Compliance
Die Zeitschrift für Compliance-Verantwortliche

Oktober 2021

Inhalt

© IMAGO / Steinach

Aufmacher

Compliance-Gesetzgebung: Warum bleiben Politik und Verwaltung verschont?
Bekanntermaßen ist der Gesetzgeber bei der Schaffung neuer Compliance-Gesetze ausgesprochen aktiv. Nur bei sich selbst machen Politik und Verwaltung eine Ausnahme. Warum ist das so? Eine Einordnung von Dr. Malte Passarge, Chefredakteur des Compliance-Beraters.

Praxis

© Pixabay

IT-Sicherheit: „Firmenexistenzen und Arbeitsplätze stehen auf dem Spiel"
Um der wachsenden Bedrohung durch Cyber-Angriffe zu begegnen, hat der Gesetzgeber in den vergangenen Jahren eine Reihe von Gesetzen verabschiedet und zwar nicht nur für Betreiber kritischer Infrastrukturen. Unternehmen sind angehalten, ihre IT-Sicherheitsmaßnahmen regelmäßig zu überprüfen und dem Stand der Technik anzupassen. In einem einstündigen Webinar führte Dr. Anne Förster, Taylor Wessing, Ende September durch eine Expertendiskussion zum Thema.

Recht

© Pixabay

Innovativ – und jetzt?
Der Verordnungsentwurf der Europäischen Kommission zur Regulierung künstlicher Intelligenz vom 21. April 2021 (KI-VO) nimmt sich einer umfassenden Regulierung eines zentralen zukunftsträchtigen Themas an. Lesen Sie hier Auszüge aus dem ausführlichen Beitrag von Jan Pohle aus der Oktober-Ausgabe des Compliance-Beraters

Recht

© IMAGO / Ikon Images

Fünf Jahre Geschäftsgeheimnis-Richtlinie – eine Erfolgsgeschichte?
Die Richtlinie (EU) 2016/943 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen ist seit fünf Jahren in Kraft. Das zu ihrer Umsetzung geschaffene neue Stammgesetz zum Schutz von Geschäftsgeheimnissen – das GeschGehG – gilt seit Ende April 2019, muss sich also seit gut eineinhalb Jahren in der Praxis beweisen. Aber, ist es eine Erfolgsgeschichte?

Veranstaltungen

9. November 2021 | Webinar | **Der Aufsichtsrat in der Unternehmenskrise**

11. November 2021 | München oder Online | **Deutsche Arbeitsrechtskonferenz 2021**

11. November 2021 | Frankfurt am Main oder Online | **Datenschutz in der Praxis**

26. November 2021 | Frankfurt am Main oder Online | **Umsetzung der EU-Richtlinie „Unfaire Handelspraktiken in der Lebensmittellieferkette"**

Compliance-Gesetzgebung: Warum bleiben Politik und Verwaltung verschont?

Bekanntermaßen ist der Gesetzgeber bei der Schaffung neuer Compliance-Gesetze ausgesprochen aktiv. Nur bei sich selbst machen Politik und Verwaltung eine Ausnahme. Warum ist das so? Eine Einordnung von Dr. Malte Passarge, Chefredakteur des Compliance-Beraters.

„Bestenfalls einer Bananenrepublik würdig" seien die Zustände bei der FIU, meint Dr. Malte Passarge zur Integrität von Politik und Verwaltung in Deutschland.

Die laufenden Änderungen im Geldwäschegesetz und § 261 StGB, das LkSG, TransparenzregisterG, GeschGehG sowie der stark wachsende Bereich ESG mit der EU-Taxonomie-Verordnung, EU-Offenlegungsverordnung, Non-Financial-Reporting – und nicht zu vergessen die vorerst gestoppten VerSanG und HinweisgeberschG: Angesichts dieser ausgeprägten Regelungsfreude stellt sich die Frage, wem mit diesen Gesetzen tatsächlich geholfen ist.

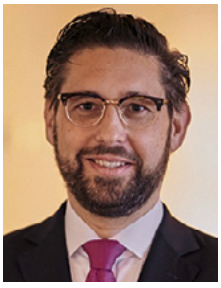
Der Gesetzgeber greift immer tiefer in die unternehmerischen Prozesse ein, indem er detailliert vorgibt, auf welche Art und Weise gewünschtes Verhalten, umfangreiche Analysen und Prozesse umzusetzen sind, anstatt grundlegende Pflichten vorzugeben und die Umsetzung den Unternehmen selbst zu überlassen. Die Eigenverantwortung der Unternehmen für die Umsetzung von Compliance wird diesen zulasten einer überbordenden Dokumentationspflicht entzogen. Dabei sind diese nicht immer zweckmäßig, sondern stellen lediglich komplexitätserhöhende additive digitale Dokumentationsruinen dar.

Wer aber ernsthaft die nachhaltige Umsetzung von Compliance bei Unternehmen fordert, muss vor allem den Rechtsstaat fördern und die Justiz viel stärker finanzieren. Tatsächlich scheitert eine nachhaltige Umsetzung von Compliance allzu oft im Flaschenhals der Justiz. Wenn Verfahren wegen Compliance-Verstößen vor dem Arbeitsgericht an ideologischen Schranken scheitern und nicht umgesetzt werden können oder strafrechtliche Verfahren sich über Jahre hinziehen, verzweifeln Unternehmen nicht zu Unrecht an der Schizophrenie von gesetzlichen Verpflichtungen und deren Umsetzungsbeschränkungen durch die Justiz. Um die derzeit geltende Diktion aufzugreifen kann man hier gewiss von einer Justizkatastrophe sprechen.

Blickt man auf Politik und Verwaltung stellt sich die Frage, aus welchem Grunde dieser Bereich von der Compliance-Gesetzgebung verschont bleibt. Freilich steht es der öffentlichen Hand frei in ihren Behörden und Unternehmen Motor der Compliance-Entwicklung zu sein, doch findet man hier Compliance ausgesprochen selten. Warum ist die öffentliche Hand nicht Vorreiter der politisch wichtigen Themen (Gleichberechtigung, Compliance und Menschenrechte), die von privatrechtlichen Unternehmen lautstark eingefordert werden?

Blickt man in die Gesetzesbegründungen des VerSanG wird eine Wahrnehmung der Wirtschaft deutlich, die nicht immer vom Bezug zur Realität geprägt ist. Schon die Titelbegebung des VerSanG als „Entwurf eines Gesetzes zur Stärkung der Integrität in der Wirtschaft" könnte man als Frechheit bezeichnen. Als ob ein Gesetz integres Verhalten stärken könnte – oder ein solcher Bedarf besteht. Anscheinend geht die Politik davon aus, dass die Wirtschaft nicht ausreichend integer ist.

Der Gang des Gesetzgebungsverfahrens war gewiss kein Beispiel für einen integren und demokratischen Prozess. Nachdem der erste, nicht-öffentliche Entwurf „irgendwie" durchgesickert war, gab es einige Änderungen, die kompetenten und ernsthaften Bedenken der Verbände wurden nicht berücksichtigt, ein kaum überarbeiteter Entwurf wurde nach nur wenigen Tagen durch den Bundestag getrieben.



HDH

Dr. Malte Passarge ist Rechtsanwalt und Fachanwalt für Handels- und Gesellschaftsrecht und Partner in der Kanzlei HUTH DIETRICH HAHN Rechtsanwälte PartGmbB, Vorstand des Instituts für Compliance im Mittelstand (ICM) und Geschäftsführer von Pro Honore e. V. sowie Chefredakteur des Compliance-Beraters.

Doch wie integer sind Politik und Verwaltung? Bestenfalls einer Bananenrepublik würdig sind die Zustände bei der FIU. Der Wirtschaft wurden umfangreiche Meldepflichten auferlegt, an deren Ende eine Behörde steht, die nicht im Ansatz über die erforderlichen Ressourcen verfügt. Dass nun die Staatsanwaltschaft wegen Strafvereitelung gegen eine Behörde ermitteln und Justiz- und Finanzministerium durchsuchen muss, ist nicht zu fassen. Schlimmer nur der fehlende Aufschrei der Öffentlichkeit.

In dieser Liga spielt auch das Verhalten der BaFin rund um Wirecard. Jedes Wirtschaftsprüfungsunternehmen muss die Aktienbeteiligungen seiner Mitarbeiter abfragen und melden- bzw. eben untersagen. Demgegenüber dürfen Mitarbeiter der Aufsichtsbehörde (!) völlig uneingeschränkt mit Aktien der überwachten Unternehmen handeln. Dass dabei auch Insiderinformationen missbraucht werden könnten, scheint niemandem aufgefallen zu sein – oder gar gestört zu haben. Dass eine solche Aufsichtsbehörde gerichtlich gegen Journalisten vorgeht, die Missstände zu Recht aufdecken, hätte für Aufruhr gesorgt, wenn dies in Russland geschehen wäre, bei uns führt es lediglich zu einem Schulterzucken.

Wer benötigt tatsächlich mehr Compliance Gesetzgebung – die Wirtschaft oder Politik und Verwaltung?

Auch wenn der Gesetzgeber das Thema Compliance für sich entdeckt hat, ist dies gewiss keine Neuerung für die Wirtschaft. Spätestens seit dem Siemens-Skandal ist Compliance in der deutschen Wirtschaft angekommen und Gegenstand guter Unternehmensführung. Dies auch ohne die treusorgende Hilfe der Politik. Eine Belastung sind aber überflüssige Formalismen, die gerade eine ernsthafte Compliance erschweren.

Wie in vielen anderen Bereichen zeigt sich auch hier die Hybris von Politik und Verwaltung. Angesichts der oben dargestellten Skandale und der Vorkommnisse rund um die Selbstbedienung diverser Parteien erwartet der Bürger nach der Wahl mit Spannung das „Gute Gesetz zur Stärkung der Integrität in Politik und Verwaltung" und das „Gute Gesetz zur Schaffung besserer Gesetze".

Dr. Malte Passarge

WEBINAR

Der Aufsichtsrat in der Unternehmenskrise: Rechte, Pflichten, Haftungsgefahren

» Dienstag, 9. November 2021 | 10.00 - 12.00 Uhr

Ihr Referent:

Prof. Dr. Daniel Graewe, LL.M.,
ist Rechtsanwalt und Direktor des Instituts für angewandtes Wirtschaftsrecht in Hamburg. Es ist einer der führenden Gesellschaftsrechtler und spezialisiert auf die Beratung von Leitungs- und Kontrollorganen. Graewe ist Mitherausgeber der in der dfv Mediengruppe, Fachbereich Recht und Wirtschaft, erscheinenden Fachzeitschrift zum Thema Restrukturierung und Interimsmanagement „Der Sanierungsberater".

Ihre Inhalte:

- Unternehmenskrisen, ihre Stadien und ihre Erkennungsmerkmale
- Besondere Rechte und Pflichten von Kontrollorganen in der Krise
- Kontrollinstrumentarium
- Haftungsgefahren

Unternehmenskrisen stellen – insbesondere infolge der COVID-19-Pandemie – ein verbreitetes Problem dar. Ihre Bewältigung stellt das Management regelmäßig vor große Aufgaben. Auch für Kontrollorgane bedeuten Restrukturierungsszenarien eine besondere Herausforderung, treffen sie doch im Vergleich zur normalen Geschäftstätigkeit des Unternehmens besondere Anforderungen bei ihren Beratungs- und Überwachungsaufgaben.
Dieser Umstand – ebenso wie die besonderen Kontrollinstrumente – sind vielen Mitgliedern von Kontrollorganen jedoch nicht immer präsent, wie Sanierungspraxis und Rechtsprechung zeigen. Dies hat sich erst jüngst wieder in der Verurteilung eines Aufsichtsrats zu einer Millionenzahlung an Schadensersatz niedergeschlagen, weil eine Krisensituation vom Kontrollgremium nicht erkannt und daher auch nicht entsprechend gehandelt wurde.

Teilnahmegebühr:

149,00 Euro zzgl. MwSt.
5% Frühbucherrabatt bis 1. Oktober.

Anmeldeschluss 9. November, 9:00 Uhr.

Die Teilnahmegebühr bitten wir nach Erhalt der Rechnung zu überweisen. Die Anmeldung ist übertragbar. Bei Stornierung bis 29. Oktober wird eine Bearbeitungsgebühr von 25,00 Euro erhoben. Danach ist die volle Teilnahmegebühr zu entrichten.

Zugangsdaten & Übertragung:

Wir verwenden für die digitale Übertragung der Veranstaltung das Meeting-Tool „Zoom". Bitte stellen Sie vorab sicher, dass „Zoom" bei Ihnen installiert werden kann. Sie können „Zoom" testen unter www.zoom.us/test. Die Zugangsdaten zur Veranstaltung erhalten Sie rechtzeitig vorab per E-Mail.

Anmeldung

unter www.ruw.de/Aufsichtsrat oder per Mail an Stephen.Hain@dfv.de

dfv Mediengruppe

Name/Vorname

Kanzlei/Firma

Straße PLZ/Ort

Telefon E-Mail

Datum/Unterschrift

Partner: GRAEWE

Medienpartner: Betriebs Berater · Der Sanierungs Berater · Recht der Internationalen Wirtschaft · Compliance Berater

Deutscher Fachverlag GmbH · Ansprechpartner: Stephen Hain
Mainzer Landstraße 251 · 60326 Frankfurt · Tel: 069 7595 2712 · Fax: 069 7595 1150 · Stephen.Hain@dfv.de

IT-Sicherheit: „Firmenexistenzen und Arbeitsplätze stehen auf dem Spiel“

Um der wachsenden Bedrohung durch Cyber-Angriffe zu begegnen, hat der Gesetzgeber in den vergangenen Jahren eine Reihe von Gesetzen verabschiedet und zwar nicht nur für Betreiber kritischer Infrastrukturen. Unternehmen sind angehalten, ihre IT-Sicherheitsmaßnahmen regelmäßig zu überprüfen und dem Stand der Technik anzupassen. In einem einstündigen Webinar führte Dr. Anne Förster, Taylor Wessing, Ende September durch eine Expertendiskussion zum Thema.

© Pixabay

Das Bild vom Einzeltäter ist überholt – inzwischen stehen „Fabriken“ hinter Cyber-Angriffen.

Ein ganzer Flickenteppich von Regelungen sei zu beachten, erläuterte Mareike Christine Gehrmann, Fachanwältin für IT-Recht bei Taylor Wessing, und nannte beispielhaft das IT-Sicherheitsgesetz 2.0, Regelungen der EU zur IT-Sicherheit und natürlich die DSGVO, die besonders auf personenbezogene Daten schaue, und deshalb besonders betrachte, wie Schutzmaßnahmen für IT-Systeme zum Schutz von personenbezogenen Daten beitragen können. „Die Automobilindustrie hat sich internationale Standards zur IT-Sicherheit gegeben.“ Vor allem Unternehmen, die international tätig sind, müssten im Rahmen der Produktentwicklung genau schauen, was im jeweiligen Land gilt.

Wolfgang Straßer, Geschäftsführer der @yet-GmbH, nannte drei Haupteinfallstore für Cyber-Kriminelle: Phishing-Attacken, das Ausnutzen von Lücken in den Systemen (Firewalls etc.) und „tatsächlich auch immer noch der berühmte USB-Stick, der irgendwo auf dem Betriebsgelände fallen gelassen und von einem Mitarbeiter in einen PC des Unternehmens gesteckt wird“.

Rolf Fellmann, Geschäftsführer der dSales Plus GmbH, ergänzte: „Wir sollten nicht vergessen, dass eine Lücke im System auch sein kann, das Pendel zu stark ausschlagen zu lassen. Das ist der Fall, wenn Systeme so stark abgesichert werden, dass Menschen nicht mehr arbeiten können und sich dann andere Wege zum Informationsaustausch suchen – z.B. über die private E-Mail-Adresse.“

Straßer wies auf die Schäden hin, die Cyber-Angriffe verursachen: Der Digitalverband Bitkom beziffert den jährlichen Gesamtschaden für die deutsche Wirtschaft 2020/2021 durch Cyber-Angriffe auf 223 Mrd. Euro. Trotz dieser immensen Zahl wüssten viele Unternehmen nicht, wie sie vorgehen sollen, wenn ein Angriff erfolgt. „Das haben viele Unternehmen nicht auf dem Schirm. Dabei sind die ersten Schritte besonders wichtig: Wen sprechen wir an? Was sollte ich keinesfalls tun?“ Straßer beschrieb, dass manche Unternehmen versuchten, dem Schaden durch Löschen zu begegnen. „Das sollten Sie aber auf keinen Fall tun, denn dann sind keine Spuren mehr da, die nachverfolgt werden können.“

Wichtig sei, dass jedes Unternehmen individuell für sich selbst definiere, welche Schritte im Fall eines Angriffs unternommen werden müssten. Zwar gebe es Hilfestellungen und Leitlinien, „die passen aber nie genau auf die Unternehmensstruktur: Welche Kunden muss ich informieren etc. – das ist für jeden unterschiedlich. Das sollte jeder für sich individuell festlegen und dann auch mal geübt haben“.

Gehrmann lenkte den Blick auf kleinere Unternehmen, die zunehmend ins Visier der Behörden gelangen. Denn „jedes Unternehmen ist aufgrund der allgemeinen zivilrechtlichen Regelungen verpflichtet, sich zu schützen und natürlich auch aufgrund der DSGVO. Da gibt es auch abseits kritischer Infrastrukturen viel Potenzial, was es zu schützen gilt.“ Eine weitere Frage könne auch sein, „welche Verpflichtungen mir meine Kunden mitgegeben haben“.

Fellmann appellierte, dass IT-Sicherheit auf die Geschäftsleitungsebene gehöre. „Das ist eine riesige Verantwortung. Die Frage ist ja auch, wer haftet für solche Fälle.“

Förster bekräftigte: „Natürlich ist die Geschäftsführung dazu da, ein Compliance-System zu entwickeln und dazu gehört auch die IT-Security. Die Geschäftsführung ist auch gefordert, die Mitarbeiter verstärkt zu schulen.“

Straßer lenkte den Blick auf die Wertschöpfung, die ohne IT nicht mehr vorstellbar sei. „Auch darum gehört das Thema in die Geschäftsleitung und in das Risikomanagement. International tätige Unternehmen mit angloamerikanischen Investoren geben inzwischen auch entsprechende Goals vor.“

„Nicht zu vergessen ist, dass auch der Reputationsschaden immens ist“, ergänzte Gehrmann.

Zumindest das finanzielle Risiko ließe sich durch eine Cyber-Versicherung mindern. „Allein das, was die Forensiker an Kosten produzieren, ist immens. Jedes Gerät, das in einem Netz ist, das verschlüsselt wurde, muss angepackt und neu aufgesetzt werden. Dazu kommen noch die Ausfallkosten, wenn nicht weiter produziert werden kann.“

Gehrmann erinnerte daran, dass Grundvoraussetzung dafür, überhaupt eine entsprechende Versicherung zu bekommen, aber ein gewisser IT-Security-Standard ist. „Nur die Versicherung ist darum sicher keine Lösung.“

Zum Ende der Runde bat Förster um einen Ausblick auf die kommenden Jahre.

„Wir müssen mehr digitalisieren, um effizienter zu werden. Das erhöht natürlich auch den Aufwand für IT-Security“, sagte Fellmann und forderte viel stärker interdisziplinär an das Thema Cyber-Security heranzugehen: „Bei aller Sicherheit müssen wir in den Unternehmen auch arbeitsfähig bleiben.“

Gehrmann stellte weitere Verschärfungen durch den Gesetzgeber in Aussicht. „Die neue BSI-Kritis-Verordnung hat noch Lücken und setzt noch nicht das IT-Sicherheitsgesetz 2.0 um. Da wird es nochmal eine Anpassung geben. Der Gesetzgeber nimmt das Thema aber auch an diversen anderen Stellen in den Fokus.“

Straßer sieht die maximale Abhängigkeit von der IT auf Unternehmen zukommen. Und damit auch eine rasante Erhöhung der Zahl und der Organisation der Angreifer. „Das sind Fabriken die da angreifen. Darum brauchen wir Awareness top-down – vom Vorstand bis zum Sachbearbeiter muss das gesichert sein.“ Denn am Ende stünden Firmenexistenzen und Arbeitsplätze auf dem Spiel. *chk*

Innovativ – und jetzt?

Der Verordnungsentwurf der Europäischen Kommission zur Regulierung künstlicher Intelligenz vom 21. April 2021 (KI-VO) nimmt sich einer umfassenden Regulierung eines zentralen zukunftsträchtigen Themas an. Lesen Sie hier Auszüge aus dem ausführlichen **Beitrag von Jan Pohle aus der Oktober-Ausgabe des Compliance-Beraters**.

©Pixabay

KI ist überall und weltweit und darum nun auch ein Fall für die EU-Regulierung.

KI dringt als ein Treiber der Digitalisierung in immer mehr Lebensbereiche vor: ob im Finanz- und Versicherungssektor, im Verkehrs- und Gesundheitswesen oder im Sicherheitsbereich. KI ist überall und das weltweit. Auch wenn 61 % der Europäer KI gegenüber positiv eingestellt sind, sehen immerhin 88 % KI skeptisch. Darauf hat die Kommission mit ihrem Vorschlag reagiert. Wird dieser verabschiedet, müssen Unternehmen in erheblichem Maße tätig werden, um die Vorgaben der Verordnung zu erfüllen, so sie künstliche Intelligenz entwickeln, vertreiben oder auch nur nutzen wollen.

Trotz differenzierter Reaktionen der EU-Mitgliedstaaten auf das Weißbuch, hat die EU-Kommission eine KI-VO vorgeschlagen, die für Anbieter von KI oder deren Ergebnisse im EU-Kontext ebenso einen erheblichen Mehraufwand bedeuten würde, wie für Nutzer, Importeure und Vertriebsmittler. Ziel der neuen Verordnung ist es sicherzustellen, dass alle KI-Systeme in der EU sicher sind und zu bestehenden Grundrechten und EU-Werten nicht im Widerspruch stehen. Gleichzeitig will die Kommission durch Schaffung von Rechtssicherheit Investitionen und Innovationen im Bereich KI erleichtern und so den Binnenmarkt für rechtmäßige, sichere und vertrauenswürdige KI-Systeme entwickeln.

Privat

Jan Pohle ist Rechtsanwalt und Partner bei DLA Piper UK LLP, Köln. Schwerpunkte seiner Tätigkeit sind Digitalisierung, Outsourcing, Datenschutz und Cybercrime. Er ist Autor zahlreicher Veröffentlichungen zum IT- und Datenschutzrecht sowie Lehrbeauftragter der Universität Oldenburg (Informationsrecht).

In persönlicher Hinsicht knüpft Art. 2 Abs. 1 lit a) bis c) KI-VO die Anwendbarkeit der KI-VO an die jeweilige Tätigkeit der möglichen Akteure an. Adressaten der Verordnung sind Anbieter von KI-Systemen, die diese in der EU in Verkehr bringen oder in Betrieb nehmen, unabhängig vom Ort ihrer Niederlassung, Nutzer von KI-Systemen, die sich in der Union befinden und Anbieter und Nutzer von KI-Systemen unabhängig vom Ort ihrer Niederlassung, wenn das vom System hervorgebrachte Ergebnis in der Union verwendet wird. Der Begriff des Anbieters, der unmittelbar bzw. mittelbar Entwickler von KI-Systemen erfasst, und der des Nutzers werden in diesem Zusammenhang in Art. 3 Nr. 2 und 4 definiert. Mit der niederlassungsunabhängigen Definition des Art. 2 Abs. 1 lit c) KI-VO geht der Anwendungsbereich der Verordnung territorial über das Gebiet der EU hinaus.

Bestimmte KI-Praktiken verbietet die KI-VO in Art. 5 KI-VO insgesamt. Hierzu zählt z.B. die Verwendung sog. unterschwelliger Techniken außerhalb des Bewusstseins einer Person, um das Verhalten einer Person in einer Weise wesentlich zu beeinflussen, die körperlichen oder psychischen Schaden verursacht oder verursachen kann.

Die Regulierung hochriskanter KI-Systeme bildet sachlich-technisch den wesentlichen Schwerpunkt der KI-VO, die in Art. 6 KI-VO definiert sind. In der Definition von Hochrisiko-KI liegt eine zentrale Weichenstellung für die Anwendung zahlreicher und regelungsintensiver Bestimmungen der KI-VO. Da die Kommission die Definition infolge der bewusst offenen und damit dynamischen Gestaltung des Anhang III, auf den Art. 6 KI-VO verweist, in Zukunft anpassen und weitere Techniken aufnehmen kann, empfiehlt es sich für Unternehmen mit möglichen Berührungspunkten, sich für den Fall, dass die KI-VO verabschiedet wird, nicht nur mit der dann aktuellen Definition von Hochrisiko-KI im Detail auseinanderzusetzen und zu eruieren, ob vertriebene oder genutzte KI-Systeme als hochriskant einzustufen sind, sondern die Rechtsentwicklung insoweit laufend zu überwachen.

Derzeit nimmt das Gesetzgebungsverfahren um die KI-VO seinen vorgegebenen Lauf, dessen Abschluss nicht vor 2023 zu erwarten ist. In der Annahme, dass der Entwurf mit diesem Regelungsgehalt im Wesentlichen Bestand haben wird, sollten Unternehmen den weiteren Gesetzgebungsprozess beobachten und rechtzeitig Vorkehrungen treffen, um nicht von dem Inkrafttreten der Verordnung überrascht zu werden – auch wenn der Entwurf derzeit eine 24-monatige Vorlauffrist vorsieht. Beantworten sollten sie rechtzeitig insbesondere, ob ihr jeweiliger Tätigkeitsbereich sie als Anbieter, Händler, Importeur oder autorisierter Repräsentant im Sinne der Verordnung qualifiziert. In einem nächsten Schritt sollten alle Akteure prüfen, ob die verwendeten KI-Systeme als hochriskant i. S. v. Art. 6 KI-VO einzustufen sind. Trifft das zu, ist den Unternehmen angeraten, sich und ihre außereuropäischen Vertragspartner auf die umfassenden und vielfältigen Dokumentations-, Überwachungs-, Transparenz- und Mitteilungspflichten vorzubereiten, indem sie Zuständigkeiten klären und erste entsprechende Prozesse entwickeln. Es lohnt sich allein angesichts drastischer Bußgelddrohungen die Aufgaben zu identifizieren, zu konzeptionieren und zu implementieren.

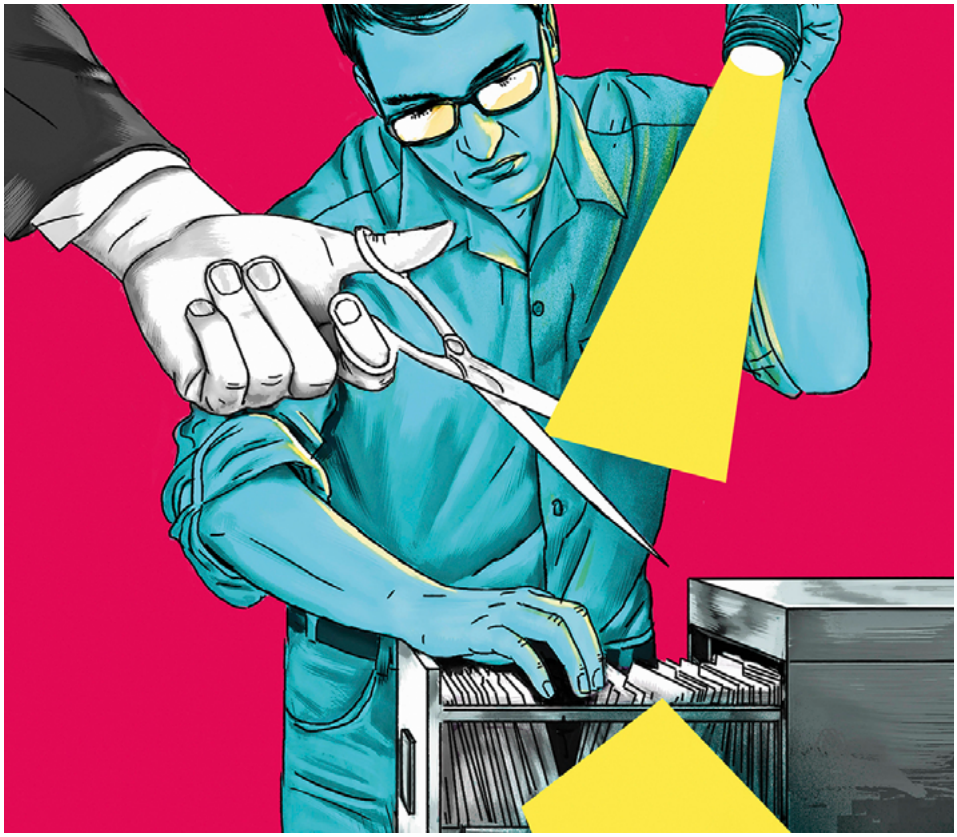
Jan Pohle

IMPRESSUM

Verlag
Deutscher Fachverlag GmbH, Mainzer Landstraße 251, 60326 Frankfurt am Main
Registergericht AG Frankfurt am Main HRB 8501
USt-IdNr. DE 114139662
Geschäftsführung: Peter Esser (Sprecher), Sönke Reimers (Sprecher), Thomas Berner, Markus Gotta
Aufsichtsrat: Andreas Lorch, Catrin Lorch, Peter Ruß
Redaktion: Christina Kahlen-Pappas (verantwortlich), Telefon: 069 7595-1153, E-Mail: christina.kahlen-pappas@dfv.de
Verlagsleitung: RA Torsten Kutschke, Telefon: 069 7595-1151, E-Mail: torsten.kutschke@dfv.de
Anzeigen: Eva Triantafillidou, Telefon: 069 7595-2713, E-Mail: Eva.Triantafillidou@dfv.de
Mitherausgeber:
BEITEN BURKHARDT Rechtsanwaltsgesellschaft mbH
Fachbeirat: Gregor Barendregt, Carl Zeiss AG; Andrea Berneis, thyssenkrupp Steel Europe AG; Ralf Brandt, LTS Lohmann Therapie-Systeme AG / Drug Delivery Systems Beteiligungs GmbH; Joern-Ulrich Fink, Central Compliance Germany, Deutsche Bank AG; James H. Freis, Jr., Chief Compliance Officer, Deutsche Börse AG; Otto Geiß, Fraport AG; Mirko Haase, Hilti Corporation; Dr. Katharina Hastenrath, Frankfurt School of Finance & Management; Corina Käsler, Head of Compliance, State Street Bank International GmbH; Olaf Kirchhoff, Schenker AG; Torsten Krumbach, msg Systems AG; Dr. Karsten Leffrang, Getrag; Prof. Dr. Bartosz Makowicz, Europa-Universität Viadrina Frankfurt/Oder; Thomas Muth, Corpus Sireo Holding GmbH; Stephan Niermann; Dr. Dietmar Prechtel, Osram GmbH; Dr. Alexander von Reden, BSH Hausgeräte GmbH; Hartmut T. Renz, Citi Chief Country Compliance Officer, Managing Director, Citigroup Global Markets Europe AG; Dr. Barbara Roth, Chief Compliance Officer, UniCredit Bank AG; Jörg Siegmund, Getzner Textil AG; Eric S. Soong, Group Head Compliance & Corporate Security, Schaeffler Technologies AG & Co. KG; Elena Späth, AXA Assistance Deutschland GmbH; Dr. Martin Walter, selbstständiger Autor, Berater und Referent für Compliance-Themen; Heiko Wendel, Rolls-Royce Power Systems AG; Dietmar Will, Audi AG.
Jahresabonnement: kostenlos
Erscheinungsweise: monatlich (10 Ausgaben pro Jahr)
Layout: Uta Struhalla-Kautz, SK-Grafik, www.sk-grafik.de

Fünf Jahre Geschäftsgeheimnis-Richtlinie – eine Erfolgsgeschichte?

Die Richtlinie (EU) 2016/943 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen ist seit fünf Jahren in Kraft. Das zu ihrer Umsetzung geschaffene neue Stammgesetz zum Schutz von Geschäftsgeheimnissen – das GeschGehG – gilt seit Ende April 2019, muss sich also seit gut eineinhalb Jahren in der Praxis beweisen. Aber, ist es eine Erfolgsgeschichte?



© IMAGO / Ikon Images

Wirksamer Schutz von vertraulichen Informationen ist in allen Geschäftsbereichen unabdingbar.

Auf europäischer Ebene war und ist die Harmonisierung des Rechts der Geschäftsgeheimnisse ein ambitioniertes Vorhaben. Angesichts einer zunehmend datenbasierten und durch digitale Prozesse geprägten Wirtschaft bestand (und besteht) ein unabweisbares Bedürfnis nach einem wirksamen Schutz von vertraulichen Informationen in allen Geschäftsbereichen. Ein solcher Schutz ist ein wichtiger Teil der rechtlichen Rahmenbedingungen für die Unternehmenstätigkeit im Binnenmarkt und ein nicht zu unterschätzender Standortfaktor. Europa ist nur dann für innovative Unternehmen attraktiv, wenn deren Innovationstätigkeit und die dabei hervorgebrachten Ergebnisse einen möglichst einheitlichen rechtlichen Schutz genießen. Die Richtlinie leistet hierzu einen wichtigen Beitrag.

Die Entstehung der Richtlinie fand in Deutschland noch vergleichsweise geringe Aufmerksamkeit. Viele Unternehmen, aber auch andere Betroffene (z. B. Medienschaffende), nahmen die Richtlinie und ihre Vorgaben erst näher wahr, als sie bereits in Kraft getreten war und die Umsetzung in das deutsche Recht näher rückte. Für inhaltliche Einflussnahmen war es zu diesem Zeitpunkt bereits zu spät, zumal dem deutschen Gesetzgeber vielfach nur ein eingeschränkter Umsetzungsspielraum zur Verfügung stand.

Positiv zu bewerten ist das Bestreben des Unionsgesetzgebers, die Grundstrukturen des Geschäftsgeheimnisschutzes an dem Schutz des geistigen Eigentums auszurichten. Wenngleich die Richtlinie die Unterschiede zwischen Geschäftsgeheimnissen und Rechten des geistigen Eigentums betont, unterstreicht vor allem das Rechtsdurchsetzungssystem der Richtlinie die unverkennbare Verwandtschaft und Nähe dieser beiden Bereiche. Das ist sachgerecht, weil geistiges Eigentum und Geschäftsgeheimnisse in der Praxis Hand in Hand gehen.

Privat

Prof. Dr. Christian Alexander ist Universitätsprofessor für Bürgerliches Recht, Wirtschaftsrecht und Medienrecht an der Friedrich-Schiller-Universität Jena.

Ebenfalls zu den Stärken gehört die Regelungstechnik der Richtlinie, die zwischen stets erlaubten Verhaltensweisen, Rechtsverletzungen und ausnahmsweise zulässigen Handlungen differenziert. Gerade der Erlaubniskatalog des Art. 3 Abs. 1 der Richtlinie erschien zunächst sehr ungewöhnlich. Dass ein solcher Regelungsansatz sinnvoll ist, zeigt das Beispiel Deutschlands, wo seit vielen Jahrzehnten das Reverse Engineering – wenngleich mit Differenzierungen – als unzulässig galt. Art. 3 Abs. 1 lit. b) der Richtlinie beendete diesen Irrweg und führte zu klaren Verhältnissen.

Die Richtlinie weist aber auch strukturelle Schwächen auf. So resultiert aus der merkwürdigen Mischung aus Voll- und Mindestharmonisierung manche Unklarheit: Ist beispielsweise der zentrale Begriff des Geschäftsgeheimnisses vollharmonisierend? Dagegen spricht, dass Art. 2 Nr. 1 in Art. 1 Abs. 1 UAbs. 2 der Richtlinie, dem Katalog der vollharmonisierenden Bestimmungen, nicht ausdrücklich erwähnt ist. Dafür spricht, dass der Begriff des Geschäftsgeheimnisses in vollharmonisierenden Bestimmungen (etwa in Art. 3 und 5 der Richtlinie) vorausgesetzt wird.

Unbefriedigend ist weiterhin, dass sich die Richtlinie zu einigen wichtigen Themen des Geschäftsgeheimnisschutzes überhaupt nicht äußert. So lässt sie offen, welche Rechtsnatur Geschäftsgeheimnisse haben; sehr vage spricht EwGr. 2 von einer „Ergänzung" oder „Alternative zu Rechten des geistigen Eigentums". Es fehlen nähere Aussagen zum praktisch sehr bedeutsamen Schutz von Geschäftsgeheimnissen innerhalb von Arbeitsverhältnissen und nach deren Beendigung. Auch zu Rechtsgeschäften über Geschäftsgeheimnisse schweigt die Richtlinie.

In der Rechtsprechung des EuGH spielt die Richtlinie bislang nur eine untergeordnete Rolle. Die Datenbank des Luxemburger Gerichts weist nur wenige Einträge zur Richtlinie auf. Aufschlussreich könnten aber Aussagen in der aktuellen Rechtssache C-54/21 sein, die den Schnittbereich von Vergaberecht und dem Schutz von Geschäftsgeheimnissen betrifft.

Ist die Richtlinie also eine Erfolgsgeschichte? Die bisherigen Erfahrungen zeigen, dass die Richtlinie gewiss nicht über jeden Zweifel erhaben ist und auch in Zukunft Fragen und Probleme aufwerfen wird. Im Großen und Ganzen darf man sie aber zu den gelungenen Projekten der EU zählen. *Prof. Dr. Christian Alexander*