PROF. DR. THOMAS HOEREN UND DR. REINER MÜNKER*

# Die neue EU-Richtlinie zum Schutz von Betriebsgeheimnissen und die Haftung Dritter

## A. Einführung

Mit der neuen EU-Richtlinie zum Schutz von Betriebsgeheimnissen[1] muss bis Juni 2018 ein völlig neues Regime zum Schutz von betriebsinternem Know-how geschaffen werden. Auch wenn das Bundesjustizministerium bislang keinen Entwurf veröffentlichen konnte, ist klar, dass sich hier ein neues Spezialgesetz zum Schutz von Betriebsgeheimnissen abzeichnet. Dieses Gesetz wird eine grundlegendere Reform, weit über den Rahmen von § 17 bis § 19 UWG hinaus, zur Folge haben. Neu sind vor allem die Vorstellungen aus Brüssel zur Haftung Dritter bei der Verletzung von Geheimhaltungsvereinbarungen, wie im Weiteren zu schildern sein wird.

## B. Die neue Regelung in Art. 4 Abs. 4 der Richtlinie

Art. 4 Abs. 4 der Richtlinie regelt, dass der Erwerb und die Ingebrauchnahme von Geschäftsgeheimnissen unrechtmäßig ist, wenn die Person zum Zeitpunkt des Erwerbs oder der Ingebrauchnahme weiß oder hätte wissen müssen, dass das Geschäftsgeheimnis direkt oder indirekt von einer anderen Person stammt, die ihrerseits das Geschäftsgeheimnis nach Art. 4 Abs. 3 unrechtmäßig benutzt oder offenlegt. Das Delikt ist nicht zu verwechseln mit § 17 Abs. 2 Nr. 1 UWG, welcher auch die Betriebsspionage Dritter regelt. Dort wird das Sichverschaffen oder Sichern eines Betriebsgeheimnisses sanktioniert, wenn es durch Anwendung technischer Mittel, Herstellung einer verkörperten Wiedergabe des Geheimnisses oder Wegnahme einer Sache, in der das Geheimnis verkörpert ist, geschieht. Es geht also nur um die Pönalisierung technischer Mittel, nicht um das Aushorchen von Mitarbeitern des Geheimnisinhabers.[2]

Die neue Regelung entspricht vielmehr der Geheimnishehlerei nach § 17 Abs. 2 Nr. 2 UWG. Zunächst muss ein Betriebsgeheimnis von dem Täter oder einem Dritten unbefugt erlangt worden sein. Dann geht es um die Mitteilung oder Verwertung dieses Wissens. Schwierig ist die „sonst unbefugte Verschaffung oder Sicherung des Geheimnisses". Die wiederholte Nutzung des gleichen Begriffs mit dogmatisch völlig unterschiedlichem Sinngehalt innerhalb derselben Vorschrift wird zu Recht in der Literatur als höchst fragwürdige Gesetzgebungstechnik bezeichnet.[3] Die Vortat muss nicht vom Täter des § 17 Abs. 2 Nr. 2 UWG selbst begangen worden sein, wenn es sich um eine Tat iSv § 17 Abs. 2 Nr. 1 UWG handelt. Die Vortat muss nur in den Fällen des § 17 Abs. 2 Nr. 2 Var. 1 und 2 UWG vorsätzlich begangen worden sein. Hingegen werden unter die generalklauselartige Var. 3 nicht zwingend nur vorsätzliche Formen der Erlangung gefasst. In diesem Fall ist die Strafnorm allerdings nur anwendbar, wenn es sich bei der Vortat bereits um eine eigene Handlung des Täters handelt.[4] Ausreichend ist die Kenntniserlangung mittels mehrerer Stationen, sog. Mitteilungsketten. Nur für § 17 Abs. 2 Nr. 2 Var. 3 UWG gilt etwas anderes, dort heißt es „sich unbefugt verschafft oder gesichert". Jede indirekte Nutzung fällt unter die Verwertung. Dabei bleiben Ergebnisse, die mittels solcher Erkenntnisse erzielt werden, von Anfang an und in der Regel dauerhaft mit dem Makel der Rechtswidrigkeit behaftet.[5] Im Falle der Verwendung von kaufmännischen Informationen könnte eine Verwertung von Kundendaten auch in der Kontaktaufnahme mit Kunden oder in der Einspeisung in die eigene Kundendatenbank bestehen.[6] Erforderlich sind subjektiv ein alle objektiven Tatbestandsmerkmale umfassender Vorsatz und das Hinzutreten besonderer Absicht. Es gibt keinen gutgläubigen Erwerb von Unternehmensgeheimnissen, da es hierfür an einem Rechtsscheinträger fehlt. Ab dem Zeitpunkt des Bösgläubigwerdens kann der Täter zur Verantwortung gezogen werden. Art. 39 Abs. 2 TRIPS sieht einen Geheimnisschutz gegen einen Dritten vor, wenn dieser bei Erwerb der Information wusste oder infolge grober Fahrlässigkeit nicht wusste, dass ein unlauterer Akt der Erlangung vorausging. TRIPS lässt mithin auch grobe Fahrlässigkeit genügen (Art. 39 Abs. 2 TRIPS iVm Fn. 10). § 17 Abs. 2 Nr. 2 UWG sieht jedoch zwingend Vorsatz vor und stellt somit höhere Anforderungen, weshalb das deutsche Recht als nicht TRIPS-konform angesehen wird.[7] *Kalbfus* schlägt zur Schließung dieser Schutzlücke vor, Art. 39 Abs. 2 TRIPS als Schutzgesetz iSv § 823 Abs. 2 BGB zu betrachten.[8]

Art. 4 Abs. 4 der Richtlinie stellt dies dadurch klar, dass unerheblich ist, ob der Dritte das Unternehmensgeheimnis unmittelbar oder nur mittelbar von dem Erstverletzer erlangt hat. Ein Dazwischentreten gutgläubig Handelnder schadet daher nicht. Der Makel der rechtswidrigen Vortat infiziert

---

* Prof. Dr. Thomas Hoeren ist Direktor der zivilrechtlichen Abteilung des Instituts für Informations-, Telekommunikations- und Medienrecht an der Westfälischen Wilhelms-Universität Münster. Dr. Reiner Münker ist Vorsitzender des Deutschen Schutzverbands gegen Wirtschaftskriminalität e. V. Die Autoren danken den studentischen Hilfskräften Leonhard Weitz und Nele Klostermeyer für die Mithilfe bei den Recherchen zu den Fußnotenbelegen.

1 Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates v. 8.6.2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung.

2 *Kalbfus*, Know-how-Schutz in Deutschland zwischen Strafrecht und Zivilrecht – welcher Reformbedarf besteht?, 2011, S. 134.

3 *Kalbfus*, Know-how-Schutz in Deutschland zwischen Strafrecht und Zivilrecht – welcher Reformbedarf besteht?, 2011, S. 137; MüKo-Lauterkeitsrecht/*Brammsen*, 2. Aufl. 2014, § 17 UWG Rn. 115.

4 *Kalbfus*, Know-how-Schutz in Deutschland zwischen Strafrecht und Zivilrecht – welcher Reformbedarf besteht?, 2011, S. 147 Fn. 653; MüKoLauterkeitsrecht/*Brammsen*, 2. Aufl. 2014, § 17 UWG Rn. 111.

5 BGH 19.3.2008 – I ZR 225/06, WRP 2008, 938 (939); BGH 19.12. 1984 – I ZR 133/82, GRUR 1985, 294 (296).

6 OLG Saarbrücken 24.7.2002 – 1 U 901/01, GRUR-RR 2002, 359.

7 *Kalbfus*, Know-how-Schutz in Deutschland zwischen Strafrecht und Zivilrecht – welcher Reformbedarf besteht?, 2011, S. 148; Beier/Schricker/*Krasser*, From GATT to TRIPs, 1996, S. 216, 224; *Reger*, Der internationale Schutz gegen unlauteren Wettbewerb und das TRIPS-Übereinkommen, 1999, S. 272; *Müller*, Der Schutz von Know-how nach dem TRIPS-Übereinkommen, 2003, S. 145; für eine Modifikation des Tatbestandes *Amelunxen* DB 1983, 2347 (2348).

8 *Kalbfus*, Know-how-Schutz in Deutschland zwischen Strafrecht und Zivilrecht – welcher Reformbedarf besteht?, 2011, S. 149.

die gesamte Kette.[9] Mangels Publizität des Geschäftsgeheimnisses kann dem Gutgläubigen daher allein aufgrund von Erwerb, Nutzung oder Offenlegung kein Unlauterkeitsvorwurf gemacht werden. Das Kenntniskriterium beseitigt die Nähe des Betriebsgeheimnisses zum Ausschließlichkeitsrecht, indem es die Unlauterkeit der Handlung des passiven Empfängers und damit die Rechtswidrigkeit des Handelns begründet. Erst das Wissen oder grob fahrlässige Nichtwissen um die rechtswidrige Vortat begründet die Unlauterkeit der Handlung. Für die Handlung des Erstverletzers war nach Art. 39 Abs. 2 TRIPS Vorsatz oder grobe Fahrlässigkeit gefordert, wohingegen die Handlung des Dritten jetzt bereits rechtspflichtwidrig sein soll, wenn er wusste oder „unter den gegebenen Umständen" hätte wissen müssen, dass eine rechtswidrige Vortat bestand. Wegen ungerechtfertigter Wertungswidersprüche schlägt die Literatur vor, grobe Fahrlässigkeit zu verlangen.[10] Dies soll aus der Formulierung „unter den gegebenen Umständen" ableitbar sein. Die Nachforschungspflichten seien wertungsmäßig bei einfacher Fahrlässigkeit für den Dritten unzumutbar.[11] Das würde auch einen Gleichlauf mit § 932 Abs. 2 BGB bringen. Nachforschungspflichten dürften nach dieser Ansicht erst entstehen, wenn sich Anhaltspunkte für die Unlauterkeit der Ersthandlung ergeben. So sinnvoll auch ein Gleichlauf mit den Wertungen des TRIPS-Abkommens ist, spricht der Wortlaut der Richtlinie gegen diese Literaturmeinungen. Die Richtlinie spricht ausdrücklich von Vorsatz oder Fahrlässigkeit und kennt die Einschränkung der Fahrlässigkeit auf den Spezialfall der groben Fahrlässigkeit nicht. Dementsprechend kommen für die betroffenen Unternehmen eine Fülle von Compliance-Pflichten neu hinzu, wie im Folgenden dann noch zu spezifizieren sein wird.

## C. Die erweiterte Haftung des Produzenten

Nach Art. 4 Abs. 5 der Richtlinie ist die Produktion, das Angebot oder die Vermarktung von rechtsverletzenden Produkten oder der Import oder Export rechtsverletzender Güter ein unrechtmäßiger Gebrauch eines Geschäftsgeheimnisses, wenn die Person, die diese Aktivitäten durchführt, weiß oder hätte wissen müssen, dass das Geschäftsgeheimnis unrechtmäßig benutzt wurde iSv Art. 4 Abs. 3 der Richtlinie.

Die Vorschrift ist schwer zu verstehen. Was sind „infringing goods"? Muss das Produkt unter Verletzung des Geschäftsgeheimnisses produziert worden sein? Man nehme zum Beispiel den Fall, dass jemand von einem ehemaligen Angestellten der Konkurrenz die Kundendaten nutzt, um seine Produkte besser auf dem Markt zu platzieren. Das Produkt ist insofern unverdächtig, als es eklatant nicht unter Verletzung eventueller Markenrechte erstellt worden ist. Damit ist die Vermarktung von Produkten, die fremde Geschäftsgeheimnisse beinhalten, regelmäßig auch eine Verwertung und Ingebrauchnahme fremder Geschäftsgeheimnisse und damit selbst ein Verstoß gegen Art. 4 Abs. 4 der Richtlinie.

Anders als zuvor ist im Rahmen des Art. 4 Abs. 5 der Richtlinie nicht die Nutzung des Unternehmensgeheimnisses, sondern die Nutzung rechtsverletzender Produkte iSv Art. 2 Nr. 4 erforderlich. Es genügt, wenn der nach Art. 4 Abs. 5 Handelnde die Produkte, die auf Grundlage des Unternehmensgeheimnisses von einer anderen Person genutzt werden, in Serie produziert, anbietet, in den Verkehr bringt oder sie für diese Zwecke importiert, exportiert oder lagert. Ziel ist es, den Wiedereintritt rechtsverletzender Produkte in die EU zu unterbinden.[12] Den rechtsverletzenden Produkten ist stets zu eigen, dass sie durch die Nutzung von rechtswidrig erworbenen, offengelegten oder genutzten Unternehmensgeheimnissen entstanden sind. Die persönliche Vorwerfbarkeit und damit ein Rückbezug zur Lauterkeit wird erst durch das Erfordernis der Kenntnis oder grob fahrlässigen Unkenntnis geschaffen. Die Norm setzt daher sowohl einen Makel des Produkts als auch ein unlauteres Verhalten voraus.

## D. Spezifische Sorgfaltspflichten für externe Unternehmen

Für ein externes Unternehmen ist es wichtig, die eigenen Sorgfaltspflichten für den Umgang mit Geheimnisträgern genauestens zu bestimmen und in die Praxis umzusetzen.

### I. Festlegung des Status quo

Dies setzt zunächst eine Festlegung des Status quo voraus. Es bedarf zunächst einer Form der Klassifizierung von Geheimnissen als riskant und besonders geheimnisträchtig. In diese permanent zu aktualisierende Liste gehören Kundendaten, Fabrikationspläne, Konstruktionszeichnungen, der Source Code nebst interner Dokumentation des Programmierers und die Verzeichnisse mit den internen Zulieferern. Es ist unerlässlich für das Unternehmen, genau zu wissen, wer Geheimnisträger ist und mit welchen Geheimnissen diese Person umgeht. Dazu kommt eine Analyse der Datenströme, was die Verteilung eines Geheimnisses angeht. Im Grunde ähnelt dieser Pflichtenkatalog insoweit dem Datenschutzrecht und dem dort angesiedelten Verfahrensverzeichnis. Allerdings weiß man auch aus dem Datenschutzrecht, wie viel Arbeit, Kosten und Mühen in einem gelungenen und vollständigen Verfahrensverzeichnis liegen kann. Außerdem muss dieses Verzeichnis kontinuierlich weitergepflegt werden, was bei Unternehmen ab gewissen Größenordnungen und flexiblem Einsatzfeld schwierig sein dürfte. Letztendlich kann man dies nur mithilfe eines eigenen Geheimnisschutzbeauftragten und eventuell einem dazugehörigen Team realisieren. Außerdem setzt ein solches Verfahren ein entsprechendes Klassifizierungssystem für geheimnisträchtige Dokumente voraus, mit dem diese Dokumente abhängig von Risikoklassen eingestuft werden. Zu bestimmen ist auch, in welchen Organisationseinheiten des Unternehmens der Geheimnisschutz eine besondere Rolle spielt. Datensensible Bereiche können insbesondere die Bereiche Forschung und Entwicklung wie auch M&A sein. Gefährdet ist auch die Vertriebsabteilung wegen der Kundendaten. In der Matrix gilt es auch zu bestimmen, welche Mitarbeiter anfällig sind für Geheimnisverrat.

9 *Wiese*, Die EU-Richtlinie über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen, 2017, S. 142; *Heinzke* CCZ 2016, 179 (181).

10 *Wiese*, Die EU-Richtlinie über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen, 2017, S. 147.

11 *Wiese*, Die EU-Richtlinie über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen, 2017, S. 147.

12 So Erwägungsgrund 28, Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates v. 8.6.2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung.

Genauere Identifizierungsmöglichkeiten bietet auch die digitale Klassifizierung der Herkunft von Datenträgern und Dateien. Es bieten sich Digital Rights Managementsysteme oder die Kennzeichnung von Dokumenten über Metadaten an. USB-Sticks oder DVDs sollten als eindeutig vom Unternehmen stammend bezeichnet werden. Wichtig ist auch, dass die allgemein anerkannten Standards der Datensicherheit und Informationssicherheit eingehalten werden. Besondere Blicke sollten dabei auf die Versendung verschlüsselter E-Mails gerichtet werden. Ähnlich sensibel ist die Nutzung privater Gerätschaften für die Speicherung und Weitergabe von Unternehmensdaten. Insofern ist die Diskussion um Geheimnisschutz auch eine allgemeine Kontroverse zur Sensibilisierung für den Schutz von Information gegen unbefugte Nutzung etwa durch Hacker oder mittels Viren. Die im Arbeitsvertrag zu regelnden Geheimhaltungspflichten sind nicht nur zu sanktionieren, sondern auch als Anreiz für die Motivation von Arbeitnehmern zu verstehen. Es bedarf einer Unternehmenskultur des Geheimnisses, welche auch Anreize für die Arbeitnehmer zur Einhaltung der Geheimnisschutzbestimmungen gibt. Es geht hier um die Sensibilisierung der Arbeitnehmer bei ihrer täglichen Nutzung der Daten und die Entwicklung eines Gespürs im Unternehmen. Hier sollte auch über die Rechtsabteilung oder die Compliance-Abteilung ein Ansprechpartner für Zweifel an der Rechtmäßigkeit benannt werden. Dieser Beauftragte hat die Mitarbeiter entsprechend aktuell zu schulen und die Regelwerke und Richtlinien entsprechend laufend aktuell zu halten.

## II. Der neue Mitarbeiter und der Input in das Unternehmen

Dann bedarf es über den Status quo auch einer Kanalisierung, was den Input in das Unternehmen angeht. Wenn ein Arbeitnehmer wechselt, muss das neue Unternehmen als Basisprinzip den neuen Beschäftigten ausdrücklich darauf hinweisen, dass dieser keine Dokumente und Dateien vom alten Arbeitgeber in das neue Beschäftigungsverhältnis mitnehmen darf. Hinzuweisen ist auch auf denkbare Folgen einer solchen Mitnahme und Einbringung bis hin zur Kündigung des neuen Arbeitnehmers. Gern gesehen sind ausgeschiedene Mitarbeiter, weil sie ihre aus der früheren Anstellung erhaltenen Erfahrungen auch später beim neuen Arbeitgeber einsetzen dürfen. Dem Mitarbeiter ist aber verwehrt, auf Unterlagen zurückzugreifen, die er während der Beschäftigungszeit verfasst hat. Es bedarf daher besonderer Richtlinien und Verhaltenskodizes für neu eingestellte Mitarbeiter.

## III. Der Output und der ausgeschiedene Arbeitnehmer

Das Gleiche gilt für den Output. Hier muss festgelegt werden, dass der ausscheidende Arbeitnehmer alle Dateien und Texte zu löschen hat. Zu löschen sind auch alle alten E-Mails, zumindest was den Zugriff des alten Arbeitnehmers betrifft. Sieht der Unternehmer, dass der Arbeitnehmer wechseln will, muss spätestens nach diesem Zeitpunkt eine Kontrolle des Arbeitsplatzes möglich sein, mit einem Verbot der Verwendung von USB-Sticks und unter Ausschluss der Nutzung externer IT-Strukturen.

Es bedarf auch in einem Arbeitsvertrag von vornherein der Regelung von nachvertraglichen Geheimhaltungspflichten, wobei auf eine möglichst einfache Beschreibung der Strafbarkeitsrisiken, kombiniert mit einfachen Fällen und Verhaltenshinweisen, geachtet werden sollte. Bei den nachvertraglichen Pflichten können die Pflichten im Arbeitsvertrag konkret benannt werden oder sich allgemein aus dem Arbeitsvertrag ergeben. Die Wirksamkeit von nachvertraglichen Geheimhaltungspflichten scheitert in der Regel am Grundsatz der Wissensfreiheit bei dem Arbeitgeberwechsel.

Besondere Umstände,[13] die ausnahmsweise eine Geheimhaltungsvereinbarung auch ohne ausdrückliche Regelung zulassen, sind:

- die Stellung des Arbeitnehmers im Unternehmen,
- dessen langjährige Betriebszugehörigkeit,
- die Herkunft der Informationen (hat der Arbeitnehmer diese selbst generiert oder nur kopiert?).

Zu bedenken ist auch, dass uU der Arbeitnehmer seine eigene Kündigung provoziert hat, um sein Wissen möglichst effizient an anderer Stelle wieder einsetzen zu können. Auch in der Entscheidung des BGH zu Industrieböden[14] wurde anerkannt, dass ausnahmsweise auch eine Nachwirkung dienstvertraglicher Pflichten, insbesondere der Pflicht zur Verschwiegenheit, in Betracht kommt. Auch das Bundesarbeitsgericht[15] geht davon aus, dass der ausscheidende Beschäftigte auch ohne entsprechende Geheimhaltungsvereinbarung auf Grund nachwirkender Treuepflicht arbeitsrechtlich zur Verschwiegenheit über Geschäfts- und Betriebsgeheimnisse verpflichtet ist. Ihm sei nur die Verwertung des erworbenen „Erfahrungswissens" gestattet.

Als allgemein bekannt sei vorausgesetzt, dass das deutsche Recht Wettbewerbsverbote zulasten des ehemaligen Arbeitnehmers nur gegen Zahlung einer großzügig bemessenen Karenzentschädigung vorsieht.[16] Daher sollte man sinnvollerweise eher eine Geheimhaltungsvereinbarung wählen als ein Wettbewerbsverbot.

## IV. Das Geheimhaltungsverbot zwischen den Unternehmen

Diese Geheimhaltung ist auch beim Arbeitnehmerwechsel im Vertrag zwischen dem alten Unternehmen und dem neuen Unternehmen so zu regeln, dass die Weitergabe der Betriebsgeheimnisse des alten Arbeitgebers strafbewehrt untersagt wird. Schwierigkeiten macht allerdings die Bemessung einer angemessenen Vertragsstrafe. Allgemeingültige Beträge können einzelfallbedingt nicht genannt werden. Zu bedenken ist, dass nach § 348 HGB im kaufmännischen Verkehr eine Herabsetzung der eventuell zu hohen Vertragsstrafe nicht zulässig ist.[17] Zu bedenken ist auch, dass der Geheimnisbereich für das betroffene Unternehmen sehr sensibel ist; Geheimnisse sind keine Geheimnisse mehr, wenn sie verraten werden.

Zu bedenken sei auch das Instrument eines Abwerbeverbots. Ein solches Verbot könnte zwar mit § 75 f HGB kolli-

13 Harte-Bavendamm/Henning-Bodewig/*Harte-Bavendamm*, UWG, 4. Aufl. 2016, § 17 Rn. 54.
14 BGH 21.12.1962 – I ZR 47/61, NJW 1963, 856.
15 BAG 15.12.1987 – 3 AZR 474/86, NZA 1988, 502; BAG 15.6.1993 – 9 AZR 558/91, NZA 1994, 502; BAG 19.5.1998 – 9 AZR 394/97, NZA 1999, 200; ausführlich zur Rechtsprechung des BAG Harte-Bavendamm/Henning-Bodewig/*Harte-Bavendamm*, UWG, 4. Aufl. 2016, § 17 Rn. 55.
16 ErfK/*Oetker*, 18. Aufl. 2018, § 74 HGB Rn. 15.
17 Baumbach/Hopt/*Hopt*, HGB, 37. Aufl. 2016, § 348 Rn. 6.

dieren, der schon nach früherer Rechtsprechung analoge Anwendung fand, wenn es sich bei den betroffenen Mitarbeitern nicht um Handlungsgehilfen gem. § 59 HGB handelte.[18] Ein derartiges Verbot hat der BGH in einer neueren, am 22.9.2014 veröffentlichten Entscheidung[19] auch auf Abwerbeverbote Business-to-Business angewendet. Der Senat lässt aber Ausnahmen von dem Verbot zu. So soll § 75 f HGB nicht Anwendung finden, wenn das vertragliche Abwerbeverbot nicht hauptsächlich ist und einem besonderen Vertrauensverhältnis der Parteien oder einer besonderen Schutzbedürftigkeit einer der beiden vertragschließenden Seiten Rechnung trägt. Hier kommen wieder die EU-Richtlinie und der besondere Akzent im künftigen Recht auf den Geheimhaltungsvereinbarungen zum Tragen. Wenn das abgeworbene Unternehmen durch hinreichend konkrete Geheimhaltungsvereinbarungen deutlich macht, dass bestimmte Informationen und Unterlagen besonders schutzbedürftig sind, rechtfertigt es damit auch die Reichweite eines zulässigen Abwerbeverbotes. Als bspw. zulässige Abwerbeverbote nennt der BGH auch „Abwerbeverbote, die bei Risikoprüfung vor dem Kauf von Unternehmen oder Unternehmensbeteiligungen vereinbart werden", Abwerbeverbote „bei einer Abspaltung von Unternehmensteilen oder Konzerngesellschaften" sowie Abwerbeverbote „bei Vertriebsvereinbarungen zwischen selbstständigen Unternehmen".[20] Zu beachten ist auch, dass nach Auffassung des BGH solche Abwerbeverbote nur nach Maßgabe einer zeitlichen Obergrenze von zwei Jahren zulässig sind. Insofern verweist der BGH auf die Rechtsprechung zu nachvertraglichen Wettbewerbsverboten und Kundenschutzklauseln sowie auf § 74 a Abs. 1 S. 3 HGB.

## E. Fazit und Konsequenzen

Es kommen also spätestens ab Juni 2018 auf die beteiligten Unternehmen sehr hohe Compliance-Pflichten in Bezug auf den Schutz von Geheimnissen zu. Maßnahmen zur Umsetzung sollten eher früher als später eingeführt und konsequent implementiert werden. Die Checkliste für notwendige Tätigkeiten ist lang und ohne die Bereitstellung eines spezialisierten Geheimnisbeauftragten wohl kaum zu meistern.

**KONTAKT:**

Prof. Dr. Thomas Hoeren
Universität Münster
Institut für Informations-, Telekommunikations- und Medienrecht (ITM)
Leonardo-Campus 9
48149 Münster
Tel.: 0251/8338600
Fax: 0251/8338601
hoeren@uni-muenster.de

Dr. Reiner Münker
Geschäftsführendes Vorstandsmitglied
Deutscher Schutzverband gegen Wirtschaftskriminalität e.V.
Landgrafenstraße 24 B
61348 Bad Homburg
Tel.: 06172/121530
Fax: 06172/84422
muenker@wettbewerbszentrale.de

18 BGH 30.4.1974 – VI ZR 153/72, NJW 1974, 1282; BGH 27.9.1983 – VI ZR 294/81, NJW 1984, 116.
19 BGH 30.4.2014 – I ZR 245/12, NJW 2014, 3442.
20 BGH 30.4.2014 – I ZR 245/12, NJW 2014, 3442 (3445).

RECHTSANWALT VOLKER STÜCK*

# Überwachung und Kontrolle von Arbeitnehmern nach neuer Rechtsprechung – Empfehlungen für Arbeitgeber im Brennpunkt von Compliance, Datenschutz und Arbeitsrecht

## A. Grundsätze des BAG zur Überwachung von Arbeitnehmern

Führt der Arbeitgeber Überwachungsmaßnahmen oder Kontrollen zur Prävention oder Aufklärung von Compliance-Verstößen durch, muss er darauf achten, dass er sich dabei nicht selbst incompliant verhält, was bei einem schweren Verstoß ggf. ein Beweisverwertungsverbot zur Folge haben könnte, wenn durch die Verwertung im Prozess erneut Persönlichkeitsrechte verletzt würden.[1] Hierzu und zum Beschäftigtendatenschutz hat das BAG in jüngster Zeit in mehreren Entscheidungen wichtige Grundsätze aufgestellt und Präzisierungen vorgenommen, die Geschäfts-/Personalleitung und Compliance Officer kennen und beachten sollten. Dies insbesondere vor dem Hintergrund der am 25.5.2018 in Kraft tretenden Änderungen im Datenschutz durch Art. 88 DSGVO bzw. des § 26 BDSG nF (= § 32 BDSG aF) sowie deutlich verschärften Sanktionen, insbesondere deutlich erhöhten Bußgeldern

* Der Autor ist Leiter Personal & Compliance Beauftragter Hochspannungsprodukte (PGHV) der ABB AG in Hanau. Er ist Verfasser zahlreicher arbeitsrechtlicher Aufsätze, Urteilsbesprechungen, Referent, Mitautor eines Kommentars zum Berufsbildungsgesetz und Mitherausgeber eines Personal Online Moduls. Der Beitrag gibt seine persönliche Auffassung wieder.

1 BAG 13.12.2007 – 2 AZR 537/06, NJW 2008, 2732 = NZA 2008, 1008 = DB 2008, 1633; Plath/*Stahmer/Kuhnke*, BDSG/DSGVO Kommentar, 2. Aufl. 2016, § 32 BDSG Rn. 139 f.