www.compliance-berater.de

CB

Compliance Berater

BEWÄHRTE QUALITÄT 5 JAHRE Compliance-Berater BEWÄHRTE QUALITÄT

6 / 2019

Betriebs-Berater Compliance

29.5.2019 | 7.Jg
Seiten 181–224

Fachmedien Recht und Wirtschaft | dfv Mediengruppe | Frankfurt am Main

CB-BEITRAG

Christian Graßie, RA, und Dr. Mayeul Hiéramente, RA

Praxisprobleme bei der IT-Durchsuchung

Im Zeitalter der multimedialen Kommunikation und Datenarchivierung stehen mittlerweile regelmäßig die digitalen Speichermedien und Kommunikationssysteme im Fokus der staatlichen Ermittlungen. Längst sind die Strafverfolgungsbehörden dazu übergegangen, IT-Forensiker anzustellen, welche die Durchsuchungsmaßnahmen begleiten und die staatlichen Ermittlungsbehörden vor Ort bei der Suche und Sicherstellung von Daten unterstützen. Hierdurch entstehen für Unternehmen in der Praxis besondere Herausforderungen.

I. Einleitung

Längst gehören Strafverfahren gegen Verantwortliche und leitende Angestellte von Unternehmen zum Alltag des deutschen Wirtschaftsstrafrechts. Die Zahl der diesbezüglichen Ermittlungsverfahren ist in den vergangenen Jahren stark angestiegen. Unternehmerische Entscheidungen werden seitens staatlicher Ermittlungsbehörden vermehrt unter dem Blickwinkel des Strafrechts geprüft. Neben der Verhängung von Strafen gegen die beteiligten Individualpersonen droht den betroffenen Unternehmen regelmäßig die Festsetzung einer Verbandsgeldbuße nach den Vorschriften des Ordnungswidrigkeitenrechts (§§ 30, 130 OWiG). Ausgangspunkt vieler staatlicher Ermittlungsverfahren ist die Durchsuchung bei den betroffenen Individualpersonen oder Unternehmen. Ziel der Ermittlungsbehörden ist die umfassende Sicherstellung von Beweismitteln bereits zu Beginn des Verfahrens. Insbesondere bei geschäftlichen Vorgängen, die längere Zeit zurück liegen, soll so der Verlust von Geschäftsunterlagen und Daten mit Verfahrensrelevanz verhindert werden.

II. Die IT-Durchsuchung nach §§ 102 ff. StPO

Die Zulässigkeit einer (IT-) Durchsuchung richtet sich nach den Vorschriften der §§ 102 ff. StPO. Danach ist es den Ermittlungsbehörden gestattet, die Räumlichkeiten oder Gegenstände eines Beschuldigten (§ 102 StPO) oder unbeteiligten Dritten (§ 103 StPO) zu durchsuchen, soweit dies dem Auffinden von Beweismitteln dient und ein entsprechender Anfangsverdacht für die Begehung einer konkreten Straftat vorliegt. In der Praxis werden dabei an die Voraussetzungen des Verdachtsgrades keine überspannten Anforderungen gestellt. Ausreichend ist bereits das Vorliegen eines sogenannten Anfangsverdachts, mithin zureichende tatsächliche Anhaltspunkte dafür, dass strafbares Verhalten gegeben ist. Den Ermittlungsbehörden kommt bei der Beurteilung ein weitreichender Ermessensspielraum zu. Als taugliches Durchsuchungsobjekt kommen sowohl Wohn- und Geschäftsräumlichkeiten als auch Personen und Sachen in Betracht. Umfasst sind dabei auch EDV-Anlagen und Datenträger. Die Strafprozessordnung differenziert insofern nicht.

Soweit im Rahmen der Durchsuchung seitens der Ermittlungsbehörden Beweismittel aufgefunden werden, die für die strafrechtliche Untersuchung von Bedeutung sein können, dürfen diese nach § 94 StPO sichergestellt werden. Für den Fall, dass die Beweismittel nicht freiwillig herausgegeben werden, erfolgt deren Beschlagnahme gemäß §§ 94 Abs. 2, 98 StPO. Die Vorschriften der Sicherstellung und Beschlagnahme finden dabei sowohl auf bewegliche (Schriftstücke, Urkunden etc.) als auch auf unbewegliche (Grundstücke, Räume etc.) Gegenstände Anwendung. Als bewegliche Gegenstände i. S. d. § 94 StPO gelten hierbei auch Datenträger sowie die darauf gespeicherten digitalen Informationen.[1] Insofern hat bereits das Bundesverfassungsgericht entschieden, dass die §§ 94 ff. StPO eine hinreichende Ermächtigungsgrundlage für die Sicherstellung und Beschlagnahme von Datenträgern und den darauf vorhandenen Daten darstellen.[2] Das gilt auch für die Sicherstellung und Beschlagnahme von E-Mails, die auf dem Mailserver eines Providers zwischen- oder endgespeichert sind.[3]

Beschränkt werden die Eingriffsnormen der Durchsuchung (§§ 102 ff. StPO) sowie der Sicherstellung und Beschlagnahme (§§ 94 ff. StPO) durch den Verhältnismäßigkeitsgrundsatz. Bei der Sicherstellung und Beschlagnahme von Datenträgern und den darauf vorhandenen Daten ist daher wegen der hohen Eingriffsintensität seitens der Ermittlungsbehörden darauf zu achten, dass ein Zugriff auf für das Ermittlungsverfahren bedeutungslose Informationen und vertrauliche Daten unbeteiligter Dritter im Rahmen des Vertretbaren vermieden wird.[4] Ferner ist zu prüfen, ob die Anfertigung von Kopien der verfahrensrelevanten Daten für den Ermittlungszweck ausreichend ist.[5]

III. Praxisprobleme in der Durchsuchungssituation im IT-Bereich

Die schiere Masse der auf Unternehmensservern, Computern und Mobilfunkgeräten gespeicherten Daten sowie die Streubreite von Ermittlungen im digitalen Raum stellen die Praxis immer wieder vor große Herausforderungen. Hinzu kommt, dass die relevanten Normen

1 *Meyer-Goßner/Schmitt*, 61. Aufl. 2018, § 94 Rn. 4.
2 BVerfG, 12.4.2005 – 2 BvR 1027/02, NJW 2005, 1917, 1919.
3 BVerfG, 16.6.2009 – 2 BvR 902/06, NJW 2009, 2431, 2434.
4 BVerfG, 12.4.2005 – 2 BvR 1027/02, NJW 2005, 1917, 1921.
5 *Park*, Durchsuchung und Beschlagnahme, 4. Aufl. 2018, S. 210 m. w. N.

der StPO (§§ 94 ff., 102 ff. StPO) die virtuelle Durchsuchung und Dokumentensichtung zwar grundsätzlich erfassen, allerdings weder passgenau noch anwendungsfreundlich sind. Daher sollen hier die wichtigsten Themenfelder dargestellt werden, mit denen sich Geschäftsleitung und Rechtsabteilung von Unternehmen im Falle einer Durchsuchungssituation konfrontiert sehen.

1. Sichtung, Selektion, Spiegelung

Die Beschlagnahme von großen Datenmengen fällt den Ermittlungsbehörden naturgemäß leichter, als kistenweise Aktenordner abzutransportieren und händisch auszuwerten. Die Sicherung eines E-Mail-Accounts, ganzer Verzeichnisse oder gar Festplatten ist eine verfahrensökonomische Leichtigkeit. Dieser Umstand verleitet die Ermittler häufig dazu, bei der Sicherung von Daten zunächst großzügig vorgehen zu wollen. Bei einer Unternehmensdurchsuchung nach § 103 StPO sind den Ermittlungsbehörden indes auch hier tatsächliche und rechtliche Grenzen gesetzt. Die praktische Handhabbarkeit großer Datenmengen (mit Blick auf eine später erforderliche Auswertung) als auch der Verhältnismäßigkeitsgrundsatz gebieten eine gewisse Zurückhaltung.

Bevor großflächig Daten sicherstellt oder beschlagnahmt werden, hat regelmäßig eine Sichtung der jeweiligen Daten zu erfolgen (vgl. § 110 StPO), um deren Verfahrensrelevanz bestimmen zu können. Klassischerweise erfolgt diese Sichtung durch IT-Forensiker des LKA, die sich, während die Kollegen mit der physischen Durchsuchung der Unternehmensräumlichkeiten beschäftigt sind, einen Überblick über die unternehmensinterne Datenstruktur verschaffen. Im Idealfall kann die Sichtung bereits während der laufenden Durchsuchungsmaßnahme abgeschlossen und eine Sicherung auf die vom Durchsuchungsbeschluss erfassten Daten beschränkt werden. Teilweise erfolgt eine Sichtung anhand von Suchbegriffen und mittels des Einsatzes spezieller forensischer Software (z. B. X-ways Forensics).[6] Gelingt eine Sichtung vor Ort aufgrund der Komplexität der IT-(Infra-)Struktur nicht oder erschweren Zugangssicherungen und der Einsatz spezieller Datenmanagement-Software die Sichtung, hat dies zumeist eine „vorläufige Sicherstellung“[7] eines größeren Datensatzes zur Folge. Die Sichtung wird dann in der Regel in den Räumlichkeiten der Ermittlungsbehörden fortgesetzt.[8] Diese Sichtung dient der Selektion der erforderlichen Beweismittel und soll gewährleisten, dass nur diejenigen Daten sichergestellt oder beschlagnahmt werden, die verfahrensrelevant sind.

Da Sicherstellung und Beschlagnahme regelmäßig bis zum Abschluss des Verfahrens – mithin mehrere Jahre – aufrechterhalten werden können, soll eine frühzeitige Selektion einen extensiven Zugriff auf Unternehmensinterna unterbinden. Den Behörden ist eine Sicherstellung und Beschlagnahme von Datenmassen, deren potentielle Beweiserheblichkeit nicht überprüft wurde, rechtlich untersagt.[9] Eine scharfe Abgrenzung bereitet jedoch gerade zu Beginn eines Verfahrens häufig Schwierigkeiten. Zu Unrecht beschlagnahmte Daten sind grundsätzlich herauszugeben oder zu löschen.[10] Auf die Einhaltung dieser Maßgaben kann entweder im Dialog mit der Staatsanwaltschaft, z. B. mittels einer gemeinsamen Sichtung von sog. „Datencontainern“, oder auf dem formalen Weg mittels gerichtlicher Überprüfung nach § 98 Abs. 2 S. 2 StPO bzw. im Wege der Beschwerde nach § 304 StPO hingewirkt werden.

Die Art und Weise der Datensicherung hängt vom Einzelfall ab. Insbesondere bei technischen Geräten, die weiterhin durch Unternehmensmitarbeiter genutzt werden sollen, ist es aus Verhältnismäßigkeitsgründen regelmäßig geboten, dass die Behörden eine forensische Datensicherung (Spiegelung) erstellen und das Original zur weiteren Nutzung herausgeben.[11] Ob ein solches Vorgehen bereits in der konkreten Durchsuchungssituation vor Ort möglich ist, hängt stark von der handelnden Behörde ab. Auch bei der Sicherung von Daten eines Unternehmensservers wird regelmäßig eine Datensicherung auf einer Festplatte des LKA erfolgen, so dass es einer Beschlagnahme des Originals nicht bedarf.

2. Die Dokumentation der Datensicherung

Ein gängiges Praxisproblem bei der Sicherstellung und Beschlagnahme von Daten ist die unzureichende Dokumentation der behördlichen Beweiserhebung. Zwar wird im Anschluss an die Durchsuchung regelmäßig ein „Sicherstellungsverzeichnis“ ausgehändigt. Der Betroffene hat nach § 107 S. 2 StPO das Recht „ein Verzeichnis der in Verwahrung oder in Beschlag genommenen Gegenstände“ zu verlangen. Während dort in der Regel physische Gegenstände (Ordner, Mobiltelefone, Laptops etc.) aufgelistet und beschrieben werden, findet sich im Hinblick auf die IT-Durchsuchung meist nur der pauschale Hinweis, es habe eine Datensicherung auf einer behördeneigenen Festplatte stattgefunden. In (seltenen) Fällen findet man in der Akte einen Screenshot, aus dem sich die ungefähre Verzeichnisstruktur bzw. die betroffenen Dateinamen erahnen lassen.

Das Fehlen einer nachvollziehbaren Dokumentation erschwert in der Praxis die Geltendmachung von Beschlagnahmeverboten (z. B. wegen fehlender Verfahrensrelevanz) und Löschungsansprüchen massiv. Daher ist im Rahmen der Durchsuchung auf jeden Fall für eine eigenständige, parallele Dokumentation des Datenzugriffs (z. B. durch IT-Mitarbeiter des Unternehmens) Sorge zu tragen. Daneben ist oftmals auch ein Dialog mit der Staatsanwaltschaft zielführend. So erklären sich einige Staatsanwaltschaften auf Nachfrage bereit, dem Betroffenen eine Kopie der von ihnen erstellten Datensicherung zur Verfügung zu stellen, damit dieser Inhalt und Ausmaß des Grundrechtseingriffs mit seinen Anwälten bewerten und über die weitere Vorgehensweise entscheiden kann.

3. Die Datensichtung auf externen Servern

In Zeiten stetig wachsender Datenmengen werden Daten und Datenverarbeitungsprozesse immer häufiger – z. B. in eine Cloud – ausgelagert oder zentral bei einer Konzerngesellschaft angesiedelt. So lassen sich IT-Infrastrukturkosten reduzieren und eine einheitliche Datenspeicherung und -sicherung gewährleisten. Dies hat zur Folge, dass vor allem archivierte Datenbestände nicht immer „in den Räumlichkeiten“ des Durchsuchungsobjekts gelagert sind. Diesem Umstand trägt die Strafprozessordnung in § 110 Abs. 3 StPO Rechnung.[12] Diese Regelung ermächtigt die Ermittlungsbehörden zum Zugriff auf externe Speichermedien, sofern auf diese von einem Speichermedium in den durchsuchten Räumlichkeiten zugegriffen werden kann.[13] Der Zugriff auf inländische externe Server oder die Cloud ist daher grund-

6 Zu den Risiken siehe *Hiéramente*, wistra 2016, 432.
7 Siehe hierzu *Hauschild*, in: MüKo-StPO, 1. Aufl. 2014, § 110 Rn. 8 ff.
8 Zur Frage des Anwesenheitsrechts siehe *Peters*, NZWiSt 2017, 465 m. w. N.
9 BVerfG, 12.4.2005 – 2 BvR 1027/02,, NJW 2005, 1917, 1920 f.
10 *Hiéramente/Basar*, NStZ 2018, 681.
11 *Greven*, in: KK-StPO, 7. Aufl. 2013, § 94, Rn. 4.
12 Vgl. auch *Bär*, Handbuch Wirtschafts- und Steuerstrafrecht, 4. Aufl. 2014, 27. B. Rn. 23 ff.
13 Zu den möglichen Grenzen siehe *Burhoff*, Handbuch für das strafrechtliche Ermittlungsverfahren, 8. Aufl. 2019, Rn. 1739.

sätzlich von der Durchsuchungsbefugnis des im Durchsuchungsbeschluss bezeichneten Objekts erfasst.[14]

Eine wesentliche Begrenzung der Durchsuchungsbefugnisse resultiert indes aus dem völkerrechtlichen Souveränitätsprinzip. Anders gestaltet sich die rechtliche Situation daher, wenn sich der betreffende Server und mithin auch die betroffenen Daten im Ausland befinden. Werden die Daten im Zeitpunkt der Durchsuchung im Ausland gespeichert, so würde sich der über das Internet auf diese Daten zugreifende Staat Ermittlungsbefugnisse in einem Drittstaat anmaßen und so die existierenden Regelungen zur Rechtshilfe umgehen.[15] Der Zugriff auf im Ausland befindliche Daten ist seitens der Ermittlungsbehörden grundsätzlich nur im Wege eines förmlichen Rechtshilfeersuchens möglich. Deutschen Verfolgungsbehörden ist es nicht gestattet, ihre Ermittlungshandlungen ohne die Zustimmung des betroffenen (Dritt-) Landes vorzunehmen. Steht fest, dass sich der Speicherort der Daten nicht in Deutschland befindet, ist ein Zugriff grundsätzlich ausgeschlossen.

Wegen der hohen Komplexität und teilweise immensen Dauer von justiziellen Rechtshilfeersuchen wurde im Jahr 2001 die sog. Cybercrime-Konvention (CCC), ein völkerrechtliches Abkommen zur Bekämpfung von Cyberkriminalität, geschaffen, die inzwischen von mehr als 50 Staaten unterzeichnet wurde.[16] Diese Konvention lässt in eng umgrenzten Ausnahmefällen einen unmittelbaren Zugriff auf Daten im Ausland explizit zu. So ist der grenzüberschreitende Zugriff gemäß Art. 32 CCC in einigen Fällen auch gänzlich ohne die Genehmigung der Vertragsparteien (Drittstaat) gestattet. Dies gilt z. B. soweit öffentlich zugänglich gespeicherte Computerdaten (Open Source[17]/offene Quellen) betroffen sind, ungeachtet der Frage, wo diese sich befinden. Davon sind selbstverständlich nicht solche Daten erfasst, auf die nur mittels einer Schnittstelle eines im – nicht öffentlich zugänglichen – Durchsuchungsobjekt befindlichen Endgeräts zugegriffen werden kann.[18] Weiterhin ist der Zugriff nach Art. 32 b) CCC dann gestattet, wenn sich die gespeicherten Computerdaten im Hoheitsgebiet eines anderen Vertragsstaates befinden, jedoch ein Zugriff mittels eines Computersystems im Hoheitsgebiet des ermittelnden Staates möglich ist und wenn die Ermittlungsbehörden des ermittelnden Staates die rechtmäßige und freiwillige Zustimmung der Person einholen, die rechtmäßig befugt ist, die Daten mittels dieses Computersystems weiterzugeben. Soweit die Voraussetzungen des Art. 32 CCC nicht erfüllt sind, ermöglicht die Cybercrime-Konvention darüber hinaus ein „beschleunigtes" (Rechtshilfe-)Verfahren zur Sicherung von Daten (Art. 29 CCC), erlaubt allerdings keinen Direktzugriff inländischer Ermittlungsbehörden auf Daten im Ausland, ohne die Einwilligung des Dateninhabers.[19] Die Sicherung hat durch den Staat zu erfolgen, in dem die Daten physisch gelagert werden.[20]

Vereinzelt wird suggeriert, dass jedenfalls innerhalb der Europäischen Union ein Recht zum direkten Zugriff bestehe.[21] Dies ist unzutreffend. Der ins Feld geführte Art. 5 des Rahmenbeschluss 2003/577/JI erfordert bereits nach dem ausdrücklichen Wortlaut eigene Maßnahmen des Vollstreckungsstaats. Es handelt sich mithin um eine Form der – innerhalb der EU deutlich vereinfachten – Rechtshilfe. Eine analoge Anwendung des Art. 20 Abs. 4 des „Übereinkommen über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union" kommt ebenfalls nicht in Betracht. Erstens handelt es sich um eine Ermittlungsmaßnahme (Telekommunikationsüberwachung), die nur unter erschwerten Bedingungen und mit einem richterlichen Beschluss zulässig ist (vgl. §§ 100a, 100b StPO). Es bestehen, zweitens, Zweifel an der Vergleichbarkeit. Die Norm regelt den typischen Fall, dass sich der inländische Nutzer eines Telekommunikationsmittels – im Regelfall ein Mobilfunkgerät – im europäischen Ausland befindet und dort das Gerät nutzt. Die Überwachung laufender Kommunikation, bei der es aufgrund der Flüchtigkeit des gesprochenen Wortes aus ermittlungstaktischen Gründen regelmäßig besonders eilbedürftig ist, unterscheidet sich von dem einmaligen, offenen Zugriff auf Daten, die in der Vergangenheit entstanden sind. Drittens ist angesichts der vielfältig normierten Sicherungsmöglichkeiten im vereinfachten Verfahren eine planwidrige Regelungslücke nicht ersichtlich. Schließlich ist zu berücksichtigen, dass nach Art. 20 Abs. 4 b) ohne Zustimmung des anderen Staates im Regelfall keine Verwendung der Daten zulässig ist.[22] Auch neuere bzw. geplante Entwicklungen im europäischen Rechtshilferecht[23] ändern an dieser Herangehensweise nichts.[24] Zwar sollen in Zukunft auch Anbieter von Clouddiensten unmittelbar in die Pflicht genommen werden, im Ausland befindliche Daten herauszugeben. Eine Befugnis der Ermittlungsbehörden zum eigenen Zugriff auf die Daten soll damit aber auch zukünftig nicht einhergehen.

Verweigert ein Unternehmen bei einer Durchsuchung den Zugriff auf im Ausland gespeicherte Daten, so hat eine Serversichtung zu unterbleiben. Die Regelung des § 110 Abs. 3 StPO stellt insofern keine ausreichende Ermächtigungsgrundlage für den unmittelbaren Zugriff auf im Ausland befindliche Daten dar. Irrelevant ist insoweit, in welchem ausländischen Staat sich die Daten im Zeitpunkt der Sicherung befinden. Wird die Sichtung der Server seitens der Ermittlungsbehörden dennoch in Kenntnis des Belegenheitsorts der Daten im Ausland sowie unter Umgehung der Rechtshilfevorschriften fortgeführt und stellt sich die Datensicherung mithin als bewusste und willkürliche Umgehung rechtlicher Vorgaben dar, kann dies im Einzelfall zu einem Verwertungsverbot führen,[25] was eine Herausgabe- bzw. Löschungspflicht hinsichtlich der Daten nach sich zieht.[26]

Ist der konkrete Belegenheitsort der Daten nicht bekannt, eine Aufbewahrung in Deutschland jedoch möglich, ist die rechtliche Bewertung derzeit noch gerichtlich ungeklärt. Vereinzelt wird vertreten, dass

14 *Singelnstein*, NStZ 2012, 592, 598; *Zerbes/El-Ghazi*, NStZ 2015, 425, 428.

15 Vgl. auch *Bär*, Handbuch Wirtschafts- und Steuerstrafrecht, 4. Aufl. 2014, 27 B. Rn. 27; *Warken*, NZWiSt 2017, 329, 338.

16 Vgl. hierzu https://www.coe.int/de/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=LhCOfjLj (letzter Zugriff: 19.2.2019).

17 Vgl. BVerfG, Beschluss vom 21.6.2016, 2 BvR 637/16, Rn. 30 f.; *Bruns*, in KK-StPO, 7. Aufl. 2013, § 110. Rn. 8a; *Park*, Durchsuchung und Beschlagnahme, 4. Aufl. 2018, S. 254.

18 *Soiné*, NStZ 2018, 497, 500; wohl auch *Zerbes/El-Ghazi*, NStZ 2015, 425, 430; a. A. *Hegmann*, in: BeckOK StPO, 31. Ed. 15.10.2018, § 110, Rn. 15.

19 *Bär*, Handbuch Wirtschafts- und Steuerstrafrecht, 4. Aufl. 2014, 27 B. Rn. 29.

20 *Hauschild*, in: MüKo-StPO, 1. Aufl. 2014, § 110 Rn. 18; *Soiné*, NStZ 2018, 497, 500.; *Zerbes/El-Ghazi*, NStZ 2015, 425, 430; *Bär*, ZIS 2011, 53, 55. Unklar daher *Hegmann*, in: BeckOK StPO, 31. Ed. 15.10.2018, § 110, Rn. 15.

21 So wohl *Hegmann*, in: BeckOK StPO, 31. Ed. 15.10.2018, § 110, Rn. 15. Unklar *Hauschild*, in: MüKo-StPO, 1. Aufl. 2014, § 110 Rn. 18.

22 Zur Frage der Zustimmung allgemeine auch *Burchard*, ZIS 2018, 249, 256.

23 Zur Europäischen Ermittlungsanordnung vgl. *Böhm*, NJW 2017, 1512; *Burchard*, ZIS 2018, 190, 196; zum Kommissionsentwurf einer „Verordnung des Europäischen Parlaments und des Rates über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen", COM (2018) 225 Final, 17,4,2018 (abrufbar unter: https://db.eurocrim.org/db/de/doc/2975.pdf), vgl. *Burchard*, ZIS 2018, 190 und ZIS 2018, 249.

24 *Warken*, NZWiSt 2017, 417, 419 f.

25 *Park*, Durchsuchung und Beschlagnahme, 4. Aufl. 2018, S. 254. Zu den Grenzen siehe *Hauschild*, in: MüKo-StPO, 1. Aufl. 2014, § 110 Rn. 18; *Bär*, Handbuch Wirtschafts- und Steuerstrafrecht, 4. Aufl. 2014, 27 B. Rn. 30.

26 Zur Löschung siehe *Basar/Hiéramente*, NStZ 2018, 681.

insofern im Zweifel von einer rechtmäßigen Ermittlungshandlung im Inland auszugehen sei.[27] Ebenso wird vertreten, dass im Zweifelsfall eine Sicherung vollständig zu unterbleiben habe.[28] Eine obergerichtliche Klärung dieser Rechtsfrage steht bislang allerdings noch aus. Unabhängig hiervon ist aus hiesiger Sicht jedenfalls zu fordern, dass bei drohendem Beweismittelverlust – wie von § 110 Abs. 3 StPO vorgesehen aber behördenseits meist geflissentlich ignoriert[29] – lediglich eine Sicherung der Daten erfolgt. Vor einer inhaltlichen Sichtung oder gar Beschlagnahme, sollte dem Betroffenen die Möglichkeit gegeben werden, binnen angemessener Frist zum Belegenheitsort vorzutragen.

4. Die Nachfrage nach dem Passwort

Die Durchsuchungssituation geht für die Betroffenen regelmäßig mit einer psychischen und physischen Belastung einher. Dabei spielt die Unsicherheit über Ziel und Ausmaß der Durchsuchung sowie den Kreis der möglichen Beschuldigten eine gewichtige Rolle. Betroffene haben berechtigterweise Angst, Fehler zu machen. Dies wird dann virulent, wenn sie nicht nur passiv eine Durchsuchung zu dulden haben, sondern von den Ermittlungsbehörden zur aktiven Mitwirkung aufgefordert werden. Ein praxisrelevanter Fall ist die Frage der Ermittlungsbehörden nach Passwörtern zu Mobilfunkgeräten, Laptops oder zur (Unternehmens-) Cloud und Servern. Mangels eindeutiger Regelungen in der StPO herrscht insoweit oft Unklarheit über den Grad der bestehenden Mitwirkungspflichten.

Eindeutig ist, dass ein Beschuldigter nicht verpflichtet ist, Passwörter preiszugeben und so an der eigenen Überführung mitzuwirken. Die verfassungs- und strafprozessrechtlich verankerte Selbstbelastungsfreiheit (*nemo-tenetur*-Prinzip) erlaubt es dem Beschuldigten, die Auskunft auf sämtliche Fragen zu verweigern. Er ist nicht verpflichtet, aktiv an der Sachverhaltsaufklärung mitzuwirken.[30] Mithin ist der Beschuldigte in verfassungskonformer Auslegung auch nicht nach § 95 Abs. 1 StPO zur Herausgabe von Gegenständen verpflichtet.[31] Ähnlich verhält es sich bei (noch) nicht selbst beschuldigten Unternehmensmitarbeitern, mithin Zeugen, die aber berechtigterweise annehmen müssen, dass sie sich bei der Mitwirkung in die Gefahr der Strafverfolgung bringen würden. Die Annahme eines Auskunftsverweigerungsrechts liegt dann nahe, wenn die strafrechtlichen Vorwürfe einen Bezug zur betrieblichen Tätigkeit des Unternehmens aufweisen (z. B. §§ 266, 299 StGB, § 23 GeschGehG). Diese Mitarbeiter können daher gemäß § 55 StPO die Auskunft auf solche Fragen verweigern, die sie bei wahrheitsgemäßer Beantwortung selbst der Gefahr der Strafverfolgung aussetzen würde. Darüber hinaus darf gegenüber einem Auskunftsverweigerungsberechtigten (§ 55 StPO) die Mitwirkung an der Herausgabe von Beweisgegenständen nach § 95 StPO nicht erzwungen werden.[32] In Zweifelsfällen kann sich der betroffene Mitarbeiter vor einer Auskunft nach § 68b Abs. 1 S. 1 StPO[33] mit einem anwaltlichen Zeugenbeistand austauschen. Nach § 163 Abs. 4 Nr. 1 StPO entscheidet bei bestehenden Zweifeln über die Zeugeneigenschaft sowie das Vorliegen des Auskunftsverweigerungsrechtes nach § 55 StPO im Ermittlungsverfahren abschließend die Staatsanwaltschaft. Ein Rechtsmittel ist gegen diese Entscheidung nicht gegeben, § 163 Abs. 5 StPO.[34]

Häufig wird die Frage nach den Passwörtern unmittelbar an die Geschäftsleitung oder den Leiter der IT gerichtet. Diese fallen bei Straftaten einzelner Mitarbeiter seltener in den Kreis der Auskunftsverweigerungsberechtigten i. S. d. § 55 StPO. Zudem verfügt die IT häufig über die wesentlichen Passwörter zu Endgeräten sowie E-Mail-Accounts der Mitarbeiter[35] oder kann mittels der Eingabe eines Administrator-Passworts lokale Zugangssicherungen (z. B. Sperrbildschirme) umgehen. Mithin stellt sich in der Folge die Frage, inwieweit Personen zur Herausgabe von Passwörtern verpflichtet sind, die nicht selbst Beschuldigte sind oder denen kein Auskunftsverweigerungsrecht nach § 55 StPO zusteht.

a) Spezialregelung zur Passwortherausgabe, § 100j Abs. 1 S. 2 StPO

§ 100j Abs. 1 S. 2 StPO regelt den Auskunftsanspruch der Ermittlungsbehörden gegenüber Telekommunikationsdiensteanbietern und zielt auf die PIN und PUK von Mobilfunkgeräten ab.[36] Erfasst sind aber auch vom Nutzer selbst vergebene Zugangssicherungen, die beim Telekommunikationsdiensteanbieter gespeichert sind.[37] Passwörter für den Zugang zu einer Cloud sind hingegen nicht von der Norm erfasst, da diese nicht von einem Anbieter nach dem TKG erhoben werden und der Cloud-Anbieter nicht der richtige Adressat ist.[38]

Die Regelung des § 100j Abs. 1 S. 2 StPO ist für Ermittlungsbehörden auch in Wirtschaftsstrafsachen von Relevanz und erlaubt diesen, hinsichtlich bei der Durchsuchung aufgefundener Mobilfunkgeräte mit unüberwindbarer Zugangssicherung, die Anfrage beim Telekommunikationsdiensteanbieter (z. B. Telekom, Vodafone etc.). Erforderlich ist für die Beweisgewinnung grundsätzlich ein richterlicher Beschluss.[39] Nach teilweise vertretener Ansicht ist ein Unternehmen, das die private Nutzung von Telefonen und Internet gestattet, als Diensteanbieter anzusehen.[40] Allerdings hat der Gesetzgeber in § 100j Abs. 1 StPO klargestellt, dass nur eine „geschäftsmäßige" Diensterbringung die Mitwirkungspflicht begründet.[41] Adressat ist mithin nicht das Unternehmen oder deren Mitarbeiter selbst.

b) Allgemeine Mitwirkungspflichten nach §§ 48 ff. und § 95 StPO

Dementsprechend stellt sich in der Praxis vielfach die Frage, ob unbeteiligte Unternehmensmitarbeiter oder die Unternehmensführung nach den allgemeinen Vorschriften der StPO zur Mitwirkung – in Form

27 *Meyer-Goßner/Schmitt*, 61. Aufl. 2018, § 110, Rn. 7b.
28 *Park*, Durchsuchung und Beschlagnahme, 4. Aufl. 2018, S. 261.
29 Mahnend auch *Park*, Durchsuchung und Beschlagnahme, 4. Aufl. 2018, S. 260 f.
30 BGH, 28.7.2009 – 3 StR 80/09, NStZ 2009, 705.
31 *Menges*, in: Löwe-Rosenberg, 27. Aufl., 2018, § 95, Rn. 14.
32 *Menges*, in: Löwe-Rosenberg, 27. Aufl., 2018, § 95, Rn. 16; *Wohlers/Greco*, in: SK-StPO, 5. Aufl. 2016, § 95, Rn. 21.
33 Hierzu allgemein *Gillmeister*, NStZ 2018, 561.
34 Zur richterlichen Mitwirkung beim Erlass von Ordnungsmitteln s. u.
35 Zu den Möglichkeiten der Passwortvergabe bei Mobilfunkgeräten siehe *Bäumerich*, NJW 2017, 2718.
36 Zu den praktischen Grenzen siehe *Bär,* MMR 2013, 700, 702.
37 *Graf*, in: BeckOK StPO, 31. Ed. 15.10.2018, § 100j, Rn. 15; *Hauck*, in: Löwe-Rosenberg, 27. Aufl., 2018, § 100j, Rn. 10.
38 *Wicker*, MMR 2014, 298; *Hauck*, in: Löwe-Rosenberg, 27. Aufl., 2018, § 100j, Rn. 15a; *Greco*, in: SK-StPO, 5. Aufl. 2016, § 100j, Rn. 11; a. A. *Graf*, in: BeckOK StPO, 31. Ed. 15.10.2018, § 100j, Rn. 19. Unklar bei *Bär,* MMR 2013, 700, 702.
39 Zu Strafbarkeitsrisiken für Ermittlungsbeamte bei der Umgehung siehe *Bär*, Handbuch Wirtschafts- und Steuerstrafrecht, 4. Aufl. 2014, 27 C. Rn. 124; *Graf*, in: BeckOK StPO, 31. Ed. 15.10.2018, § 100j, Rn. 16, 18; *Hauck*, in: Löwe-Rosenberg, 27. Aufl., 2018, § 100j, Rn. 12.
40 Siehe Übersicht bei *Wybitul*, NJW 2014, 3605; *Veit*, NZWiSt 2015, 334.
41 *Hauck*, in: Löwe-Rosenberg, 27. Aufl., 2018, § 100j, Rn. 27 *Greco*, in: SK-StPO, 5. Aufl. 2016, § 100j, Rn. 19.

der Passwortherausgabe – verpflichtet sind. Teilweise wird vertreten, dass eine Pflicht zur Mitwirkung aus § 95 Abs. 1 StPO – der Pflicht zur Herausgabe von Beweismitteln im eigenen Gewahrsam – folge.[42] Hier gilt es zu unterscheiden:

Eine Herausgabepflicht könnte sich unmittelbar auf die auf dem zugangsgesicherten Datenträger befindlichen Daten beziehen. Nach verbreiteter Ansicht soll § 95 Abs. 1 StPO – wie auch § 94 StPO – neben körperlichen Gegenständen auch elektronische Daten erfassen, die mittels Kopie oder Ausdruck herausgeben werden können.[43] Anerkannt ist insoweit allerdings, dass eine – ggfs. mit Ordnungsmitteln durchsetzbare – Herausgabepflicht nur für die Gegenstände oder Daten besteht, die derart konkretisiert sind, dass eine Beschlagnahme nach § 94 StPO erfolgen könnte.[44] Dies ist in der Durchsuchungssituation regelmäßig nicht der Fall.

Nach diesem Ansatz ließe sich weiter argumentieren, dass sich die Herausgabepflicht nach § 95 Abs. 1 StPO auch auf das Passwort selbst bezieht. Insoweit ist aber eindeutig, dass die Pflicht nach § 95 StPO nicht die Offenlegung von persönlichem Wissen, sondern einzig die Herausgabe bereits existierender Gegenstände erfasst. Sind die gesuchten Passwörter im Zeitpunkt der Anfrage nicht schriftlich oder datentechnisch festgehalten, scheidet eine Verpflichtung nach § 95 Abs. 1 StPO aus. Verfügt der Leiter der IT allerdings über eine Liste der Mitarbeiter- und Administratorenpasswörter, so ist die Anwendung des § 95 Abs. 1 StPO nicht *per se* ausgeschlossen. Insoweit stellt sich nur die bislang kaum diskutierte Frage, ob Gegenstände, wie z. B. ein (digitaler) Schlüssel, denen kein Beweiswert im Hinblick auf das Tatgeschehen zukommt, von den §§ 94 ff. StPO („als Beweismittel") erfasst werden.

Eine vergleichbare Frage stellt sich im Hinblick auf § 48 Abs. 1 S. 2 StPO. So ist die Frage aufzuwerfen, ob die reine Mitwirkung bei der Ermittlung von Beweismitteln von der Aussagepflicht eines Zeugen erfasst ist. Sofern man insoweit eine Zeugenpflicht bejaht, stellt die Durchführung einer zeugenschaftlichen Vernehmung des Leiters der IT-Abteilung ein probates Mittel zur Ermittlung eines Passworts dar. Dogmatisch begegnet diese – vielfach seitens der Ermittlungsbehörden vertretene – Auffassung allerdings gewissen Zweifeln. Die Pflicht des Zeugen beschränkt sich grundsätzlich auf die Bekundung eigener Wahrnehmungen zur Tat- und Schuldfrage, mithin Schilderungen eigenen Wissens zu dem in Rede stehenden Tatgeschehen. Ob hiervon auch die Preisgabe eines Passworts umfasst ist, dass allenfalls mittelbar Erkenntnisse zur Tat- und Schuldfrage erbringt, ist zumindest diskussionswürdig. Beide Möglichkeiten der Ermittlung von Passwörtern – Herausgabeverlangen und Zeugenvernehmung – werden aus einem weiteren Grund kritisch gesehen. So weisen *Sieber* und *Graf* darauf hin, dass das Bundesverfassungsgericht im Hinblick auf eine Herausgabepflicht von Zugangssicherungen besondere Hürden aufgestellt und der Gesetzgeber in § 100j Abs. 1 S. 2, Abs. 3 S. 1 StPO einen Richtervorbehalt eingeführt hat. Beide Autoren sehen eine Umgehung dieser Regelungsvorgaben als problematisch an.[45] Aufgrund der Eingriffsintensität der Maßnahme sei ein Rückgriff auf die allgemeinen Regelungen nicht unproblematisch.

Für die Praxis lässt sich indes festhalten, dass sich Strafverfolgungsbehörden in einer Durchsuchungssituation erfahrungsgemäß auf die Herausgabepflicht nach § 95 Abs. 1 StPO und/oder die Zeugenpflichten nach §§ 48 ff. StPO unbeteiligter Unternehmensmitarbeiter berufen werden, um eine Mitteilung von Passwörtern zu erzwingen.[46] Ordnungsgelder können im Falle der unberechtigten Verweigerung des Zeugnisses gemäß § 163 Abs. 4 Nr. 4 StPO seitens der Staatsanwaltschaft festgesetzt werden. Die Verhängung von Ordnungshaft steht indes unter Richtervorbehalt.

IV. Handlungsmöglichkeiten für Unternehmen

Für Unternehmen empfiehlt es sich, bereits im Vorfeld einer Durchsuchung klare Verhaltensregeln festzulegen und Mitarbeiter und Verantwortliche in regelmäßigen Abständen zu schulen. Zum Schutz des Unternehmens und der Mitarbeiter ist es wichtig, dass diese ihre Rechte und Pflichten kennen und dahingehend aufgeklärt werden, wie sie sich in der konkreten Situation zu verhalten haben, um Risiken und Schäden zu vermeiden. Daneben ist auch in technischer Hinsicht eine gezielte Vorbereitung angezeigt.

1. Festlegung klarer Zuständigkeiten und Arbeitsabläufe

Um für den Ernstfall einer Durchsuchung optimal vorbereitet zu sein und angemessen reagieren zu können, empfiehlt es sich daher, vorab klare Zuständigkeiten und Arbeitsabläufe festzulegen. Dies erfordert zunächst die Benennung von Mitarbeitern, die im Rahmen einer Durchsuchung als Ansprechpartner der Ermittlungsbehörden fungieren können. Neben der Benennung eines Durchsuchungsbeauftragten (Legal Counsel o. ä.), der im Durchsuchungsfall die Schnittstelle zwischen der Geschäftsleitung, der betroffenen Abteilung bzw. den Mitarbeitern und den Verfolgungsbehörden bildet, empfiehlt es sich, einen externen Strafverteidiger hinzuzuziehen.

Daneben ist es erforderlich, einen IT-Beauftragten zu bestimmen, der die Durchsuchung auf Seiten des Unternehmens in technischer Hinsicht begleitet. Dieser kann bei Bedarf und nach erfolgter Abstimmung mit dem Durchsuchungsbeauftragten und dem Strafverteidiger als direkter Ansprechpartner der IT-Forensiker der Ermittlungsbehörden fungieren. Es ist dabei nicht erforderlich, dass dieser selbst alle Geschäftsabläufe kennt, vielmehr muss er mit der technischen Infrastruktur sowie der Serverlandschaft vertraut sein. Insoweit wird sichergestellt, dass den Ermittlungsbehörden im Falle der Kooperation der entsprechende technische Zugriff gewährt werden kann und alle IT-spezifischen Fragen unmittelbar beantwortet werden können.

2. Klare Regelungen zur Aufbewahrung und Speicherung von Daten

Um im Falle einer Durchsuchung sofort angemessen reagieren zu können, empfiehlt es sich weiter, dass die Unternehmensmitarbeiter klare Anweisungen zur Ablage und Speicherung von Daten für die einzelnen Unternehmensbereiche und Abteilungen erhalten. Diese sollten sowohl die Archivierung von Geschäftsunterlagen als auch die Ablage von digitaler Kommunikation (E-Mails) umfassen. Auf diese

42 Ob die Pflicht das Unternehmen oder die handelnden Personen trifft, ist für die Praxis von nachrangiger Bedeutung, vgl. hierzu *Menges*, in: Löwe-Rosenberg, 27. Aufl., 2018, § 95, Rn. 13; *Wohlers/Greco*, in: SK-StPO, 5. Aufl. 2016, § 95, Rn. 10.

43 Siehe Übersicht bei *Wohlers/Greco*, in: SK-StPO, 5. Aufl. 2016, § 95, Rn. 29. Zur fehlenden Pflicht einer Bereitstellung in leserlicher Form siehe *Sieber*, Straftaten und Strafverfolgung im Internet, 2012, C 9, 121.

44 Vgl. zur Reichweite des § 95 vgl. *Menges*, in: Löwe-Rosenberg, 27. Aufl., 2018, § 95, Rn. 19.

45 *Sieber*, Straftaten und Strafverfolgung im Internet, 2012, C 9, 121. *Graf*, in: BeckOK StPO, 31. Ed. 15.10.2018, § 100j, Rn. 18.

46 Im Ergebnis auch *Burhoff*, Handbuch für das strafrechtliche Ermittlungsverfahren, 8. Aufl. 2019, Rn. 1740.

Weise wird sichergestellt, dass die seitens der Ermittlungsbehörden im Rahmen der Durchsuchung geforderten Daten schnell identifiziert, deren Belegenheitsort ermittelt und die Daten im Anschluss bereitgestellt werden können.
Zudem ist es erforderlich, dass auf Seiten des Unternehmens durchgängig bekannt ist, ob sich die Daten im Inland oder im Ausland befinden und wie ein entsprechender Zugriff gewährleistet werden kann. Falls sich die Daten teilweise im Ausland befinden, ist es hilfreich, wenn man den Ermittlungsbehörden den genauen Belegenheitsort benennen kann. Dazu sollten etwaige Verträge mit Cloudanbietern oder externen IT-Dienstleistern bereitgehalten werden, aus denen sich der Belegenheitsort der Daten ergibt. Auch im Hinblick auf die Vorgaben der DSGVO, u.a. Art. 28, sollte grundsätzlich Klarheit darüber bestehen, wo und durch wen Mitarbeiterdaten gespeichert und verarbeitet werden.
Soweit das Unternehmen – etwa bei der selbstständigen Aufarbeitung strafrechtlicher Vorgänge – belastende Beweismittel auswertet und speichert, kann erwogen werden, diese gezielt von den übrigen Unternehmensdaten zu isolieren, um sie im Durchsuchungsfall – soweit ein strafprozessualer Beschlagnahmeschutz nicht gegeben ist – kurzfristig und ohne weitere Beeinträchtigung herausgeben zu können.

3. Rechtliche Empfehlung zur Bereitstellung von Daten

In der Regel empfiehlt es sich, die Durchsuchung aktiv zu unterstützen. Ziel sollte es sein, im Wege der Kooperation auf eine schnelle Erledigung der Maßnahme hinzuwirken und langwierige Durchsuchungen – ggf. verbunden mit medialer Aufmerksamkeit oder weiteren Zwangsmaßnahmen – zu verhindern. Allerdings sollte das konkrete Vorgehen jeweils zu Beginn der Maßnahme zwischen dem Durchsuchungsbeauftragen und dem Strafverteidiger abgestimmt werden.
Im Falle einer Kooperation sollte sich die Mitarbeit jedoch darauf beschränken, den Ermittlungsbehörden den Belegenheitsort der konkret geforderten Daten aufzuzeigen. Dabei sollte – um überbordende Sicherstellungen zu vermeiden – ein möglichst präziser und abschließender Hinweis erfolgen, um zu verhindern, dass nicht betroffene Daten als „Beifang" enden. Auch eine Nennung einzelner Passwörter dürfte regelmäßig angezeigt sein, um die Beschlagnahme von Datenträgern, Computern und Mobilfunkgeräten zu vermeiden, die dem unmittelbaren Zugriff der staatlichen Behörden unterliegen. Eine darüber hinausgegebene Erörterung zur Sache selbst sollte – jedenfalls während der laufenden Durchsuchung – mit Blick auf eigene strafrechtliche Risiken der beteiligten Mitarbeiter zunächst vermieden werden.
Gleichwohl sollte seitens des Unternehmens einer freiwilligen Herausgabe der Daten und Beweismittel stets widersprochen und auf eine behördliche Beschlagnahme hingewirkt werden. Dieser Widerspruch ist keinesfalls als fehlende Kooperation gegenüber den Behörden zu verstehen, er dient vielmehr der Verhinderung des Verlustes strafprozessualer Rechte (Disposition über Verwertungsverbote) sowie der Vermeidung möglicher Schadensersatzforderungen von Kunden oder Dritten, durch eine unberechtigte – häufig existieren diesbezüglich umfangreiche vertragliche Regelungen – Herausgabe von Daten. Ein Widerspruch ist auch deshalb sinnvoll, weil es im – freilich eher seltenen – Einzelfall geboten sein kann, nach Abschluss der Durchsuchungssituation bestimmte Rechtsfragen auszufechten und sich aktiv zur Wehr zu setzen.

Soweit sich die Unterlagen und Daten auf deutschem Hoheitsgebiet befinden, ist deren Beschlagnahme ein rein formaler Akt, der für die Ermittlungsbehörden mit keinerlei Mehrarbeit verbunden ist und dem Unternehmen gleichwohl Rechtssicherheit gibt. Anders stellt sich die Situation dar, wenn sich die Daten im Ausland befinden. Ein behördlicher Zugriff ist hier nur mittels eines (vereinfachten) Rechtshilfeersuchens oder mit ausdrücklicher Zustimmung des Berechtigten möglich. An dieser Stelle ist in enger Abstimmung mit dem Verteidiger einzelfallbezogen zu entscheiden, welches Vorgehen gewählt wird und ob eine Zustimmung erfolgen kann. Abzuwägen gilt es das Risiko einer länger andauernden Durchsuchungsmaßnahme sowie weiterer Zwangsmaßnahmen gegen die Gefahr des Verlustes von strafprozessualen Verfahrensrechten und möglicher zivilrechtlicher Schadensersatzansprüche.

V. Fazit

Durchsuchungen stellen im geschäftlichen Alltag deutscher Unternehmen absolute Ausnahmesituationen dar, welche die Betroffenen regelmäßig vor große Herausforderungen stellen. Neben den hohen strafrechtlichen Risiken der persönlichen Betroffenen drohen auch dem Unternehmen häufig erhebliche Sanktionen. Die beteiligten Personen sind vielfach überfordert und häufig nicht in der Lage, angemessen zu reagieren. Die umfangreiche behördliche Sicherung von Unternehmensdaten stellt hierbei ein besonderes Risiko im Rahmen einer Durchsuchungsmaßnahme dar. Den Verantwortlichen und Mitarbeitern fehlt gerade in diesem Bereich die Kenntnis von bestehenden Rechten und Pflichten sowie das erforderliche technische Verständnis. Es empfiehlt sich daher für Unternehmen, sich bereits im Vorfeld gezielt auf diese Situation vorzubereiten.

AUTOR

Rechtsanwalt **Christian Graßie** *ist ein auf die Verteidigung im Wirtschaftsstrafrecht spezialisierter Strafverteidiger der Kanzlei Dr. Felix Dörr & Kollegen, Frankfurt. Er berät und vertritt Individualpersonen und Unternehmen inallen Fragen des Wirtschaftsstrafrechts.Vor seiner Beschäftigung als Strafverteidiger war er fünf Jahre als Staatsanwalt in Nordrhein-Westfalen tätig.*

Rechtsanwalt **Dr. Mayeul Hiéramente**, *FAStR, verteidigt Einzelpersonen und Unternehmen in allen Bereichen des Wirtschaftsstrafrechts. Er ist Partner der auf Wirtschaftsstrafrecht und Arbeitsrecht spezialisierten Kanzlei Fuhlrott Hiéramente & von der Meden Partnerschaft von Rechtsanwälten mbB (FHM), Hamburg.*

Compliance-Berater Zitierweise CB: / ISSN 2195-6685

CHEFREDAKTION:
Dr. Malte Passarge (V.i. S. d.P.), Passarge, Prudentino & Rhein Rechtsanwälte PartGmbB – Studio Legale, Große Johannisstraße 19, 20 457 Hamburg, Tel: 040-4 14 25 51-0, passarge@ppr-recht.de

REDAKTION:
Christina Kahlen-Pappas, Tel. 0151-27 24 56 63, christina.kahlen-pappas@dfv.de

HERAUSGEBER:
Prof. Dr. Frank Beine, WP / StB
Hanno Hinzmann
Manuela Mackert
Dr. Philip Matthey
Univ.-Prof. Dr. Annemarie Matusche-Beckmann
Dr. Dirk Christoph Schautes
Prof. Dr. Martin Schulz, LL.M. (Yale)
Eric S. Soong
Prof. Dr. Gregor Thüsing, LL.M. (Harvard), Attorney at law (New York)
Dr. Martin Wienke

BEIRAT:
Dr. Martin Auer
Dr. Martin Bünning, RA / StB
Dr. José Campos Nave, RA / FAHaGesR / FAStR
Dr. Peter Christ, RA / FAArbR
Dr. Susanne Jochheim, RAin
Dr. Ulf Klebeck, RA
Tobias Neufeld, LL.M. (London), RA / FAArbR, Solicitor (England & Wales)
Jürgen Pauthner, LL.M. (San Diego), MBA
Mario Prudentino, RA
Dr. Manfred Rack, RA
Dr. Sarah Reinhardt, RAin / FAArbR
Dr. Roman Reiß, RA / FAStR
Gunther A. Weiss, LL.M. (Yale), RA, Attorney at law (New York), Advokát (Praha)
Wolfgang Werths
Tim Wybitul, RA / FAArbR
Prof. Dr. Dr. Jörg Zehetner, RA

dfv Mediengruppe

VERLAG: Deutscher Fachverlag GmbH, Mainzer Landstr. 251, 60326 Frankfurt am Main, Tel. 069-7595-2788, Fax 069-7595-2780, Internet: www.dfv.de, verlag@betriebs-berater.de

GESCHÄFTSFÜHRUNG: Angela Wisken (Sprecherin), Peter Esser, Markus Gotta, Peter Kley, Holger Knapp, Sönke Reimers
AUFSICHTSRAT: Klaus Kottmeier, Andreas Lorch, Catrin Lorch, Peter Ruß
GESAMTVERLAGSLEITUNG FACHMEDIEN RECHT UND WIRTSCHAFT: RA Torsten Kutschke
Tel. 0 69-75 95-27 01, Torsten.Kutschke@dfv.de

REGISTERGERICHT: AG Frankfurt am Main, HRB 8501

BANKVERBINDUNG: Frankfurter Sparkasse, Frankfurt am Main, Kto.-Nr. 34 926 (BLZ 500 502 01)

In der dfv Mediengruppe, Fachmedien Recht und Wirtschaft, erscheinen außerdem folgende Fachzeitschriften: Betriebs-Berater (BB), Causa Sport (CASP), Recht der Internationalen Wirtschaft (RIW), Datenschutz-Berater (DSB), Der Steuerberater (StB), Europäisches Wirtschafts- und Steuerrecht (EWS), Kommunikation & Recht (K&R), Netzwirtschaften & Recht (N&R), Zeitschrift für Vergleichende Rechtswissenschaft (ZVglRWiss), Zeitschrift für das gesamte Handels- und Wirtschaftsrecht (ZHR), Recht der Finanzinstrumente (RdF), Wettbewerb in Recht und Praxis (WRP), Zeitschrift zum Innovations- und Technikrecht (InTeR), Zeitschrift für das gesamte Lebensmittelrecht (ZLR) und Zeitschrift für Umweltpolitik & Umweltrecht (ZfU), Zeitschrift für Wett- und Glücksspielrecht (ZfWG), Zeitschrift für Neues Energierecht (ZNER).

ANZEIGEN:
Lena Moneck, lena.moneck@dfv.de
Es gilt Preisliste Nr. 7.

Bereichsleitung Finanzen und Medienservices: Thomas Berner, Tel. 069/7595-1147

Leitung Produktion: Hans Dreier, Tel. 069/7595-2463

Leitung Logistik: Ilja Sauer, Tel. 069/7595-2201

VERTRIEB: Ayhan Simsek, Tel. 069-7595-2782, ayhan.simsek@dfv.de

ERSCHEINUNGSWEISE: monatlich. Nicht eingegangene Hefte können nur bis zu 10 Tage nach Erscheinen des nächstfolgenden Heftes kostenlos reklamiert werden.

BEZUGSPREISE: Jahresvorzugspreis (11 Ausgaben): 509 Euro inkl. Vesandkosten und MwSt., Sonderpreis für Studenten und Referendare: 140,– Euro. Beorderungsgebühr jährlich (fällt an bei Fremdzahler): 2 Euro netto. Preis des Einzelheftes: 51,95 Euro. Auslandspreise auf Anfrage. Rechnungslegung erfolgt jährlich. Die Abonnementgebühren sind im Voraus zahlbar. Der Abonnementvertrag ist auf unbestimmte Zeit geschlossen. Eine Kündigung ist jederzeit bis 3 Monate vor Ende des Bezugszeitraumes möglich. Liegt dem Verlag zu diesem Zeitpunkt keine Kündigung vor, verlängert sich das Abonnement automatisch um ein weiteres Jahr zum dann gültigen Jahrespreis, zahlbar im Voraus. Auslandspreise auf Anfrage. Die Zeitschrift und alle in ihr enthaltenen Beiträge und Abbildungen sind urheberrechtlich geschützt.

Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlags unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen. Die Verlagsrechte erstrecken sich auch auf die veröffentlichten Gerichtsentscheidungen und deren Leitsätze, die urheberrechtlichen Schutz genießen, soweit sie vom Einsender oder von der Redaktion redigiert bzw. erarbeitet sind.

Keine Haftung für unverlangt eingesandte Manuskripte. Mit der Annahme zur Alleinveröffentlichung erwirbt der Verlag alle Rechte, einschließlich der Befugnis zur Einspeisung in eine Datenbank.

Autorenmerkblatt herunterladbar unter: www.compliance-berater.de

© 2019 Deutscher Fachverlag GmbH, Frankfurt am Main

SATZ: DFV – inhouse production

DRUCK: medienhaus Plump GmbH, Rolandsecker Weg 33, 53 619 Rheinbreitbach

VORSCHAU CB 7/2019

Dr. Katharina Hastenrath, RAin

Strategische Projektplanung eines Compliance Management Systems

Andreas Haak, RA, Dr. Maria Brakalova, RAin, und **Dr. Barbara Thiemann, LLM (Bristol),** RAin

Internationale Handelspolitik geprägt durch nationales Sicherheitsdenken – Teil 2

Prof. Dr. Christian Kersting

Zivilrechtliche Konzernhaftung im Kartellrecht – Teil 1

Dr. Rita Pikó, RAin

Compliance bei Stiftungen

BB 22/2019

WIRTSCHAFTSRECHT

Dr. Udo Kornmeier, RA, und **Anne Baranowski**, LL. M., RAin

Das Eigentum an Daten – Zugang statt Zuordnung

STEUERRECHT

Dipl.-Finw. **Georg Eder**, RA, und **Dr. Jörg Dehn**, RA

Sind Verrechnungspreisanpassungen zollwertrechtlich relevant? – Eine kritische Bestandsaufnahme anlässlich des EuGH-Grundsatzurteils Hamamatsu (C-529/16)

Prof. DDr. Gunter Mayr

Neue Digitalkonzernsteuer auf Onlinewerbung in Österreich

Prof. Dr. Dieter Dziadkowski

Zum Einkommensteuertarif 2019: Berücksichtigung des Grundfreibetrags

BILANZRECHT UND BETRIEBSWIRTSCHAFT

Prof. Dr. Michael Hommel, StB, **Tessa Kunkel**, M.Sc., und **Theresa Zick**, M.Sc.

Passive Rechnungsabgrenzungsposten – Statische Interpretation durch die neuere Rechtsprechung?

ARBEITSRECHT

Bernd Weller, RA/FAArbR, und **Johannes Reuther**

BB-Rechtsprechungsreport zur Arbeitnehmermitbestimmung nach dem BetrVG Teil III: Organisationsrechte des Betriebsrats

Das Compliance-Berater-Serviceteam beantwortet Ihnen alle Fragen rund um den CB
Servicetelefon 069/7595-2788, Fax 069/7595-2760
E-Mail kundenservice@compliance-berater.de