüber hinaus aufgrund von vielen Internet-verbundenen Komponenten, Anlagen, Standorten und Unternehmen große Angriffsflächen für Eingriffe in industrielle Anlagen, sei es durch externe Dritte oder gar eigene Mitarbeiter. Darüber hinaus können aufgrund des hohen Grades der Vernetzung und des Zugriffs auf immer umfangreichere Datenbestände zielgerichtete Cyberangriffe auf Daten und Know-how viel weitreichendere Folgen haben und sukzessive Folgeangriffe vereinfachen. Schließlich wächst mit der zunehmenden Komplexität der IT-Infrastruktur auch die Gefahr von technischem Fehlverhalten und damit des ungewollten Abflusses von Geschäftsgeheimnissen.

Trotz dieser Gefahren scheinen allerdings viele Unternehmen vermehrt auf den Schutz durch formale Schutzrechte wie Patente oder Marken zu verzichten und schützen sensible (d. h. potenziell wettbewerbsrelevante) kaufmännische oder technische Informationen nunmehr als Geschäftsgeheimnisse. Die Gründe für die „Abkehr" von formalen Schutzrechten liegen mehr oder weniger auf der Hand: in einem technologiegetriebenen Wirtschaftsumfeld, in dem Entwicklungen immer schnelllebiger und Innovationszyklen immer kürzer werden, scheuen Unternehmen oft die scheinbar zeit- und kostenintensive Anmeldung, Aufrechterhaltung und Verteidigung klassischer Schutzrechte. Demgegenüber erscheint der Geschäftsgeheimnisschutz relativ kostengünstig, ist zeitlich unbegrenzt und umfasst grundsätzlich auch kaufmännische Informationen.

Sowohl der europäische als auch der deutsche Gesetzgeber haben die steigende Bedeutung des Geheimnisschutzes für die Innovationsfähigkeit von Unternehmen erkannt und mit neuen gesetzlichen Regelungen darauf reagiert. Der europäische Gesetzgeber hat die Richtlinie (EU) 2016/943 vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsgeheimnisse vor rechtswidrigem Erwerb sowie rechtwidriger Nutzung und Offenlegung (Geschäftsgeheimnis-RL) erlassen, um den Geheimnisschutz innerhalb des europäischen Wirtschaftsraums zu harmonisieren. Der deutsche Gesetzgeber hat mit Erlass des Gesetzes zum Schutz von Geschäftsgeheimnissen (GeschGehG) Ende April 2019 die Geschäftsgeheimnis-RL weitestgehend wortlautgetreu umgesetzt.

Das GeschGehG enthält einige aus deutscher Sicht bemerkenswerte Neuerungen.[1] Besondere Bedeutung für Unternehmen hat die neue Definition des Geschäftsgeheimnisses, wonach eine Information (1) weder allgemein bekannt

1 Vgl. zu den prozessualen Regelungen der „Geschäftsgeheimnisstreitsache" §§ 15 ff. GeschGehG sowie zum – im deutschen Recht untypischen – Anspruchsausschluss bei Unverhältnismäßigkeit § 9 GeschGehG.

noch ohne Weiteres zugänglich, (2) daher von wirtschaftlichem Wert und (3) Gegenstand angemessener Geheimhaltungsmaßnahmen gewesen sein muss, um als Geschäftsgeheimnis qualifiziert werden zu können.

Auf den ersten Blick scheint die neue Definition kaum Raum für Geschäftsgeheimnisse in Industrie 4.0-Umgebungen zu lassen. Die Vernetzung von Akteuren und der dynamische Austausch von (Echtzeit-)Daten scheinen eher für die Offenkundigkeit von Informationen als deren Geheimnischarakter zu sprechen. Es stellt sich auch die Frage, wie angemessene Geheimhaltungsmaßnahmen in einer Umgebung realisiert werden sollen, die der steten Generierung und des (unternehmensübergreifenden) Austauschs von Daten bedarf.

Der europäische bzw. deutsche Gesetzgeber wollten durch die neuen Regelungen gerade die Innovations- und Wettbewerbsfähigkeit kleiner und mittlerer Unternehmen (KMU), und zwar auch im Umfeld von Industrie 4.0, stärken.[2] Die neuen gesetzlichen Regelungen dienen also gerade nicht der Beschränkung, sondern der Stärkung von Unternehmen. Industriedaten sollten daher auch künftig unter den geltenden Voraussetzungen einem effektiven Geschäftsgeheimnisschutz zugänglich sein und nicht zum Gegenstand neuer Offenlegungspflichten gemacht werden.

Unternehmen müssen daher die neuen gesetzlichen Anforderungen an Unternehmen mit der Notwendigkeit der Vernetzung und des dynamischen Datenaustauschs in Einklang bringen. Es ist eine Balance zu schaffen zwischen der Einrichtung notwendiger Schutzmaßnahmen einerseits sowie der Wahrung ihrer Praktikabilität und Handhabbarkeit im Rahmen von Industrie 4.0-Anwendungen andererseits.

Die in diesem Ergebnispapier dargestellten Handlungsmöglichkeiten sollen Orientierung für einen souveränen Umgang von Unternehmen mit den Regelungen des GeschGehG im Kontext von Industrie 4.0 geben. Eine gefestigte Rechtsprechung zum neuen GeschGehG existiert zwar noch nicht. Allerdings sollten die Akteure der Industrie 4.0 bereits ersichtliche Gestaltungsspielräume nutzen.

2 Vgl. u.a. Erwägungsgründe (2) und (3) der Geschäftsgeheimnis-RL sowie BT-Drs. 19/4724, S. 21.

Daten und Informationen als „Geschäftsgeheimnisse“

Von der Vernetzung zur Offenkundigkeit

A: Steckbrief

Worum geht es:

Ein Geschäftsgeheimnis ist eine Information, die geheim oder nicht ohne Weiteres zugänglich ist (§ 2 Nr. 1 GeschGehG). Demgegenüber sollen typische Industrie 4.0-Anwendungen wie Remote Access, Condition Monitoring, die Nutzung von Datenaustauschplattformen oder externen Cloud-Diensten im Rahmen vernetzter Produktionsprozesse den zeitlich und räumlich unabhängigen Zugriff unterschiedlichster Akteure auf (Echtzeit-) Zustands- und/oder Nutzungsdaten von Maschinen oder Produktionsprozessen gewährleisten. Dieser Zugriff einer Vielzahl an Akteuren auf Informationen innerhalb bi- oder multilateraler Geschäftsbeziehungen erschwert die Qualifikation sensibler Informationen als Geschäftsgeheimnisse. Denn mit jedem weiteren Geschäftspartner oder externen Dienstleister wächst der Kreis der Personen, die Zugriff auf die generierten oder genutzten Informationen haben, und damit die Gefahr, dass eine Information offenkundig bzw. ohne Weiteres zugänglich wird. Unsicherheiten darüber, wie hoch die Anforderungen an die Zugänglichkeit einer Information sein müssen, könnten zu einem „Wettrüsten“ an Sicherheitsmechanismen und damit einer Behinderung des freien Datenflusses zwischen den beteiligten Akteuren führen.

Sich ergebende Fragen:

- Wann ist eine Information „geheim“?
- Wann ist eine Information „nicht ohne Weiteres zugänglich“?

B: Juristische Einschätzung

Bereits nach bisheriger Rechtsprechung des BGH durfte eine Information nicht „allgemein bekannt“ oder „leicht zugänglich“ sein, um überhaupt als Geschäftsgeheimnis qualifiziert werden zu können.[3] Unterschiede bei der Wortwahl des GeschGehG im Vergleich zur Definition des BGH sind lediglich der Vorgabe durch die Geschäftsgeheimnis-RL geschuldet; ein Bruch mit den bisher entwickelten Grundsätzen der Rechtsprechung zum Geheimnischarakter einer Information war vom Gesetzgeber nicht beabsichtigt.[4] Sie dienen daher für das neue GeschGehG als Orientierung.

1. Faktischer Bekanntheitsgrad ist Maßstab

Ob eine Information geheim oder nicht ohne Weiteres zugänglich ist, bestimmt sich grundsätzlich nach dem faktischen Bekanntheitsgrad der Information. Ist eine Information erst einmal allgemein bekannt bzw. ohne Weiteres zugänglich geworden, hat sie ihre Geheimnisqualität unwiderbringlich (!) verloren. Ob das Geheimnis unter Verstoß gegen Geheimhaltungspflichten preisgegeben wurde, ist für den Verlust der Geheimnisqualität irrelevant. Der Verstoß spielt nur für die Frage nach daraus resultierenden Ansprüchen des ursprünglichen Geheimnisinhabers auf Unterlassung, Auskunft und Schadensersatz eine Rolle.

2. Bisherige Grundsätze

Eine Information ist geheim, wenn sie nur einem eng begrenzten, im Wesentlichen geschlossenen Personenkreis zugänglich ist. Es kommt für den Verlust der Geheimnisqualität maßgeblich darauf an, ob der Geheimnisinhaber die Kontrolle über den Kreis der informierten Personen verloren hat. Die Kontrolle kann auch durch vertragliche Regelungen sichergestellt werden, sofern diese faktisch durch die Vertragspartner auch gelebt werden und sie nicht bloße „Hülse“ sind. So beseitigt z. B. die Nutzung datenbasierter Servicedienste (wie Condition-Monitoring) grundsätzlich nicht den Geheimnischarakter der ausgetauschten bzw. abgerufenen sensiblen Informationen, solange die

3 Vgl. zu den folgenden Ausführungen Köhler in: Köhler/Bornkamm/Feddersen, UWG, § 17 Rn. 6 ff. m.w.N.

4 Vgl. BT-Drs. 19/4724 S. 24.

betreffenden Informationen lediglich zwischen Maschinenbetreiber, -hersteller und ggf. externem Service-Dienstleister ausgetauscht werden. Gleiches gilt für die Einspeisung von Daten in und die Nutzung von Daten aus der Verwaltungsschale: Wenn auch Informationen in der Verwaltungsschale zwischen allen Partnern der Wertschöpfungskette ausgetauscht werden können (z. B. Lieferanten, Entwicklungspartnern, Systemintegratoren, Betreibern und Servicepartnern), so sind die ausgetauschten sensiblen Daten geheim, soweit sich der Kreis der zugriffsberechtigten Personen auf ebendiese Partner beschränkt.

Eine Information ist daher jedenfalls nach Veröffentlichungen im Rahmen von Schutzrechtsanmeldungen wie Patenten, Gebrauchsmustern oder Designs[5] offenkundig geworden; ein rechtlicher Schutz auf Grundlage des GeschGehG scheidet ab der Veröffentlichung aus.

Als ohne Weiteres zugänglich gilt eine Information, wenn sie ohne größeren Zeit- oder Kostenaufwand erlangt werden kann. Maßgeblich sind dafür stets die konkreten Umstände des Einzelfalls. Die bisherige Rechtsprechung hat allerdings Fallgruppen entwickelt, die in der Regel indizieren, dass eine Information (nicht) leicht bzw. ohne Weiteres zugänglich ist:

- Hat ein Geheimnisinhaber gar keine oder offenkundig unzureichende Schutzmaßnahmen getroffen, kann die Information bereits als offenkundig betrachtet werden; darauf, ob getroffene Geheimhaltungsmaßnahmen unzureichend waren, kommt es nicht mehr an. So beseitigt z. B. fehlender Passwortschutz oder die beliebige Weitergabe von Passwörtern wohl bereits den Geheimnischarakter gespeicherter Informationen.

- Der zeitlich bzw. örtlich unabhängige Zugang mehrerer Akteure zu sensiblen Informationen beseitigt in der Regel nicht ihren Geheimnischarakter. Denn im Rahmen von Industrie 4.0-Kooperationen hat (bislang) jeweils nur ein eng begrenzter, über Vertragsbedingungen zugelassener und im Wesentlichen geschlossener Personenkreis Zugriff auf die maßgeblichen Informationen bzw. Daten – und nicht etwa jedermann. Damit ist z. B. die Nutzung von Remote Access Services mittels Smartphone, Tablet oder PC ist aus Sicht des Geheimnisschutzes grundsätzlich unbedenklich. Gleiches gilt für den Zugriff auf die in der Verwaltungsschale eines Assets enthaltenen Daten und Metadaten.

- Die Kenntnis von Betriebsangehörigen des Geheimnisinhabers schadet der Qualifikation einer Information als Geschäftsgeheimnis grundsätzlich nicht, denn Arbeitnehmer unterliegen gegenüber ihrem Arbeitgeber zumindest nebenvertraglichen Geheimhaltungspflichten.

- Ebenso unschädlich ist die kontrollierte (!) Offenlegung gegenüber externen Dienstleistern oder sonstigen Geschäftspartnern wie Kunden oder Lieferanten.

- Erst, wenn rechtliche oder faktische Kontrollmechanismen gar nicht existieren oder funktionslos sind, ist die Information ohne Weiteres zugänglich geworden.

C: Handlungsoptionen und Handlungsempfehlungen

Unternehmen, die neue Geschäftsmodelle und/oder Technologien im Kontext von Industrie 4.0 entwickeln, sollten zunächst umfassend abwägen, ob sie ihr Know-how mittels klassischer Schutzrechte (z. B. Patente, eingetragene Designs) oder als Geschäftsgeheimnisse schützen wollen. Sie müssen bei dieser Abwägung die Stoßrichtung der verfügbaren Schutzformen berücksichtigen: Während z. B. Patente eine neue technische Lösung und Designrechte die Erscheinungsform eines Produktes schützen, betrifft der Geheimnisschutz die auf der Inhaltsebene sensiblen Informationen. Geheimnisschutz kann beispielsweise sinnvoll sein, wenn diese Informationen nicht durch klassische Schutzrechte schützbar sind, oder wenn eine Verletzung klassischer Schutzrechte durch Dritte nicht nachweisbar ist, weil es sich um nur rein intern verwendete Apparate und Verfahren sowie zugehörige Informationen (z. B. KI-Algorithmen für Data Analytics Services) handelt, deren Anwendung sich im verkauften Produkt oder Service nicht niederschlägt, Darüber hinaus spielen auch die Kosten für die Erlangung klassischer Schutzrechte und andere wirtschaftliche Faktoren eine Rolle bei der Wahl der passenden Schutzstrategie. Während z. B. im Bereich mobiler Telekommunikation Innovationszyklen relativ kurz sind, kann es im Bereich Maschinenbau bei längeren Innovationszyklen wirtschaftlich sinnvoller sein, formale Schutzrechte anzumelden und Geschäftspartnern Nutzungsrechte an den erteilten Patenten, Designs oder Marken zu erteilen. Auch ist zu bedenken, dass im Verletzungsfall die Erfolgsaussichten bei der Durchsetzung klassischer Schutzrechte aufgrund umfangreicherer Rechtsprechung aktuell noch besser

5 Bisher st. Rspr. BGH GRUR 1976, 140 (142).

einschätzbar sind als bei Geschäftsgeheimnissen. Zudem bieten Geschäftsgeheimnisse keinen Schutz vor einer unabhängigen parallelen Erarbeitung und Kommerzialisierung der Informationen durch Dritte. Die Schutzstrategie ist möglichst frühzeitig, bestenfalls noch während der Entwicklungsphase neuer Anwendungen, Services oder Technologien, zu entwickeln, denn nach deren Veröffentlichung im Rahmen einer Schutzrechtsanmeldung scheidet Schutz nach dem GeschGehG jedenfalls aus.

Sofern Unternehmen den Schutz aus dem GeschGehG beanspruchen wollen, müssen sie sowohl durch faktische als auch vertragliche Maßnahmen ihre Kontrolle über den „Mitwisserkreis“ sicherstellen:

- Unternehmen müssen in jedem Fall bereits faktisch die Geheimhaltung sensibler Informationen sicherstellen. Sie müssen den Kreis der Personen und Unternehmen auf das nötige Maß beschränken, die tatsächlich Zugriff auf sensible Informationen haben, (sog. „Need-to-know-Basis“). Das gilt sowohl für etablierte Geschäftspartner als auch für externe Dritte, die punktuell oder zur Erfüllung einzelner datenbasierter Dienstleistungen beauftragt werden.

- Die sichere Identifizierbarkeit der zugriffsberechtigten Personen bzw. Unternehmen ist untrennbar mit der Beschränkung des zugriffsberechtigten Personenkreises verknüpft. Für den sicheren Datenaustausch muss klar sein, dass Sender und Empfänger von Informationen diejenigen sind, für die sie sich ausgeben, und dass sie berechtigt sind, die jeweiligen Informationen zu senden und zu empfangen. Die Zuweisung eindeutiger Netzwerkadressen für Personen, Organisationen und Produktionsmittel ist nunmehr unter anderem mit dem neuen Web-Standard IPv6 möglich.

- Es empfiehlt sich, flankierend zur faktischen Sicherstellung der Kontrolle über den zugriffs- und nutzungsberechtigten Personenkreis den Zugang zu und die Weitergabe von sensiblen Informationen mit Mitarbeitern, Geschäftspartnern oder sonstigen externen Dritten explizit vertraglich zu regeln. Unternehmen sollten hierzu separate Geheimhaltungsvereinbarungen schließen oder zumindest Geheimhaltungsklauseln in Lizenz-, Kooperations- oder Lieferverträge aufnehmen. Geheimnisinhaber sollten insbesondere vertraglich die Weitergabe von sensiblen Informationen an Dritte verbieten. Dazu gehört, den Zugriff und die Nutzung sensibler Informationen auf strikter Need-to-know-Basis vertraglich vorzuschreiben. Beauftragt z. B. ein Geheimnisinhaber einen Dienstleister mit der Analyse von Datensammlungen sollte er vertraglich vereinbaren, dass der Dienstleister die übermittelten Daten lediglich zur Aufbereitung der Analyseberichte und nicht für sonstige, ggf. sogar eigene Zwecke verwendet. Gleiches gilt für die Inanspruchnahme von Remote Access Services oder Condition Monitoring.

- Entsprechende Geheimhaltungsvereinbarungen bzw. -klauseln müssen die betreffenden Informationen so konkret wie möglich bezeichnen. Es muss für die Vertragsparteien deutlich werden, welche Informationen von der Geheimhaltungspflicht erfasst sein sollen. Dabei können die Vertragsparteien auf beispielhafte Aufzählungen zurückgreifen, die Kennzeichnung sensibler Informationen vereinbaren, auf die sich die Geheimhaltungspflicht beziehen soll, oder aber sensible Informationen bestimmter Forschungs- oder Kooperationsbereiche als geheimhaltungspflichtig einstufen.

Der wirtschaftliche Wert von Informationen

A: Steckbrief

Worum geht es:

Um als Geschäftsgeheimnis zu gelten, muss eine Information einen wirtschaftlichen Wert haben. Das GeschGehG gibt keinen Maßstab vor, wie der wirtschaftliche Wert eines potenziellen Geschäftsgeheimnisses zu bestimmen ist. Was für einen Maschinenhersteller eine wertvolle Information darstellen kann, muss nicht zwingend auch für den Maschinenbetreiber wirtschaftlichen Wert haben. Mit jedem zusätzlichen Akteur wird die Frage nach der Werthaltigkeit der jeweils geteilten Information verschärft.

Sich ergebende Fragen:

- Wie bestimmt sich der wirtschaftliche Wert einer Information?

B: Juristische Einschätzung

Nach der Gesetzesbegründung zu § 2 Nr. 1 lit. a GeschGehG hat eine Information einen wirtschaftlichen Wert, wenn ihre Erlangung, Nutzung oder Offenlegung ohne Zustimmung des Inhabers dessen wissenschaftliches oder technisches Potenzial, geschäftliche oder finanzielle Interessen, strategische Position oder Wettbewerbsfähigkeit negativ beeinflussen.[6]

Kurz gesagt: Eine Information verkörpert einen realen oder potenziellen Handelswert, wenn sie für die Geschäftstätigkeit und/oder Wettbewerbsfähigkeit des Geheimnisinhabers von Bedeutung ist.

Dies steht auch in Einklang mit der Natur der Geschäftsgeheimnis-RL sowie des GeschGehG als Lauterkeitsrecht: Der Gesetzgeber hat bewusst auf die Schaffung von Ausschließlichkeitsrechten verzichtet, das GeschGehG bietet nur Schutz gegen bestimmte unlautere Verhaltensweisen. Es kommt also nicht darauf an, ob eine Information objektiv von Wert ist, sondern ob sie für den Geheimnisinhaber wirtschaftlich wertvoll ist und ob die Erlangung, Nutzung oder Offenlegung dieses Geheimnisses unrechtmäßig und damit unlauter erfolgt.

Lediglich belanglose Informationen sind vom Schutz des GeschGehG ausgenommen.

C: Handlungsoptionen und Handlungsempfehlungen

Der Wert einer Information ist nicht statisch festgelegt, sondern hängt von der allgemeinen Marktsituation, der Position des Geheimnisinhabers sowie anderer Marktakteure ab. Diese dynamische Wertentwicklung von Informationen hat Auswirkungen auf die Art und den Umfang der zu ergreifenden Geheimhaltungsmaßnahmen. Wird eine Information im Laufe der Zeit wirtschaftlich wertvoller, so müssen Unternehmen auch mehr Schutzmaßnahmen zur Sicherstellung ihrer Geheimhaltung treffen und vice versa.

Mit der Bewertung einer Information einhergehen muss daher stets auch eine Überprüfung der bestehenden Schutzmaßnahmen auf ihre Angemessenheit hin. Bleiben die bestehenden Schutzmaßnahmen ihrer Art und Qualität nach hinter dem Wert der Information zurück, muss das Schutzkonzept angepasst werden.

Bei der Bestimmung des Werts einer Information sollte das Unternehmen auch stets berücksichtigen, wem gegenüber es eine Information offenbaren möchte bzw. wem gegenüber sie (potenziell ungewollt) offenbart werden könnte. Für einen Komponentenzulieferer von Maschinen trägt die Mitteilung etwaiger Wartungs- und Standzeiten des Maschinenbetreibers nur mittelbar zur Verbesserung der Marktposition bei; er kann Schwächen seiner Komponenten so identifizieren und zukünftig ein besseres Produkt anbieten. Demgegenüber sind die Standzeiten für etwaige direkte Konkurrenten des Maschinenbetreibers unmittelbar marktrelevant und damit wertvoller. Aus diesem Grund sind gegenüber direkten Konkurrenten stärkere Schutzmaßnahmen zu ergreifen als gegenüber dem Komponentenzulieferer, vgl. hierzu das Kapitel „Angemessene Geheimhaltungsmaßnahmen im Kontext von Industrie 4.0“.

6 Vgl. BT-Drs. 382/18, S. 20.

Daten, Metadaten und Geschäftsgeheimnisse

A: Steckbrief

Worum geht es:

Bei der Nutzung von Industrie 4.0-Anwendungen wird eine Vielzahl von Daten und Informationen erzeugt, Geschäftspartnern gegenüber offengelegt und/oder genutzt. Beispielhaft seien Sensorprozessdaten, Fehlerdaten bzw. -diagnosen, Verschleißdaten, Gerätezustände, aber auch Nutzungszeiten, Verbrauchsdaten, die Ausbringung von Maschinen, Rezepturen oder Programmzustände genannt. Bei der Mehrzahl der erzeugten oder genutzten Daten handelt es sich um bloße Datenansammlungen, bei denen dem Einzeldatum mangels Informationsgehalts keine Geheimnisqualität zukommt.

Anders kann es sich allerdings bei Metadaten bzw. Metainformationen verhalten. Metadaten sind strukturierte Daten, die Informationen über die Merkmale anderer Daten enthalten (z. B. Name der Information, physikalische Einheit, Wertebereich, Zeitstempel). Metadaten dienen typischerweise der Strukturierung und Kontextualisierung größerer Datensammlungen. So lassen sich Datensets erstellen, deren Informationsgehalt über das bloße Einzeldatum hinausgeht und von diesem völlig verschieden sein kann. Insbesondere mithilfe der Verwaltungsschale ist es möglich, Metadaten eines Assets, wie z. B. die Energieeffizienz einer Maschine oder dessen Einsatzzeiten, in strukturierter Form als Teilmodelle zu beschreiben und für dessen Zustandsüberwachung in Echtzeit oder gar die Erstellung von Simulationen zu nutzen. Auf die Daten der Verwaltungsschale haben in der Regel alle am Asset während seines Lebenszyklus beteiligten Akteure Zugriff und können somit Erkenntnisse aus den vorhandenen Daten schöpfen. Aber auch bei der Inanspruchnahme von Data Analytics Services werden große Mengen an Maschinendaten strukturiert sowie kontextualisiert und damit erst für den Auftraggeber für die Weiterentwicklung und Verbesserung seiner Produkte und Produktionsprozesse nutzbar gemacht. Da Metadaten bzw. Metainformationen große Datenmengen in Kontext setzen, haben sie in der Regel sogar einen größeren wirtschaftlichen Wert als die dadurch jeweils beschriebenen und kategorisierten Datenmengen selbst.

Demgegenüber sind die Erkenntnismöglichkeiten des einzelnen Akteurs darüber, welche Metadaten durch welchen Akteur auf welche Weise (insbesondere zur Schaffung von weiterführenden Erkenntnissen im Sinne von „Meta-Metadaten“) erlangt, genutzt oder offengelegt werden, beschränkt.

Sich ergebende Fragen:

- Ab wann haben Metadaten selbst und die in den Metadaten enthaltenen Informationen Geheimnisqualität?
- Wie lassen sich Metadaten schützen, die Geschäftsgeheimnisse darstellen oder Rückschlüsse auf Geschäftsgeheimnisse zulassen?

B: Juristische Einschätzung

Für die Einordnung von Metadaten bzw. der in ihnen enthaltenen Informationen als Geschäftsgeheimnisse ist maßgeblich, ob die Metadaten einen schutzfähigen Inhalt und einen konkreten Unternehmensbezug aufweisen.

Nach dem GeschGehG können nur „Informationen“ mit semantischer Bedeutungsebene Geschäftsgeheimnisse sein, nicht bloße Daten, Zeichen oder Symbole.[7] Metadaten müssen somit Kenntnisse über Sachverhalte und/oder Personen darstellen bzw. beinhalten, wie z. B. die Einsatzzeiten einer Maschine.

Darüber hinaus muss ein potenzielles Geschäftsgeheimnis wohl auch weiterhin einen konkreten Unternehmensbezug aufweisen. Nach bisheriger Rechtsprechung des BGH[8] musste die jeweilige Information eine Tatsache sein, die im Zusammenhang mit einem bestimmten Betrieb steht. Das Merkmal des „Unternehmensbezugs“ ist nicht explizit in den neuen Gesetzeswortlaut aufgenommen worden. Der wirtschaftliche Wert einer Information hängt allerdings maßgeblich davon ab, auf welches Unternehmen sich die Information bezieht. Deutsche Gerichte werden daher voraussichtlich am Erfordernis des Unternehmensbezugs weiter festhalten.

7 Vgl. zum Sinngehalt von „Informationen“ Becker in: Gloy/Loschelder/Danckwerts, Wettbewerbsrecht, 5. Auflage 2019, § 63 Rn. 5 ff.

8 Vgl. BGH NJW 2006, 830 (838) m.w.N.

Als Faustregel gilt: Metadaten, die der bloßen Kategorisierung von Datenmengen dienen, sind mangels Bezugs zu einem konkreten Unternehmen in der Regel (!) keine Geschäftsgeheimnisse. Dienen Metadaten allerdings der Kontextualisierung, so weisen sie einen Unternehmensbezug auf und können damit Geschäftsgeheimnisse sein. Die Prüfung beider Fallgruppen auf einen konkreten Unternehmenszug ist im Einzelfall unerlässlich: Nicht jedes Ergebnis der Kontextualisierung von Informationen muss einen konkreten Unternehmensbezug aufweisen und umgekehrt.

Der Veranschaulichung dient folgendes Beispiel: Ein externer Dienstleister, der für einen Maschinenbetreiber Data Analytics Services durchführt, kann (und soll) anhand der ihm überlassenen Maschinendaten Erkenntnisse über die Effizienz des Produktionsverfahrens sammeln und dem Maschinenbetreiber zur Verfügung stellen. Wie effektiv der konkrete Auftraggeber arbeitet ist eine wettbewerbsrelevante Information und in der Regel Ergebnis eines Vergleichs der Maschinendaten mit allgemeinen Marktdaten oder sogar Daten von Wettbewerbern, also das Ergebnis von Kontextualisierung der Maschinendaten. Die Effizienz des Produktionsverfahrens des Auftraggebers kann damit grundsätzlich ein Geschäftsgeheimnis sein. Betrachtet allerdings der externe Dienstleister die Effizienz der Produktionsverfahren mehrerer deutscher Auftraggeber und zieht daraus die Erkenntnis, dass deutsche Maschinenbauer im Vergleich zu US-amerikanischen Unternehmen eine höhere Effizienzrate haben, so ist diese Erkenntnis zwar Ergebnis einer Kontextualisierung von Metadaten, es fehlt dem Ergebnis jedoch der Bezug zu einem konkreten Unternehmen. Diese allgemeine Marktinformation ist als solche also kein Geschäftsgeheimnis, obwohl sie das Ergebnis der Kontextualisierung von Metadaten ist. Lediglich die Tatsache, dass der externe Dienstleister über diese allgemeine Markinformation verfügt, ist dessen Geschäftsgeheimnis, da die Information in konkretem Bezug zum Unternehmen des externen Dienstleisters steht. Ob den Auftraggebern ebenfalls Rechte an diesem Geheimnis zustehen, die die Datengrundlage für die Analysetätigkeit zur Verfügung gestellt haben, ist wiederum Frage der Inhaberschaft nach § 2 Nr. 2 GeschGehG, vgl. hierzu das Kapitel „Angemessene Geheimhaltungsmaßnahmen im Kontext von Industrie 4.0“.

C: Handlungsoptionen und Handlungsempfehlungen

Datennutzer, die nicht Geheimnisinhaber sind, dürfen nach § 3 Abs. 2 GeschGehG ein Geschäftsgeheimnis erlangen, nutzen oder offenlegen, wenn dies durch Rechtsgeschäft gestattet ist. Im Umkehrschluss kann also der Datengeber grundsätzlich auch die Erlangung, Nutzung oder Offenlegung von Geschäftsgeheimnissen durch Vertrag ausschließen. Ein umfassendes Verbot macht allerdings nur in den wenigsten Fällen Sinn. Für Geheimnisinhaber ist es kaum möglich, die Entdeckung und Erlangung von Metainformationen und damit sensibler Erkenntnisse über das eigene Unternehmen durch Geschäftspartner oder externe Dienstleister allumfassend zu antizipieren oder gar auf einer „Need-to-know-Basis“ zu reglementieren. Im Gegenteil: Bei den meisten datenbasierten Services und Produkte soll der freie Datenfluss gerade zur Automatisierung bzw. Verbesserung von Produktionsprozessen beitragen, dem Rohdatengeber kommt es gerade auf die Schaffung und Erlangung von Metadaten durch den Datennutzer an. Beschränkungen des Datenflusses scheitern faktisch schlicht auch am Datenvolumen und beseitigen Effizienzgewinne.

Es bedarf vielmehr ausdrücklicher Regelungen zur Nutzung und Weitergabe erlangter oder ermittelter Metainformationen. Datengeber sollten vertragliche Regelungen treffen, die die Nutzung von aufgrund von Metadaten erlangten Geschäftsgeheimnissen zu Zwecken außerhalb des Vertragszwecks ausschließen oder zumindest unter einen Zustimmungsvorbehalt stellen, sofern es die Verhandlungssituation zulässt und ein Nutzungsverbot bzw. Zustimmungsvorbehalt nicht im Widerspruch zum Vertragszweck steht. Sofern in multilateralen Kooperations- oder Geschäftsverhältnissen unterschiedlichen Akteuren feste Rollen zugeordnet werden, bietet es sich an, ausdrücklich Nutzungszwecke festzulegen. So sollten z. B. Entwickler von Maschinenkomponenten Metadaten wie materialbedingte Wartungsleistungen auch nur zur Verbesserung der von ihnen konkret gelieferten Maschinenkomponente nutzen dürfen. Gleiches gilt für die Weitergabe von sensiblen Metadaten an Subunternehmer oder sonstige Dritte.

Inhaberschaft und rechtmäßige Kontrolle

A: Steckbrief

Worum geht es:

Industrie 4.0-Anwendungen zeichnen sich durch die Vernetzung unterschiedlicher Akteure mit unterschiedlichen Rollen aus, die jeweils Zugriff auf von ihnen selbst oder anderen Akteuren generierte Informationen haben. So wird z. B. die Verwaltungsschale eines Assets angelegt und im Laufe seines Lebenszyklus mit Informationen wie Typ des Assets, Betriebsparameter, Lebensdauer, Nutzungszeiten und -auslastung oder Wartung(szeiten) angereichert. Input liefern dabei nicht nur der Hersteller und der Betreiber des Assets, sondern z. B. auch Lieferanten von Komponenten, Entwicklungspartner, Systemintegratoren oder Servicepartner. Informationen und Metainformationen werden zwischen diesen Akteuren unternehmensübergreifend ausgetauscht und bilden in der Regel die Grundlage für Condition Monitoring, Predictive Maintenance oder andere datenbasierte Dienstleistungen auf Basis von Data Analytics Services zur Weiterentwicklung und Verbesserungen des Assets. Das Unternehmen, das in der Verwaltungsschale hinterlegte Daten nutzen kann, und das Unternehmen, auf das sich die Daten beziehen, sind nicht personenidentisch.

Bei der Nutzung von Data Analytics Services nehmen Unternehmen in der Regel Cloud-Technologien externer Anbieter in Anspruch, um die stetig wachsenden Datenmengen überhaupt verarbeiten, ad-hoc auswerten sowie wieder in die Fertigungsprozesse geben zu können. In derzeit noch begrenzten Anwendungsfällen bedienen sich Kooperationspartner auch Datenaustauschplattformen.

Mit dieser Dezentralisierung der Datenhaltung geht nicht nur eine faktische Erweiterung des Personenkreises einher, der Zugriff auf Geschäftsgeheimnisse hat, sondern auch des Kreises der potenziellen Geheimnisinhaber.

Die Frage nach der Inhaberschaft von Geschäftsgeheimnissen ist zentral für den Schutz nach dem GeschGehG: Denn nur dem Geheimnisinhaber stehen sämtliche Ansprüche aus der Verletzung von Geschäftsgeheimnissen wie Auskunft, Unterlassung und Schadensersatz zu.

Sich ergebende Fragen:

- Wer gilt als Inhaber eines Geschäftsgeheimnisses in einer von Beginn an dezentral angelegten Datenhaltung?

B: Juristische Einschätzung

1. Akteure und Rollen

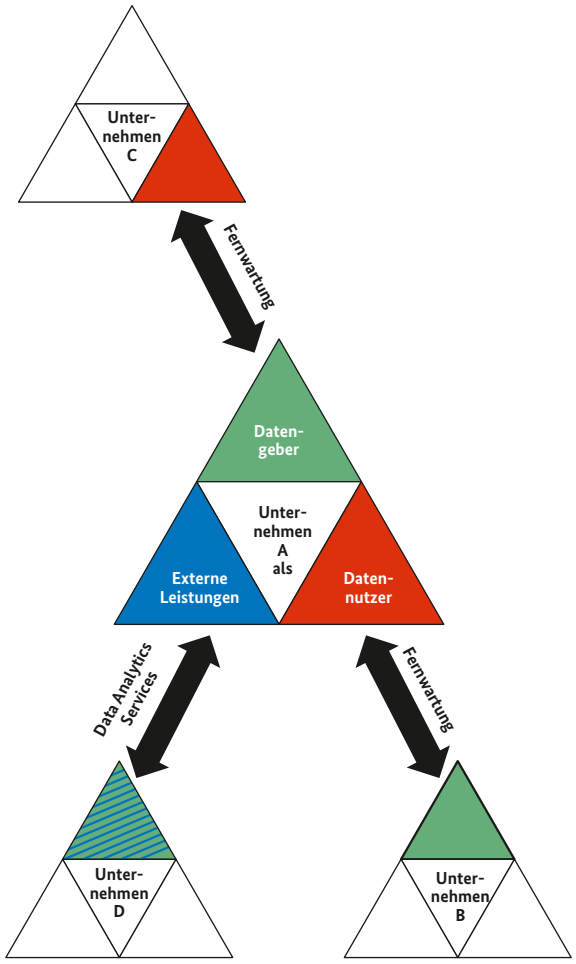
Während des Lebenszyklus eines Assets kann ein Akteur gegenüber den anderen Akteuren im jeweiligen bilateralen Verhältnis unterschiedliche Rollen gleichzeitig ausfüllen.

Erbringt ein Maschinenhersteller Condition Monitoring-Dienste gegenüber einem Maschinenbetreiber, ist er regelmäßig Datennutzer. Denn er verwendet die vom Maschinenbetreiber generierten Rohdaten (Stand-, Ausfall-, Wartungszeiten) als Datengrundlage für seine Dienstleistung. Derselbe Maschinenhersteller ist gegenüber einem Komponentenhersteller aber Datengeber, wenn er Fernwartungsdienste, Data Analytics Services oder sogar Augmented Reality-Anwendungen des Komponentenherstellers in Anspruch nimmt (vgl. Abbildung 1). Je nachdem, welches Geschäftsverhältnis betrachtet wird, ist der Maschinenhersteller Datennutzer oder Datenanbieter.

Ebenso bedienen sich Maschinenhersteller häufig Leistungen durch externe Dritte bei der Entwicklung, Erbringung oder dem Verkauf von datenbasierten Dienstleistungen. So erfordert die Vernetzung sowie Organisation von Produktionsmitteln oft den Zukauf von digitalen Produkt- und Dienstleistungskomponenten auch durch den Maschinenhersteller, z. B. notwendiger IT-Infrastruktur, der Entwicklung individueller Software, externer Speicherplatz etc. Der Auftraggeber ist Datengeber, wenn es dem Auftragnehmer Rohdaten für die Durchführung solcher Data Analytics Services zur Verfügung stellt, aber Datennehmer, wenn es die Analyseergebnisse des Auftragnehmers nutzt.

Um Geschäftsgeheimnisse den beteiligten Akteuren in bi- oder multilateralen Verhältnissen rechtlich zuordnen zu können, muss zwischen den jeweiligen Rollen der Unternehmen im Verhältnis zueinander unterschieden und jedes Rechtsverhältnis gesondert betrachtet werden.

Abbildung 1: Rollen eines Unternehmens im Kontext von Industrie 4.0



Quelle: Plattform Industrie 4.0

2. Grundsätze zur Geheimnisinhaberschaft

Zur Geheimnisinhaberschaft heißt es in § 2 Nr. 2 GeschGehG lediglich:

„Inhaber eines Geschäftsgeheimnisses [ist] jede natürliche oder juristische Person, die die rechtmäßige Kontrolle über ein Geschäftsgeheimnis hat."

Der Gesetzgeber hat – wie bei formalen Schutzrechten – auf eine Zuweisung von Geschäftsgeheimnissen zu deren „Schöpfer" verzichtet. Geheimnisinhaber ist nicht zwangsläufig die natürliche Person, die eine konkrete Information geschaffen hat, z. B. der jeweilige Mitarbeiter eines Cloud-Service-Dienstleisters, der für seinen Arbeitgeber eine Datenanalyse durchführt. Angesichts des Einsatzes von Machine Learning und künstlicher Intelligenz macht eine solche Zuordnung auch wenig Sinn, denn es gibt häufig gar keine natürliche Person, die als Schöpfer in Betracht käme.

Der Gesetzgeber hat allerdings auch auf gesetzliche Regelungen verzichtet, was unter „Kontrolle" und deren „Rechtmäßigkeit" zu verstehen ist. Zu ihrer näheren Bestimmung kann aber auf die zu Art. 39 Abs. 2 TRIPS[9] vorhandenen Grundsätze zurückgegriffen werden, dem der Begriff der „rechtmäßigen Kontrolle" entlehnt ist.

„Kontrolle" meint die tatsächlich ausgeübte Herrschaft über eine Information. Es kommt für die Ausübung von Kontrolle nicht auf etwaige rechtliche Regelungen zur Nutzung, Verwertung oder Schaffung von Informationen an, sondern auf die tatsächlichen Gegebenheiten. Kontrolle über eine Information übt insbesondere aus, wer sie ungehindert an Dritte weitergeben kann.

§ 2 Nr. 2 GeschGehG beschränkt die Ausübung von Kontrolle nicht auf eine einzige Person. Grundsätzlich können mehrere Akteure nebeneinander Kontrolle über eine Information ausüben. Nimmt z. B. ein Unternehmen Data Analytics Services eines anderen Unternehmens in Anspruch und stellt im Zuge dessen dem Serviceunternehmen Rohdaten zur Verfügung, so üben beide Unternehmen die Kontrolle über die Rohdaten aus, denn Datengeber und Datennutzer haben gleichermaßen Zugriff auf die jeweiligen Rohdaten.

9 Art. 39 Abs. 2 TRIPS lautet auszugsweise: „Natürliche und juristische Personen haben die Möglichkeit, zu verhindern, dass Informationen, die rechtmäßig unter ihrer Kontrolle stehen, ohne ihre Zustimmung auf eine Weise, die den anständigen Gepflogenheiten zuwiderläuft, Dritten offenbart, von diesen erworben oder benutzt werden, solange diese Informationen

a) in dem Sinn geheim sind, dass […]"

Der Begriff der „Kontrolle“ setzt auch nicht voraus, dass sie nur von dem Unternehmen ausgeübt werden kann, auf das sich das Geschäftsgeheimnis bezieht. Ein Geschäftsgeheimnis muss zwar inhaltlich einen Unternehmensbezug aufweisen. Das davon erfasste Unternehmen und der Geheimnisinhaber können aber grundsätzlich personenverschieden sein, solange der Geheimnisinhaber nur faktisch Zugriff auf die Information hat.

Weiter muss die Kontrolle über ein Geschäftsgeheimnis rechtmäßig ausgeübt werden. Hier erlangen die Erlaubnistatbestände des § 3 GeschGehG Bedeutung. So darf ein Geschäftsgeheimnis insbesondere erlangt werden durch eigenständige Entdeckung oder Schöpfung, vgl. § 3 Nr. 1 GeschGehG, oder erlangt, genutzt oder offengelegt werden, wenn dies durch Gesetz, aufgrund eines Gesetzes oder durch Rechtsgeschäft gestattet ist. Für die rechtliche Beurteilung der Rechtmäßigkeit kann es keinen Unterschied machen, ob ein Unternehmen ein Geschäftsgeheimnis z. B. im Rahmen oder außerhalb einer F&E-Kooperation erlangt hat, solange in beiden Fällen das Unternehmen eigenständige Forschungsleistungen erbracht hat und somit eine eigenständige Schöpfung gemäß § 3 Nr. 1 GeschGehG vorliegt.[10]

3. Folgen für die (Mit-)Inhaberschaft von Geschäftsgeheimnissen in bi- und multilateralen Kooperationsverhältnissen

Im Verhältnis mehrerer Akteure untereinander gilt daher:

a) Hat ein Datengeber einem Datennutzer Zugang zu Geschäftsgeheimnissen verschafft, bleibt der Datengeber weiterhin Geheimnisinhaber, sofern er weiterhin (auch) die rechtmäßige Kontrolle über die offenbarten Geschäftsgeheimnisse behält. Stellt also ein Maschinenbetreiber sensible Informationen auf einer Datenaustauschplattform zur Verfügung, so verliert er bei ausreichenden Kontrollmöglichkeiten nicht seine Eigenschaft als Geheimnisinhaber.

   Der Anbieter der Datenaustauschplattform tritt in der Regel als weiterer Geheimnisinhaber neben den Datengeber als originärem Geheimnisinhaber, denn er kann faktisch auf die jeweiligen Geschäftsgeheimnisse zugreifen und wird hierzu in der Regel auch vertraglich berechtigt sein, vgl. § 3 Abs. 2 GeschGehG. Gleiches gilt für weitere Nutzer der Datenaustauschplattform, die vertraglich zum Zugriff auf und zur Nutzung von verfügbaren Geschäftsgeheimnissen berechtigt sind.

b) Dieselben Überlegungen finden auch auf Metainformationen Anwendung, die Geschäftsgeheimnisse darstellen oder den Rückschluss auf solche zulassen. Wer (weiter) Kontrolle über solche Metainformationen ausübt, ist Geheimnisinhaber, es sei denn die tatsächliche Herrschaftsbefugnis ist durch Gesetz oder vertragliche Vereinbarungen beschränkt bzw. aufgehoben worden. Die Rechtmäßigkeit der Kontrollausübung kann insbesondere durch eigenständige Entdeckung nach § 3 Abs. 1 Nr. 1 GeschGehG begründet werden, sofern Metadaten durch eigene Strukturierungs- oder Analysebemühungen externer Dritter generiert wurden.

   Der (Roh-)Datengeber selbst ist in der Regel nicht Geheimnisinhaber ohne eine anderslautende vertragliche Vereinbarung. Denn er übt keine tatsächliche Herrschaft über Metadaten aus, die der (Roh-)Datennutzer generiert hat. Erst wenn der (Roh-)Datennutzer dem (Roh-)Datengeber Zugriff auf die von ihm generierten Metadaten gewährt, erlangt der (Roh-)Datengeber darüber die tatsächliche Kontrolle. Demgegenüber hat der Datennutzer regelmäßig unbeschränkten Zugriff auf das Geschäftsgeheimnis und hat es typischerweise durch eigenständige Schöpfung erlangt. Der Datennutzer ist damit primärer Geheimnisinhaber. Dass die Metadaten im Auftrag des Datengebers ermittelt wurden, der letztlich das wirtschaftliche Interesse an den Metainformationen hat, steht einem solchen Ergebnis nicht entgegen; denn das wirtschaftliche Interesse ist nicht Voraussetzung für die Ausübung rechtmäßiger Kontrolle.

   Das Konzept der rechtmäßigen Kontrolle birgt also die Gefahr der Vervielfachung von Anspruchsberechtigten in sich, wenn keine eindeutigen anderslautenden vertraglichen Regelungen getroffen werden. Dies kann zu Problemen bei der Wahrnehmung von Zugriffs- und Verwertungsrechten führen. Denn nach der gesetzlichen Konzeption ist jeder beteiligte Akteur originär aus dem GeschGehG berechtigt und kann daher die Ansprüche aus der Verletzung eines Geschäftsgeheimnisses aus eigenem Recht geltend machen. Es existieren keine ausdrücklichen

10 Diese Annahme wird auch durch die Gesetzesbegründung zum GeschGehG bestätigt, denn der Gesetzgeber ist dort davon ausgegangen, dass auch ein Lizenznehmer neben dem Lizenzgeber als originärem Geheimnisinhaber berechtigt sein kann. Ein derartiger Verweis macht nur Sinn, wenn der Lizenznehmer durch Rechtsgeschäft zum rechtmäßigen Inhaber durch den Lizenzgeber gemacht wurde.

Vorgaben im GeschGehG, wie das Verhältnis von originär Berechtigten untereinander ausgestaltet ist.

Der Rückgriff auf die allgemeinen Regelungen zur Bruchteilsgemeinschaft trägt den Besonderheiten des Schutzregimes für Geschäftsgeheimnisse und den Anforderungen der Industrie 4.0 nicht ausreichend Rechnung. Zwar ist durch das neue GeschGehG der Geheimnisschutz der Systematik des Immaterialgüterschutzes angenähert worden. Der Gesetzgeber hat aber weiterhin bewusst auf die Schaffung absoluter Ausschlussrechte verzichtet. Das GeschGehG gewährt Schutz nur gegen bestimmte unlautere Verhaltensweisen der Geheimniserlangung oder -nutzung. Die Regelungen der Bruchteilsgemeinschaft sind demgegenüber auf absolute Rechte und Vermögenspositionen zugeschnitten. Darüber hinaus erschweren die Vorschriften zur gemeinschaftlichen Verwaltung sowie zur Beschlussfassung eine effektive wirtschaftliche Verwertung von Geschäftsgeheimnissen.

C: Handlungsoptionen und Handlungsempfehlungen

Wie bereits bei der Nutzung von formalen Schutzrechten wie Patent-, Gebrauchsmuster oder Designrechten müssen die beteiligten Akteure vertragliche Regelungen treffen, mit denen die Geschäftsgeheimnisse den Akteuren eindeutig zugeordnet und Regelungen für den Streitfall getroffen werden:

- Nach der bestehenden Gesetzeslage führt die Nutzung datenbasierter Dienstleistungen in den meisten Fällen zu einer Verdoppelung bzw. Vervielfachung der Geheimnisinhaberschaft. Die resultierende Gemengelage bestehender Rechte und deren Verhältnis zueinander entspricht in der Regel nicht dem Interesse der beteiligten Unternehmen. Aus diesem Grund sollten in jedem Fall ausdrückliche Regelungen zur Inhaberschaft an Geschäftsgeheimnissen getroffen werden, insbesondere ob sich die Geheimnisinhaberschaft nach den gesetzlichen Regelungen zur Bruchteilsgemeinschaft gestalten soll oder nicht.

- Sofern die gesetzlichen Regelungen – wie zu empfehlen ist – abbedungen werden, sollten Datengeber auf eine explizite Klarstellung in ihren Verträgen hinwirken, dass sie weiterhin Inhaber aller offenbarten Geschäftsgeheimnisse bleiben, ggf. unter Ausschluss einer etwaigen Inhaberschaft des Datennutzers;

- Hinsichtlich neu generierter bzw. aufgrund oder in Metadaten erlangter und/oder offengelegter Geschäftsgeheimnisse sollten die beteiligten Akteure die Inhaberschaft an Geschäftsgeheimnissen klar einem, mehreren oder allen Akteuren zuordnen. Als Orientierung kann das primäre (!) wirtschaftliche Interesse an den generierten Geschäftsgeheimnissen dienen: Soweit der Rohdatengeber gerade für die Gewinnung bestimmter Metainformationen bezahlt, soll ihm grundsätzlich auch das Verwertungsrecht an diesen Informationen und Erkenntnissen, also die Inhaberschaft zustehen. Im Übrigen ist die Interessenlage im Einzelfall maßgeblich;

- Die Akteure sollten stets im Blick behalten, dass – unabhängig von der Zuweisung der Inhaberschaft als Ganzes – spezielle Regelungen zur Offenlegung, Nutzung und Verwertung von Geschäftsgeheimnissen möglich sind. So kann ein Unternehmen, das Data Analytics Services in Anspruch nimmt und im Zuge dessen Rohdaten zur Verfügung stellt, beispielsweise die Inhaberschaft der Analyseergebnisse beanspruchen, dem Servicedienstleister jedoch das Recht gewähren, die Ergebnisse zur Verbesserung der eigenen Analyseprozesse zu nutzen (nicht jedoch zu sonstigen, marktbezogenen Aktivitäten);

- Sofern Datennutzer und Datengeber gemeinsam Inhaber von Geschäftsgeheimnissen sind, sollten die Akteure dringend Regelungen zum Innenverhältnis treffen und sich nicht auf die Regelungen zur Bruchteilsgemeinschaft verlassen. Die Parteien sollten insbesondere Regelungen zu Nutzungs- und Verwertungsrechten, gemeinsamer Entscheidungsfindung und Abstimmung, sowie zur Rechtsverfolgung im Verletzungs- und Streitfall abschließen.

Angemessene Geheimhaltungsmaßnahmen im Kontext von Industrie 4.0

A: Steckbrief

Worum geht es:

Nach dem neuen GeschGehG ist eine Information nur dann ein Geschäftsgeheimnis, wenn sie Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen ist. Während nach der alten Rechtslage ein subjektiver Geheimhaltungswille ausreichte, muss nun der Geheimnisinhaber objektiv angemessene Maßnahmen zum Schutz seiner sensiblen Informationen getroffen haben, um überhaupt in den Schutzbereich des GeschGehG zu fallen.

Ein Mindeststandard oder sonstige Vorgaben zur Ausgestaltung der Schutzmaßnahme existiert allerdings weder auf deutscher noch auf europäischer Ebene. Auch eine gefestigte deutsche Rechtsprechung hat sich zu dieser Frage bisher noch nicht entwickeln können. Es ist somit den Marktteilnehmern überlassen, angemessene Maßnahmen zu ergreifen.

Um den Schutz des GeschGehG in Anspruch nehmen zu können, müssen angemessene Geheimhaltungsmaßnahmen zum Schutz sensibler Daten getroffen werden, die aber nicht die operative Tätigkeit von Unternehmen im Kontext von Industrie 4.0 unnötig beschränken. Die Besonderheit bei der Erstellung eines angemessenen Schutzkonzeptes im Kontext von Industrie 4.0 besteht darin, der organisations-, länderübergreifenden und vor allem dynamischen Vernetzung von Industrieanlagen und deren Komponenten angemessen Rechnung zu tragen.

Sich ergebende Fragen:

- Wie ist ein Schutzsystem im Kontext von Industrie 4.0 zu gestalten, das den gesetzlichen Anforderungen des GeschGehG genügt?

B: Juristische Einschätzung

Sowohl der europäische als auch der deutsche Gesetzgeber haben keinen Mindeststandard an Schutzmaßnahmen vorgegeben. Allerdings enthalten die Gesetzesmaterialien einige Orientierungspunkte für die Beurteilung angemessener Geheimhaltungsmaßnahmen.

Die Art der erforderlichen Geheimhaltungsmaßnahmen hängt danach grundsätzlich (1) von der Art des Geschäftsgeheimnisses im Einzelnen und (2) den konkreten Umständen der Nutzung ab. Die Maßnahme muss also auf das konkret (!) zu schützende Geschäftsgeheimnis und dessen konkrete Gefahrenlage zugeschnitten sein. In der Fachliteratur wird üblicherweise zwischen Maßnahmen rechtlicher, organisatorischer und technischer Art unterschieden.[11] Erst diese technischen und organisatorischen Maßnahmen stellen regelmäßig den notwendigen Bezug zum „konkreten" Geschäftsgeheimnis her. Dabei müssen die Maßnahmen keineswegs perfekt sein oder den größtmöglichen Schutz für die jeweilige Information darstellen. Das neue Gesetz bezweckt vor allem den Unternehmensschutz und verlangt daher auch nur „den Umständen nach" vernünftige und wirtschaftlich sinnvolle Maßnahmen. Es soll ein angemessenes Verhältnis zwischen dem Wert des Geheimnisses und den Kosten von Schutzmaßnahmen bestehen Das Gesetz verlangt auch keine Schutzmaßnahmen, die die Funktionalität und die Geschäftstätigkeit eines Unternehmens unangemessen beeinträchtigen. Ziel der gesetzlichen Regelung ist, dass Unternehmen ihre Schutzbemühungen auf die für ihre Wettbewerbsfähigkeit wichtigsten Informationen konzentrieren.

Vor diesem Hintergrund müssen Unternehmen also die relevanten Geschäftsgeheimnisse identifizieren und bewerten. Sie müssen die relevanten Gefahren, die dem jeweiligen Geschäftsgeheimnis konkret drohen, identifizieren, um schließlich die dafür angemessenen Geheimhaltungsmaßnahmen zu treffen.

Im Kontext von Industrie 4.0 bestehen neben den üblichen Gefahren durch den fahrlässigen Umgang mit sensiblen Informationen vor allem Bedrohungen für Systeme zur Fertigungs- und Prozessautomatisierung. Industrie 4.0-Anwendungen und Prozesse bieten aufgrund der zahlreichen Internet-verbundenen Komponenten, Anlagen, Standorte und Unternehmen große Angriffsflächen für Eingriffe in

11 Vgl. z.B. Reinfeld, Das neue Gesetz zum Schutz von Geschäftsgeheimnissen, 1. Auflage 2019, § 1 Rn. 152; Hohn-Hein/Barth in Fritzsche/Münker/Stollwerck, BeckOK UWG, 13. Edition 2021, § 2 Rn. 15 ff.

industrielle Anlagen. Zu den potenziellen Gefahren gehören Infektionen mit Schadsoftware über das Internet und Intranet, das Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware, der zielgerichtete Einbruch über Fernwartungszugänge, Kompromittierung von Smartphones im Produktionsumfeld, die Kompromittierung von Extranet und Cloud-Komponenten sowie die unberechtigte Nutzung von Fernwartungszugängen. Zudem können aufgrund des hohen Grades der Vernetzung und des Zugriffs auf immer umfangreichere Datenbestände Angriffe viel weitreichendere Folgen haben und sukzessive Folgeangriffe vereinfachen. Mit der zunehmenden Komplexität der IT-Infrastruktur wächst auch die Gefahr von technischem Fehlverhalten und damit des ungewollten Abflusses von Geschäftsgeheimnissen.

C: Handlungsoptionen und Handlungsempfehlungen

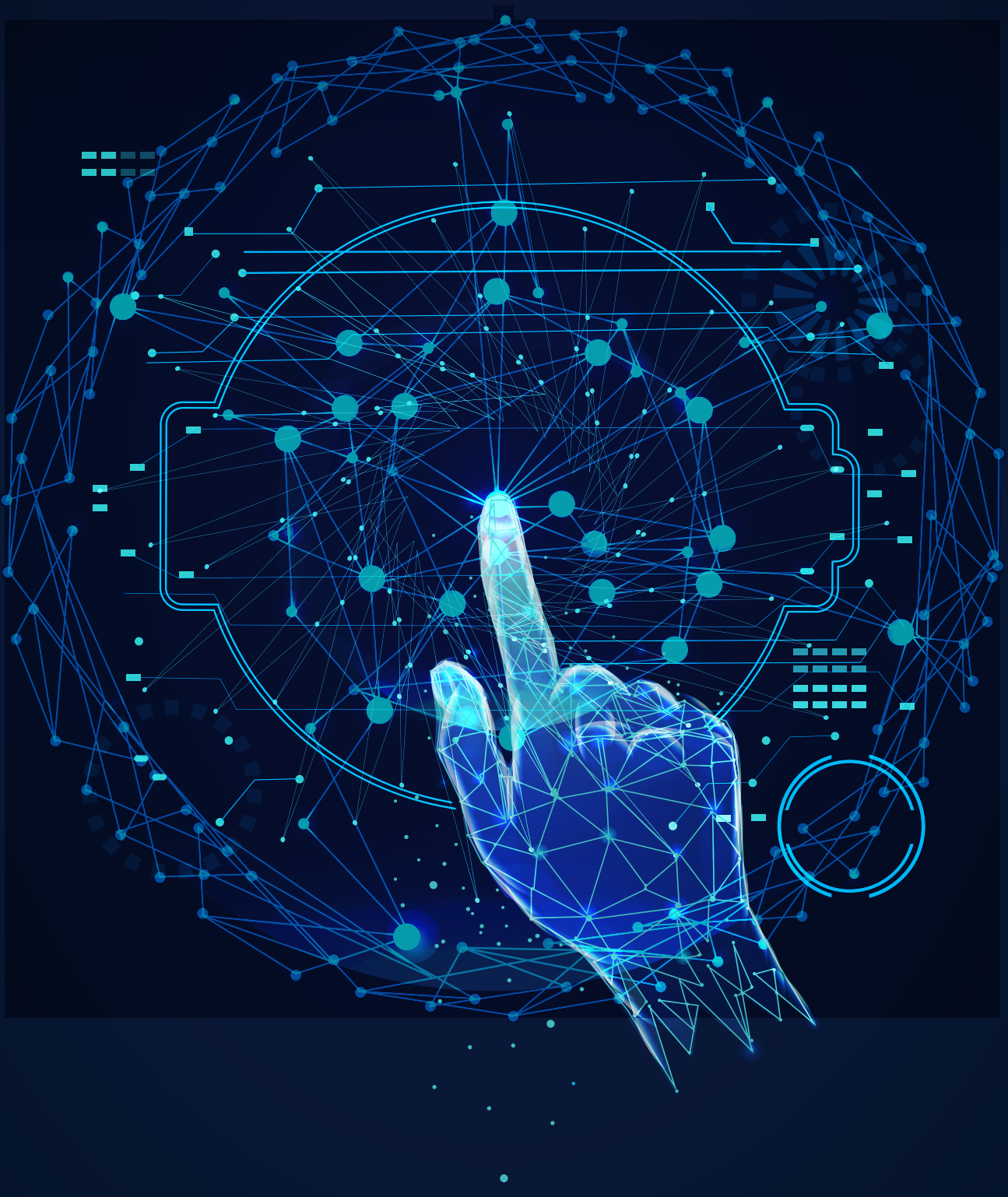
Einen detaillierten Überblick über die im Kontext von Industrie 4.0 relevanten Sicherheitsmaßnahmen geben die Veröffentlichungen der Arbeitsgruppen „Sicherheit vernetzter Systeme“ sowie „Referenzarchitekturen, Standards und Normung“. Orientierung bei der Implementierung eines geeigneten Schutzklassenkonzepts bietet insbesondere der Leitfaden „IT-Security in der Industrie 4.0“ [12], der die notwendigen organisatorischen Rahmenbedingungen sowie rein technische Schutzmaßnahmen detailliert darstellt. Es sollen hier lediglich schlaglichtartig einige Schutzmechanismen benannt werden, die universell für eine Vielzahl von Geschäftsgeheimnissen sinnvolle Schutzmaßnahmen darstellen:

- Berechtigungsmanagement: Unabhängig von der Art des jeweiligen Geschäftsgeheimnisses sollten Unternehmen ihren Geschäfts- und Kooperationspartnern nur Zugang zu solchen Geschäftsgeheimnissen gewähren, die für die Durchführung der Kooperation zwingend notwendig sind („Need-to-know-Basis“); insbesondere der Zugriff auf die Verwaltungsschale muss auf die am jeweiligen Lebenszyklus des Produkts beteiligten Akteure beschränkt werden.
- Identitäts-Management und Authentifizierung: Die Integrität und Vertrauenswürdigkeit jedes Kommunikationssystems sind sicherzustellen. Digitalisierung und Vernetzung erfordern zwingend Vertrauen in die Korrektheit eigener und externer Daten. Insbesondere Internetbasierte Kommunikationsverbindungen müssen vor unberechtigten internen und externen Zugriffen gesichert werden. Die Zuweisung von Passwörtern, die Einrichtung von Virenschutzprogrammen, Firewalls, verschlüsselte Kommunikation, Signaturen, ausreichende Protokollierung sowie sonstige technische Schutzmechanismen gegen die Manipulation von Kommunikationsnetzwerken ist essentiell. Für Details wird auf das Diskussionspapier „Integrität von Daten, Systemen und Prozessen als Kernelement der Digitalisierung“ in Zusammenarbeit mit ZVEI verwiesen.[13]
- Rechtliche Schutzmaßnahmen: Vertraulichkeitsvereinbarungen sowie Regelungen zur Nutzung und Weitergabe sensibler Informationen sind als flankierende Maßnahmen zu technischen und organisatorischen Maßnahmen zu ergreifen. Bei den vertraglichen Regelungen ist insbesondere darauf zu achten, die betroffenen Geschäftsgeheimnisse möglichst konkret zu bezeichnen. Mit Blick auf Metadaten empfiehlt es sich, zur Konkretisierung auf die im Rahmen eines bestimmten Projektes, einer bestimmten Kooperation oder eines bestimmten Geschäftsbereichs offengelegten oder genutzten Geschäftsgeheimnisse abzustellen.
- Sensibilisierung von Mitarbeitern: Da häufig die fahrlässige Weitergabe von Informationen Grund für den Abfluss sensibler Informationen ist, sollten insbesondere Mitarbeiter sensibilisiert und im Umgang mit sensiblen Informationen regelmäßig geschult werden.
- Wartung und Evaluation: Das Schutzkonzept sollte regelmäßig in Bezug auf einzelne Geschäftsgeheimnisse sowie in seiner Gesamtheit auf seine Funktionalität, Effektivität und Relevanz regelmäßig geprüft werden. Die technischen Schutzmaßnahmen bedürfen darüber hinaus der regelmäßigen Betreuung und Wartung.

12 Abrufbar unter https://www.bmwi.de/Redaktion/DE/Publikationen/Studien/it-sicherheit-fuer-industrie-4-0.html.

13 Abrufbar unter https://www.de.digital/DIGITAL/Redaktion/DE/Publikation/industrie-4-0-diskussionspapier.html.

Grenzüberschreitender Schutz von Geschäftsgeheimnissen



A: Steckbrief

Worum geht es:

Kooperationen im Kontext von Industrie 4.0 beschränken sich selten auf rein nationale Sachverhalte. Bereits die Nutzung des Internets als Kommunikationsmedium und damit häufig im Ausland belegener Server schafft einen grenzüberschreitenden Bezug. Auch die Akteure selbst können in unterschiedlichsten Rechtsräumen angesiedelt sein, die nicht zwingend das gleiche Schutzniveau für Geschäftsgeheimnisse aufweisen wie in Deutschland und der EU. Im Kontext von Industrie 4.0 kommt es aber auf einen möglichst ungehinderten – auch grenzüberschreitenden – Datenverkehr an. Hinzu treten häufig regulatorische Barrieren für den freien Datenverkehr, die insbesondere die Geheimhaltung sensibler Informationen betreffen. In vielen Ländern existieren geographische Speicheranforderungen, aufgrund derer z. B. Server im Land eines Akteurs liegen müssen, oder indirekte Barrieren wie die Zugänglichkeit und sofortige Zugriffsmöglichkeit von Aufsichtspersonen auf Datenspeicher, die zwingende Verwendung bestimmter Infrastrukturen, Genehmigungserfordernisse sowie Anforderungen an die Segregation von Daten. Zusätzlich treten Schwierigkeiten der Rechtsdurchsetzung hinzu. Auch wenn in einer ausländischen Rechtsordnung generell ein hohes Schutzniveau bestehen sollte, so bedeutet dies nicht zwangsläufig, dass auch die Durchsetzung von Rechten wegen Verletzung von Schutzrechten ohne Weiteres für ausländische Unternehmen möglich ist.

Sich ergebende Fragen:

- Wie können Geschäftsgeheimnisse in grenzüberschreitenden Sachverhalten geschützt werden?

B: Juristische Einschätzung

Grundsätzlich ist zwischen innereuropäischen Sachverhalten und solchen mit Drittstaatenbezug zu differenzieren.

Seit Erlass der Geschäftsgeheimnis-RL und deren Umsetzung durch die Mitgliedstaaten ist das Schutzniveau innerhalb der EU insgesamt hoch und weitestgehend einheitlich. Die Richtlinie ist nunmehr in allen Mitgliedstaaten (mit Ausnahme von Zypern) in nationales Recht umgesetzt. Auch verblieb den Mitgliedstaaten bei Umsetzung der Richtlinie nur ein geringer Gestaltungsspielraum. Nach Art. 1 Abs. 1 Unterabsatz 2 der Geschäftsgeheimnis-RL sind die Vorgaben der Richtlinie zu Erwerb, Nutzung und Offenlegung von Geschäftsgeheimnissen, zu den Rechtsfolgen bei Verletzung sowie prozessualen Regelungen zwingend umzusetzen gewesen. Das Schutzniveau innerhalb des europäischen Binnenmarktes wurde damit deutlich harmonisiert, bestehende Unterschiede wurden weitgehend beseitigt. Sofern also Akteure grenzüberschreitend im europäischen Binnenmarkt tätig werden, können sie sich bzgl. Geheimnisbegriff, erlaubten Handlungen und prozessualem Schutz an den Kernregelungen des neuen GeschGehG orientieren. Gleichzeitig ist zu beachten, dass innerhalb der EU etwaige Barrieren des freien Datenverkehrs einzelner Mitgliedstaaten stets an der Verwirklichung des europäischen Binnenmarktes zu messen sind. Die Anforderungen an die Rechtfertigung derartiger Barrieren sind damit innerhalb der EU relativ hoch.

Auch die Durchsetzung von Rechten auf Grundlage des GeschGehG ist innerhalb der EU auf Grundlage der Verordnung Nr. 1215/2012 des Europäischen Parlaments und des Rates vom 12. Dezember 2012 über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen (sog. „Brüssel Ia-VO“) harmonisiert. Hat ein Unternehmen in einem grenzüberschreitenden Fall bei einem Gericht eines Mitgliedstaates ein vollstreckbares Urteil wegen Verletzung eines Geschäftsgeheimnisses erwirkt, so kann es die Vollstreckung dieses Urteils direkt in einem anderen Mitgliedsstaat betreiben.

Anders verhält es sich im Verhältnis zu Drittstaaten, wie z. B. den USA, China und Russland. Soweit Informationen an Anwender oder Anbieter in Drittstaaten übermittelt werden, gestaltet sich die Rechtslage in dreierlei Hinsicht uneinheitlich.

Erstens ist trotz der Vereinheitlichungsbemühungen auf internationaler Ebene, beispielsweise durch Unterzeichnung des TRIPS-Abkommens, das Schutzniveau in Drittstaaten oft deutlich unterschiedlich. So ist der Schutz häufig heterogen geregelt und an unterschiedliche Voraussetzungen geknüpft.

Zweitens bestehen auch nationale Unterschiede bei der prozessualen Geltendmachung von Ansprüchen wegen der Verletzung von Geschäftsgeheimnissen. So ist es für ein in der EU ansässiges Unternehmen in vielen Drittstaaten problematisch, ein Gerichtsverfahren im Ausland zu betreiben, ausländische Urteile anerkennen zu lassen sowie nationale oder ausländische (anerkannte) Urteile im Ausland zu vollstrecken.

Drittens verfügen Drittstaaten wie die USA, China oder Russland über regulatorische Bestimmungen zu Datenübermittlung, -abfluss und -zugriff aus oder in diese Länder, die Kooperationen im Rahmen von Industrie 4.0 stark beschränken.[14] Die regulatorischen Vorgaben zielen vorwiegend auf die Kontrolle bzw. Kontrollierbarkeit von Daten und Datenströmen ab. Insbesondere wenn kritische Infrastrukturen der betroffenen Heimatländer wie Kommunikation, Verkehr, Informationstechnik oder medizinische Versorgung durch die Industrie 4.0-Kooperation betroffen sind, unterliegen sowohl in- als auch ausländische Unternehmen häufig strengen Regelungen hinsichtlich Datensicherheitsanforderungen und Meldepflichten. So bestehen z. T. Vorschriften zur Datenlokalisierung, d.h. bestimmte Datensätze oder Datenarten müssen in einem bestimmten Land vorgehalten werden. Viele Drittstaaten treffen auch Datenschutzregelungen, die die Übermittlung personenbezogener Daten aus und in Drittländer betreffen. Regelungen zur nationalen Sicherheit erlauben nationalen Regierungen und Behörden den Zugriff auf bestimmte Daten oder beschränken bzw. verhindern deren Übermittlung. Ebenso existieren Einfuhr- und Ausfuhrkontrollbestimmungen für Hardware und Software bzw. Datenträger.

C: Handlungsoptionen und Handlungsempfehlungen

Im Vorfeld jeder Kooperation mit ausländischen Geschäfts- oder Kooperationspartnern müssen Unternehmen der EU die bestehenden rechtlichen Rahmenregelungen zum Schutz ihrer Geschäftsgeheimnisse genau prüfen. Ungenauigkeiten oder falsch verstandene „Sparsamkeit“ können hohe Folgekosten verursachen, wenn die rechtlichen Rahmenbedingungen im „Zielland“ durch starke staatliche Kontrolle des Informationsflusses geprägt sind. Insbesondere nationale Vorschriften zur Ausfuhrkontrolle sowie etwaig bestehende internationale und/oder bilaterale Investitionsschutzabkommen (sog. „Bilateral Investment Treaties“, kurz „BIT“) sind mit in den Blick zu nehmen.

Die verfügbaren Rechtsquellen sollten auf Regelungen geprüft werden, die Auswirkungen auf getroffene oder zu treffende technische und organisatorische Schutzmaßnahmen haben. Da rechtliche Sicherungsmechanismen aus den vorgenannten Gründen in grenzüberschreitenden Sachverhalten mit Drittstaaten häufig weniger erfolgsversprechend als im europäischen Rechtsraum sind, sollten Unternehmen den Fokus ihrer Schutzmaßnahmen auf technische und organisatorische Schutzmaßnahmen legen. Die konkrete Ausgestaltung des technischen Schutzkonzepts muss dabei auch einer Überprüfung durch nationale Behörden mit Blick auf Ausfuhrbestimmungen oder sonstige sicherheitsrelevante Vorschriften standhalten. Angesichts der Fülle von Vorschriften ist die Einholung von Rechtsrat unverzichtbar.

Deutsche Unternehmen sollten ebenfalls prüfen, ob die Geltung deutschen Rechts und ein deutscher Gerichtsstand wirksam vertraglich vereinbart werden können und auf die Vereinbarung solcher Klauseln hinwirken. Rechte und Pflichten der Vertragsparteien im Umgang mit Geschäftsgeheimnissen sollten explizit benannt werden, insbesondere wenn die vertragliche Vereinbarung der Geltung deutschen Rechts und/oder ein deutscher Gerichtsstand faktisch nicht durchzusetzen ist. Hierdurch wird der Auslegungs- und Interpretationsspielraum ausländischer Gerichte möglichst klein gehalten.

14 Einen detaillierten Überblick über bestehende Hemmnisse des freien Datenverkehrs in Europa, Russland, China und den USA gibt die IMPULS-Studie der Stiftung für den Maschinenbau, den Anlagenbau und die Informationstechnik mit dem Titel „Digitale Marktabschottung: Auswirkungen von Protektionismus auf Industrie 4.0“, September 2019.

Weiter sollten deutsche Unternehmen bereits im Vorfeld von Vertragsverhandlungen prüfen, ob der Heimatstaat des Geschäftspartners Unterzeichnerstaat der Haager Übereinkommen[15] ist sowie zwischen Deutschland und dem Heimatstaat ein Vollstreckungsübereinkommen besteht, um im Streitfall die Rechtsdurchsetzung in Drittstaaten betreiben zu können.

Schließlich müssen Unternehmen im Blick behalten, dass in vielen ausländischen Staaten die Schiedsgerichtsbarkeit als Alternative zu staatlichen Gerichten anerkannt ist. Im Gegensatz zu staatlichen Gerichten bieten Schiedsgerichte den Vorteil, dass die Verhandlungen nicht öffentlich stattfinden und damit der Geheimnisinhaber nicht Gefahr läuft, durch einen Prozess sein Geschäftsgeheimnis zu verlieren. Zwar wurden mit dem GeschGehG auch prozessuale Regelungen zur Wahrung des Geheimnischarakters in Zivilverfahren aufgenommen. Diese finden aber nur Anwendung bei einer sog. „Geschäftsgeheimnisstreitsache", also Streitigkeiten wegen der Verletzung von Geschäftsgeheimnissen. Es kann allerdings auch notwendig sein, Geschäftsgeheimnisse als Verteidigungs- oder Beweismittel in anderen Streitigkeiten vorzutragen, für die die speziellen Regelungen des GeschGehG dann nicht gelten. In derartigen Konstellationen kann eine vertraglich vereinbarte Schiedsklausel die Geheimhaltung sensibler Informationen sicherstellen.

15 Gemeint sind das Haager Übereinkommen über die Zustellung gerichtlicher und außergerichtlicher Schriftstücke im Ausland in Zivil- und Handelssachen vom 15. November 1965 sowie das Haager Übereinkommen über die Beweisaufnahme im Ausland in Zivil- und Handelssachen vom 18. März 1970.

AUTOREN

Dr. Alexander Duisberg, Bird & Bird LLP | RA Roksana Hosseini, LL.M., Bird & Bird LLP

Diese Publikation wird durch die Unter-Arbeitsgruppe „IP-Recht" sowie durch die AG „Rechtliche Rahmenbedingungen" der Plattform Industrie 4.0 getragen.

www.plattform-i40.de