Handlungsbedarf für Personalabteilungen

Geschäfts-geheimnisschutz

Das Geschäftsgeheimnisgesetz (GeschGehG) ist nunmehr rund ein Jahr in Kraft. Damit soll dem Verlust von sensiblen, vertraulichen und werthaltigen Informationen entgegnet werden. Ein Unternehmen kann sich aber nur dann auf diesen Schutz berufen, wenn es seine Geheimnisse ausreichend geschützt hat. Dies setzt insbesondere arbeitsrechtliche Maßnahmen voraus, die unternehmensseitig zu treffen sind. Was sind die wichtigsten Sicherungsmaßnahmen und welche Reaktionsmöglichkeiten gibt es beim „Geheimnisverlust"?

1 NOTWENDIGKEIT ANGEMESSENER GEHEIMHALTUNGSMASSNAHMEN

Der Begriff des Geschäftsgeheimnisses (vgl. zum GeschGehG generell bereits Schmid/Willems, AuA 2/19, S. 88) ist in § 2 Nr. 1 GeschGehG definiert.

VORSCHRIFT – § 2 GESCHGEHG

Begriffsbestimmungen
„Im Sinne dieses Gesetzes ist
1. Geschäftsgeheimnis eine Information
a) die weder insgesamt noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen, allgemein bekannt oder ohne Weiteres zugänglich ist und daher von wirtschaftlichem Wert ist und
b) die Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber ist und
c) bei der ein berechtigtes Interesse an der Geheimhaltung besteht; (...)"

Die Verpflichtung, „den Umständen nach angemessene" Maßnahmen zu treffen, ist der wesentliche Unterschied im neuen Geheimnisschutzrecht im Vergleich zur vormaligen Rechtslage im UWG. Danach war es noch ausreichend, dass es sich um eine schützenswerte Information handelt, an der nach den objektiven Umständen ein Geheimhaltungswillen erkennbar war. Dies genügt nach dem aktuellen Recht nicht mehr.[1]

Auf Unternehmensseite ist damit als erster Schritt im Wege eines strukturierten Vorgehens (vgl. Fuhlrott in: Fuhlrott/Hiéramente, BeckOK GeschGehG, 2. Edition, § 2 Rdnr. 23) die

- Identifizierung von relevantem, schützenswertem Know-how vorzunehmen,
- das sodann in verschiedene „Schutzstufen" zu unterteilen ist und
- für die jeweils im Anschluss konkrete Schutzmaßnahmen festzulegen sind.

Ein unternehmensseitiges Schutzkonzept ist damit der erste Schritt und Voraussetzung für die Implementierung geeigneter Schutzmaßnahmen. Als Beispiele zu ergreifender denkbarer Geheimhaltungsmaßnahmen werden in der Gesetzesbegründung (BT-Drs. 19/4724, S. 24 f.) technische Zugangshürden, allgemeine interne Richtlinien und Anweisungen sowie insbesondere arbeitsrechtliche Sicherungsmechanismen genannt. Für die Frage, welches Schutzniveau für welches Geheimnis notwendig ist, gibt die Begründung zudem sieben zu berücksichtigende Kriterien an die Hand:

1. der Wert des Geschäftsgeheimnisses und dessen Entwicklungskosten,
2. die Natur der Informationen,

PRAXISTIPP

[1] Die Verpflichtung zum Treffen von Schutzmaßnahmen trifft nicht nur Großkonzerne. Sie gilt für Unternehmen aller Größen. Zwar können von einem multinationalen Konzern mit eigener IT- und Sicherheitsabteilung strengere Vorkehrungen als von einem kleineren Mittelständler verlangt werden; ein Tätigwerden ist aber auch hier erforderlich.

© freshidea/stock.adobe.com

3. die Bedeutung für das Unternehmen,
4. die Größe des Unternehmens,
5. die üblichen Geheimhaltungsmaßnahmen im Unternehmen,
6. die Art der Kennzeichnung der Informationen,
7. vereinbarte vertragliche Regelungen mit Arbeitnehmern und Geschäftspartnern.

Das Arbeitsrecht und entsprechende Sicherungsmaßnahmen sind daher kein Selbstzweck, sondern stellen einen wichtigen Baustein im unternehmensseitigen Schutzkonzept dar.

2 ARBEITSRECHTLICHE SICHERUNGSMASSNAHMEN

Wichtige arbeitsrechtliche Schutzmaßnahmen, die unternehmensseitig erwogen und eingeführt werden können, sind insbesondere (im Einzelnen s. Fuhlrott, a. a. O., § 2 Rdnr. 39 ff.):

- sorgfältige Auswahl bei der Einstellung von Mitarbeitern oder der Beschäftigung von Leiharbeitnehmern in sensiblen Bereichen,
- Gebrauch von Weisungen und Einsatz allg. Arbeitsvertragsbedingungen, wie Anweisungen zum Umgang mit sensiblen Daten, zu deren Speicherung oder deren Export und Behandlung,
- arbeitsvertragliche Verpflichtungen bzw. Belehrungen über die Bedeutung des Geheimnisschutzes im Unternehmen und Aufsetzen bestimmter Handlungsvorgaben oder Meldepflichten in geheimnisschutzrelevanten Bereichen,
- regelmäßige Mitarbeiterschulungen und Sicherheitsunterweisungen,
- Prüfung der durch den Beschäftigten erlangten Informationen, insbesondere bei Arbeitnehmerkündigungen,
- Regelungen zum Fortbestand der Verschwiegenheitspflicht oder Abgabe entsprechender Versicherungen im Rahmen von Aufhebungs- und Abwicklungsverträgen.

Arbeitgeber sollten Arbeitsverträge daher mit Blick auf die derzeitig verwendeten Regelungen zur Vertraulichkeit überprüfen und entsprechend ergänzen. Bestehende Verträge können durch die Unterzeichnung einer Zusatzvereinbarung das notwendige Schutzniveau erreichen. Nicht übersehen darf man dabei, dass viele der arbeitsrechtlichen Sicherungsmaßnahmen Beteiligungsrechte des Betriebsrats berühren.[2]

Zwar betreffen Regelungen und Vorgaben zur Handhabe sensibler Daten vorrangig die Erfüllung der Arbeitspflicht und somit das mitbestimmungsfreie Leistungsverhalten. Je nach ihrer konkreten Ausgestaltung können sie aber überdies – vergleichbar mit allgemeinen Compliance-Programmen – auch den Bereich des Ordnungsverhaltens tangieren (vgl. zur Mitbestimmung gem. § 87 Abs. 1 Nr. 1 BetrVG bei Compliance-Programmen: Fitting, 29. Aufl., § 87 BetrVG Rdnr. 71 m. w. N.; s. a. LAG Schleswig-Holstein, Beschl. v. 6.8.2019 – 2 TaBV 9/19, EWiR 2020, S. 29, m. Anm. Fuhlrott, vgl. auch AuA 12/19, S. 724). Zudem wird der Mitbestimmungstatbestand des § 87 Abs. 1 Nr. 6 BetrVG oftmals erfüllt sein, sofern die Überwachung in Form technischer Einrichtungen wie der Protokollierung erfolgter Zugriffe o. ä. erfolgt. Hierbei ist zu beachten, dass es zur Eröffnung des Mitbestimmungsrechts bereits genügt, dass die technische Einrichtung zur Überwachung der Leistung grundsätzlich in der Lage ist, selbst wenn diese faktisch gar nicht erfolgt und eine Leistungskontrolle der Mitarbeiter seitens des Unternehmens auch gar nicht beabsichtigt ist (st. Rspr. seit BAG, Beschl. v. 9.9.1975 – 1 ABR 20/74, NJW 1976, S. 261; s. auch Kania in: ErfK, 20. Aufl., § 87 BetrVG Rdnr. 55).

Zu beachten ist allerdings, dass die dargestellten Anforderungen zwar unabdingbar für einen effektiven Geheimnisschutz nach dem GeschGehG sind, jedoch für arbeitsrechtliche Sanktionen keine notwendige Voraussetzung. Den Beschäftigten trifft – unabhängig von den Pflichten nach dem GeschGehG – die arbeitsvertragliche Nebenpflicht, die Rechte seines Vertragspartners nicht zu ver-

PRAXISTIPP

[2] Regelmäßig werden die Mitbestimmungsrechte des § 87 Abs. 1 Nr. 1 BetrVG (Ordnungsverhalten) und Nr. 6 (technische Überwachungseinrichtung) sowie ggf. auch datenschutzrechtliche Normen (insb. § 26 BDSG) betroffen sein. Der Abschluss einer entsprechenden Betriebsvereinbarung zum Geheimnisschutz ist daher empfehlenswert.

PRAXISTIPP

[3] Die – derzeit noch freiwillige – Schaffung von effektiven und in der Belegschaft positiv wahrgenommenen Hinweisgebersystemen ist eine Möglichkeit, um das praktische Risiko der Offenlegung von Geheimnissen gegenüber Behörden oder gar der Presse zu minimieren.

PRAXISTIPP

[4] Die Ermittlungsmaßnahmen der Staatsanwaltschaft reichen naturgemäß viel weiter als die zivilrechtlichen Optionen, die Unternehmen zustehen. So können insbesondere auch E-Mail-Postfächer betriebsfremder Personen oder private E-Mail-Accounts des Mitarbeiters eingesehen werden oder im Rahmen einer Hausdurchsuchung weitere Informationen sichergestellt werden. Zudem genügt ein einfacher Verdacht, damit die Staatsanwaltschaft Ermittlungen aufnimmt und tätig wird.

PRAXISTIPP

[5] Strafrechtliche Ermittlungen lassen sich zwar formal nicht steuern und werden von der Staatsanwaltschaft eigenständig geführt. Regelmäßig sind Staatsanwaltschaften jedoch gewillt, mit dem geschädigten Unternehmen zusammenzuarbeiten, so dass die Ermittlungsmaßnahmen koordiniert werden und auf Unternehmensseite keine unabgestimmten Beschlagnahmen etc. erfolgen.

letzen. Somit ist er bereits aus dem Arbeitsverhältnis verpflichtet, geheimhaltungsbedürftige Informationen Dritten gegenüber nicht zu offenbaren (BAG, Urt. v. 16.3.1982 – 3 AZR 83/79, NJW 1983, S. 134). Daran ändert sich auch durch das GeschGehG nichts (Apel/Walling, DB 2019, S. 891, 896; Fuhlrott/Hiéramente, DB 2019, S. 967, 970). Der Verrat vertraulicher Informationen stellt daher auch weiterhin eine arbeitsrechtliche Pflichtverletzung dar. Je nach Schwere kann diese den Arbeitgeber zur außerordentlich fristlosen Kündigung des Arbeitsverhältnisses berechtigen (Fuhlrott, a. a. O., § 2 Rdnr. 35 f.).

3 UMGANG MIT WHISTLEBLOWING

Das Gesetz hat eine weitere Thematik in den Mittelpunkt der Diskussion gerückt. Mit § 5 Nr. 2 GeschGehG hat der Gesetzgeber erstmals eine ausdrückliche Regelung geschaffen, die es Hinweisgebern erlaubt, bei Fehlverhalten im Unternehmen an die Öffentlichkeit zu treten. Handelt ein solcher „zur Aufdeckung einer rechtswidrigen Handlung oder eines beruflichen oder sonstigen Fehlverhaltens" und ist „die Erlangung, Nutzung oder Offenlegung geeignet (...), das allgemeine öffentliche Interesse zu schützen", so liegt keine Verletzung des Handlungsverbots des § 4 GeschGehG und damit auch keine Strafbarkeit nach § 23 GeschGehG vor. Der Gesetzgeber hat zwar in § 1 Abs. 3 Nr. 4 GeschGehG klargestellt, dass die Rechte und Pflichten aus dem Arbeitsverhältnis unberührt bleiben. Dennoch geht mit der Neuregelung eine Privilegierung des Whistleblowers einher, die nach alter Rechtslage deutlich umstrittener war.

Für Unternehmen ist diese Regelung besonders sensibel, weil auch die Offenlegung von Geschäftsgeheimnissen, die der Hinweisgeber als unethisches „sonstiges Fehlverhalten" einstuft, nach dem – wenn auch unklar formulierten – Willen des Gesetzgebers zulässig sein soll. Auch in der Rechtsprechung (OLG Oldenburg, Beschl. v. 21.5.2019 – 1 Ss 72/19) ist eine weitgehende Ausnahme von der Strafbarkeit der Offenlegung von Betriebsinterna aus ethischen Gründen akzeptiert worden: „Nach den rechtsfehlerfrei getroffenen Feststellungen des Amtsgerichts verfolgte der Angeklagte mit seinem Aufruf das Ziel, auf eine von ihm als rechtswidrig beurteilte Exportpraxis des Unternehmens hinzuweisen und eine Diskussion hierüber innerhalb und außerhalb des Unternehmens anzustoßen. Der behauptete Export von Giftstoffen in die USA, die dort auch zur Vollstreckung der Todesstrafe Verwendung finden, stellt dabei jedenfalls ein ethisch zu missbilligendes Verhalten dar, welches nach dem Willen des Gesetzgebers dem Begriff des beruflichen oder sonstigen Fehlverhaltens unterfallen soll (vgl. Gesetzesbegründung zu § 5 GeschGehG, BR-Drs. 382/18 S. 25)."

Unternehmen sollten sich auf die neuen Realitäten des Schutzes von Whistleblowern vorbereiten und bereits jetzt Anreize dafür schaffen, dass sensible Themen intern angesprochen und adressiert werden. Dies erlaubt es dem Arbeitgeber auch, etwaige Missverständnisse eines potenziellen Hinweisgebers frühzeitig auszuräumen und tatsächlichen Missständen abzuhelfen. Die Folgekosten einer Veröffentlichung von Betriebsinterna können zudem beträchtlich sein.[3]

Eine zeitige Vorbereitung ist auch aufgrund der weiteren rechtspolitischen Entwicklungen ratsam. Aufgrund der Vorgaben der Richtlinie 2019/1937/EU müssen bis zum 17.12.2021 weiter gehende Regelungen zum Schutz von Hinweisgebern durch die Mitgliedstaaten erlassen werden. Hiernach ist u. a. die Schaffung von Hinweisgebersystemen notwendig. Die behördliche Meldung wird daher in Zukunft kein gesetzlicher Ausnahmefall mehr sein (vgl. auch Garden/Hiéramente, BB 2019, S. 963).

4 VORBEREITUNG FÜR DEN KRISENFALL

Die Erfahrungen in der Praxis lehren, dass Unternehmen zwar häufig diverse Maßnahmen zum Schutz von Geschäftsgeheimnissen ergreifen, diese aber oft nur unzureichend dokumentieren und strukturieren. Daher bedarf es zumeist aufwendiger Recherchen, um die wichtigen Informationen aus bestimmten Abteilungen zusammenzutragen. Dies macht sich im Krisenfall deutlich bemerkbar und kann schwerwiegende Konsequenzen haben.

Bei Anhaltspunkten dafür, dass ein (ehemaliger) Mitarbeiter Geschäftsgeheimnisse kopiert oder gar an die Konkurrenz weitergibt, ist absolute Eile geboten. Besteht die Gefahr, dass Wettbewerber sich Kenntnisse von internen Informationen und Prozessen verschaffen, erfordert dies eine schnelle Reaktion seitens des Arbeitgebers, um weiteren Schaden abzuwenden. So sollte man neben arbeitsrechtlichen Maßnahmen (z. B. Kündigung, Freistellung etc.) umgehend prüfen, ob entweder zivilrechtliche Ansprüche auf Unterlassen und Datenlöschung gegen den Geheimnisverletzter oder Dritte geltend zu machen sind oder gar eine Strafanzeige zu stellen und auf Durchsuchungsmaßnahmen durch Staatsanwaltschaft und Kriminalpolizei hinzuwirken ist. All dies ist indes nur vielversprechend, wenn sich die dafür maßgeblichen Informationen zeitnah abrufen lassen.

CHECKLISTE: UNTERNEHMENSSEITIG EINZULEITENDE NOTFALLMASSNAHMEN

- ☐ Einschalten und Information weiterer beteiligter Abteilungen
- ☐ Prüfen und ggf. Sperren von Zugriff auf IT-Infrastruktur und E-Mail-Accounts
- ☐ Feststellen von Zugriffsmöglichkeiten auf Aktenbestände
- ☐ Dokumentation illegaler Zugriffe auf Geschäftsgeheimnisse
- ☐ Darlegung bestehender Sicherungsmaßnahmen
- ☐ Prüfen der Beteiligung Externer oder anderer Mitarbeiter
- ☐ Abwägen der Erstattung von Strafanzeige und Strafantrag
- ☐ Geltendmachen von Unterlassungsansprüchen nach § 6 GeschGehG
- ☐ Einleiten arbeitsrechtlicher Maßnahmen
- ☐ Geltendmachen von Schadensersatzansprüchen

Im Idealfall erfolgt die Koordination über die Personalabteilung des Unternehmens. Diese verfügt regelmäßig bereits über die notwendigen Erkenntnisse zu Dauer und Umfang der Beschäftigung, Abreden zur Nutzung der IT-Infrastruktur (bspw. die Bereitstellung von Firmenlaptops und -handys, Nutzungsbeschränkungen bei der E-Mail-Nutzung) und etwaigen arbeitsvertraglichen Vertraulichkeitsvereinbarungen. Darüber hinaus ist HR gerade in den sensiblen Phasen eines Beschäftigungsverhältnisses (z. B. Eigen- oder Fremdkündigung) involviert und verfügt daher über das notwendige Risikobewusstsein.

Weitere beteiligte Stellen sind die Rechtsabteilung, die Unternehmenssicherheit, der Compliance-Beauftragte, der Datenschutzbeauftragte und oftmals auch die IT-Abteilung.

5 DAS STRAFRECHT ALS CHANCE

Kann nachgewiesen werden, dass Geschäftsgeheimnisse i. S. d. § 2 Nr. 1 b) GeschGehG angemessen geschützt wurden und Mitarbeiter oder Dritte illegal Zugriff auf derartige Informationen erlangt haben, kommt eine Strafbarkeit der handelnden Akteure nach § 23 GeschGehG in Betracht. In Abs. 1 Nr. 3 ist der Fall einer Verletzung eines Geschäftsgeheimnisses durch einen Beschäftigten explizit unter Strafe gestellt:

VORSCHRIFT – § 23 ABS. 1 GESCHGEHG

Verletzung von Geschäftsgeheimnissen
„Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer zur Förderung des eigenen oder fremden Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber eines Unternehmens Schaden zuzufügen,
(...)
3. entgegen § 4 Absatz 2 Nummer 3 als eine bei einem Unternehmen beschäftigte Person ein Geschäftsgeheimnis, das ihr im Rahmen des Beschäftigungsverhältnisses anvertraut worden oder zugänglich geworden ist, während der Geltungsdauer des Beschäftigungsverhältnisses offenlegt."

Diese Strafnorm eröffnet einen bunten Strauß an Handlungsoptionen, die im Krisenfall ebenfalls in Erwägung gezogen werden sollten. Dabei steht in der wirtschaftsstrafrechtlichen Praxis regelmäßig nicht die Frage im Vordergrund, ob es schlussendlich zu einer strafrechtlichen Ahndung der involvierten Akteure kommt. Die Musik spielt hier im Ermittlungsverfahren. Die Regelungen der Strafprozessordnung erlauben es dem geschädigten Arbeitgeber nämlich, auch im Rahmen des Verfahrens die Interessen des Geheimnisinhabers zu wahren und aktiv zu verteidigen.

So lässt sich u. a. eine Strafanzeige platzieren, um Maßnahmen der Beweissicherung durch die ermittelnden Behörden zu erreichen. Dies kann von der Beschlagnahme (§§ 94 ff. StPO) bis hin zur Sicherung von Geschäftsunterlagen im Rahmen einer Durchsuchung (§§ 102 ff. StPO) reichen. Letztere kann auch bei Dritten erfolgen (z. B. einem Konkurrenzunternehmen), sofern belastbare Anhaltspunkte dafür bestehen, dass sich dort Beweismittel befinden.[4]

Der Verletzte einer Straftat kann darüber hinaus über einen Rechtsanwalt Einsicht in die Verfahrensakte nehmen (§ 406e Abs. 1 StPO) und so Erkenntnisse gewinnen, die für die zivilrechtliche Geltendmachung von Ansprüchen oder eine arbeitsrechtliche Auseinandersetzung dienlich sein können. Zudem helfen die Erfahrungen oft auch, für die Zukunft etwaige eigene Sicherheitslücken zu schließen.

Damit die Geschäftsgeheimnisse in einem Strafverfahren effektiv geschützt werden, kann ein Geschädigter einer Straftat nach § 23 GeschGehG auch als Nebenkläger in einer Hauptverhandlung auftreten (§ 395 Abs. 1 Nr. 6 StPO) und dort zahlreiche Verfahrensanträge stellen. Eine derartige Begleitung ist oft sinnvoll, weil Gerichtsverhandlungen im Regelfall öffentlich sind und Richter und Staatsanwälte zum Teil für die Thematik sensibilisiert werden müssen.[5]

Diese Handlungsoptionen sollten Personalabteilung und Geschäftsleitung in Erwägung ziehen, da sie regelmäßig einen Mehrwert für die eigene Rechtsdurchsetzung bieten können. Dabei sollte man auch berücksichtigen, dass etwaige voreilige eigene Schritte die Erfolgsaussichten strafprozessualer Maßnahmen beeinträchtigen könnten. Die Einbindung der Strafverfolgungsbehörden ist dabei wahrlich kein Automatismus und auch nicht immer ratsam. Dennoch lohnt es sich häufig, darüber vertieft nachzudenken. Vor allem bei der Weitergabe von sensiblen Unternehmensdaten (bspw. Kundenlisten, Kalkulationen, Konstruktionsplänen) sollten die ersten Schritte wohl bedacht sein. Hier werden die Weichen für das weitere Vorgehen gestellt.

6 FAZIT

Daten und vertrauliche Informationen sind oftmals das „Gold" der Zukunft. Sie zu schützen, ist nicht nur aus wirtschaftlichen Gründen sinnvoll, sondern auch rechtlich zwingend notwendig, um sich auf die effektiven Verteidigungsmöglichkeiten des GeschGehG berufen zu können. Diese sind durchaus vielfältig und setzen sich aus arbeits-, zivil- und strafrechtlichen Handlungsoptionen zusammen, die wohlbedacht eingesetzt und gewählt werden können.

FEEDBACK

Hat Ihnen der Beitrag gefallen? Sagen Sie uns Ihre Meinung! Alle Infos auf www.auaplus.de

UNSERE AUTOREN

Prof. Dr. Michael Fuhlrott
Rechtsanwalt, Fachanwalt für Arbeitsrecht, Partner, FHM Rechtsanwälte, Hamburg

Dr. Mayeul Hiéramente
Rechtsanwalt, Fachanwalt für Strafrecht, Partner, FHM Rechtsanwälte, Hamburg