Ambiguous Legal Issues in Internal Investigations and Audits

CEJ
COMPLIANCE ELLIANCE JOURNAL

Dr. Hendrik Schneider & Michele DeStefano
Editorial

Lucian E. Dervan
Internal Investigations and the Evolving Fate Of Privilege

Christian Pelz
Ambiguities in International Internal Investigations

Sascha Süße & Carolin Püschel
Collecting Evidence in Internal Investigations in the Light of Parallel Criminal Proceedings

---

Tim Wybitul
How to Conduct E-Mail Reviews in Germany

Micha-Manuel Bues
Compliance Tech

Jens Bergmann
When Compliance Fails

Content Curators:
Michele DeStefano (University of Miami School of Law)
Dr. Hendrik Schneider (University of Leipzig Faculty of Law)

ISSN 2365-3353
Volume 2 • Number 1
Winter 2016

Compliance Elliance Journal (CEJ)
Volume 2, Number 1, 2016
ISSN: 2365-3353
This version appears in print and online. CEJ is published twice per year, in the summer and winter.

Title: Ambiguous Legal Issues in Internal Investigations and Audits

Content Curators:
Michele DeStefano, University of Miami School of Law and LawWithoutWalls
Dr. Hendrik Schneider, University of Leipzig Faculty of Law

Technical Support:
Hans-Henning Gonska
Kristin Kißling
Antonia Orterer

Website: www.cej-online.com

Email: info@cej-online.com

Address:
Klostergasse 12
04109 Leipzig, Germany

Telephone: +49 0341 / 97 35 220

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

Ambiguous Legal Issues in Internal Investigations and Audits

TABLE OF CONTENTS

I. MICHELE DESTEFANO & DR. HENDRIK SCHNEIDER 1
Editorial

II. LUCIAN E. DERVAN 3
Internal Investigations and the Evolving Fate Of Privilege

III. CHRISTIAN PELZ 14
Ambiguities in International Internal Investigations

IV. SASCHA SÜßE & CAROLIN PÜSCHEL 26
Collecting Evidence in Internal Investigations in the Light of Parallel Criminal Proceedings

V. TIM WYBITUL 59
How to Conduct E-Mail Reviews in Germany

VI. MICHA-MANUEL BUES 78
Compliance Tech

VII. JENS BERGMANN 85
When Compliance Fails

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

EDITORIAL

AMBIGUOUS LEGAL ISSUES IN INTERNAL INVESTIGATIONS AND AUDITS

It gives us great pleasure to introduce you to our second edition of the Compliance Elliance Journal (CEJ).

This edition, we have chosen to focus on "Ambiguous Legal Issues in Internal Investigations and Audits" given the rise in number and significance of internal corporate investigations worldwide. There are attributing factors to this growth. First, internal investigations enable control over the facts of the case and technology has increased the ability to attain data. The results of internal investigations enable corporations to thoroughly consider when and where they report facts to the public as well as to the authorities. Second, the declining resources of the investigating authorities play as vital a role as the growing complexity of the cases does. Indeed, the process and oversight of Internal Investigations has become a market itself. Corporations utilize internal and external experts and consultant to help conduct and analyze the results of internal investigations. Third, internal investigations are not only an opportunity to earn (or spend) money but also a Bermuda triangle of legal risks for corporations in any country. We believe we can learn from each other by sharing information and commentary about this rich risky market. For these reasons, we have chosen to dedicate an entire edition of CEJ to risks and rewards of internal investigations.

Our current edition begins with the author Lucian E. Dervan. In "Internal Investigations and the Evolving Fate of Privilege", he provides valuable insights regarding internal investigations from the US perspective. In our second piece, entitled "Ambiguities in International Internal Investigations", Dr. Christian Pelz deals with the international aspects of internal investigations, including the criminal liability risks to which the investigated corporate employees are exposed. Thereafter follows a depiction of internal investigations under existing German law in the article "Collecting Evidence in Internal Investigations in the Light of Parallel Criminal Proceedings" written by Dr. Sascha Süße and Carolin Püschel.

The journal then turns to the means used to conduct investigations and expose malfeasance: technology and big data. In his essay, "How to Conduct E-Mail Reviews in Germany," Tim Wybitul emphasizes, among other things, the legal requirements that apply to the analysis and inspection of business emails. This commentary is followed by Dr. Micha-Manuel Bues' paper, "Compliance Tech," in which Dr. Bues focuses on the use of big data to ensure compliance and conduct internal investigations.

Lastly, the organizational sociological perspective of compliance is then featured by Dr. Jens Bergmann in his piece entitled "When Compliance Fails".

With our best regards,

Michele DeStefano & Dr. Hendrik Schneider
Founders and Content Curators of CEJ

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

INTERNAL INVESTIGATIONS AND THE EVOLVING FATE OF PRIVILEGE[1]

Lucian E. Dervan

AUTHOR

Professor Dervan joined the Southern Illinois University School of Law faculty in 2009 and focuses his teaching and scholarship on domestic and international criminal law. He is a member of the American Bar Association Criminal Justice Section's Council and serves as a member of the Advisory Committee of the NACDL White Collar Criminal Defense College at Stetson. Professor Dervan has been invited to speak about criminal law before various organizations and bodies, including the United States House of Representatives' Judiciary Committee, the United States Sentencing Commission, and the International Criminal Tribunal for the former Yugoslavia. Prior to joining the SIU School of Law, Professor Dervan served as a law clerk to the Honorable Phyllis A. Kravitch of the United States Court of Appeals for the Eleventh Circuit. He also spent six years in private practice with King and Spalding LLP and Ford and Harrison LLP. Professor Dervan provides expert testimony and consulting services regarding both domestic and international criminal law, including white collar crime, internal corporate investigations (both domestic and international), and plea bargaining (individual and corporate).

ABSTRACT

In 1981, the United States Supreme Court delivered a landmark ruling in Upjohn Co. v. United States. The decision made clear that the protections afforded by the attorney-client privilege apply to internal corporate investigations. This piece examines the fundamental tenets of Upjohn, discusses some recent challenges to the applicability of privilege to materials gathered during internal investigations, and considers the manner in which the international nature of modern internal investigations adds complexity and uncertainty to the field.

---

[1] Thank you to my research assistant, Zachary Lessard, for his assistance with this piece.

TABLE OF CONTENTS

I. INTRODUCTION 5

II. KELLOGG BROWN & ROOT 6

III. WAL-MART 8

IV. BANK OF CHINA 10

V. CONCLUSION 13

I. INTRODUCTION

In 1981, the United States Supreme Court was asked to consider the applicability of the attorney-client privilege to a corporate internal investigation in the case of *Upjohn Co. v. United States*.[2] The case stemmed from an internal investigation into questionable payments to foreign officials by employees of a pharmaceutical manufacturer. As part of the internal investigation, the corporation distributed a questionnaire to its employees seeking relevant information regarding such payments. The responses were then reviewed by the corporation's General Counsel and outside attorneys. Eventually, several governmental entities became involved in the matter, including the Internal Review Service, who was interested in the tax consequences of the payments. As part of its inquiry, the IRS requested copies of the questionnaire responses provided to investigating counsel by Upjohn's employees. The company refused on the basis of the attorney-client privilege and the matter was litigated to the Supreme Court.

In reaching its decision in the case, the Supreme Court considered the lower court's assertion that the privilege did not apply "[t]o the extent that the communications were made by officers and agents not responsible for directing Upjohn's actions in response to legal advice . . . for the simple reason that the communications were not the 'client's.'"[3] In the lower court's opinion, only those in the corporation's "control group" were covered by the privilege. In considering the matter, the Supreme Court rejected the "control group" approach, stating that the test "frustrates the very purpose of the privilege by discouraging the communication of relevant information by employees of the client to attorneys seeking to render legal advice to the client corporation."[4] In explaining its decision, the Court reminded the parties of the historical purpose of the privilege.

> The attorney–client privilege is the oldest of the privileges for confidential communications known to the common law. Its purpose is to encourage full and frank communication between attorneys and their clients and thereby promote broader public interests in the observance of law and administration of justice. The privilege recognizes that sound legal advice or advocacy serves public ends and that such advice or advocacy depends upon the lawyer's being fully informed by the client.[5]

Consistent with the spirit and purpose of this language, the Court concluded that the

---

2 449 U.S. 383 (1981).

3 *Id.* at 388.

4 *Id.* at 392.

5 *Id.* at 389.

questionnaires were covered by the attorney-client privilege.

The *Upjohn* decision made clear that the protections afforded by the attorney-client privilege apply to internal corporate investigations and interactions between investigating counsel and employees. Nevertheless, challenges to the applicability of the privilege have continued as adversarial parties have sought to gain access to materials from these inquiries. This piece examines three such examples and considers the lessons learned for corporations and their counsel in each.

II. KELLOGG BROWN & ROOT

One of the most publicized cases regarding internal investigations and privilege in recent years is the *Kellogg Brown & Root* ("KBR") matter in the District of Columbia. In the *KBR* case, a whistleblower argued that the corporation had defrauded the government related to military contracts in Iraq.[6] During discovery, the whistleblower requested documents regarding a prior internal investigation of the matter conducted by in-house counsel at the company. KBR refused, asserting that the investigation had been undertaken to obtain legal advice and, therefore, the materials sought were protected from disclosure by the attorney-client privilege.[7] In reviewing the matter, the district court concluded that the materials were not protected from disclosure because the defendant had not shown that "the communication would not have been made 'but for' the fact that legal advice was sought."[8] According to the district court, "KBR fail[ed] to carry its burden to demonstrate that the attorney-client privilege applies to the COBC documents. Most importantly, the Court finds that the COBC investigations were undertaken pursuant to regulatory law and corporate policy rather than for the purpose of obtaining legal advice."[9]

In 2014, the United States District Court for the District of Columbia overturned the lower court ruling, concluding that the "same considerations that led the Court in *Upjohn* to uphold the corporation's privilege claims apply here."[10] In reaching its decision, the appellate court offered important clarifications regarding the *Upjohn* decision. First, the court made clear that *Upjohn* "does not hold or imply that the involvement of

---

6 *In re Kellogg Brown & Root, Inc. et al.*, 756 F.3d 754, 756 (D.C. Cir. 2014). Many of the cases discussed and referenced herein also include issues related to the work-product doctrine. This article, however, will only focus on the cases as they related to the attorney-client privilege.

7 *See id.*

8 *Id.*

9 *United States ex rel. Barko v. Halliburton Company*, 37 F.Supp.3d 1, 5 (D.D.C. 2014).

10 *In re Kellogg Brown & Root, Inc. et al.*, 756 F.3d at 757.

outside counsel is a necessary predicate for the privilege to apply."[11] Second, the court explained that "communications made by and to non-attorneys serving as agents of attorneys in internal investigations are routinely protected by the attorney-client privilege."[12] Third, the court noted that *Upjohn* does not require a "company to use magic words to its employees in order to gain the benefit of the privilege for an internal investigation."[13]

The appellate court in the *KBR* case also rejected the lower court's argument that the company's internal investigation did not deserve privilege protection because it was the result of regulatory requirements and corporate policies. The appellate court stated, "So long as obtaining or providing legal advice was one of the significant purposes of the internal investigation, the attorney-client privilege applies, even if there were also other purposes for the investigation and even if the investigation was mandated by regulation rather than simply an exercise of company discretion."[14] As part of this analysis, the appellate court rejected the lower court's use of a "but for" test to determine if a communication was properly protected by the attorney-client privilege.[15]

> [T]he District Court's novel ["but for"] approach would eradicate the attorney-client privilege for internal investigations conducted by businesses that are required by law to maintain compliance programs, which is now the case in a significant swath of American industry. In turn, businesses would be less likely to disclosure facts to their attorneys and to seek legal advice, which would "limit the valuable efforts of corporate counsel to ensure their client's compliance with the law." *Upjohn*, 449 U.S. at 392.[16]

The appellate court concluded by determining that the district court "clearly erred."[17]

Despite the strong language from the appellate court in the *KBR* case, the plaintiffs in the matter continued to challenge the applicability of the attorney-client privilege.[18] The matter eventually made its way to the United States Supreme Court, which denied the

---

11 *Id* at 758.

12 *Id.*

13 *Id.*

14 *Id.* at 758-59. As part of this analysis, the appellate court also rejected the lower court's use of a "but for" test with regard to the purpose of the communication. *See id.* at 759.

15 *See id.* at 759.

16 *Id.* at 759.

17 *See id.* at 760.

18 *See Kellogg Brown & Root, Inc. et al.*, 2015 WL 4727411 (D.C. Cir. Aug. 11, 2015).

plaintiff's writ of certiorari in January 2016.[19] The *KBR* matter is a strong signal that, despite *Upjohn*, investigating counsel must be prepared for potential litigation regarding the applicability of the attorney-client privilege to internal investigations. To this end, counsel must be vigilant in ensuring that the investigation and any subsequent disclosures are made with a full understanding and appreciation of the risks of such challenges.

III. WAL-MART

Another internal investigation matter that has garnered recent attention is the dispute over the applicability of the attorney-client privilege to an internal investigation conducted by Wal-Mart related to alleged violations of the Foreign Corrupt Practices Act. The matter began when the New York Times published a story in April 2012 regarding potential bribery by employees of Wal-Mart in Mexico.[20] The article included allegations that Wal-Mart executives had been aware of the conduct since 2005, and failed to adequately respond.[21] In particular, the article alleged that Wal-Mart had conducted an ineffective internal investigation, allowing the same general counsel of Wal-Mart de Mexico who was implicated in the scandal to lead the inquiry.[22] In June 2012, the Indiana Electrical Workers Pension Trust Fund IBEW ("IBEW"), a Wal-Mart shareholder, contacted the company and requested access to documents related to the company's investigation of the bribery allegations.[23] Wal-Mart provided some materials, but declined to provide documents that that they argued were protected by privilege or not necessary and essential to the trust fund's inquiry.[24] The issue eventually moved into the Delaware Court of Chancery, which ordered Wal-Mart to produce the documents under what is known as the *Garner* doctrine.[25] The matter was then appealed to the Delaware Supreme Court, which also focused on the *Garner* doctrine to determine whether the plaintiffs were entitled to the materials.[26]

---

19 *See United States ex rel. Barko v. Kellogg Brown & Root, et al.,* U.S., No. 15-589*, cert. denied* (Jan. 16, 2016).

20 *See* David Barstow, *Vast Mexico Bribery Case Hushed Up by Wal-Mart After Top-Level Struggle*, New York Times (April 21, 2012), *available at* http://www.nytimes.com/2012/04/22/business/at-wal-mart-in-mexico-a-bribe-inquiry-silenced.html?pagewanted=all&_r=0

21 *See id.*

22 *See id.*

23 *See Wal-Mart Stores Inc. v. Indiana Electrical Workers Pension Trust Fund IBEW*, 95 A.3d 1264, 1268-69 (Del. 2014)

24 *See id.* at 1269.

25 *See id*. at 1270 (citing *Garner v. Wolfinbarger*, 430 F.2d 1093 (5th Cir. 1970)).

26 *See id.*

The *Garner* doctrine "allows stockholders of a corporation to invade the corporation's attorney-client privilege in order to prove fiduciary breaches by those in control of the corporation upon showing good cause."[27] In determining whether good cause exists, the Garner court established a number of factors for consideration.

There are many indicia that may contribute to a decision of presence or absence of good cause, among them the number of shareholders and the percentage of stock they represent; the bona fides of the shareholders; the nature of the shareholders' claim and whether it is obviously colorable; the apparent necessity or desirability of the shareholders having the information and the availability of it from other sources; whether, if the shareholders' claim is of wrongful action by the corporation, it is of action criminal, or illegal but not criminal, or of doubtful legality; whether the communication is of advice concerning the litigation itself; the extent to which the communication is identified versus the extent to which the shareholders are blindly fishing; the risk of revelation of trade secrets or other information in whose confidentiality the corporation has an interest for independent reasons.[28]

In this matter, because the IBEW was a shareholder, much of the contention centered on the necessity of breaching the privilege to obtain the information sought.

After reviewing the facts of the case and the *Garner* doctrine, the Delaware Supreme Court affirmed the lower court decision ordering Wal-Mart to produce the privileged materials.[29] In reaching its decision, the Delaware Supreme Court noted the importance of the attorney-client privilege and stated, "[T]he *Garner* doctrine fiduciary exception to the attorney-client privilege is narrow, exacting, and intended to be very difficult to satisfy."[30] Nevertheless, the court reasoned that the plaintiff's had satisfied this high bar. The conclusion was reached, in part, because the focus of the suit was on the internal

---

27 *See id.* at 1276.

> The attorney-client privilege still has viability for the corporate client. The corporation is not barred from asserting it merely because those demanding information enjoy the status of stockholders. But where the corporation is in suit against its stockholders on charges of acting inimically to stockholder interests, protection of those interests as well as those of the corporation and of the public require that the availability of the privilege be subject to the right of the stockholders to show cause why it should not be invoked in the particular instance.

Id.

28 *Id.* at 1276 n.32 (quoting *Garner*, 430 F.2d at 1104).

29 *Id.* at 1280.

30 *Id.* at 1278.

investigation itself, rather than the underlying bribery.[31] This led the court to conclude that providing access to the privileged investigatory materials was necessary and essential to the IBEW's claims. As the lower court stated when considering the matter, "[W]here there is a colorable basis that part of the wrongdoing was in the way the investigation itself was conducted, I think it's very difficult to find those documents by other means."[32]

As shareholder suits related to allegedly improper or inadequate internal investigations grow, counsel must be cognizant of the possibility that plaintiffs might attempt to overcome privilege protections using the *Garner* doctrine.[33] This should serve as a reminder to corporations of the importance of engaging independent outside counsel to conduct thorough and credible investigations when potential serious misconduct is discovered.[34] If the Wal-Mart investigation itself had not been at issue here, it is probable that the *Garner* exception to the privilege protection might not have been invoked and the materials might have remained protected from compelled disclosure.

IV. BANK OF CHINA

The above cases demonstrate the increasing frequency with which challenges are being brought regarding the application of privilege to internal investigation materials. While the above cases center on the application of United States privilege law, the growing international nature of internal investigations means that foreign privilege laws are also of vital importance. As noted in my 2011 article, *International White Collar Crime and the Globalization of Internal Investigations*, understanding how privilege laws vary by jurisdiction is imperative for investigating counsel.[35]

---

31 *See Wal-Mart Stores Inc.,* 95 A.3d at 1278 ("The record reflects that IBEW's proper purposes sought information regarding the handling of the WalMex Investigation, whether a cover-up took place, and what details were shared with the Wal-Mart Board. The Court of Chancery explained that the documents IBEW sought under *Garner* 'go to those issues.'").

32 *Id.* at 1279.

33 *See e.g. In re Lululemon Athletica Inc.*, 220 Litigation, C.A. No. 9039-VCP (April 30, 2015) (in which the Delaware Court of Chancery ordered the company to produce certain privileged documents to plaintiffs related to an investigation of potential insider trading).

34 *See* Lucian E. Dervan, *International White Collar Crime and the Globalization of Internal Investigations*, 39 FORDHAM URBAN LAW JOURNAL 361 (2012); *Responding to Potential Employee Misconduct in the Age of the Whistleblower: Foreseeing and Avoiding Hidden Dangers*, 3 BLOOMBERG CORPORATE LAW JOURNAL 670 (2008).

35 Lucian E. Dervan, *International White Collar Crime and the Globalization of Internal Investigations*, 39 FORDHAM URBAN LAW JOURNAL 361 (2012).

> [O]ne must be familiar with privilege laws in the jurisdictions, both regional and national, involved in an international internal investigation as the rules vary dramatically by country and subject matter. While the different variations of privilege can have a myriad of impacts on an internal inquiry, two will be mentioned here specifically. First, the role of inhouse counsel, including a corporation's general counsel, must be closely examined. While it is common for in-house counsel in the United States to perform a preliminary inquiry to determine whether outside counsel is required for a more extensive investigation, in some jurisdictions the materials and information collected during this initial appraisal of the situation might not be protected from compulsory disclosure. . . Second, counsel must be aware of the possibility that attorneys from one region of the globe might not enjoy any privilege protections in certain jurisdictions, even if they are independent outside counsel. . . While grappling with the difficulties presented by these divergent privilege rules is challenging, conducting an international internal investigation without consideration of their impact on the course and conduct of the inquiry could be fatal.[36]

The potential ramifications for the existence of varying approaches to the attorney-client privilege around the world is well illustrated by the *Bank of China* case.[37]

The *Bank of China* case stems from the death of Daniel Wultz and the injuries suffered by Yekutiel Wultz in a 2006 suicide bombing in Tel Aviv, Israel.[38] The attack was carried out by the Palestinian Islamic Jihad ("PIJ"), an organization designated a terrorist group subject to economic sanctions.[39] In response, the Wultz family filed suit against the bank and others in federal court in the United States, alleging, among other things, that the bank had provided material support to the PLI in violation of United States law. According to the plaintiffs, the Bank of China failed to comply with the economic sanctions against the PIJ and facilitated wire transfers for the organization that "were instrumental in helping the PIJ to plan and execute terrorist attacks."[40] During discovery in the matter, the plaintiffs sought documents from the Bank of China, including materials located in China and related to "anti-money laundering ("AML") and compliance procedures and investigations."[41] The bank, however, refused to provide certain materials, alleging they were protected from disclosure by the attorney-client privilege. In

---

36 *Id.* at 372-73.

37 *See* Wultz v. Bank of China Ltd., 304 F.R.D. 384 (S.D.N.Y. 2015); Wultz v. Bank of China ltd., 979 F. Supp. 2d 479 (S.D.N.Y. 2013).

38 *See* Wultz, 979 F. Supp. 2d at 483.

39 *See* Wultz v. Bank of China Ltd., 811 F. Supp. 2d 841, 844 (S.D.N.Y. 2011).

40 *Id.*

41 *Wultz,* 979 F. Supp. 2d at 484.

response, the plaintiffs filed a motion to compel.

In addressing the dispute, the court first determined which privilege law was applicable in the matter. This was of vital significant because of distinctions between the privilege laws of the United States and China. After examining choice of law precedent, the court concluded that some documents were government by Chinese law and others were governed by American law.[42] With regard to the documents governed by Chinese law, the court quickly disposed of the issue by noting that Chinese law does not recognize the attorney-client privilege.[43] As a result, the court ordered the bank to produce those materials government by Chinese law and dated prior to receipt of the plaintiff's demand letter on January 28, 2008, which date marked the beginning of litigation in the case.[44] With regard to the documents government by American law, the court focused on whether the protections afforded by the attorney-client privilege should be extended to communications between employees of the company and members of the company's Legal and Compliance Department in China. The plaintiffs argued that the company's in-house counsel in China were "not required to have legal degrees or bar certificates" and, therefore, communications with them were not entitled to protection by the attorney-client privilege.[45] The Bank of China responded by arguing that the Chinese in-house counsel were the "functional equivalent" of attorneys and were permitted to offer legal advice.[46] The court agreed with the plaintiffs and concluded that the bank had failed to establish that the communications satisfied the requirements of the attorney-client privilege.[47]

> The *United Shoe* principle justifies the protection of the attorney-client privilege for circumstances where a lawyer—whose authority derives from her position as a

---

42 *See id.* at 489-92. The court utilized a "touch base" analysis in determining which country's privilege laws should apply. This analysis asks which country "has the 'predominant' or 'the most direct and compelling interest' in whether those communications should remain confidential, unless that foreign law is contrary to the public policy of this forum." *Id.* at 486.

43 *See id.* at 492-93 ("BOC does not seriously contest the proposition that Chinese law does not include the attorney-client privilege or work-product doctrine as understood in American law.").

44 *See id.* at 492 ("U.S. privilege law applies to all documents created after January 28, 2008 that do in fact relate to the demand letter and the subject matter that gave rise to this lawsuit, because those documents pertain to American law "or the conduct of litigation in the United States.").

45 *Id.* at 493.

46 *See id.*

47 *See id.*

> Defendant has failed to carry its burden of establishing that the documents contain "communications (1) between a client and his or her attorney (2) that are intended to be, and in fact were, kept confidential (3) for the purpose of obtaining or providing legal assistance, or attorneys' mental impressions, opinions or legal theories concerning specific litigation."

Id. (internal citation omitted).

> member of the bar—is engaged to provide legal advice. While the Chinese legal system may be developing, the distinctions between lawyer and in-house counsel are clear and presumably exist for a good reason. I see no compelling reason to depart from the long-standing principle of *United Shoe* and create a "functional equivalency" test for the invocation of the attorney-client privilege when applying United States law. To the extent BOC has claimed privilege over communications from, to and among members of legal or other departments who are not licensed attorneys, the attorney-client privilege does not apply.[48]

In concluding its discussion of the privilege issue, the court reminded the parties of the fundamental rule that "[p]rivilege does not apply to 'an internal corporate investigation . . . made by management itself.'"[49]

The *Bank of China* case is an important example of the complexities and potential pitfalls that can result from the international and cross-border nature of modern internal corporate investigations. The decision of the court in the *Bank of China* case to compel the disclosure of materials from the investigation makes clear that counsel must consider and react to varying global standards regarding the applicability of privilege when structuring and conducting an investigation. This includes understanding that privilege laws in foreign jurisdictions may determine the outcome of discovery disputes in not only foreign venues, but also in United States courts.

V. CONCLUSION

In 1981, the United States Supreme Court made clear in *Upjohn* that the protections afforded by the attorney-client privilege apply to internal corporate investigations. Nevertheless, the application of such privilege protections remains an evolving field as new challenges are brought and new complexities are introduced. As investigating counsel continue engaging in these matters, it remains vital that privilege considerations and changes in this area of law remain at the forefront of their minds as they both structure and conduct inquiries.

---

48 *Id.* at 495. The quote refers to *United States v. Shoe*, 89 F. Supp. 357 (D.C. Mass. 1950).

49 *Id.* at 496; *see also* Lucian E. Dervan, *International White Collar Crime and the Globalization of Internal Investigations*, 39 FORDHAM URBAN LAW JOURNAL 361, 367-73 (2012) (discussing the importance of using legal counsel when conducting internal investigations).

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

AMBIGUITIES IN INTERNATIONAL INTERNAL INVESTIGATIONS

Christian Pelz

AUTHOR

Dr. Christian Pelz is a partner at the international law firm Noerr LLP and a specialist in criminal law and tax law. He heads the white-collar crime group at Noerr LLP. Dr. Pelz is a lecturer in criminal law at the University of Augsburg and a member of the Center for Criminal Compliance at Justus-Liebig-University Giessen.

TABLE OF CONTENTS

I. CONFIDENTIALITY AND ACCESS TO INFORMATION 16

II. IN-HOUSE LEGAL PRIVILEGE 18

III. NOTIFICATION REQUIREMENTS 19

IV. ATTORNEY-CLIENT PRIVILEGE OF INVESTIGATORS 22

V. MONEY LAUNDERING 23

VI. AMBIGUITY IN COMPANY INTEREST 24

VII. CONCLUSION 25

The settings and circumstances of internal investigations are as manifold as life itself. They are conducted according to the usual customs of the company and the legal tradition in its jurisdiction. Internal investigations differ depending on their scope and goals. A compliance audit examining whether local management adhered to internal rules and regulations and compliance processes is conducted differently compared to an investigation following a whistle-blower report. Internal investigations conducted in parallel with criminal investigations or those of supervisory authorities or aimed at supporting these investigations often follow other rules. Just as the particular circumstances of internal investigations can differ considerably, the legal issues raised by them can be equally varied and complex, in particular in group-wide cross-border investigations. All affected companies and corporate bodies, holding companies and affiliates or even different departments within one company, the management and supervisory boards of the companies, their shareholders, employees, business partners and other external players often have varied and conflicting interests which sometimes cannot easily be resolved and many of which are protected by applicable local laws.

In the following I would like to address some typical areas in international internal investigations in which legal conflicts exist between holding companies and affiliates or within participating entities and functions: Some of these are often overlooked when defining the scope or methods of an internal investigation and its legal limits.

I. CONFIDENTIALITY AND ACCESS TO INFORMATION

Privacy and data protection issues are of major concern in any kind of compliance review, compliance audit and in particular in international internal investigations.[1] Data might be transferred from one corporate body (affiliate) to another (holding company) and/or to different jurisdictions. Even regular or random controls by the internal audit or compliance department of the holding company can trigger similar complex privacy issues which need legal assessment under all applicable laws in all affected jurisdictions. Even if awareness of these issues exists within a group of companies, it often first has to be raised at foreign law enforcement agencies.[2] Privacy issues can require the company to delete any reference to or redact personal data, in particular names, or other information which easily allows the identification of an individual.[3] This can make it impossible to

1 Tim Wybitul, *chapter II note I*, *in* Internal Investigations (Thomas C. Knierim et al eds., 2012); Thomas C. Knierim, *chapter 5 note 140*, *in* Handbuch des Wirtschafts- und Steuerstrafrechts (Heinz-Bernd Wabnitz & Thomas Janovsky, 4th ed. 2006).

2 Ralf Deutlmoser & Alexander Filip, *European Data Privacy versus U.S. (e-)Discovery Obligations - A Practical Guide For Enterprises,* ZEITSCHRIFT FÜR DATENSCHUTZ (ZD) (6/2012).

3 Tim Wybitul, *Interne Ermittlungen auf Aufforderung von US-Behörden – ein Erfahrungsbericht*, BETRIEBS-BERATER (BB) 606, 610 (12.2009); Stephan Spehl & Thomas Grützner, *§ 6 (Germany), in* Corporate Internal Investigations note 159 (Spehl/Grützner, 2013).

provide documents or emails without redacting parts of them and requires the depersonalisation of investigation reports.

Apart from privacy laws, it is not always the case that the internal audit or compliance department or an external law firm or auditing firm which has been instructed to conduct an internal investigation can access information and data in possession of a company which has not requested the audit. In almost all jurisdictions, the management of a company is duty-bound to protect its trade and business secrets. This is one of the duties of managers and employees arising from their employment contracts, the company's articles of association, or statutory civil or criminal law provisions. This covers, amongst other things, details on contractual relations with customers and vendors, how a contract was acquired, how the company has interacted with competitors and similar matters. Whether or not or to what extent a trade or business secret can be disclosed to other parties, even if they belong to the same group of companies, must be determined on a case-by-case basis. The laws of more than one jurisdiction may apply if the secrets of a company are available in branch offices or shared service centres situated in various countries.

A secret can be disclosed if the party whose interest is to be protected by the confidentiality obligation consents thereto. Whether the consent of the management is sufficient or whether the consent of the supervisory board or the shareholders is also required, must be determined on the basis of applicable national law. The same applies to the question of which requirements relating to form and other prerequisites must be met.

Confidentiality clauses in contracts can oblige a contractual party to keep all information related to that contract confidential even with respect to holding companies. Controls by holding companies or vague compliance requirements do not nullify such confidentiality obligations. Although the holding company may feel that it has a legitimate interest in obtaining such information, the affiliate's obligation under applicable law may be different. Non-compliance with contractual confidentiality obligations normally results in a breach of contract and places the breaching party at risk of the other contractual party asserting its right to obtain a remedy, in particular to termination and/or damages. Additionally, it must be taken into account that results obtained in an internal investigation by violation of such confidentiality obligations may not be used against the other contractual party.
In certain cases, the breach of confidentiality obligations can also constitute a criminal offence. If the offence is designed to protect business secrets of the company from unlawful disclosure by management or employees, the consent of the competent body of the company will eliminate criminal risk. However, if the contractual party is a governmental or semi-governmental entity or company, statutory confidentiality regulations in that party's jurisdiction may apply. This may in particular apply if business or contracts with national security authorities, secret services or their procurement entities are concerned. Applicable law may provide that even the granting of access to employees of a contractual party requires prior notification and/or the consent of the other contractual

party, and even more if access is to be granted to employees of outside parties. A violation of these statutory confidentiality rules may entail criminal law risks. Both the breaching party, its directors or officers as well as all individuals who were unlawfully given access to the information may be at risk of having committed espionage or related crimes. The result in such cases can be, for example, that a document or email search in an internal investigation on alleged bribery requires the prior consent of the bribed party. Similarly, Articles 271 and 273 of the Swiss Criminal Code prohibit the gathering of evidence or collection of business secrets which will or might be used in proceedings or litigation in foreign countries and, thus, limits the potential use of information gathered or revealed in the course of internal investigations on Swiss soil.[4]

II. IN-HOUSE LEGAL PRIVILEGE

Legal privilege issues are usually discussed with respect to the protection of privileged information from disclosure to law enforcement agencies and prosecutors. Similar problems arise in internal investigation situations with respect to the disclosure of information to the compliance department or the internal investigators, at least for those jurisdictions which acknowledge legal privilege with respect to advice given by in-house counsel.[5] Depending on whether legal privilege is a right of members of the legal profession, as in the Netherlands, or a right of the client, the client's consent to disclosure to the internal investigators may be required. This leads to the question of who the client is, irrespective of whether advice was given by in-house counsel or external counsel. The company or also the manager concerned?

Example:
The managing director of a Romanian affiliate of a Japanese company approaches the regional legal department on what steps he, as a managing director, must take after becoming aware of rumours that the sales department may have used a dubious consultant for the acquisition of a contract.

In such contexts it cannot easily be said that the managing director did not act in a personal capacity, but as a function holder of the affiliate. In many situations it is difficult to determine whether the instructions were (solely) aimed at obtaining advice on what the legal obligations of the company are, but (additionally) what he in his capacity as

4 Mark Livschitz, *§ 12 (Switzerland), in* Corporate Internal Investigations note 21 et seq (Spehl/Gruetzner, 2013).

5 Hilmar Raeschke-Kessler, *The production of documents in international arbitration - a commentary on article 3 of the new IBA Rules of Evidence*, ARBITRATION INTERNATIONAL 411 (2002); Gabrielle Kaufmann-Kohler & Antonio Bärtsch, *Discovery in international arbitration: How much is too much?* ZEITSCHRIFT FÜR SCHIEDSVERFAHREN (SCHIEDSVZ) 13, 19 f. (2004).

function holder is required to do. The answer to this question determines whether access to that information requires the consent of the manager concerned as well. This could be difficult if he or she is or may become a suspect in the investigation or has already left or been dismissed from the company. Similar questions arise regarding the scope of protected information, in particular if the consent of employees providing information to in-house counsel for giving advice to the client is also required.

III. NOTIFICATION REQUIREMENTS

In many cases, the results of the internal investigations will be used to meet mandatory requirements under applicable law, to immediately stop any illegal activities, to attempt remediation if deficiencies or weaknesses in processes and controls are discovered or to take appropriate employment measures up to the dismissal of the individuals involved. Companies usually have broad discretion to disclose the findings of internal investigations to law enforcement agencies. This depends mostly on the corporate culture of the company, legal traditions in the jurisdictions affected and whether a zero tolerance policy is interpreted in such a way that all violations of criminal law or particular violations will be disclosed to prosecutors or other law enforcement agencies.

Certain jurisdictions do have leniency programmes principal witness arrangements) in place or provide for principal witness arrangements (like Section 209b Austrian Code of Criminal Procedure) if an offence is disclosed voluntarily or the disclosing party is the first to inform law enforcement agencies about criminal conduct and makes a significant contribution to the full disclosure and investigation of the notified conduct. Such leniency programmes can lead to a reduction in fines. For example, Article 16 of the Brazilian Law 12,846 (Clean Companies Act) establishes that upon participation in a leniency programme, corporate fines will be reduced by two-thirds. Other jurisdictions provide for exemption from criminal prosecution, e.g. Articles 290 (3) and 292 (2) of the Criminal Code of Romania or Sections 371, 398a and 378 (3) of the Fiscal Code of Germany. Companies have wide discretion on whether to make use of these leniency possibilities or to refrain from doing so.[6] In many jurisdictions there is a lack of experience regarding whether these provisions have been applied at all or how they will be applied in practice.

In other jurisdictions there are compulsory notification requirements, either in general or in particular situations. Most jurisdictions provide for mandatory notification of certain forthcoming infringements of law, mainly serious offences. Some of them are connected to health and safety violations, violations of technical safety requirements or

6 Gerald Spindler, AktG, *section 93, in* Münchener Kommentar note 54 (Wulf Goette et al eds., 3rd ed. 2008); Christian Pelz, *Offenbarungs- und Meldepflichten bei Internal Investigations, in* Festschrift für Jürgen Wessing 614 (Heiko Ahlbrecht et al eds., 1st ed. 2016).

environmental hazards. For example, this applies to Chapter 15 Section 10 of the Finnish Criminal Code. Disclosure requirements may result if the internal investigation reveals that unsafe or dangerous products have been distributed or sold which may require a product warning or a recall.

Certain jurisdictions also impose an obligation to notify law enforcement agencies of criminal conduct committed in the past. For example, Article 108 of the Criminal Procedure Code of the People's Republic of China obliges every organisation and individual to notify law enforcement agencies if a crime is suspected. Comparably, under Article 77 of the Law 906/2004 of Columbia, anyone who has knowledge of a past offence must file a notification. In both countries, the duty to inform law enforcement agencies is a general civic duty. A violation of such duty does not, however, incur criminal liability.

The duty of legality is a major pillar of all compliance systems worldwide, requiring the company, its managers and employees to abide by the rules of law, at home and abroad. In particular, managers can become liable for damages if they do not ensure that the company complies with all applicable domestic and foreign law.[7] Taking compliance seriously and in a strict dogmatic manner, the company has to notify the law enforcement agencies of such criminal conduct; otherwise it will be difficult to explain to their employees that the company expects full compliance with the law from its employees, but itself supports cherry-picking and decides on a case-by-case basis whether it is appropriate to meet legal requirements.

It can be argued that non-compliance with these laws does not impose a legal risk on the company and flouting the law may only cause reputational but not financial harm. Although this is true from a commercial perspective, such convenient decisions undermine the acceptance and notion of compliance as a whole.

It becomes much more difficult to resolve these conflicts if non-compliance can be enforced by sanctions. Sometimes sanctions are minimal, such as those in Art. 274 Criminal Code of the United Arab Emirates, under which non-notification of a crime can be penalised with a fine of up to 1,000 dirhams (equivalent to approximately EUR 240 or USD 250). From a financial perspective there will be room to weigh up the commercial interests of the company with the consequences of non-compliance. However, other jurisdictions provide for severe criminal sanctions including imprisonment for violation of notification requirements. For example Sec. 316 (1) Crime Act 1900 of New South Wales, Sec. 34 Prevention and Combatting of Corrupt Activities Act of South Africa or

7 Regional Court Munich 10.12.2013 - 5 HK O 1387/10, NZWiSt 2013, 183, 187; Christian Pelz, *We observe local law – Strafrechtskonflikte in internationalen Compliance-Programmen*, CORPORATE COMPLIANCE ZEITSCHRIFT (CCZ) 234, 237 (2013).

Art. 441 of Law 599/2000 of Colombia provide for fines and/or imprisonment if past criminal conduct is not disclosed to the relevant law enforcement agencies. Whilst these criminal law provisions require both intent and proof that a crime was committed, internal investigations often cannot furnish full proof of a criminal offence but only a more or less high degree of suspicion, so that – from a pragmatic perspective – there may be some room left for argumentation. However, the law can be different in other jurisdictions. Article 368 of the Czech Criminal Code or Article 340 of the Criminal Code of Slovakia, for example, provide that each individual is obliged to notify law enforcement agencies about the mere suspicion of certain criminal conduct, such as bribery offences. Such obligation is imposed on any person within the reach of the applicable law. In jurisdictions which acknowledge criminal liability of companies, the obligation is imposed on companies as well. In addition to this, each natural person within the scope of application of that law is obliged to meet the notification requirements. This may apply to board members of the relevant company, future board members, or every employee residing in the territory where the relevant act took place who learns about such suspicion. Notwithstanding this, the internal investigators, once they learn or have knowledge of such suspicion and are residing in the territory of such jurisdiction, even temporarily, are also required to make such notification.

If lawyers or accountants act as internal investigators, conflicts between such notification requirements and the obligation to protect attorney-client privilege may result. Whilst most countries acknowledge attorney-client privilege, it needs to be determined whether such privilege applies only to attorneys and accountants admitted to the local bar or if it is also granted to foreign lawyers and accountants. In most jurisdictions, attorneys and accountants admitted in one EU Member State can request admission in another Member State for certain activities or proceedings and then enjoy the same protection as local attorneys. However, this may not apply to internal investigations, but only to legal proceedings. Further, it is questionable whether suspicion obtained by investigating books and records of a company is protected by attorney-client privilege, in particular if the lawyer or accountant has not received such information from or on behalf of their client.

This problem becomes more complex if the violation of professional secrecy obligations also constitutes a criminal offence under the laws of the country in which the internals investigator are admitted or practise. The professionals concerned then have a problem: they will be criminally liable under the laws of the country in which they were admitted to practise if they disclose information or would do so under the laws of where the investigation is taking place if they refrain from disclosing it. The only option this leaves these professionals is to decide which offence they would prefer to commit. It might be a defence argument that a person cannot be held criminally liable if either reaction would lead to the violation of criminal law. Whether or not such a defence would be acknowledged is a question of applicable national jurisdiction. There are virtually no court precedents and uncertainty will therefore remain. It would be unjust to rule out this defence due to the fact that professionals in an internal investigation voluntarily put

themselves in a situation in which they had to notify the authorities and that by accepting such a mandate remit, the notification requirement prevails. Investigators who are not bound by professional secrecy cannot even rely on this defence but have no other option from a legal point of view but to meet the disclosure requirements.

In my experience, internal investigators in such situations will most likely refrain from complying with the notification requirement and accept that they will commit a criminal offence (provided they even know about their notification requirements). This is driven by a pragmatic approach: The internal investigators will most likely be admitted and practise in a foreign jurisdiction and will only be temporarily subject to the scope of application of these criminal law provisions on notification for a considerably short period of time, thus considerably reducing the actual risk of prosecution.

IV. ATTORNEY-CLIENT PRIVILEGE OF INVESTIGATORS

Usually when conducting an internal investigation, companies try to protect attorney-client privilege and attorney-work privilege as best as possible. In international internal investigations it is a must to determine the prerequisites and scope of attorney-client privilege in all affected jurisdictions before starting work. One must not forget to analyse this question from all aspects. Whilst information gathered by the internal investigator usually falls within the scope of attorney-client privilege, it must be assessed in which direction the scope provides protection. Usually, only the client is protected by the privilege which leads to the next question of who the client is. Accepting multiple instructions from more than one company of a group of companies is risky since each client might waive privilege separately so that remaining clients might no longer be protected against disclosure of information which is not only theirs. Often it will be difficult to determine who the owner of a secret is so that, in cases of doubt, the consent of all owners may be required. Further, if members of the compliance or internal audit department form part of the investigation team, knowledge which they obtain during the internal investigation is not protected since they are not acting in the capacity of attorneys or accountants, but within the scope of their usual work duties. To obtain full protection they may not form part of the investigation team and not obtain additional knowledge which they do not already have.

In international investigations it always is necessary to obtain local counsel for the assessment of factual questions or legal analysis. The scope of attorney-client privilege of local counsel is determined by applicable local law. In certain jurisdictions, China for

example, attorney-client privilege does not explicitly exist at all[8] or the scope of such privilege is extremely unclear. Other jurisdictions provide for attorney-client privilege only for certain members of the legal profession. In the Ukraine, for example, attorneys working for foreign law firms, rather than Ukrainian law firms, are exempt from the privilege of professional secrecy. In Russia, for example, only trial attorneys admitted as "advocats", are protected by professional secrecy[9] whilst client-attorney communication with regular attorneys is not protected at all. This must be taken into account when defining the scope of work of local counsel because even within one law firm, communication with one attorney may be privileged whilst it is not with another.

V. MONEY LAUNDERING

Anti-money laundering legislation in many jurisdictions requires obliged entities and natural persons to report suspicious transactions. Article 23 (2) of the Third Anti-Money Laundering Directive[10] and Article 34 (2) of the upcoming Fourth EU Anti-Money Laundering Directive[11], which must be transposed into the law of the Member States no later than 26 June 2017, provides that members of the legal profession and auditors may not disclose such information which they receive from, or obtain on, one of their clients, in the course of ascertaining the legal position of their client, or performing their task of defending or representing that client in, or concerning, judicial proceedings, including providing advice on instituting or avoiding such proceedings, whether such information is received or obtained before, during or after such proceedings. Otherwise, pursuant to Art. 22 (1) (a) of the Third Anti-Money Laundering Directive, reporting obligations exist if the obliged entity knows or has reasonable grounds to suspect that money laundering or terrorist financing is being or has been committed or attempted.

The reporting obligation applies not only to present and future financial transactions, but it also encompasses cases in which the obliged entity subsequently obtains knowledge of facts indicating that a transaction was or could have been related to money laundering. Whilst members of the legal profession and accountants are exempted from the reporting obligation due to the fact that conducting an internal investigation will be regarded as "ascertaining the legal position for their client", reporting obligations continue to apply to other persons. This may lead to the result that the investigated compa-

8 Michelle Gon & Ping Zheng, *§ 3 (China), in* Corporate Internal Investigations, note 68 (Spehl/Gruetzner 2013); Benjamin Miao/Peter Yuen/Melody Wang, *chapter 7 (China), in* The International Investigations Review, 104 (Nicolas Bourtin, 3rd ed. 2013).

9 Ekaterina Kobrin, *§ 10 (Russia), in* Corporate Internal Investigations, note 111 (Spehl/Gruetzner 2013).

10 Directive 2005/60/EC of 26 October 2005, Official Journal L 309/15.

11 Directive (EU) 2014/849 of 20 May 2015, Official Journal L 141/73.

ny or people participating in the investigation team without being a member of the legal profession are obliged to file a suspicious transaction report to the competent FIU. Applicable national law determines the details of the reporting obligation, in particular whether a strong suspicion of money laundering is required or a vague suspicion is sufficient.

Apart from submitting a suspicious transaction report, it must also be determined whether and to what extent criminal activity for the benefit of a corporate body or according to which a corporate body is enriched will taint assets of such company.

Example:
The Romanian entity R of a Japanese holding company obtained contracts with customer C by corrupt means. C pays the purchase price of €1 million to the accounts of R, which then show a balance of €6 million.

Will all payments received by R from C be regarded as the proceeds of a crime? Will a dividend payment of R to the holding company be made with tainted assets? Will the shares in the affiliate be regarded as the proceeds of a crime?

If assets are tainted, it must be determined whether this will lead to a contamination of the assets in full or only in part. In our example, will the transfer of the purchase price taint the whole bank account of C or just the relevant portion?[12] In the latter case, if C makes a payment of €2 million, will the whole sum be regarded as partially tainted or will it be considered untainted as long as the amount remaining in the bank account is higher than the funds of criminal origin? The answer to these questions will vary from jurisdiction to jurisdiction. Depending on the answers to these questions, it must be determined whether each and every transfer and re-transfer will be considered money laundering and whether remedies exist (and if so, which ones) to avoid the contamination of subsequent transactions.

VI. AMBIGUITY IN COMPANY INTEREST

Whether an internal investigation is conducted and how to respond to investigation results are always important decisions. It is unanimously agreed that to immediately stop any illegal activity and to ensure adherence to law in the future is of utmost importance. A differentiated approach is necessary when determining whether prosecutors and law enforcement agencies should be contacted. If self-reporting leads to immunity

12 The German Federal Supreme Court in its decision of 20.05.2015 - 1 StR 33/15, NJW 2015, 3254 held that a "considerable portion" of illegal funds will taint the whole account. The court did not elaborate on what "considerable" exactly means but states that a portion of more than 5.9 % is considerable.

from prosecution or sanctions, the decision would appear relatively easy. However, it has to be taken into account that in many cases immunity from prosecution only means that the company cannot be fined. Damage claims against the company from customers or third parties will still be possible. The same might apply to disgorgement of profits. If self-reporting only leads to a reduction in fines it must carefully be determined whether such voluntary disclosure will pay off. In many cases this is difficult to decide. It might be the case that the costs of the investigation are much higher than the expected reduction of fines. A different approach might be necessary in countries like the US, which has a tendency to impose excessive fines. These risks as well as reputational risks, the likelihood of being otherwise disclosed or the time period until the matter becomes statute-barred have to be assessed. In international cases, limitation periods in many countries are much longer than in others. There is also a risk of double punishment in two jurisdictions. Under Section 54 Schengen Convention the *ne bis in idem* principle applies only between EU Member States.[13] Even then, risks remain. It is first necessary for the other EU Member State to acknowledge this principle in the same way the other does. Secondly, protection can only be obtained for the same criminal conduct. This does not apply if one country does not prosecute due to limitation reasons or for offences which exist only in one jurisdiction but not in the other.

VII. CONCLUSION

Conducting an internal investigation always requires a careful and thorough assessment of all legal consequences which may arise from the findings. This in turn requires the investigator to analyse possible investigation results in all directions beforehand. Sometimes conflicts between jurisdictions cannot be completely avoided, but in many cases their consequences can. Proactive considerations at the beginning of an investigation are an asset which cannot be appreciated highly enough. It should be the task of the compliance organisation of a company to make itself familiar with potential consequences of legal hazards. Most will not do so. The experienced investigator should bear these issues in mind.

[13] Karsten Gaede, *Transnationales „ne bis in idem" auf schwachem grundrechtlichen Fundament*, 41 NEUE JURISTISCHE WOCHENZEITSCHRIFT (NJW) 2990 (2014); Wolfgang Schomburg & Irene Suominen-Picht, *Verbot der mehrfachen Strafverfolgung, Kompetenzkonflikte und Verfahrenstransfer*, 17 NJW 1190 (2012).

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

COLLECTING EVIDENCE IN INTERNAL INVESTIGATIONS IN THE LIGHT OF PARALLEL CRIMINAL PROCEEDINGS

Sascha Süße & Carolin Püschel

AUTHORS

Dr. Sascha Süße, LL.M. (corporate criminal law), M.A. (criminology), is a lawyer and partner of ROXIN Rechtsanwälte LLP, one of the leading law firms in Germany that specialize exclusively in corporate criminal law and criminal tax law. Dr. Süße is the head of the firm-wide expert group for Criminal Compliance & Internal Investigations and of the corresponding practice group Compliance of the ROXIN Alliance, an international network of leading law firms specializing in corporate criminal law in 30 countries worldwide. Before joining ROXIN, he was manager at the Forensic Services and Compliance department of a major accounting firm. He is an expert in the area of Compliance counseling, in particular with regard to the implementation and monitoring of Compliance systems. Dr. Süße has long-lasting experience in leading internal investigations and the representation of companies and individuals in criminal preliminary and principal proceedings. Dr. Süße is co-publisher and -editor of the monthly appearing "Newsdienst Compliance" published by C.H. Beck and is the author of several literature contributions regarding Compliance issues. Furthermore, he has been adopting a number of teaching assignments connected to his practice area for many years now, inter alia at the Universities of Augsburg, Bremen and Bielefeld, and is a regular speaker at Compliance events. He can be reached at suesse@roxin.de.

Carolin Püschel, LL.B., joined ROXIN Rechtsanwälte LLP in 2013 as a research assistant and is a member of the editorial staff of the monthly appearing "Newsdienst Compliance" published by C.H. Beck. Ms Püschel studied at Bucerius Law School (Hamburg, Germany) and Santa Clara University School of Law (California, USA) with an emphasis on corporate criminal law and graduated from Bucerius Law School in 2011. After completing her first state exam, she worked as a research assistant for Prof. Dr. Frank Saliger and PD Dr. Florian Knauer at the chair for criminal law, criminal procedure and philosophy of law at Bucerius Law School from 2012 to 2014. She has contributed as co-author to several articles on Compliance issues and regularly holds lecture accompanying seminars concerning criminal law for study groups at Bucerius Law School, while continuing to work on her doctoral thesis. She can be reached at pueschel@roxin.de.

TABLE OF CONTENTS

I. INTRODUCTION 29
A. What are internal investigations? 29
B. In what constellations are they conducted? 30
C. What are the typical accusations that are investigated? 31
D. How is the company involved in the investigated accusations? 31
E. Why do companies conduct internal investigations? 32
F. Who precisely performs them? 35
G. What is done? 35

II. COLLECTING EVIDENCE 36
A. E-mail searches 36
B. Interviewing employees 37
C. Review of documents 38
D. Background researches 38

III. RISKS OF PARALLEL CRIMINAL PROCEEDINGS FOR THE COMPANY 39
A. Risk of the company's premises being searched 39
B. Risk of an employee's habitation being searched 40
C. Risk of documents being seized 43
D. Risks resulting from testimonies of employees 46
1. The questioning of employees during a search 47
2. The utilization of statements of employees made in interviews 48
a. The duty of employees to participate in interviews 48
b. The utilization of interview protocols 49
E. Risk of a collision of investigative actions 50

IV. WAYS FOR COMPANIES TO REDUCE RISKS 51
A. Cooperation with the prosecution authorities 52
1. Conflicting priorities 52
2. Reasons why companies accept risks 53
3. Reducing risks by communication 54
4. Considering further measures to reduce risks 55
B. Proper documentation of an internal investigation 55
C. Conducting state-of-the-art interviews 55
D. Labeling documents of an internal investigation with their purpose 56
E. Providing trainings and witness assistance for employees 57

V. CONCLUSION 58

I. INTRODUCTION

Over the last decade, it has become more and more common for companies in Germany to internally investigate any detected or alleged cases of misconduct of their employees. In fact, investigating compliance violations within the company, especially potential criminal offenses, bringing them to an end and sanctioning those who committed them are the three main duties of the company's management with regard to "reactive" or "repressive" compliance. In some cases, an internal investigation is conducted parallel to pending criminal proceedings and sometimes, due to the misconduct of single employees, sanctions against the company and its management can be impending. The internal investigation then also becomes a means of defense. Obviously, such internal investigations are especially difficult as the collected evidence might at the same time have negative implications for the outcome of the criminal proceedings. The following article analyzes the challenges that companies face in conducting an internal investigation and collecting evidence parallel to ongoing criminal proceedings.

A. What are internal investigations?

The management's duty to investigate all cases of suspected misconduct is widely accepted and deprives from corporate[1] as well as administrative law regulations[2]. If the management of a company fails to investigate reliable information on potential misconduct it receives and does not stop and avenge any such detected behavior, it can become liable to the company for damages occurring from that misconduct. In the "Neubürger" decision, the District Court (Landgericht) of München I has explicitly defined the management's omission to take appropriate measures to investigate cases of misconduct about which it had been informed as a breach of its duty to implement and monitor an effective compliance management system.[3]

As there is a duty to investigate, this also means that a company is allowed to investigate on its own if suspicions of misconduct occur. Thus, it is not limited to rely on possible state investigations. In fact, both might take place parallel to each other.[4]

1 E.g. Section 93 Paragraph 1 1st sentence and Section 116 of the Stock Corporation Act and Section 43 Paragraph 1 of the Law on Limited Liability Companies.

2 In particular Section 130 of the Act on Regulatory Offenses.

3 *See* LG München I, Urteil vom 10.12.2013 – 5 HK O 1387/10 = NDCOMPLIANCE 22101 (2014), Paragraph I 2 (a) of the grounds.

4 Florian Wettner & Marius Mann, *Informationsrecht und Informationspflichten bei Internen Untersuchungen*, DEUTSCHES STEUERRECHT 655, 656 (2014).

The aim of an internal investigation usually is to gather information about any alleged facts, in order to evaluate whether any misconduct exists and in case of affirmation, who has done what, when, how and why. The company therefore may perform a number of investigative actions such as reviewing data and documents as well as interviewing employees. The results, usually summed up in an investigation report, form the basis for the evaluation of the risks at which the misconduct might put the company and for the decision about the next steps to be taken by the management.

While the term "internal investigation" has been common in other legal systems for decades, in Germany its occurrence has only risen over the last ten years. Furthermore, there is no codified special law with regard to the conduct of an internal investigation. The limits for any investigative action are hence the regulations of the applicable substantive civil and criminal law. In practice, a number of legal questions regarding the conduct but also the relation between private and state investigations remain yet open.

B. In what constellations are they conducted?

The initiation of an internal investigation often depends on the time when the alleged misconduct gets to the management's attention and whether any third party, especially a prosecution authority, has knowledge of the suspicions in question.

Sometimes an internal investigation is merely conducted because of an internal hint or an irregularity detected in an internal audit, without any external knowledge of the facts to be investigated at all. In these cases, there is usually no external pressure on the conduct of the internal investigation. Thus, it is to some extent at the discretion of the company if an external criminal proceeding is performed. Only if the company decides to actively involve the authorities, the authorities will evaluate whether an initial suspicion is constituted.

However, this condition changes as soon as there is a risk that the internal information will become public. That might be the case e.g. if there is a whistleblower who announces to give his information to the prosecution authorities or if an external audit, e.g. by the fiscal authorities, is about to take place. Finally, in other cases, state proceedings are already going on. Less critical constellations among them are those in which the person or whistleblower that has reported an offense to the prosecution authorities informs the company about the proceedings at the same time. That might be the case e.g. when the criminal proceedings are initiated parallel or prior to a pending civil law suit. Sometimes the company is also informed by reports in the media or can conclude that proceedings are ongoing or expectable, because it gets to know that a competitor is already under investigation. Again, in these cases the company has the chance to proactively contact the prosecution authorities before any compulsory measures are undertaken, and offer to cooperate and investigate the allegations internally.

Depending on the case and the expected involvement of the management and the com-

pany itself, the prosecution authorities might sometimes also contact the company in advance with regard to ongoing proceedings against one of its employees.

The most unappreciative cases, however, are usually those in which the proceedings are disclosed by compulsory measures against the company, in particular by a search. In these cases, the company's leeway in decision making is much narrower and cooperating with the prosecution authorities often becomes inevitable. Additionally, the company does not have the knowledge advantage it has when it is the first to become aware of the suspicions, but instead has to catch up with what the accusations are and what the prosecution authorities know or presume to know.

C. What are the typical accusations that are investigated?

There are basically two main categories of accusations that can be differentiated.

First, there are cases, in which the company is supposed to be a victim, i.e. has been betrayed by its employee without benefiting from the employee's actions. Examples are that an employee has accepted bribes from a supplier to contract with him although the products are of minor quality in comparison to those of other competitors or that an employee has committed fraudulent actions and transferred company funds to his private accounts.

The second category comprises constellations, in which the company might or does benefit from its employee's misconduct. Typical offenses are such that are committed in the assumed interest of the company, such as active bribery, often by using slush funds, tax evasions or fraud against a third party. In practice, those constellations are highly relevant in which these offenses were enabled by a violation of organizational or supervisory duties by a company's executive (Section 130 of the Act on Regulatory Offenses).

D. How is the company involved in the investigated accusations?

The risks imposed on the company obviously differ with regard to the two aforementioned categories.

In the vast majority of cases of the first category, the fronts are clear: the employee did act to the disadvantage of the company and thereby committed an offense, while the company – from a legal point of view – did nothing wrong, i.e. unlawful. Therefore, the company will usually not be at risk to be additionally sanctioned for what the employee did. Even more, the companies and any prosecution authority's interest will be concurrent, i.e. both will have the interest to hold the employee liable for what he did.

However, though any possible criminal proceedings occurring from that misconduct might not put the company at risk, the prosecutor's investigation itself and any compulsory measures accompanied by it might do so. For example, a search might be likely to

attract public attention and also the mere disclosure of what happened might include the risk of severe reputational damages, especially in cases where the misconduct discloses a weakness in the company's internal control system.

It should also be noted that even in these cases, depending on the facts of the single case, a prosecution authority might take another point of view and investigate a possible liability of the company or its management. That might in particular be the case, if the employee's offense was enabled by a significant lack of adequate compliance procedures and controls due to an omission of the company's management (cf. Section 130 of the Act on Regulatory Offenses).

Thus, then the same situation as in the second category would exist: In these cases, there is a risk of severe sanctions against the company and the members of its management themselves. The main risk in such cases under German law – besides reputational and other immaterial risks – is a fine under Section 30 of the Act on Regulatory Offenses, especially in connection with Section 17 Paragraph 4 of the Act on Regulatory Offenses. Sanctions can be up to EUR 10 Mio and significantly higher in cases where any benefits the company has gained are skimmed. Additionally, the exclusion from public tenders or civil claims from business partners may ensue.

The members of the management might be subject to personal fines of up to 1 Mio EUR (Section 130 of the Act of Regulatory Offenses), labor law consequences and, as the already mentioned "Neubürger" decision shows,[5] substantial civil claims for damages.

In cases under foreign law, e.g. the FCPA, or where an international body, such as the World Bank, is involved, even higher financial sanctions or more severe sanctions of another kind, e.g. exclusion from any World Bank project, might be impending. In any case, defining the role of the company with regard to the alleged misconduct and by that determining the risks the company might face, belongs to the most important tasks to be performed by the company's compliance function.[6] The question whether a company is just a victim or whether it might be subject to sanctions itself can significantly influence the process of the internal investigation and the way it is conducted.

E. Why do companies conduct internal investigations?

5 supra I. A.; LG München I, Urteil vom 10.12.2013 – 5 HK O 1387/10 = NDCOMPLIANCE 22101 (2014).

6 Cf. Sascha Süße, *Der Compliance Officer im Fokus behördlicher Ermittlungen*, NEWSDIENST COMPLIANCE 71004 (2015).

As the constellations, in which internal investigations are conducted, differ, the same applies to the reasons why they are performed.[7] However, one basic aim underlies all internal investigations: To keep the negative impact arising from the misconduct or breach of law as little and low as possible for the company and the members of its management.

If the company is a victim with regard to a single employee's misconduct, the internal investigation aims to define any damage that might have occurred and to allow the management to determine how successful any reclaims against the employee or involved third parties might be. In such cases, the company will initiate all necessary sanctions against the employee, which might include charging a criminal offense. The latter might be particularly necessary if there are strong indications for the alleged misconduct, but the last and convincing evidence cannot be retrieved by the company without the help of a state agency, such as the evidence of an incoming payment to or a withdrawal from the employee's private bank account, to which the company has and can get no access, but a prosecutor might. Additionally, in cases of complex economic contexts or where large amounts of data and information have to be reviewed and processed, it might be in the company's interest to properly prepare the data for the prosecution authorities in order to catalyze preliminary proceedings or to ensure that the case is not closed because of a lack of factual understanding by the prosecutor.[8] Cooperating with the prosecution authorities might in these cases be inevitable, not least in order for the management to fulfill its duty to secure all civil claims the company might have.

In cases where criminal or administrative proceedings against the company itself and/or its organs or other top-level management are pending, conducting an internal investigation is a means of cooperation with the prosecution authorities. This cooperation is not compulsory, since none of the parties is – in principle – legally obliged to cooperation or disclosure.[9] However, in this cooperative-scenario, the company usually undertakes

7 Cf. Folker Bittmann, *Die verfahrensrechtliche Relevanz der Einrichtung einzelner Compliance-Maßnahmen – Interne Ermittlungen aus Sicht der Staatsanwaltschaft*, *in* Handbuch Criminal Compliance § 34 B. III. 3., 1295, No.131 (Thomas Rotsch ed., 2015) with further references in footnote 26.

8 For details *see* Helmut Görling, *Compliance und Strafrecht*, *in* Compliance Aufbau – Management – Risikobereiche Chapter 6, 454 f., No. 22 ff. (Helmut Görling et al eds., 2010).

9 Tine Golombek, *Pflichten von Geschäftsleitungs- und Überwachungsorganen bei Verdacht auf Unregelmäßigkeiten im Unternehmen*, JOURNAL DER WIRTSCHAFTSSTRAFRECHTLICHEN VEREINIGUNG 163, 169 (2012); for an obligation to disclosure to public authorities, if there is a case in which there arises an obligation to correct a fiscal declaration pursuant to Section 153 of the Fiscal Code, cf. Oliver Sahan, *Korruption als steuerstrafrechtliches Risiko*, *in* Recht-Wirtschaft-Strafe, FS Erich Samson, 605 f. (Wolfgang Joecks et al. eds., 2010); Björn Krug & Christoph Skoupil, *Die steuerliche Korrekturpflicht nach § 153 AO bei im Rahmen von Inter-*

some or even the major part of the (internal) investigative work and commits to forwarding the (essential) results of the internal investigation to the public authorities.[10] In exchange, the company is able to exercise at least some or more influence on the course of the investigation. This cooperation also aims at reducing the risk for the company to be exposed to compulsory measures such as searches.[11] Usually, the prosecution authorities will accept to refrain from such measures only as long as they are convinced that the company's internal investigation is conducted proper and transparent. Furthermore, cooperating with the prosecution authorities and supporting them with information and evidence might be considered as a mitigating factor by the prosecution authorities in cases where the company faces a fine, and thus reduce the monetary burden imposed on the company.[12]

Finally, there are constellations, in which the cooperation between company and prosecution authority goes even further and the internal investigation is conducted by the company, respectively its criminal lawyers, on behalf of the prosecution authority.[13] In these cases, all investigative actions are usually closely coordinated between the two.

It should be noted that especially in cases where international, i.e. US-, authorities are involved, a cooperation as described regularly constitutes the only factual option if the company wants to walk out of this crisis safe and sound, and that the expectations regarding the company's willingness to disclose all kinds of misconduct is distinctively higher.

Secondary, but nevertheless often equally important, further intentions when conducting an internal investigation are getting information about the company's compliance and internal control system, getting to know the truth, collecting the information for

nal Investigations erlangten Erkenntnissen zu korruptiven Handlungen in Unternehmen, NEUE ZEITSCHRIFT FÜR WIRTSCHAFTS-, STEUER- UND UNTERNEHMENSSTRAFRECHT 453, 453 (2015).

10 This scenario is sometimes referred to as "the privatisation of criminal law enforcement", cf. Jürgen Taschke, *Compliance-Sachverhalte und Ablauf eines Wirtschaftsstrafverfahrens – Wechselwirkungen zwischen internen Untersuchungen und Strafverfolgungsmaßnahmen*, *in* Handbuch Criminal Compliance § 36 B., 1413, No. 2 (Thomas Rotsch ed., 2015).

11 Axel Kallmeyer & Matthias Freund & Oliver Kraft, *Exkurs zum 3. und 4. Kapitel: Richtiges Verhalten bei Ermittlungen*, *in* Korruption und Kartelle bei Auftragsvergaben 153 (Matthias Freund et al eds., 2008).

12 Tine Golombek, *Pflichten von Geschäftsleitungs- und Überwachungsorganen bei Verdacht auf Unregelmäßigkeiten im Unternehmen*, JOURNAL DER WIRTSCHAFTSSTRAFRECHTLICHEN VEREINIGUNG 163, 170 (2012); Dorothee Krull, *Rechtliche Vorgaben*, *in* Handbuch Internal Investigations Chapter 3, 107, No. 57 (Karl-Christian Bay ed., 2013).

13 Cf. Sascha Süße & Ken Eckstein, *Aktuelle Entwicklungen im Bereich „Interne Untersuchung"*, NEWSDIENST COMPLIANCE 71009 (2014).

any claims the company might have or it needs to recover assets as well as internally stressing that the company does not tolerate misconduct and thereby strengthening the compliance management system.

F. Who precisely performs them?

Internal investigations are performed by the company which has an interest in clarifying certain facts related to any potential misconduct of its employees or management or simply by the company that has to defend itself. The principal or, speaking in terms of internal processes, the owner of the internal investigation usually is the management, i.e. the executive board. In certain constellations, e.g. when the accusations under investigation are raised against one or several members of the executive board, the supervisory board may initiate the internal investigation. The investigation as a whole is regularly delegated to one function below the management level, often to the general counsel or to the compliance officer, whose responsibility it is to coordinate and ensure the adequate, efficient and compliant conduct of the investigation. In larger companies, detailed processes are determined with regard to the steps that have to be taken, the company functions that have to be involved and the external expertise that has to be obtained. However, in practice, especially in medium sized or small companies or in companies which put their focus on repressive compliance for the first time, one very often realizes that these processes do not exist or are not clearly defined with regard to the assignment of competences. Especially in those cases where parallel criminal proceedings exist, these shortcomings can lead to a number of negative consequences.

The coordination function will need support by a number of other company functions, such as internal audit, human resources, finance, IT, public relations and the operative units such as senior management of sales and distributions or research and development. Additionally, especially in cases of parallel criminal proceedings, the involvement of a lawyer specialized in corporate criminal law will be mandatory. In international cases, foreign lawyers are often needed as further support. Depending on the evidence that has to be retrieved and the amount and availability of the company's in-house know how, an external IT-Forensic expert has to be involved. In some cases, the supplementary expertise of an accounting firm or a forensic department of such might be valuable. However, it should not be overseen that with a growing number involved, the coordination task becomes more complex and, from the point of view of a prosecution authority, also the number of potential informants rises.

G. What is done?

First of all, the hypotheses which will be investigated by the company have to be determined and precisely defined. In the course of the investigation these might be amended or adjusted due to further knowledge gained in the meantime. However, especially where the suspicion of a committed crime is investigated and parallel criminal proceedings are pending, working with hypotheses is important in order to focus the investiga-

tion on what is relevant and not to waste time on maybe interesting, but legally irrelevant facts.

One main task for those conducting the internal investigation is to collect evidence for justifying the hypotheses defined and for supporting or defending against any accusation under investigation by the prosecution authorities. The collecting of evidence itself must certainly be compliant with all applicable laws, i.e. must not violate any criminal, data protection or labor laws. Also, it must be defined for what purposes the evidence is collected, i.e. for defending the company, for bringing criminal, labor or civil charges against the employee, for recovering assets etc. Such usage also stresses the importance of properly gaining any evidence, because otherwise, its utilization in a later court hearing might be at risk.

All evidence collected is usually put together to draft the story line of what has happened, and summed up in a report on the results of the internal investigation, which will usually be discussed and agreed upon with the compliance or legal function within the company, and finally presented to the management as the basis for deciding about the further measures to be taken.

II. COLLECTING EVIDENCE

As described, collecting evidence is one of the main tasks while conducting an internal investigation. Basically, in practice one can differentiate between three kinds of evidence: First, written evidence, both digital and hard-copy, such as e-mails, letters, notes, and also accounts, invoices or other supporting documents; secondly, oral evidence, which is provided to the internal investigators by employees or the management; and thirdly, evidence gathered from background researches, such as information from databases or public registers.

There are several ways to collect these evidences, with e-mail searches, interviewing employees, reviewing documents and performing background researches being the most important ones.

A. E-mail searches

Today, communication via e-mail has become the most important way to exchange

information, also in business.[14] Therefore, e-mail searches are an important source of knowledge for the purposes of internal investigations, while at the same time, they are very often considered a substantial impairment of rights by employees and work councils. Though several questions regarding the preconditions for the permissibility of e-mail searches are still controversially discussed,[15] these preconditions are usually met in the context of criminal offenses, especially in cases where a concrete suspicion against a concrete employee exists and parallel state investigations are ongoing.[16] Companies can also reduce possible risks relating to e-mail searches in advance by implementing a reasonable framework of internal regulations regarding the use of the company's IT-systems. [17]

With regard to the practical process, first of all the relevant data has to be determined, i.e. the hard and server drives as well as the accounts that have to be searched have to be collected and specified. Additionally, the investigation team needs to know when and how often back-ups are made. After a professional copying, time filters have to be implemented and the data has to be de-duplicated and cleaned before it can be searched. If no special in-house IT-expertise is at hand, external IT-forensic- respectively e-discovery-experts have to be involved. One crucial task that follows is the determination of search terms that ensure that the relevant documents and conversations are filtered and found. The hits produced by applying these search terms then have to be reviewed by the company or external lawyers.

B. Interviewing employees

Another essential source of knowledge to elucidate compliance-offenses is interviewing employees.[18] The majority of tasks within a company are delegated to the employees

14 Sascha Süße & Ken Eckstein, *Aktuelle Entwicklungen im Bereich „Interne Untersuchung"*, NEWSDIENST COMPLIANCE 71009 (2014).

15 Jürgen Detlef W. Klengel & Ole Mückenberger, *Internal Investigations - typische Rechts- und Praxisprobleme unternehmensinterner Ermittlungen*, CORPORATE COMPLIANCE ZEITSCHRIFT 81, 83 (2009); Anja Mengel & Thilo Ullrich, *Arbeitsrechtliche Aspekte unternehmensinterner Investigations*, NEUE ZEITSCHRIFT FÜR ARBEITSRECHT 240, 242 (2006).

16 For the prerequisites *see* Section 32 of the Federal Data Protection Act; moreover LAG Berlin-Brandenburg, Urteil vom 16.2.2011 – 4 Sa 2132/10 = NZA-RR 342, 343 (2011) and for an overview of the relevant criminal and data protection law provisions *see* Jörg Eisele, *Datenschutzstrafrecht*, *in* Handbuch Criminal Compliance § 23, 762-798 (Thomas Rotsch ed., 2015).

17 Cf. details Tim Wybitul & Wolf-Tassilo Böhm, *E-Mail-Kontrollen für Compliance-Zwecke und bei internen Ermittlungen*, CORPORATE COMPLIANCE ZEITSCHRIFT 133, 133 (2015).

18 Sascha Süße & Ken Eckstein, *Aktuelle Entwicklungen im Bereich „Interne Untersuchung"*, NEWSDIENST COMPLIANCE 71009 (2014).

who generally have the highest factual proximity and consequently the best knowledge of the concrete business processes and thus the subjects of the internal investigation. Additionally, the typical compliance violations such as corruption and anti-trust breaches are covert and victimless criminal offenses. To find all necessary evidence in writing hardly never happens, as the giving of a bribe or the concluding of a price agreement is usually done personally and/ or orally. Therefore, in many cases the line of argument needs to be based on information provided by employees. Due to the fact that this kind of inquiry is highly sensitive and unpredictable, it is important to be well prepared. Time, location, interviewer and sequence of interview partners have to be determined at first. Furthermore, the interview structure and at least general questions should be predefined. Another important aspect is what kind of interview shall be conducted – will it just be an exploratory inquiry or is the interviewee a (potential) suspect? In any case, the interviewer needs to be able to react quickly and appropriately to new situations or topics coming up in the course of the interview. Further issues are the questions how to document the information,[19] whether to present any protocol made to the interviewee and if a third person is allowed to be present, e.g. a member of the work's council or a lawyer representing the interviewee. Finally, in practice one of the most important aspects is, if and to what extent the interviewed employee is under a legal duty to present evidence at all.[20]

C. Review of documents

Besides interviewing employees and e-mail searches, there are usually documents in hard copy to be reviewed, as well. This includes organigrams, letters, contracts, financial documents, such as invoices and other supporting documents, and e-mails that have been printed, but do not exist digitally anymore. These documents can be found in different places of the company, for example in the office of the suspected employee, in his department or in the accounting department. Internal advice by other employees might be very helpful in this context.

D. Background researches

Background researches can focus on obtaining addresses or other contact details, information about businesses or companies owned or positions held by an employee, interre-

19 Thomas C. Knierim, *Die strafrechtliche Verantwortlichkeit des externen Compliance-Beraters*, *in* Handbuch Criminal Compliance § 7, 242, No. 37 (Thomas Rotsch ed., 2015).

20 Infra III. D. 2. a.

lations between employees and third parties or business partners, any former misconduct of the employee or even if a business partner might be listed on any index or even terror list.

Very often background researches are part of the preventive measures of the compliance management system, e.g. with regard to business partner screenings or the prevention of money laundering. Thus, the company might be able to revert to already used databases within the company when conducting an internal investigation. Additionally, even simple searches with common internet search engines and communication platforms might produce interesting information. Further, professional databases containing financial, personal and political information as well as public registers can be consulted.[21] Especially in an international context it might be useful to mandate professional services that conduct research locally or even on-site.

III. RISKS OF PARALLEL CRIMINAL PROCEEDINGS FOR THE COMPANY

Conducting an internal investigation is a different task for any company, as it is regularly based upon accusations against employees or members of the management and often causes disturbance within the company. It becomes even more challenging, if parallel criminal proceedings are pending. In the following, the main risks occurring from parallel criminal proceedings shall be described, while a special emphasis is put on constellations where the company or its management might be held liable for the wrongdoing of employees.

A. Risk of the company's premises being searched

The search of the company's premises can be conducted pursuant to Section 103 of the Code of Criminal Procedure even if the company itself is not suspected. Such a search might be the starting point from which the company gets to know that official proceedings are pending. If, however, the allegations come up before and a cooperative relationship[22] has been established, as it has become rather common and developed into a widely accepted model over the last years[23], the risk of such searches is considerably lower. Nev-

21 For more details *see* Steffen Salvenmoser & Heiko Schreier, *Private Ermittlungen*, *in* Handbuch Wirtschaftsstrafrecht Chapter 15, 1693 f., No. 87 ff. (Hans Achenbach et al. eds., 3rd ed. 2012).

22 supra I. E.

23 Nina Nestler, *Internal Investigations: Definition und rechtstatsächliche Erkenntnisse*, *in* Internal Investigations – Ermittlungen im Unternehmen Chapter 1, 4 ff., Nos. 5 ff., 11 ff., 16 ff. (Thomas C. Knierim et al eds., 2013).

ertheless, it should be noted that public authorities are not prevented from undertaking such additional measures, since they are even in the case of an extensively cooperative attitude of the company still legally obliged to determine the proceedings and critically scrutinize the cooperation and findings presented to them. However, in any case the prosecution authorities have to check the necessity of their actions with regard to the prohibition on excessiveness of state actions.[24]

If the company and the public authorities did either not establish a cooperative relationship or the cooperation was established but ended, usually by the public authorities and most often due to doubts of the public authorities concerning the willingness of the company to fully cooperate,[25] state investigation measures might be conducted without a (further) warning. This bears the risk to take the company by surprise, especially, if the cooperation is ended tacitly, that is without a notice to the company from the prosecution authorities.

One of the special characters of a search of the premises of a company is that it is regularly not only conducted by a higher number of officials compared to a search of an individual person's habitation, but that it is also more likely to be accompanied by media coverage.[26] In addition to these circumstances, the fact that typically a lot of documents and data will be searched and seized can often lead to severe interruptions in operating business processes.[27] The search of a company can hence often bear economical risks for the company.[28]

B. Risk of an employee's habitation being searched

Another risk that is implied by criminal proceedings parallel to internal investigations is

24 Cf. Folker Bittmann, *Internal Investigations under German Law*, COMPLIANCE ELLIANCE JOURNAL 74, 87 (2015).

25 Cf. Thomas C. Knierim, *Die strafrechtliche Verantwortlichkeit des externen Compliance-Beraters*, *in* Handbuch Criminal Compliance § 7, 253 f., No. 67 (Thomas Rotsch ed., 2015); Cornelia Gädigk, *Außensicht der Strafjustiz*, *in* Internal Investigations – Ermittlungen im Unternehmen Chapter 18, 535, No. 20 (Thomas C. Knierim et al eds., 2013).

26 TIDO PARK, HANDBUCH DURCHSUCHUNG UND BESCHLAGNAHME Nos. 854, 857 (2nd ed. 2009); Jürgen Taschke, *Compliance-Sachverhalte und Ablauf eines Wirtschaftsstrafverfahrens*, *in* Handbuch Criminal Compliance § 36, 1414, No. 6 f. (Thomas Rotsch ed., 2015).

27 TIDO PARK, HANDBUCH DURCHSUCHUNG UND BESCHLAGNAHME Nos. 854, 857, 895 (2nd ed. 2009).

28 Silvia Ziebell, *Unternehmensbezogene Auswirkungen und Einbettung in die Unternehmensabläufe*, *in* Internal Investigations – Ermittlungen im Unternehmen Chapter 12, 333 f., No. 37-42 (Thomas C. Knierim et al eds., 2013).

the risk that not only the premises of the company are searched but also the habitations of employees or the management. If the company becomes aware of the criminal proceedings for the first time due to a search of the company's premises, it is very likely that at the same time individuals at the center of the allegations get to know it as well.[29] In many cases, searches of the company's premises and the habitations of the accused are performed parallel. The personal impact of such a compulsory measure is, as one can imagine, high, because even if the officials act carefully, it is very likely that neighbors or even the media might take notice of that measure which usually leads to rumors and (further) suspicions, thereby not only affecting the professional but also the private sphere of the accused.

In addition to those individuals under suspicion, some cases have shown that there is also a risk that the compliance function or any other function conducting or coordinating a parallel internal investigation for the company might be or come into the focus of the prosecution authorities and thereby become subject to a search of their private habitations.[30]

The question if such a search is legal was the subject of legal proceedings before the German Federal Constitutional Court (Bundesverfassungsgericht). The background to these proceedings may be summarized as follows: In August 2010, a newspaper published an article made publicized criminal proceedings inter alia related to bribery charges against a company. Until then, these proceedings had been unknown to the concerned company itself. The later appellant was the authorized representative and the head of the legal department of the company and thereupon took measures to clear up the related circumstances in order to prepare a defense, such as copying relevant documents and briefing the directors regarding the results of the internal investigation and the actions of the legal department in anticipation of a search of the business premises.

After the latter had been performed at the end of 2010, the Regional Court (Amtsgericht) Stuttgart issued a second search warrant, this time with regard to the habitations of the appellant in November 2011.[31] The court stated that the appellant was suspected of having undertaken actions to destroy, cover up or remove evidence for the non-compliant behavior that was the subject of the criminal proceedings. The suspicion

29 Silvia Ziebell, *Unternehmensbezogene Auswirkungen und Einbettung in die Unternehmensabläufe*, *in* Internal Investigations – Ermittlungen im Unternehmen Chapter 12, 331, No. 25 (Thomas C. Knierim et al eds., 2013).

30 Sascha Süße, *Der Compliance Officer im Fokus behördlicher Ermittlungen*, NEWSDIENST COMPLIANCE 71004 (2015).

31 Amtsgericht Stuttgart, Beschluss vom 7.11.2011 – Az. 28 Gs 1251/11.

was based upon an e-mail written by the appellant shortly after the publication of the newspaper article. In this e-mail, the appellant informed the directors that all IT-data of an employee, who was centrally involved in the circumstances which were subject matters to the criminal proceedings, had been stored to a hard drive, which had been given to an external law firm for review. Furthermore, he informed the directors that backup copies of all paper documents had been made and that these documents were stored under seal in the legal department. Finally, he informed them that the legal department was preparing model cases in consultation with the external law firm. The purpose of these model cases was to present them to the public authorities once the criminal proceedings were communicated directly to the company.

The court held that this e-mail gave rise to the suspicion that the appellant did not only undertake legitimate actions to prepare a defense and by this e-mail mainly informed the directors about these legitimate actions, but instead indirectly informed them about the measures undertaken to destroy, cover up or remove evidence for the non-compliant behavior concerned. The appellant contested the search warrant, but the District Court of Stuttgart held up the decision of the Regional Court.[32] Thereupon, the appellant lodged a constitutional complaint.

The German Federal Constitutional Court dismissed the contested decision of the District Court on March 13th 2014, ruling that the search warrant and the decision lacked sufficient findings regarding the constitution of an adequate suspicion against the appellant as required by Section 102 of the Code of Criminal Procedure, the legal basis for the search of the habitation of the appellant.[33] The court argued that it was factually improper to base the suspicion against the appellant on actions that were well within the scope of actions objectively necessary to clear up the circumstances related to the criminal proceedings against the company. Moreover, the court held that the District Court had failed in taking into consideration that the appellant was also obliged to undertake the mentioned appropriate actions due to his position as authorized representative and head of the legal department of the company and therefore did not exceed or misuse his competences. More importantly, the court stressed that a legally adequate suspicion for a search warrant could never be based mainly on the fact that the person concerned had a factual proximity, knowledge and competence in relation to the subject of a criminal proceeding.

In conclusion, the decision of the German Federal Constitutional Court shows that a

32 Landgericht Stuttgart, Beschluss vom 29.3.2012 – Az. 17 Qs 14/12.

33 BVerfG, Beschluss vom 13.3.2014 – Az. 2 BvR 974/12 = NDCOMPLIANCE 21017 (2014).

search of the habitation of an employee of a company in the focus of the public authorities is not a mere formality, but instead has to be based on qualified facts that give rise to a suspicion against the employee himself. However, the decision shows that public authorities and courts tend to apply a particular critical position on the actions of employees in response or in apprehension of criminal proceedings against the company.

C. Risk of documents being seized

Nonetheless and as stated before, the search of the premises of a company or of the habitation of an employee is not an end in itself, but instead is ordered to gather evidence regarding the respective proceedings.[34] In the absolute majority of cases in which a search is conducted, the question therefore arises, whether the ensuing seizure of documents was legal. This question has been standing at the center of a couple of decisions by German courts. In the following, three of them, which are directly related to the conduct of internal investigations, shall highlight the different approaches that have been taken by the courts.

In the first case, the supervisory board of a company assigned an external law firm with the conduction of an internal investigation to clarify the circumstances leading to the suspicion that members of the management board had been acting in a non-compliant way while making business decisions, which caused a significant financial damage to the company. The law firm took several actions to investigate the circumstances. In particular, members of the law firm interviewed former and present employees of the company, while promising the interviewed persons that the contents of their interview would remain confidential. At the end of the investigation, the law firm gathered the relevant information within a summarizing report. This report was forwarded to the prosecutor, with whom the company (principally) cooperated. After the law firm, which was in the possession of all the documents produced during the internal investigation, declined the prosecutor's demand to surrender not only the interview protocols, but also all further minutes produced during the investigation, the Regional Court of Hamburg ordered that all relevant documents were a subject to legal seizure.[35] The District Court of Hamburg affirmed this decision.[36] Consequently, the legal finding of this case was that all relevant documentation of an internal investigation is a legal subject to seizure, if the documents were in the possession of an external law firm mandated by the company to conduct the internal investigation and therefore, so the court held, not in the possession

34 supra III. A.

35 AG Hamburg, Beschluss vom 16.9.2010 – Az. 166 Gs 226/10.

36 LG Hamburg, Beschluss vom 15.10.2010 – Az. 608 Qs 18/10 ("HSH-Nordbank").

of the defense counsel of the accused individual as – in the courts opinion – required by Section 97 of the Code of Criminal Procedure.[37]

In a second decision, the District Court of Mannheim came to a different verdict in a similar constellation, arguing that the revision of Section 160a Paragraph 1 of the Code of Criminal Procedure that had become effective on February 1st 2011 had led to a strengthening of the privileged lawyer/client relationship. Consequently, the court ruled that the seizure of documents was illegal, if the documents had been produced in the course of an internal investigation and were in the possession of an external legal counsel mandated by a company to conduct an internal investigation in relation to circumstances giving rise to official proceedings against an individual associated with the company. On the other hand, the court held that documents in the possession of the company itself were still subject to legal seizure, since these documents would not be considered protected by the privileged lawyer/client relationship.[38]

The court therefore examined the total stock of the seized documents and declared the seizure of documents illegal, if a relation to the mandate was recognizable, which was, the court held, the case for the report of the lawyers to the company and for all documentation collected for the lawyers with the intent to provide an informational basis for this report. The court then decided – against the ruling of the District Court of Hamburg – that this comprises even documents that contained statements of employees, who were essentially not part of the lawyer/client relationship, if these statements were answers to questions asked by the lawyers within their mandate, since such contents were regularly "inevitable commingled".[39] However, the court also stated that the prohibition of seizure would not stand, if other documents not falling in the given categories were improperly displaced to and stored at the premises of the lawyer with the intention to have them exempted from seizure.[40]

In the third and most recent decision, the District Court of Braunschweig had to decide in a similar constellation, whether a search of the premises of the appellant and the ensuing seizure of documents with regard to administrative charges against a company were legal. Preceding the lawsuit, there had been a search of the premises of the appellant, conducted on Mai 14th 2014, due to the criminal investigation against a person X, who

37 LG Hamburg, NJW 942 ff. (2011); critically KEN ECKSTEIN, ERMITTLUNGEN ZU LASTEN DRITTER 122 ff. (2013).

38 LG Mannheim, Beschluss vom 3.7.2012 – Az. 24 Qs 1, 2/12.

39 *See* Nos. 113-115 and 117-119 of the grounds.

40 *See* No. 116 and 122 of the grounds.

was associated with the appellant.[41] In response, the appellant engaged an independent external law firm to perform an internal investigation to clear up the related circumstances. On March 10th 2015, the authorities performed another search of the premises of the appellant, this time due to criminal tax procedures against a person Y, who was likewise associated with the appellant.[42] In the course of this second search, documents of the internal investigation of the appellant regarding the circumstances of the proceedings against X were found in the office of the chief financial officer of the appellant and later on officially seized.[43] Thereupon, the appellant contested the search and the seizure at the District Court of Braunschweig.

After deciding that the search itself was legal, the court evaluated whether the seized documents – or at least some of them – had to be classified as defense material pursuant to Section 148 of the Code of Criminal Procedure. In that case, their seizure, performed by the authorities pursuant to Section 108 Paragraph 1 of the Code of Criminal Procedure (chance discovery), would have been prohibited and consequently illegal. Since the court ruled that documents for defense purposes must be exempted from seizure, if they are in the possession of the incriminated person, the only argument against the classification of the concerned documents as defensive works was that there had been no proceedings against the appellant itself at the time of the internal investigation. Therefore, it was questionable whether the seized documents could nonetheless have been produced with the intent to use them for defense purposes.

The court however ruled that documents could also be worth being protected as documentation for defense purposes, if a person was apprehensive of future criminal or administrative proceedings and if the documents were, due to this apprehension, produced with the intent to prepare a defense. Considering the means of defense preparation, the court furthermore held that the conduction of an internal investigation could be qualified as a substantial means of preparing an effective defense, if its purpose was to gain information regarding an assumed criminal or administrative offense. Thus, the court ruled that documents produced during an internal investigation have to be treated as documents for defense purposes, if they have the recognizable corresponding objective to prepare a future defense.

Regarding the present case, the court found that the appellant had reason to assume that the first search of his premises and the related charges against X might be followed by

41 AG Braunschweig, Beschluss vom 23.4.2014 – Az. 7 Gs 1017/14.

42 AG Braunschweig, Beschluss vom 20.1.2015 – Az. 7 Gs 174/15.

43 AG Braunschweig, Beschluss vom 25.3.2015 – Az. 7 GS 735/15.

administrative proceedings against the company and/or its organs or subsidiaries. Additionally, the court found that the internal investigation had focused on the clarification of circumstances relating to this specific issue and that the documents were not only gathered by an independent external law firm, which was mandated especially for the conduct of the internal investigation, but were also dated to approximately half a year after the first search, so that there was a recognizable timely connection to the search and the proceedings against X. Consequently, the court ruled that some of the seized documents were exempted from seizure at least insofar as they had been produced with the recognizable intent to prepare a defense as shown with reference to the standards mentioned by the court. However, while the court decided that the internal investigation report was exempt from seizure, it stressed that the report of the internal audit in this case was a legitimate subject to seizure, since the latter was produced earlier and merely stated that its purpose was "future behavior and actions" without further relation to defensive actions or a defense strategy.[44]

Looking at these cases, it becomes obvious that there is no consistent approach by the courts with regard to the seizure of documents produced in internal investigations, whether they are found in the company or at the advising law firm. As no all-embracing decision by the German Supreme Court (BGH) is apparent, some legal uncertainty remains as well as the risk that a prosecution authority will at first instance insist that the seizure of documents of the aforementioned kind is legal.

D. Risks resulting from testimonies of employees

As we have seen above, information provided by employees is one of the most important sources for the employer when collecting evidence in an internal investigation.[45] Likewise, they are of great importance for criminal proceedings by the prosecutor. Thus, in several different constellations, the prosecutor and the officials acting for him try to get statements and testimonies from employees of the company. The main underlying question in all those constellations is, whether the employee is required to give evidence, either to the authorities or the company – or to both.

In general, employees cannot rely on the right to refuse testimony as a professional bearer of secrets pursuant to Section 53 of the Code of Criminal Procedure if they are acting

44 LG Braunschweig, Beschluss vom 21.7.2015 – Az. 6 Qs 116/15 = NDCOMPLIANCE 21021 (2015).

45 supra II. B.

on behalf of their company.[46] However, they have the right to refuse testimony with regard to Section 55 of the Code of Criminal Procedure, if they would incriminate themselves or a close family member.

If there are parallel criminal proceedings, two main risks arise, that are explained in the following.

1. The questioning of employees during a search

The search of a company's premises is an unusual and stressful situation for any employee involved. Providing accurate information in such a situation is not easy. Knowing this, the public authorities sometimes try to seize the hour and informally interrogate employees during the search. Even though an employee cannot rely on the aforementioned rights to refuse testimony, he will nonetheless regularly not be obliged to give testimony. On the one hand, this is due to the fact that, apart from giving the basic personal details, it is not compulsory to make statements to the police, who will regularly be the ones conducting the search.[47] On the other hand, even if a prosecutor was present during the search and asked an employee to give testimony as a witness, the employee would only have to follow this order, if handed an official summons on that very occasion and if he was given the right to consult a legal representative beforehand pursuant to Section 68b Paragraph 1 Sentence 1 of the Code of Criminal Procedure.

Nonetheless, the informal questioning of an employee during a search of the company's premises can bear risks for the company. For instance, if the employees are unaware of their rights to refuse testimony and feel intimidated by the presence and appearance of the public authorities, they might give ambiguous, false or unnecessarily excessive information. Even though the employee might only be mistaken with regard to what he said, these information will be present in the files and it becomes quite hard to correct them. Another risk might be that, when the main proceedings are directed against a business partner, legally not mandatory, extensive and maybe false statements of employees can not only harm the business partner, but also the mutual business relations

46 The right to refuse testimony pursuant to Section 52 of the Code of Criminal Procedure will normally also not apply, cf. in detail Sascha Süße, *Der Compliance Officer im Fokus behördlicher Ermittlungen*, NEWSDIENST COMPLIANCE 71004 (2015).

47 Katharina Kusnik, *Wenn die Staatsanwaltschaft im Unternehmen ermittelt: Abläufe und Verhaltensleitlinien bei einer Durchsuchung der Geschäftsräume*, CORPORATE COMPLIANCE ZEITSCHRIFT 22, 27 (2015).

and thereby the company itself.[48]

2. The utilization of statements of employees made in interviews

The second aspect is in how far the prosecutor can utilize the information that was presented to him by the company, who gained the information in the course of an internal investigation, especially during an interview, and by which an employee incriminates himself or others.

a. The duty of employees to participate in interviews

The first question coming up in this context is whether an employee has to participate in an interview demanded by the company. Often an employee might not want to answer the questions he is asked, for instance because he does not want to denunciate colleagues or more importantly, himself. The subsequent question is, if any obligation to participate also includes the obligation to provide information even if it is self-incriminating. The determining principles for answering these questions originate mainly from labor law and not from the specific provisions of criminal procedure, since an internal investigation is – in principle – solely of a private character to the company.

As a starting point, it is beyond dispute that the employee can be ordered to participate in the interview due to the employer's executive prerogative pursuant to Section 242 of the Civil Code and Section 106 of the Industrial Code.[49] Considering that the employee initially assumed the tasks delegated by the employer to him in a voluntary fashion when concluding his labor contract, it is well arguable and agreed upon that the employee is at least also principally obliged to answer all questions concerning the core aspects of his personal work activities truthfully and completely, at least if he doesn't incriminate himself.[50] Apart from this starting point, a lot of aspects concerning the rights and duties of an employee in an interview are subject to a very controversial legal debate, especially regarding the questions, if the employee is furthermore obliged to give

48 Katharina Kusnik, *Wenn die Staatsanwaltschaft im Unternehmen ermittelt: Abläufe und Verhaltensleitlinien bei einer Durchsuchung der Geschäftsräume*, CORPORATE COMPLIANCE ZEITSCHRIFT 22, 28 (2015).

49 Cf. ANJA MENGEL, COMPLIANCE UND ARBEITSRECHT 118, No. 20 (2009).

50 KLAUS MOOSMAYER, COMPLIANCE – PRAXISFADEN FÜR UNTERNEHMEN 90, No. 327 (3rd ed. 2015). The legal supplement for this entitlement of the employer is either seen in Sections 666, 675 Abs. 1 of the Civil Code, Sections 611, 241 Abs. 2 of the Civil Code, sometimes cited in conjunction with Sections 242 of the Civil Code, in case of an agency in conjunction with Sections 662 ff. of the Civil Code or in fiduciary duties generating from company law.

self-incriminating testimony,[51] if he is entitled to have a legal advisor or a member of the work council present during the interview and if and to what extent the persons conducting the interview have the obligation to instruct the employee with regard to his rights and duties (for instance regarding the – possible – right not to incriminate himself or that the information gained in the course of the interview might be forwarded to the prosecutor).[52]

Regardless of these questions, one of the risks for the company in these cases is that the statement of an employee, in which he incriminates himself or other employees, simultaneously gives evidence of the violation of the organizational and supervisory duties of the company or its organs and therefore establishes the risk that the company is later on charged due to this violation.

b. The utilization of interview protocols

Subsequently, the question arises, whether the evidence gained and protocolled in the course of the interview may be utilized by the public authorities. This is highly disputed with regard to protocols containing self-incriminating statements of employees due to the fact that – the duty to give self-incriminating statements in an interview provided – the public authorities could thereby gain a self-incriminating testimony of the concerned employee even though the employee would have had the right to refuse testimony when questioned as an accused person by the prosecution authorities themselves.[53]

51 Answering in the affirmative e.g. OLG Karlsruhe NSTZ 287 (1989); Thomas C. Knierim, *Die strafrechtliche Verantwortlichkeit des externen Compliance-Beraters*, *in* Handbuch Criminal Compliance § 7, 253 f., No. 67 (Thomas Rotsch ed., 2015); Gina Greeve & Michael Tsambikakis, *Individualvertretung im Strafverfahren*, *in* Internal Investigations – Ermittlungen im Unternehmen Chapter 17, 508, No. 20 f. (Thomas C. Knierim et al eds., 2013); Martin Diller, *Der Arbeitnehmer als Informant, Handlanger und Zeuge im Prozess des Arbeitnehmer gegen Dritte*, DER BETRIEB 313, 314 (2004) with regard to the employee's contractual main duties. Answering in the negative e.g. Imme Roxin, *Probleme und Strategien der Compliance-Begleitung in Unternehmen*, STRAFVERTEIDIGER 116, 117 (2012); Ralf Tscherwinka, *Interne Ermittlungen zwischen Selbstbelastungsfreiheit und Fürsorgepflicht*, *in* FS Imme Roxin 521, 529 (Lorenz Schulz et al. eds., 2012). Some however stress that in practice employees do regularly not refuse testimony with regard to their right to protection against self-incrimination, but with reference to blackouts *see* Gerlind Wisskirchen & Julia Glaser, *Unternehmensinterne Untersuchungen (Teil II)*, DER BETRIEB 1447, 1448 (2011); Mark Zimmer, *Rolle der Mitarbeiter bei unternehmensinternen Ermittlungen – Arbeitsrechtliche Fragen bei der Aufklärung von Compliance-Verstößen*, RISK, FRAUD & COMPLIANCE 259, 260 (2011) with reference to the aforementioned.

52 For an overview regarding these issues and the legal opinions *see* Sascha Süße & Ken Eckstein, *Aktuelle Entwicklungen im Bereich „Interne Untersuchung"*, NEWSDIENST COMPLIANCE 71009 (2014).

53 Differentiating e.g. Folker Bittmann, *Internal Investigations under German Law*, COMPLIANCE ELLIANCE JOURNAL 74, 92 ff., 95 (2015); Renate Wimmer, *Die Verwertbarkeit unternehmensinterner Untersuchungen*, *in* FS Imme Roxin 537, 542 (Lorenz Schulz et al. eds., 2012).

These objections against the utilization of self-incriminating testimonies, however, do not apply to non self-incriminating testimony of other employees. In these cases, there is always the risk that the disclosure of all the information recorded in the protocols indicates organizational or other compliance shortcomings.

On the other hand, interview protocols containing non self-incriminating statements may generally be utilized by the company, e.g. for civil and labor law proceedings against the person who has committed the wrongdoing. However, there might be the risk that interviews unlawfully conducted lead to the prohibition of utilization of the protocol for the company. With regard to the yet unsettled questions regarding the conduction of interviews the securing of the possibility to utilize the protocols might be more legally challenging than expected.[54]

E. Risk of a collision of investigative actions

Another aspect that has to be taken into consideration is that an internal investigation might conflict with criminal proceedings. That is especially relevant with regard to collecting evidence, in particular when interviewing employees. Usually, the company has an easy access to its employees. Additionally, the desire to talk to the employees as soon as the accusations come up, often with the idea that this means "everything will be cleared up soon", is quite an understandable reaction of the management or the compliance function. However, any interview with an employee means a more or less significant impact on his memory. For that reason, the prosecution authorities sometimes want to have the first grasp on employees who are witnesses, while at the same time, the company equally wants to be the first to get the information from its employee.

Furthermore, in some constellations the company might become aware of a suspicion against a certain employee and consequently might know prior to him that criminal proceedings against him are pending. In these cases, the company might come to the challenging situation to conduct an investigation, possibly at least partly against its own employee, without being allowed to inform the employee about these proceedings. While on the one hand this might be estimated as problematic in the light of the fiduciary duty of the employer,[55] on the other hand it might hinder the employer from taking

54 Cf. Dorothee Krull, *Rechtliche Vorgaben*, *in* Handbuch Internal Investigations Chapter 3, 129, No. 108 (Karl-Christian Bay ed., 2013).

55 The fiduciary duty of the employer inter alia includes the duty to protect the general right of privacy of the employee, *see* Ingrid Schmidt, Art. 2 [Allgemeine Handlungsfreiheit, Allgemeines Persönlichkeitsrecht], *in* Erfurter Kommentar zum Arbeitsrecht Part 10 Grundgesetz für die Bundesrepublik Deutschland (Art. 1 - Art. 14), No. 68 f. (Rudi Müller-Glöge et al. eds., 16th ed. 2016).

actions under labor law against the employee.[56]

In both constellations there is the risk that the company is blamed to hinder the state investigation or that the management or the compliance function are accused of obstructing the authorities (Section 258 of the Criminal Code).

Another potential risk which is generally present when conducting an internal investigation, but might rise if employees know about criminal proceedings, is that employees overeagerly modify or destroy potential evidence, e.g. e-mails, contracts or invoices. Apart from the fact that this behavior might also fulfill Section 258 of the Criminal Code, these actions can most of the times be tracked and the data be regained by the prosecution authorities, at least if digital data is concerned. Thereby, the employees also put a potential cooperation between company and prosecution authorities at risk.

IV. WAYS FOR COMPANIES TO REDUCE RISKS

As aforementioned aspects display, a number of questions concerning the relation between internal investigations and criminal proceedings remain unsettled. The reason for this is mainly based on the fact that the concept of an internal investigation is rather new to the German criminal procedural law. It basically only developed over the last decade parallel to the increased level of formalization of compliance, the attention paid to compliance matters as such and the Anglo-American influence due to extended investigative powers of foreign prosecution authorities in the context of an ever growing international business environment.[57]

56 Cf. Klaus Moosmayer, *Die verfahrensrechtliche Relevanz der Einrichtung einzelner Compliance-Maßnahmen –Interne Ermittlungen aus unternehmenspraktischer Sicht*, *in* Handbuch Criminal Compliance § 34 B. III. 1., 1272, No. 74 (Thomas Rotsch ed., 2015); for an overview of possible labour law and other actions against employees in these situations *see* DENNIS BOCK, CRIMINAL COMPLIANCE 275 f. (2011) and Dennis Bock, *Aufsichtspflichten, §§ 130, 30 OWiG*, *in* Handbuch Criminal Compliance § 8, 278 f., No. 36 f. (Thomas Rotsch ed., 2015). Imme Roxin however points out that disciplinary measures will not be necessary, if the employer cooperates with the prosecutor after he found out about the violation, since the initiating and impending of criminal proceedings are the most effective means to ensure that an employee will not commit a compliance offense again *see* Imme Roxin, *Probleme und Strategien der Compliance-Begleitung in Unternehmen*, STRAFVERTEIDIGER 116, 121 (2012).

57 *See* for example Martin Schorn & Johanna Sprenger, *Deferred Prosecution Agreements nach neuem britischen Recht - Perspektiven für unternehmensinterne Compliance und Investigations*, CORPORATE COMPLIANCE ZEITSCHRIFT 211 (2014); Markus Rübenstahl, *Der Foreign Corruption Practice Act (FCPA) der USA*, NEUE ZEITSCHRIFT FÜR WIRTSCHAFTS-, STEUER- UND UNTERNEHMENSSTRAFRECHT 401 (2012).

Nevertheless, in practice, there are a number of measures that can be taken to reduce the risks that companies face in cases of conducting an internal investigation parallel to criminal proceedings.

A. Cooperation with the prosecution authorities

It is probably true, that the general approach of a company with regard to criminal proceedings is to cooperate with the prosecution authorities and to support the process of clarifying what has actually happened.[58] This might give reason to ask why a company that cooperates should be in any way reluctant to provide the authorities with (all) interview protocols produced during an internal investigation, any draft of an investigation report or all documents that are obviously connected with the accusations, may they be incriminating or not for the company or its management. Or in other words: Could the risks described above actually pose risks also for a cooperating company?

1. Conflicting priorities

In fact, the company stands between two conflicting priorities.

On the one hand, it is willing to comprehensively cooperate in order to reduce the risk of compulsory measures and to earn brownie points as it apprehends a financial sanction. On the other hand, the company does not want to incriminate itself or (single) members of the management in the first place.

Bearing that in mind, it becomes rather likely that internal investigations conducted by a company will usually be neither totally neutral nor solely impartial. That comes with no surprise, as nobody actually expects a company to send itself to its doom without resistance. Even more, such a behavior might conflict with the management's duty to act in the best interest of the company. Nonetheless, some compliance officers sometimes describe their way of conducting internal investigations as absolutely neutral and stress that they would collect evidence regardless of the reputation or the position of the involved persons. While this approach is generally favorable, it must not be overseen that not only the company's management but also the compliance officer or any other function conducting the internal investigation on behalf of the company must act in the best interest of the company. In particular, compliance officers are neither external police

58 KLAUS MOOSMAYER, COMPLIANCE – PRAXISFADEN FÜR UNTERNEHMEN 96, No. 350 (3rd ed. 2015).

officers nor the extended arm of the prosecution authorities. Thus, within the legally acceptable options the ones that best suit the company's interest in the individual situation must be chosen.

Insofar, there are significant differences between internal investigations when cooperating with the prosecution authorities in comparison to investigations performed in an international context, especially with the SEC under the FCPA.[59] The procedure governing such investigations cannot be applied one to one on internal investigations conducted in the national context.

2. Reasons why companies accept risks

Stating that, it becomes obvious that there are reasons why the described risk scenarios above are real for the company under investigation. However, there are reasons why such a company might accept risks and e.g. refuse to hand in all evidence collected.

Being willing to cooperate, does not automatically mean to forfeit all procedural rights the company has. If the criminal proceedings are solely targeting individuals, the company is merely a witness, however an endangered one as it might become secondary participant if the preconditions of Section 30 of the Act on Regulatory Offenses are fulfilled. At the latest when the company becomes secondary participant because of a procedure under Sections 29a or 30 of the Act on Regulatory Offenses, it is, according to Sections 444, 432 Paragraph 2 of the Code of Criminal Procedure, granted the same procedural rights as an accused individual. A company can nevertheless cooperate comprehensively and still refuse to hand out every single document that has been produced or found in the course of the internal investigation on the grounds of its procedural rights. Reasons for that might be that the information included goes beyond the scope of the criminal and administrative proceedings; or that business secrets are included for which a proper protection cannot be guaranteed by the prosecutor; or single information might be misleading, because they are ambiguously drafted, and thus would arouse an unfounded initial suspicion by the prosecutor. Furthermore, as stated above, the company's management is obliged to act in the company's best interest. Thus, if only the disclosure of information for which no legal duty exists would give grounds for a sanction against the company, one can argue that the management breaches this duty.

59 For the characteristics of an investigation initiated by the SEC *see* FREDERIKE WEWERKA, INTERNAL INVESTIGATIONS – PRIVATE ERMITTLUNGEN IM SPANNUNGSFELD VON STRAFPROZESSUALEN GRUNDSÄTZEN UND ANFORDERUNGEN EINES GLOBALISIERTEN WIRTSCHAFTSSTRAFVERFAHRENS 91-110 (2012).

Finally, the management might refuse to provide certain documents because of its fiduciary duty towards its employees.

3. Reducing risks by communication

Having said this, on the other hand, when cooperating with the prosecution authorities it is indispensable that the internal investigation must be performed properly and in compliance with all applicable laws. Furthermore, any communication with the prosecution authorities must be made in good faith and without any inadmissible deceit. The aim to reduce the negative impact on the company from compulsory measures and sanctions will usually only be reached, if the company cooperates in a confiding and reliable manner with the authorities. Prosecutors will regularly check the plausibility of the information provided by the company, at least on a random basis. The involvement of an experienced criminal lawyer can ensure that the company exercises all its procedural and legal rights and at the same time refrains from collecting evidence improperly, falsifying evidence gained or inadmissibly sugar-coating the outcome of the internal investigation.

In this regard, the most crucial advice regarding a cooperation with the prosecution authorities is to maintain close and transparent communication with the authorities. In many cases, measures taken by the prosecutor that seem irrational or unexpected can be traced back to a misunderstanding in earlier communication. Therefore, it seems important to explain to the authorities what the company does in its investigation and how it conducts each single step. Depending on the approach by the prosecutor in the single case, it might be helpful to discuss an investigation map and hand out interim reports. For the discussion of operational aspects it can also be helpful to get (and stay) in touch with the investigating police unit. In the course of the criminal proceedings it is also advisable to stick to deadlines with regard to the handing in of documents or reports. In practice, however, delays are not uncommon. In such circumstances the timely and comprehensible explanation why a deadline needs to be postponed, should usually prevent negative consequences. In most cases, a deliberate “Salami-tactic”, i.e. bit by bit just admitting what is respectively already known, is not recommendable and might lead to a silent termination of the cooperation by the prosecutor. Investigation reports should be clear and easy to read and to handle, especially with regard to the appendices. When handing in documents or statements that are ambiguous, an early annotation will prevent the receiver from making wrong conclusions.

Sticking to these basic rules usually keeps the cooperation alive and supports the aims of the company. That is not contradicted by the fact that in any case the company and its lawyers must exercise all procedural rights they deem to be appropriate and compete for legal opinions or the evaluation of facts wherever necessary.

4. Considering further measures to reduce risks

However, cooperation always means advantages on both sides. Though improvements can be witnessed over the last years, very often the prosecution authorities still have neither the capacities nor the expertise to effectively evaluate the large amounts of data seized in cases of alleged economic crimes. Long durations of proceedings are the result. If evidence is stored in another country, it will be even more difficult and time consuming for the prosecutor to gain them via legal assistance of that country than just getting them handed in by the company.[60] If, however, in the course of the cooperation it becomes evident that the cooperation becomes a one way street or if commitments by the prosecution authorities were broken, it is inevitable for the company and its lawyers to fearlessly consider the termination of the cooperation.

Nevertheless, it must be stressed that in by far the most cases a once started cooperation between the company and the prosecutor works until the end of the proceedings. Still, it would be unprofessional not to take the abovementioned risks into careful consideration and to omit to reduce these risks or the possible negative effects arising from them. The following further aspects (B. to E.) should therefore be scrutinized by the internal investigator and – depending on each single case – observed where necessary.

B. Proper documentation of an internal investigation

As the case regarding the search of an employee's habitation[61] shows, documentation of the steps that have been taken in the course of the investigation is crucial. An ambiguous wording or measures taken, but not explained properly or understandable at first glance, might lead to an initial suspicion. Thus, the person responsible for the conduct of the internal investigation should ensure that the documentation is made properly and regularly, e.g. by preparing short notes or "work dones", and that it is stored centrally and easily accessible. Furthermore, wherever appropriate, legal or technical experts for conducting professional methods of collecting evidence should be involved.

C. Conducting state-of-the-art interviews

Even without parallel criminal proceedings, conducting interviews is one of the most

60 Cf. Imme Roxin, *Probleme und Strategien der Compliance-Begleitung in Unternehmen*, STRAFVERTEIDIGER 116, 117 (2012).

61 supra III. B.

common but also most ambitious tasks when conducting an internal investigation. The risk for the company in that context is that by incriminating himself the employee might also give grounds for sanctions against the company or its management. Thus, in such cases the company might also have the interest that a protocol of an interview, in which an employee has voluntarily incriminated himself, is not utilized. In other constellations, especially if the company is a victim to a fraudulent action by its employee, it is in the absolute interest of the company that the information provided by the employee can be utilized, as they might form the basis for any labor action, civil claim or criminal charge.

Thus, in any case the company should ensure that the conduct of an interview is in conformity with all applicable laws, especially that no unduly pressure is put upon the interviewee, that he is informed about the content of the questioning, that he knows the role of the interviewer and also what might happen with the information he provides, i.e. for what it might be used. Additionally, the information provided should be properly documented and, if appropriate, reviewed together with the interviewee.

D. Labeling documents of an internal investigation with their purpose

The different court decisions described above[62] show that there is still a lot of uncertainty with regard to the seizure of documents produced or collected in the course of an internal investigation. In any case, the risk remains that during a search the prosecution authorities may take a restrictive approach and try to seize them. Thus, in the first place, it is important to react properly in the very situation and to officially complain against that seizure. That should be accompanied by the demand to seal the documents concerned (cf. Section 110 Paragraph 2 Sentence 2 of the Code of Criminal Procedure) and to force a court decision on the seizure afterwards.

Some further guidance regarding suitable risk limiting measures can be drawn from the decision of the District Court of Braunschweig. As shown, the court ruled that the documentation of an internal investigation can generally be seen as intended for defending the company and therefore be exempt from seizure.[63]

Regarding the crucial factors for the acceptance of documents as defense material set out by the court, the challenge will be to demonstrate the specific "defense character" of the respective documents. This can be more difficult in some cases than in others. In the present case for instance, the internal investigation was conducted after the company

62 supra III. C.

63 supra III. C.

had been searched, which – according to the court – basically showed that the internal investigation was conducted in response to the criminal proceedings and thus with the intent to prepare a defense. With regard to cases like this, the defense character of the documents produced should be established quite easily, even if the proceedings are not yet led against the company itself. However, in most of the cases where the offense in question was committed to the (assumed) benefit of the company or a violation of Section 130 of the Act on Regulatory Offenses is at stake, proceedings with regard to Section 30 of the Act on Regulatory Offenses will be expectable, even if at the time of the beginning of the internal investigation no criminal proceedings are pending.

Furthermore, the court seemed to differentiate between documents produced by the internal audit department on the one hand and documents produced by the external law firm on the other hand. In the latter case, the documents were more likely to be considered as being produced in a defense context, since the company mandated the law firm in response to the search of the company's premises and especially for the interviews. Nevertheless, the court pointed out that documents produced by the internal audit department can principally also be exempt from seizure.

Thus, the most important criterion obviously seems to be the identifiable purpose of a document. The court held that the seizure of a document containing an audit report was legal, since the purpose of the report was not to prepare a defense for behavior in the past, but a strategy on how to behave in the future. Therefore, making sure that the defense purposes are sufficiently clear and expressively stated in the respective documents, can contribute to reduce the risk of seizure.

Additionally, all documents produced in the course of the internal investigation and for the company's defense should be stored separately from other documents of the company.[64] Apart from that, it is still advisable to keep all sensible documents for defense purposes at the law firm that defends the company.

E. Providing trainings and witness assistance for employees

Finally, risk minimizing means can be taken with regard to statements or actions of employees.

First, the employer should regularly and recurrently provide trainings for his employees

64 *See* also Ingo Minoggio, *Interne Ermittlungen in Unternehmen*, *in* Wirtschaftsstrafrecht in der Praxis Chapter 15, No. 58 (Marcus Böttger ed., 2nd ed. 2015).

regarding their rights and duties when confronted with the public authorities, especially regarding searches of the company's premises. The employer should stress the importance that employees be very restrictive or even better refusing with respect to giving information to the public authorities, in order not to endanger possible lines of defense or to present false or ambiguous evidence. However, employees could – in the interest of abbreviating the search – be allowed to support the investigating authorities on an organizational basis. Additionally, they should be informed that no evidence must be suppressed or destroyed. Most importantly, employees working at the reception of the company's premises should be trained to inform the management and the legal department immediately after the search has started so that a legal advisor can be informed or especially mandated on short notice and be present during the search.

Moreover, if an employee has to give testimony to a public prosecutor or has to appear before court, the employer should provide witness assistance to safeguard the interests of the company.

V. CONCLUSION

Conducting an internal investigation is indisputably not an easy task. However, it becomes even more challenging if parallel criminal proceedings are pending. Especially in cases where the management and the company itself are at the risk of being sanctioned, collecting evidence might include gathering evidence to the disadvantage of the principal of the internal investigation. Nevertheless, if criminal proceedings are already pending, the advisable approach in most of these cases is to cooperate with the prosecution authorities, especially in order to reduce the risks that parallel criminal proceedings impose on the company and the internal investigation conducted. These risks include in particular the search of the company's premises or an employee's or member of the management's habitation, the seizure and utilization of interview protocols and other documents produced in the course of the investigation and possible conflicts between internal and external investigative actions.

Cooperation, however, does not mean at all that the company waives all its rights. Usually, cooperation that is based on transparent proceedings, the will to clarify what has happened and a professionally conducted investigation are in the interest of both parties to the cooperation. Nevertheless, as the prosecution authorities have wide discretional powers in deciding about taking compulsory measures against the company or terminating cooperation without further notice, it is important to consider appropriate measures to safeguard the legal defense rights that the company and its management have. A close communication with the prosecution authorities, ensuring a transparent documentation of the investigative measures taken, properly labeling the relevant documents and providing trainings for employees may diminish the risks of parallel proceedings with regard to the collecting of evidence in an internal investigation significantly.

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

HOW TO CONDUCT E-MAIL REVIEWS IN GERMANY

Practical guidance to avoiding fines, exclusion of evidence and other risks

Tim Wybitul

AUTHOR

Tim Wybitul is a partner of Hogan Lovells and heads the law firm's Compliance & Investigations group in Frankfurt. He helps his clients solving problems regarding data privacy, compliance, internal investigations and labor law requirements. The German Superior Civil Court (Bundesgerichtshof) and the Superior Labor Court (Bundesarbeitsgericht) quote his publications. The German lawyer ranking handbook JUVE and other rankings list him among Germany's leading data privacy and compliance/investigations lawyers.

ABSTRACT

Information from business emails is often very important for investigating breaches of rules or for court proceedings. However, strict legal requirements apply to the analysis and inspection of emails. The following overview sets out these requirements and describes the risks resulting from failure to comply with them, while focusing primarily on more recent court rulings. The article also shows how employers can effectively mitigate or avoid legal risks when monitoring emails. One of the main focuses of the overview is on recommended actions to take in practice and a checklist for preparing for and implementing access to business email accounts.

TABLE OF CONTENTS

I. TYPICAL REASONS FOR ACCESSING BUSINESS EMAILS 61
- A. Business interests 61
- B. Statutory document retention requirements 61
- C. Requests from German authorities 62
- D. Emails as evidence in court proceedings 62
- E. Detection of breaches of the law, legal duty to conduct investigations 62

II. LEGAL REQUIREMENTS FOR THE INSPECTION OF EMAILS 63
- A. Monitoring business emails if private use is prohibited 64
- B. General prohibition on monitoring emails if private use is permitted? 64
- C. Practical significance of the possible applicability of telecommunications secrecy 66
- D. Requirements laid down by court rulings on monitoring emails if private use is permitted 67
- E. Consequences for companies 70

III. CHECKLIST: DATA PROTECTION IN THE CASE OF EMAIL ANALYSIS 70
- A. Preparation for the analysis 71
- B. Legal framework 72
- C. Implementation of the email inspection 73
- D. Documentation of the email inspection 75

IV. SUMMARY AND RECOMMENDED ACTIONS 76
- A. Approach if private use is prohibited 76
- B. Approach if private use is permitted 76

I. TYPICAL REASONS FOR ACCESSING BUSINESS EMAILS

In many situations, it may be expedient for companies to access their employees' business email accounts. Nowadays, business transactions are often only documented in emails. It is estimated that emails account for approximately 60–70% of business communication.[1] The growing significance of electronic communication within companies is also increasing the need for appropriate monitoring.[2] A number of common reasons for accessing business email communication are listed below. The focus of the following points – in keeping with their high practical significance – is primarily on monitoring emails for the purpose of internal investigations, preparing for court proceedings or for other measures relating to the investigation of internal company matters.

A. Business interests

For business purposes, it may be advantageous if access to business email accounts is not only available to the individual employee, but also to colleagues or superiors. This not only makes it easier to work together on projects or archive emails, it also enables colleagues to promptly respond to incoming communications if the employee in question is on holiday or off sick.

Companies also have a considerable interest in preventing employees from using their email account to send confidential company data to third parties or to their private email address. Such behavior by employees could fulfill the elements of the offence under sec. 17 of the German Unfair Competition Act [*Gesetz gegen den unlauteren Wettbewerb – UWG*]. In practice, the criminal disclosure of trade and business secrets is often virtually impossible without access to corporate IT systems. Legal responses require that the company in question can also prove such breaches. Any subsequent investigations or criminal proceedings are usually unable to remedy the damage caused by the outflow of data. Employers therefore have a significant economic interest in preventing the illegal outflow of data effectively and in good time before trade secrets are obtained by unauthorized parties. As a rule, this can be achieved by appropriately monitoring email correspondence.

B. Statutory document retention requirements

It may also be necessary to access business email communication in order to meet statu-

---

1 Cf. Frank Peter Schuster, *IT-gestützte interne Ermittlungen in Unternehmen – Strafbarkeitsrisiken nach den §§ 202a, 206 StGB*, 2, ZEITSCHRIFT FÜR INTERNATIONALE STRAFRECHTSDOGMATIK, 68 (2010).

2 Cf. Valerian Jenny, *in* BDSG COMMENTARY GERMAN FEDERAL DATA PROTECTION ACT [BUNDESDATENSCHUTZGESETZ – BDSG], SEC. 88 OF THE GERMAN TELECOMMUNICATIONS ACT [TELEKOMMUNIKATIONSGESETZ – TKG] margin no. 21 *et seq.* (Kai-Uwe Plath et al. eds., 1st ed. 2013).

tory document retention requirements. Electronic business communication may thus be subject to statutory document retention requirements.[3] Emails that are deemed to be commercial letters must be archived pursuant to sec. 238 II *HGB*.[4] If companies wish to meet these obligations, they must also be able to access emails stored on their systems.

C. Requests from German authorities

Furthermore, it is not uncommon for supervisory or prosecution authorities to ask companies to provide emails in order to investigate a particular matter. For example, requests may be made by public prosecutors, the German Federal Cartel Office [*Bundeskartellamt*] or the German Federal Financial Supervisory Authority [*Bundesanstalt für Finanzdienstleistungsaufsicht*]. There are often many reasons for companies to cooperate with the authorities if they receive such requests. However, companies can only provide such assistance in investigating matters if they can access business email communication.

D. Emails as evidence in court proceedings

Electronic communication also plays an important role as evidence in court proceedings.[5] In dismissal protection or damages proceedings, for example, companies can often only prove that employees have breached their duties by presenting the relevant emails. The presentation of internal emails is often requested in cross-border legal disputes, in particular in e-discovery proceedings.[6] For this purpose, too, access rights to employee email accounts are necessary.

E. Detection of breaches of the law, legal duty to conduct investigations

Criminal offences, regulatory offences or other compliance violations can frequently

---

3 E.g. pursuant to sec. 238 II of the German Commercial Code [Handelsgesetzbuch – HGB], sec. 257 I HGB or sec. 147 I of the German Tax Code [Abgabenordnung – AO].

4 Valerian Jenny (*see* footnote 2 above), sec. 88 *TKG* margin no. 21.

5 Cf. e.g. Stefan Sander, *E-Mails und die Beweisführung im Prozess*, 5 COMPUTER UND RECHT (CR) 292 (2014) with further substantiation.

6 Cf. e.g. Axel Spies, *in* Betrieblicher Datenschutz 935 et seq. (Nikolaus Forgó et al eds., 2014); *as well as* Jan Kraayvanger/Mark C. Hilgard, *Urkundenvorlegung im Zivilprozess – Annäherung an das amerikanische „discovery"-Verfahren?*, NEUE JUSTIZ (NJ) 572 (2003); Stefan Hanloser, *e-discovery*, 12 DATENSCHUTZ UND DATENSICHERHEIT (DUD), 785 (2008); Johannes Lux/Tobias Glienke, *US-Discovery versus deutsches Datenschutzrecht*, 9 RIW 603 (2010); Klaus M. Brisch/Philip Laue, *E-Discovery und Datenschutz*, 1 RECHT DER DATENVERARBEITUNG (RDV) 1 (2010); Tim Wybitul, *Interne Ermittlungen auf Aufforderung von US-Behörden – ein Erfahrungsbericht*, 12 BETRIEBS-BERATER (BB) 606 (2009); TIDO PARK, MÜNCHENER ANWALTSHANDBUCH VERTEIDIGUNG IN WIRTSCHAFTS- UND STEUERSTRAFSACHEN, 438 et seq. (Klaus Volk, 2nd ed., 2014).

only be detected or proven by monitoring emails. Secs. 30 and 130 of the German Regulatory Offences Act [*Ordnungswidrigkeitengesetz – OWiG*] set out extensive supervisory duties for companies. These provisions ultimately give rise to a legal duty to conduct internal investigations if there are suspicions pointing to possible breaches of the law. The so-called principle of legality also constitutes a further legal basis of the requirement to investigate matters that point to a breach of the provisions of the German Criminal Code [*Strafgesetzbuch – StGB*] or the *OWiG*. The *District Court* [*Landgericht – LG*] *of Munich I* only recently confirmed in a high-profile judgment that members of the management board must, as part of their legality duty, ensure that the company is organised and supervised in such a way that no breaches of the law occur[7]. Companies only meet these supervisory requirements if they can also carry out monitoring of business email communication in the case of appropriate indications.

II. LEGAL REQUIREMENTS FOR THE INSPECTION OF EMAILS

Substantial legal requirements apply to the analysis or monitoring of business email accounts.[8] In all cases, companies must comply with the strict requirements of the *BDSG*. As a rule, the proportionality principle that must be safeguarded in this respect requires a comprehensive weighing up of the interests of the employees affected by the monitoring of emails against the purpose of the monitoring pursued by the company.[9] The economic interests of the company on the one hand, and the general right to privacy of the persons affected by the inspection or analysis of their emails on the other, must be weighed against each other.

As there are not yet any court rulings setting out clear and generally valid requirements for the inspection and analysis of email accounts, monitoring emails often entails significant legal risks. If mistakes are made in the legal assessment of the permissibility of mon-

7 *So-called* "Neubürger decision", District Court of Munich I, NZG 2014, 345 (not *res judicata*; appeal filed with the Munich Court of Appeals [Oberlandesgericht – OLG] pending under 7 U 113/14); cf. *also* Spieß, CCZ 2014, 143; Meyer, DB 2014, 1063; Holger Fleischer, *Aktienrechtliche Compliance-Pflichten im Praxistest: Das Siemens/Neubürger-Urteil des LG München*, NEUE ZEITSCHRIFT FÜR GESELLSCHAFTSRECHT (NZG) 321 (2014).

8 Cf. e.g. Markus Rübenstahl & Stefanie Debus, *Strafbarkeit verdachtsabhängiger E-Mail- und EDV-Kontrollen bei Internal Investigations*, NEUE ZEITSCHRIFT FÜR WIRTSCHAFTS-, STEUER- UND UNTERNEHMENSSTRAFRECHT (NZWiSt) 69 (2012), *or* Tim Wybitul, *Neue Spielregeln bei E-Mail-Kontrollen durch den Arbeitgeber*, ZEITSCHRIFT FÜR DATENSCHUTZ (ZD) 69 (2011).

9 Cf. Martin Kock & Julia Franke, *Mitarbeiterkontrolle durch systematischen Datenabgleich zur Korruptionsbekämpfung*, NEUE ZEITSCHRIFT FÜR ARBEITSRECHT (NZA) 646, 648 (2009); Wybitul *in* Knierim/Rübenstahl/Tsambikakis, *Internal Investigations*, 2013, 294.

itoring measures, employers face risks of criminal liability,[10] fines,[11] prohibitions on using evidence with regard to the information collected,[12] claims for damages asserted by persons affected by the inspection of their emails, massive reputational damage due to negative reporting in the media and a number of other disadvantages.

A. Monitoring business emails if private use is prohibited

From a legal perspective, it can only be advised that companies prohibit the private use of business email accounts.[13] This is because the permissibility and limits of email monitoring depend heavily on whether the employer allows the private use of the corporate IT system. If the employer prohibits its employees from the private use of business email accounts, it has extremely extensive options with regard to monitoring and supervision. It can then, as a rule, access electronic communication in the company. If private use is prohibited, emails on company servers are treated similarly to business letters.[14] In this case, access to email accounts is governed by the general requirements of data protection, e.g. in the form of sec. 32 I 1 or 2 *BDSG*.[15] Ultimately, the employer must weigh up its own interest in monitoring emails against the right of those affected to informational self-determination.[16]

B. General prohibition on monitoring emails if private use is permitted?

As managing a comprehensive prohibition on private use is not possible in practice, most companies in Germany permit their employees to send and receive private emails via their business account.[17] This approach leads to considerable problems that are described in detail below.

---

10 E.g. pursuant to sec. 44 BDSG or pursuant to sec. 206 I StGB (disputed), cf. also sec. 202 a StGB.

11 In particular pursuant to sec. 43 II no. 1 BDSG.

12 Cf. e.g. BAG, NZA 2014, 143; ZD 2014, 260; *or* Stefan Brink/Tim Wybitul, *Der "neue Datenschutz" des BAG*, ZD 225 (2014) on the inadmissibility of evidence obtained in breach of data protection regulations in civil proceedings.

13 E.g. *also* Riesenhuber, *§ 32, in* Beck Online Kommentar BDSG margin no. 146 (Heinrich Amadeus Wolff et al eds., 4th ed. 2013).

14 Cf. e.g. GREGOR THÜSING, BESCHÄFTIGTENDATENSCHUTZ UND COMPLIANCE margin no. 48 et seq. (2nd ed., 2014); Katrin Stamer & Michael Kuhnke *in* Plath (footnote 2 above), § 32 margin no. 78.

15 *Likewise* Stamer/Kuhnke *in* Plath (footnote 2 above), § 32 margin no. 81.

16 Cf. Regional Labour Court [Landesarbeitsgericht – LAG] of Hamm, judgment of 10 July 2012 – 14 Sa 1711/10, BeckRS 2012, 71605; CCZ 2013, 115 with comments *by* Heinemeyer, CCZ 2013, 116.

17 E.g. also Stamer/Kuhnke, *in* Plath (footnote 2 above), § 32 margin no. 79 *or* Martin Munz, *sec. 88 TKG,* Kommentar zum BDSG margin no. 21 (Jürgen Taeger & Detlev Gabel, 2nd ed. 2013).

a) If private use is permitted, are employers subject to telecommunications secrecy? If private use is not explicitly prohibited, the question arises of whether the employer is a "provider of telecommunications services". The majority of the specialist literature to date views employers as providers of telecommunications services if they permit the private use of corporate email systems.[18] As a result, telecommunications secrecy should also apply to the relationship between the employer and the employee in the case of business emails. Supporters of this view refer to the fact that telecommunications secrecy protects not only the content of a communication conducted by email, but also the detailed circumstances of the telecommunication process.[19] The employer is, therefore, not allowed to access the emails of its employees that are stored on company servers. Otherwise, it breaches sec. 88 *TKG* and possibly also sec. 206 I *StGB*.[20] Furthermore, the majority of the data protection supervisory authorities of the German federal states and the German federal government take this view.[21]

According to this view in the specialist literature, the employer should therefore be barred from accessing *all* email correspondence of the employee.[22] This is because, in order to distinguish between private and business emails, the employer must monitor individual emails and thereby commit a breach of telecommunications secrecy, which is subject to a penalty.[23] This view presents excessive hurdles for companies and is heavily criticised in some cases due to its practical consequences.[24]

---

18 Cf. e.g. Achim Seifert, *§ 32, in* BDSG margin no. 90 (Spiros Simitis, 8th ed. 2014); Peter Gola/Christoph Klug/Barbara Körffer, *§ 32, in* BDSG margin no. 18 (Peter Gola & Rudolf Schomerus, 11th ed. 2012); Ines M. Hassemer, *Strafrechtliche Folgen des Verstoßes gegen Beschäftigtendatenschutz*, *in* Daten- und Persönlichkeitsschutz im Arbeitsverhältnis 549, 571 margin no. 91 (Stephan Weth et al eds., 2014); Theodor Lenckner & Jörg Eisele, *§ 206, in* StGB Kommentar margin no. 8 (Adolf Schönke & Horst Schröder, 28th ed. 2010); Peter Gola, *Neuer Tele-Datenschutz für Arbeitnehmer? Die Anwendung von TKG und TDDSG im Arbeitsverhältnis*, MULTIMEDIA UND RECHT (MMR) 322 (1999); Mengel, Kontrolle der Telekommunikation am Arbeitsplatz, BETRIEBS-BERATER (BB) 1445, 1449 *et seq.* (2004); Christian Oberwetter, *Arbeitnehmerrechte bei Lidl, Aldi und Co.*, NZA 609, 610 et seq. (2008); René Hoppe & Frank Braun, *Arbeitnehmer-E-Mails: Vertrauen ist gut – Kontrolle ist schlecht*, MMR 80 (2010); *ultimately similar* Munz *in* Taeger/Gabel (footnote 17 above), § 88 *TKG* margin no. 23; BeckOK *BDSG*/Riesenhuber (footnote 13 above), § 32 margin no. 144; Stamer/Kuhnke *in* Plath (footnote 2 above), § 32 margin no. 78 et seq.

19 Sec. 88 I 2 *TKG*.

20 Cf. e.g. Martin Munz (*see* footnote 17 above), sec. 88 *TKG* margin no. 20.

21 Cf. Martin Munz (*see* footnote 17 above), sec. 88 *TKG* margin no. 42.

22 E.g. Achim Seifert (*see* footnote 18 above), § 32 margin no. 92.

23 Ulrich Riesenhuber (*see* footnote 13 above), § 32 margin no. 148 describes this view, which is based on the mixing of business and private email communication, as a "scrambled egg theory". Cf. *also* Martin Munz (*see* footnote 17 above), sec. 88 *TKG* margin no. 20.

24 Cf. e.g. Ulrich Baumgartner, 363, 380, *in* Daten- und Persönlichkeitsschutz im Arbeitsverhältnis (Stephan Weth et al eds., 2012)

b) Opposing view: Employers must adhere to the requirements of the BDSG. In the more recent specialist literature, the view is frequently expressed that employers are not telecommunications providers even if they allow their employees private use of business email accounts.[25] There are better arguments in favour of this view than for a rigid application of telecommunications secrecy and a resulting absolute prohibition on monitoring.[26]

The currently prevailing view in the literature regards employers as telecommunications service providers, in particular due to the highly indeterminate wording of sec. 3 *TKG*.[27] However, one of the arguments against this interpretation is that unclearly formulated provisions must initially be interpreted in a manner that is consistent with the constitution. With regard to the question of the permissibility of accessing emails on company servers, the opposing interests of the employer [28] and the employee[29] can only be reconciled in a manner that is consistent with fundamental rights by way of practical concordance.[30] However, this can only be done by weighing up the interests concerned and not on the basis of a strict prohibition on access as stipulated by telecommunications secrecy.

Even if telecommunications secrecy does not apply, the right of users of business email accounts to informational self-determination is protected comprehensively by the *BDSG* as well as the review of proportionality to be conducted pursuant thereto.[31] Access to business email accounts is governed in particular by the data protection provisions under sec. 32 I 1 or sentence 2 *BDSG*.

C. Practical significance of the possible applicability of telecommunications secrecy

The dispute about the question of the scope of application of sec. 88 *TKG* is extremely important for companies. The decisive factor in this respect is what legal consequences could arise from accessing an employee's business emails. Ultimately, it is therefore a

25 Cf. in respect of this conflict of opinions Gregor Thüsing (*see* footnote 14 above), margin no. 74 et seq.

26 Cf. e.g. Gregor Thüsing (*see* footnote 14 above), margin no. 74 et seq.; Ulrich Baumgartner, *in* (*see* footnote 18 above), 363, 380; Tim Wybitul, *Neue Spielregeln bei E-Mail-Kontrollen durch den Arbeitgeber*, ZEITSCHRIFT FÜR DATENSCHUTZ, 69 (2011).

27 Within the meaning of sec. 3 no. 6 *TKG*.

28 E.g. art. 2 I, art. 12 I, art. 14 I of the German Basic Law [Grundgesetz – GG].

29 E.g. art. 2 I in conjunction with art. 1 I GG, art. 10 I GG.

30 As rightly stated *by* Gregor Thüsing (*see* footnote 14 above), margin no. 91.

31 As ultimately also stated in Ulrich Riesenhuber (*see* footnote 13 above), sec. 32 margin no. 146 on prohibited private use.

matter of assessing the legal consequences or of analysing the possible consequences of accessing electronic communication in a company. To do so, it is not only important to be familiar with the legal opinions outlined above. Rather, above all the decisive factor for practitioners is how courts assess the question of the possible applicability of telecommunications secrecy.

D. Requirements laid down by court rulings on monitoring emails if private use is permitted

To date, there have been no rulings of the highest court instances on the question of whether employers that permit private email use are subject to telecommunications secrecy.[32] However, in 2010 the *Regional Labor Court of Lower Saxony*[33] and in 2011 the *Regional Labor Court of Berlin-Brandenburg*[34] addressed the question of whether such employers must be treated as telecommunications providers. The result of both decisions is clear: the judges did not deem the employers concerned to be providers of telecommunications services. Consequently, employers must not take into account telecommunications secrecy in the case of their employees' business emails.[35] The more recent judgments of German courts outlined below are also along these lines.

a) Regional Labor Court of Hamm. Helpful guidance is contained in the judgment of the *Regional Labor Court of Hamm* of 10 July 2012,[36] which concerns the permissibility of the use of chat records in dismissal protection proceedings. In the case of dismissal due to serious breaches of duty, the court granted the employer very extensive options for monitoring the electronic resources provided. In contrast to the private use of business email accounts, there are a number of reasons in favor of the applicability of telecommunications secrecy with regard to the use of chat providers on a workstation. The judges ultimately left open whether the employer must be regarded as a "service provider" within the meaning of the *TKG* in respect of chatting on the workstation. Nevertheless, they granted the company highly extensive monitoring options because the company had previously stated in corresponding guidelines that employees must not expect any confidentiality when using the corporate IT systems:

This can also be applied to accessing business email communication. In its decision, the *Regional Labor Court of Hamm* expressly found that the treatment of chat records

---

32 As also stated *by* Martin Munz (*see* footnote 17 above), sec. 8 *TKG* margin no. 20.

33 Regional Labor Court of Lower Saxony, NZA-RR 2010, 406.

34 Regional Labor Court of Berlin-Brandenburg, NZA-RR 2011, 342.

35 Cf. Ulrich Fülbier & Andreas Splittgerber, *Keine (Fernmelde-) Geheimnisse vor dem Arbeitgeber?*, NEUE JURISTISCHE WOCHENSCHRIFT, 1995 (2012).

36 Regional Labor Court of Hamm, judgment of 10 July 2012 – 14 Sa 1711/10, BeckRS 2012, 71605.

must, as a rule, follow the legal treatment of emails.[37]

The fact that the *Regional Labor Court of Hamm* found in favor of the employer in its weighing up of interests, above all due to the corresponding guidelines, underlines that employers are well advised to retain extensive control and monitoring rights with regard to the IT infrastructure provided. An ever growing number of employers are responding to the more recent court rulings by revising their policy on the use of the Internet and email systems in the company. In this respect, companies should specifically state what use of corporate email systems is permitted and what is not. If the employer wants to ensure that emails can be used in subsequent court proceedings, it should primarily inform its employees of what monitoring measures they must expect and under what circumstances emails will be monitored by issuing corresponding guidelines. This is because the German Federal Labor Court [*Bundesarbeitsgericht – BAG*] is increasingly adopting the approach of not using evidence that has been collected behind the backs of employees.[38] Against this background, employers can only be advised to create a high degree of transparency.

b) Administrative Court [Verwaltungsgericht – VG] of Karlsruhe. The *Administrative Court of Karlsruhe* also expresses a clear view on the question of whether employers that permit the private use of business email accounts must be regarded as service providers within the meaning of the *TKG*:[39]

"The plaintiff invokes the provision under sec. 88 *TKG* entitled "telecommunications secrecy". Pursuant to sec. 88 I 1 *TKG*, telecommunications secrecy applies to the content of the telecommunication and its detailed circumstances, in particular whether someone is or was involved in a telecommunications process. Pursuant to sec. 88 II 1 *TKG*, every service provider is obliged to safeguard telecommunications secrecy. (...)

Even if private use is assumed to be permitted, the legislative purpose of the *TKG* prevents any use of sec. 88 *TKG*. Sec. 1 TKG indicates that the Act aims to promote private competition in the area of telecommunication, therefore that it is geared towards the legal relationships between the state and telecommunications providers as well as those between telecommunications providers. However, the spirit and purpose of the Act is not to govern internal legal relationships – e.g. between employer and employee – within companies or authorities."[40]

---

37 Regional Labor Court of Hamm, judgment of 10 July 2012 – 14 Sa 1711/10, BeckRS 2012, 71605 margin no. 179.

38 E.g. German Federal Labor Court, NZA 2014, 143; ZD 2014, 260 or NJW 2014, 810.

39 Administrative Court of Karlsruhe, NVwZ-RR 2013, 797 margin no. 65.

40 Emphasis by the author.

The *Administrative Court of Karlsruhe* thus arrives at the same conclusion as the *Regional Labor Court of Lower Saxony* and the *Regional Labor Court of Berlin-Brandenburg*. Here, too, the judges correctly reject any applicability of telecommunications secrecy in the employment relationship.

Furthermore, the decision clearly shows that, even without telecommunications secrecy, the right to privacy of those affected by the analysis of their data is protected quite effectively because the administrative judges essentially found in favor of the plaintiff to the extent that his personal data was not permitted to be used any further. They justified this conclusion on the basis of the data protection provisions applicable to the case decided on.[41]

c) Regional Labor Court of Hesse. The *Regional Labor Court of Hesse*[42], too, assesses in a similar manner the question of whether employers are providers of telecommunications services. The case in question related to the summary dismissal of an account manager for deleting business emails, customer contacts and customer appointments of the employer. In the dismissal protection proceedings, the employee submitted that he

"was able to freely dispose of his Outlook account and also used it to save and send private data. (...). Any knowledge regarding the plaintiff's behavior with respect to this data should not be used in the collection of evidence as this violates the plaintiff's general right to privacy."

This line of argument pursued by the plaintiff is consistent with the view outlined above that the employer is not permitted to access emails on company servers if it allows or tolerates the private use of email accounts.

The employer took a different view. After corresponding suspicions had arisen, it asked an expert to prepare an expert opinion in order to establish whether and which emails and other data had been deleted by the account manager. If the *Regional Labor Court of Hesse* had actually deemed the employer's actions as a violation of telecommunications secrecy due to the allegedly permitted private use of the email account, it would not have been allowed to use the expert opinion in the subsequent court proceedings. However, the *Regional Labor Court of Hesse* did not deem that it was prevented from using the expert opinion. Ultimately, the judges thus clearly rejected the restrictive view in the specialist literature. In the grounds for the judgment, the judges stated in this respect:

---

41 In particular on the basis of sec. 15 IV of the State Data Protection Act of Baden-Württemberg [Landesdatenschutzgesetz Baden-Württemberg – DSG BW].

42 Regional Labor Court of Hesse, judgment of 5 August 2013 – 7 Sa 1060/10, BeckRS 2013, 75084; ZD 2014, 377 with comments *by* Thorsten Sörup, *Außerordentliche Kündigung - Datenlöschung - Urlaubsanspruch - unzulässige Verweisung auf einzelne Tarifbestimmungen*, ZEITSCHRIFT FÜR DATENSCHUTZ, 378 (2014).

"Nor is the court prevented from using the result of the taking of evidence determined by the expert opinion, although the analysis of the hard drive submitted to the expert revealed that private emails and private contact addresses were also among the files deleted by the plaintiff.

Given that the computer was provided to the plaintiff as a work tool and the plaintiff used it to process and store a considerable volume of data that he required to perform his duties under his employment contract, the fact that private files of the plaintiff also became known by name during the taking of evidence constitutes such a minor intrusion into his privacy that this does not lead to a prohibition on the use of evidence, and therefore the question of whether the plaintiff was at all permitted to use the defendant's computer for private purposes does not need to be addressed any further."

If the *Regional Labor Court of Hesse* had assumed the possible applicability of telecommunications secrecy in the case described, it would have had to justify why it used the data in question despite the employer violating sec. 88 *TKG* and possibly also sec. 206 I *StGB*. Instead, the judges even clarify in the cited decision that telecommunications secrecy or other restrictions on data use by employers are not applicable in the core area of the employment relationship – regardless of the question of whether the company allows the private use of corporate IT systems.

E. Consequences for companies

As a result, it can be stated that, according to the correct view, telecommunications secrecy does not prevent business email communication from being monitored and analyzed. In fact, employers must adhere to the strict requirements of data protection law. The employer can take into account the general right to privacy of the employee concerned by informing its employees of the possible monitoring of email inboxes (e.g. in a works agreement or IT guidelines) and precisely specifying the conditions for monitoring. Furthermore, employers should only permit the private use of email accounts if employees have consented to any monitoring.

III. CHECKLIST: DATA PROTECTION IN THE CASE OF EMAIL ANALYSIS

The following checklist provides guidance on how to analyze and inspect business emails in accordance with data protection provisions. It does not replace the respective review of data protection requirements in the individual case. In cases of doubt, the company must always perform a review of permissibility based on the circumstances of the respective inspection of emails and the content of the communication concerned.

A. Preparation for the analysis

Companies should always carefully prepare for the monitoring of emails and establish in good time conditions that enable the electronic communication required to realize the specifically pursued purpose of the monitoring to be inspected in accordance with data protection provisions.

a) Review and, if necessary, amendment of existing IT rules. Corporate rules on email use often have a huge influence on the permissibility of analyzing email accounts. As already stated, more detailed monitoring is possible in principle if the employer has prohibited the private use of business email accounts or the users concerned have consented to monitoring. The decisive factor here is whether users are entitled to legitimately expect that email communication is not monitored. In such cases, only restricted access to electronic communication is usually allowed. The corresponding corporate rules on email use can thus have a major effect on the review of proportionality that is necessary for the specific analysis.

b) Composition of the investigation team. The group of persons with access to personal data for the purpose of analyzing emails should be restricted to the minimum needed to effectively investigate the matter. The company should clearly define duties and areas of responsibility. The "need to know" principle applies.

c) Training the investigation team. Extensive knowledge of data protection law is required in order to inspect emails in compliance with data protection provisions. Otherwise, there is, among other things, the risk of criminal liability and fines, of the information and evidence obtained being unusable and considerable reputational damage. Therefore, all members of the investigation team should be trained in the key data protection requirements.

d) Obligation to maintain data secrecy. All parties involved in the inspection must be comprehensively obliged to maintain data secrecy pursuant to sec. 5 *BDSG* and informed of the possible consequences of data protection violations. In particular, the company should also provide information on the risks of fines and criminal liability pursuant to secs. 43, 44 *BDSG* as well as secs. 201 *et seq*. *StGB*.

e) Involvement of data protection experts. As far as possible, an experienced data protection expert should attend each email inspection in order to address questions relating to the individual case. In all cases, this expert must be highly familiar with the aforementioned relevant court rulings on email inspections and on employee data protection.

f) Involvement of the data protection officer. The company's data protection officer should be involved in each phase of the email inspection. If possible, the data protection officer should perform a prior check of the specifically planned measures before the email inspection.

g) If necessary, take into account co-determination rights of the works council. As a rule, the works council has a co-determination right in respect of email inspections pursuant to sec. 87 I no. 6 of the German Works Constitution Act [*Betriebsverfassungsgesetz – BetrVG*]. If the employer disregards this co-determination right, the works council may very quickly obtain a cease and desist order preventing the email inspection from being carried out any further. In addition, sec. 80 I no. 1 *BetrVG* affords the works council extensive information rights with regard to data protection issues. In practice, the conclusion of corresponding works agreements has proven itself as a suitable way to create legal certainty.[43]

h) IT infrastructures. Technical requirements, in particular relating to documentation as well as to data backup and data analysis, are also important. There is a wide range of software solutions for inspecting emails.[44] Corresponding contractual agreements must be concluded with the providers of forensic software and services. In this respect, it must also be examined whether these provisions can be structured as commissioned data processing contracts within the meaning of sec. 11 *BDSG*. At the same time, the company should also carefully check whether the respective contracts offered by the providers meet the relevant legal requirements, cf. in particular sec. 11 II–V *BDSG*.

i) Data security. Pursuant to sec. 9 *BDSG*, a high degree of data security is stipulated in the case of email analysis in particular. This applies especially to entry, access and disclosure controls. It is imperative that these controls guarantee that information from the email inspection does not become known to any unauthorized parties. In particular, the use of USB sticks and other mobile data carriers must be effectively prohibited.

B. Legal framework

In view of the strict requirements for the lawful monitoring of internal electronic communication and the possible serious consequences of data protection errors, companies should carefully ensure that they also implement the measures specified below in order to create a sufficient legal framework.

a) General permissibility of the planned email inspection. Are there reliable statements on the general permissibility of the intended inspection of electronic communication? These could be, in particular, statements by the supervisory authorities for data protection as well as legal expert opinions by data protection experts.

43 Cf. *BAG*, NZA 2014, 551.

44 E.g. Concordance, CT Summation, Kroll Ontrak, Forensic Toolkit.

b) Possible involvement of the data protection authority. One of the safest ways to reliably rule out subsequent legal risks is to liaise with the competent supervisory authority for data protection. If the timeframe of an investigation permits this course of action, companies should certainly examine whether liaising with the data protection authority is possible and expedient in the specific individual case.

c) Data backup. The persons involved in the analysis should only inspect data that is saved in *forensic backup copies*. Intrusion into ongoing email correspondence must be avoided as a matter of urgency. In particular, it should be ensured that, in the course of the inspection of emails, no changes are made to metadata on the company's email servers. Otherwise, the subsequent evidentiary value of the inspected emails could be significantly reduced.

d) Instructions for the investigation team. The persons involved in the analysis should not read emails that are obviously private or stop inspecting private correspondence if they have already started to do so.

e) Informing the persons affected. The persons affected by the inspection of their business email correspondence should be informed as early as possible of the analysis of their electronic communication. In particular with regard to email inspections, German data protection law requires a high degree of *transparency* when handling personal data (sec. 4 II and III as well as secs. 33 *et seq*. *BDSG*).[45] It is often possible to inform the persons affected of the intended inspection of their emails after the mirroring of emails in order to create a forensic backup copy. The situation is different if there are specific indications that, otherwise, the objective of the investigation could be endangered, e.g. by wiping away traces.

C. Implementation of the email inspection

The actual inspection of the electronic communication that is decisive in order to realize the respective purpose of the monitoring is also subject to substantial requirements under data protection law.

a) Confidentiality. Any internal disclosure of the results of an email inspection should be restricted to the absolute minimum required. Any prejudgment or stigmatization of the persons affected by the investigation of the matter must be avoided.

b) Narrowing down the group of persons affected. The group of persons affected by the analysis of their emails must be strictly limited to those required to realize the objective

45 Cf. *BAG*, NZA 2014, 143.

of the monitoring. If a user has no connection to the purpose being pursued by the inspection of the emails, his business email account should not be accessed.

c) Narrowing down the email inspection. The email inspection should be strictly limited to the communication that is relevant for the matter in question, e.g. by being narrowed down to specific periods, business transactions, questionable payments, contractual relationships or agreements, business partners, other persons involved.

d) Weighing up of interests in the individual case. When examining the matter from the perspective of data protection law, it is necessary to weigh up the specific interest of the company in conducting an investigation and the right of the persons affected by the inspection of their emails to the protection of their informational self-determination. If the protection-worthy interest of the person affected by the inspection of his data in the preclusion of the analysis of his emails outweighs the other factors, the inspection *must not be carried out*.

When weighing up these interests – the realization of the objective of the investigation versus the right of the persons affected to informational self-determination – all the circumstances of the respective case and of the individual email communication must be taken into account. As a rule, this *review of proportionality in the individual case*[46] requires considerable prior knowledge of data protection law.

In particular, the respective reader of the email must assess whether the inspection of this specific electronic communication is at all *suitable* for investigating the matter in question, whether there are *milder means* of realizing the objective of the investigation just as effectively and whether the inspection is *reasonable*, i.e. can be conducted on the basis of an appropriate weighing up of the interests of the persons affected and those of the company.

If the inspection of an email is clearly unable to realize the objective of the investigation, it is not *suitable* and therefore not permissible. For this reason, emails that are obviously of an exclusively private nature may not be inspected, for example. Furthermore, the inspection of the emails in question must always be the *mildest of all equally effective means* that are available in order to investigate the matter. This requirement must be ensured in every phase of the investigation of the matter. In particular, according to the court rulings, the highest possible degree of transparency vis-à-vis the employees affected by the analysis of their emails must be ensured.

---

46 Cf. *in detail* in respect of the three-stage review standard Oliver Zöll (*see* footnote 17 above), sec. 32 BDSG margin no. 18; Tim Wybitul, *Wie viel Arbeitnehmerdatenschutz ist "erforderlich"?*, BETRIEBSBERATER, 1085 (2010); TIM WYBITUL, HDB DATENSCHUTZ IM UNTERNEHMEN 175 et seq. (2nd ed., 2014).

Even if the inspection of an email is suitable for realizing the purpose of the investigation or monitoring and constitutes the mildest of all equally effective means, this handling of personal data must always be proportionate in the narrower sense. An email inspection is *appropriate* if legitimate interests of the persons involved in the electronic communication do not outweigh the company's interest in conducting the investigation. In particular, any email inspection that concerns the core area of the affected persons' private lives, e.g. emails of an intimate nature, is prohibited.

e) Review of emails that are problematic from the perspective of data protection law. In practice, it has proved worthwhile for the person involved in the analysis to designate emails that he deems to be problematic from the perspective of data protection law. These emails should only be inspected later after a detailed review of the permissibility of the analysis under data protection law – or if other suspicions indicate that precisely the email communication in question is decisive for the specific purpose of the investigation or monitoring. The assessment of individual emails under data protection law often also changes in the course of the respective investigation because the investigators obtain further information.

f) Graduated approach. As far as possible, the actual inspection should initially focus on random samples instead of a uniform and complete check. Equally, analyses must always relate strictly to the respective objective of the investigation.

D. Documentation of the email inspection

Compliance with the above points should be *documented comprehensively* for evidentiary reasons and in order to avoid considerable disadvantages (up to and including risks of criminal liability). In particular, the points below should be clearly recorded.
As a rule, such documentation is not prepared in writing, but in electronic form. Commercial software solutions that help companies inspect emails usually have corresponding functions for preparing records of email inspections.

a) Specific purposes of the email inspection. Above all, the company should very clearly set out the purposes being pursued by the respective email inspection. This can make it much easier for the company's data protection officer to review the permissibility of the planned measures.

b) Description of the individual steps in the investigation. The company should systematically and clearly determine the individual phases of the respective measures designed to investigate the matter.

c) Search criteria used. The company should record the parameters used to select the electronic communication actually inspected.

d) Email accounts affected. Which accounts were inspected, which periods were affected

by the monitoring of emails?

e) Emails discovered that are relevant to the matter. Finally, the company should document which emails it deems relevant for the matter in question. In addition, it should also record the conclusions to be drawn from these emails for the further investigation of the matter.

IV. SUMMARY AND RECOMMENDED ACTIONS

Complex requirements apply to the monitoring of business email accounts. Considerable risks could arise from violations of the law, up to and including possible criminal liability pursuant to sec. 206 I *StGB* or secs. 44 I, 43 II *BDSG*.[47] If the recommendations specified in the above checklist are taken into account, these risks can be significantly reduced or even ruled out. Moreover, companies should review and, if necessary, thoroughly revise existing usage rules or works agreements relating to the handling of emails within the company.

A. Approach if private use is prohibited

If companies wish to access their employees' business emails in a legally secure manner, they should, if possible, prohibit the private use of company accounts. In this case, electronic communication in the company is treated similarly to business letters. As the right to privacy of the employees concerned is usually only affected to a minor extent in such cases, the weighing up of interests will mostly favor the employer. However, in this case, too, the employer should clarify as a matter of urgency which monitoring measures it reserves the right to implement.

B. Approach if private use is permitted

In practice, it is often not expedient to prohibit the private use of business emails in many cases. According to the view taken by most supervisory authorities for data protection and probably still the majority of the specialist literature, risks of criminal liability can be ruled out in the case of email monitoring due to sec. 206 I *StGB* at most by carefully drafted provisions on the use of corporate email systems.[48] In these cases, employers should only allow private use by those employees who have consented to appropriate monitoring of their electronic communication.

---

47 Cf. e.g. *BGHSt* 58, 268 = NJW 2013, 2530 with comments by Tim Wybitul, ZEITSCHRIFT FÜR DATENSCHUTZ, 509 (2013).

48 As also stated *by* Michael Walther & Mark Zimmer, *Mehr Rechtssicherheit für Compliance Ermittlungen,* BETRIEBS-BERATER, 2933, 2937 (2013).

The company can certainly instruct employees not to store sensitive or intimate content on corporate IT systems by issuing guidelines or works agreements. It can also order employees not to use company computers for any content that the employer is not supposed to monitor. If employees store private content despite this prohibition, it must be clear to them that they cannot invoke the fact that they expected the company not to access their data. This applies in particular if the employer expressly reserves the right to make random checks or to implement monitoring if there is a firm suspicion of breaches of duty.

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

COMPLIANCE TECH

Tools for a modern compliance framework

Micha-Manuel Bues

AUTHOR

Dr. Micha-Manuel Bues, M.JUR. (Oxford) is a lawyer at Gleiss Lutz since 2013. He advises on German and European antitrust law as well as on all aspects of European law. He is, amongst others, specialized in antitrust compliance programs. He also advises and lectures on the use of legal technology and runs the blog www.legal-tech-blog.de. Micha-Manuel Bues studied at the universities of Passau, Bonn, Cologne and Oxford.

Data is everywhere. The volume, variety and velocity of data coming into companies have reached unprecedented levels. It is estimated that around 5 exabytes (= 5 billion gigabytes) of data are created each day, and this number is doubling roughly every 2 years.[1] Due to the sheer amount, companies do not know which potential compliance risks are "hidden" in the data. Companies are also confronted with more regulations, tightened enforcement and heightened global competition. This gives rise to new challenges for an effective compliance framework. However, surveys indicate that companies (depending on the industry and size) are relatively slow to adopt modern technologies to address these challenges. Law firms and lawyers are also reluctant when it comes to modern data analytics.

The only way to proactively or reactively investigate or prevent compliance issues in an era of data is to understand complex data sets from multiple sources within a company. In other industries, data analytics[2] is frequently used to uncover hidden patterns, unknown correlations and other useful information. Using data analytics, data scientists and others can analyze huge volumes of data that conventional analytics and business intelligence solutions can't touch. The emerging field of "Compliance Tech" tries to utilize data analytics in conjunction with subject matter professionals to bring compliance detection and prevention into the 21th century. Compliance Tech is used to proactively seek opportunities to detect and prevent fraud, waste and abuse to ensure compliant behavior. Compliance Tech aims to make the invisible visible. Compliance Tech provides the toolset to spot patterns or trends in data that are invisible to the naked eye. This is achieved by using different techniques (which will be explained later in greater detail) which helps to retrieve, organize, structure and streamline data to make invisible patterns become visible.

Compliance Tech brings compliance investigation or prevention to a new level. It allows for anomaly detection, clustering and risk ranking through a statistical-based analysis. This approach ensures better results compared to a "traditional" rule-based approach (matching, grouping, ordering, jointing and filtering etc.) when deployed over large data sets. Data visualization and test mining are, for example, superior to traditional keyword searching. Without these tools, companies remain dependent on human identification of risks and violations, whether flagged by employees, hotline tips, whistle-blowers or government auditors. Their compliance efforts often consist only of training employees to spot misconduct, and in setting aside financial reserves to fund expensive, after-the-fact investigations by outside counsel.

This article seeks to present the technologies, methodologies, processes and practices

1 Cf. VINCENZO MORABITO, BIG DATA AND ANALYTICS 105 (2015).

2 THOMAS A. RUNKLER, DATA ANALYTICS: MODELS AND ALGORITHMS FOR INTELLIGENT DATA ANALYSIS (2015), provides a good introduction into this field.

behind Compliance Tech and will give practitioners, especially lawyers, a short overview of this rapidly emerging but still relatively unknown field. The article does not try to give a comprehensive overview of the subject but intends to familiarize compliance practitioners with some of the fundamentals of data analytics. Compliance Tech forms part of a compliance program within a company. A compliance program will be defined here as an internal program and decision policy made by a company in order to meet the standards set by government laws and regulations.[3]

Most of the technologies and methodologies deployed in Compliance Tech require **big data**[4]; a buzzword that describes a volume data so large that it is difficult to process using traditional database and software techniques.[5] An important distinction to bear in mind is between structured and unstructured data.[6] Structured data which is stored in precisely defined and described data fields. A typical example is a customer database in which each record consists of a name, address, birth date, etc. Structured data have a clear model and description and are therefore easily stored, processed and analyzed. Conversely, unstructured data do not have a precisely defined structure. This category may include images, videos, websites or content of e-mail and/or other communications. Unstructured data constitutes the absolute majority of generated data.

There are many techniques that draw on disciplines such as statistics and computer science (particularly machine learning) that can be used to analyze the structured and unstructured datasets. The following non-exhaustive list entails the most commonly used techniques in Compliance Tech. Not all of these techniques strictly require the use of big data; some can be applied to effectively smaller datasets. The techniques and methodologies are presented here in an order in which they would be typically used. Depending on the actual compliance framework required, different techniques may be used or combined to cater for the particular needs of a company.

A common first step in deploying Compliance Tech is **data acquisition**.[7] This aims to ensure a stable transfer of internal and external data and convert the data into a format suitable for further analysis. **Data mapping** serves as the initial step in data inte-

---

3 Cf. JULIA STEHMANN, COMPLIANCE-MANAGEMENT 6 ff. (2011).

4 VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW LIVE, WORK, AND THINK (2013) gives a non-scientific overview of the opportunities and challenges of big data.

5 Cf. JAMES R. KALYVAS & MICHAEL R. OVERLY, BIG DATA: A BUSINESS AND LEGAL GUIDE 1 (2015); ANIL AGGARWAL, MANAGING BIG DATA INTEGRATION IN THE PUBLIC SECTOR 73 (2015).

6 Cf. MICHAEL BRACKETT, DATA RESOURCE DATA: A COMPREHENSIVE DATA RESOURCE UNDERSTANDING 14 (2014).

7 MAURIZIO DI PAOLO EMILLIO, DATA ACQUISITIONS SYSTEMS (2013) gives a detailed introduction into this area.

gration.[8] Data mapping is the process by which different data models are linked. This uses a defined set of methods to characterize the data in a specific definition. The technique involves evaluating data values in different data sources, as well as automatically and simultaneously discovering complex mappings between the sets. Data mapping is also used to consolidate multiple databases into a single database.

Link analysis is a technique used to evaluate the relationships or connections between various types of objects (nodes), including people, organizations and transactions.[9] Link analysis is a kind of knowledge discovery that can be used to visualize data, allowing for better analysis, especially in the context of links (web links or relationship links). Link analysis might be able to detect or establish "hidden" relationships within a data set.

Social network analysis (SNA) is the process of quantitative and qualitative analysis of a given social network. SNA measures and maps the flow of relationships (ties) and relationship changes between entities.[10] Simple and complex entities (nodes) include websites, computers, animals, humans, groups, organizations and nations. Along with link analysis, SNA can, for example, help to identify related parties, conflict of interests, corruption and bid rigging.

Text mining is the analysis of data contained in natural language text.[11] The application of text mining techniques to solve business problems is called text analytics. Text analytics software can help by transposing words and phrases in unstructured data into numerical values which can then be linked with structured data in a database and analyzed with traditional data mining techniques.

Data mining is the process sorting through data to identify patterns and establish relationships.[12] Data mining parameters include:

- Association, i.e. identifying associations between events.
- Sequence or path analysis, i.e. identifying patterns where one event leads to another later event.
- Classification is a set of techniques used to identify the categories in which new data points belong, based on a training set containing data points that have al-

8 Cf. QAMAR SHAHBAZ, DATA MAPPING FOR DATA WAREHOUSE DESIGN Chapter 3 (2015).

9 Cf. B. KIRWAN & L. K. AINSWORTH, A GUIDE TO TASK ANALYSIS 116 ff. (1992).

10 Cf. IAN MCCULLOH & HELEN ARMSTRONG, SOCIAL NETWORK ANALYSIS WITH APPLICATIONS Introduction (2013).

11 Cf. STÉPHANE TUFFÉRY, DATA MINING AND STATISTICS FOR DECISION MAKING 627 (2011).

12 Cf. STEPHAN KUDYBA & RICHARD HOPTROFF, DATA MINING AND BUSINESS INTELLIGENCE: A GUIDE TO PRODUCTIVITY 37 (2001).

ready been categorized.[13]

- Clustering is used to place data elements into related groups without advance knowledge of the group definitions.[14]

Discovering patterns in data that can lead to reasonable predictions of future trends is known as **predictive analytics**.[15] The central element of predictive analytics is the predictor, a variable that can be measured for an entity to predict future behavior. Multiple predictors are combined into a predictive model, which can be used to forecast future probabilities with an acceptable level of reliability.

Data visualization is a general term for tools which help to understand the significance of a particular data set by placing it in a visual context.[16] As a result of the visualization, patterns, trends and correlations can be exposed and recognized more easily. State-of-the-art data visualization software goes beyond the standard charts and graphs used in Excel. Data visualization entails more sophisticated tools such as infographics, dials and gauges, geographic maps, sparklines, heat maps, and detailed bar, pie and fever charts. One of the most widely used visual techniques is a tag cloud. A tag cloud is a stylized way of visually representing rates of occurrences of words used to described tags. The most popular topics are normally highlighted in a larger, bolder font. Data visualization helps us to absorb large pieces of information more efficiently.

Combining the described methods significantly enhances the overall probability of detecting and preventing compliance incidents within a company. Law practitioners should a have a good understanding of these methods to ensure the best results for their clients. However in practice, there might be several challenges to overcome if a company, compliance department or law firm decides to use Compliance Tech.

One challenge with Compliance Tech is that companies or compliance teams need to understand how the tools work in practice. The challenge is to find the team with the right skillset. An ideal Compliance Tech team should be a combination of compliance experts with a legal background, and data scientists. All team members should be capable of working both with new technologies, and interpreting data to find meaningful compliance insights. However, in reality, members of compliance teams normally only

---

13 Cf. THOMAS A. RUNKLER, DATA ANALYTICS: MODELS AND ALGORITHMS FOR INTELLIGENT DATA ANALYSIS 85 (2015).

14 Cf. THOMAS A. RUNKLER, DATA ANALYTICS: MODELS AND ALGORITHMS FOR INTELLIGENT DATA ANALYSIS 103 ff. (2015).

15 COLLEEN MCCUE, DATA MINING AND PREDICTIVE ANALYSIS (2014); DEAN ABBOTT, APPLIED PREDICTIVE ANALYTICS (2014), give a good overview over the techniques used in predictive analytics.

16 Cf. Evan F. Sinar, *Chapter 5 (Data Visualization)*, in Big Data at Work 115 (Scott Tonidandel et al eds., 2015).

have a legal or non-tech background. Without proper training, they tend to have problems understanding the underlying concepts and methodologies of Compliance Tech. It is then difficult to effectively supervise the data analytic process and to apply the right technology architecture and capabilities. This expertise could either be built in-house, or outsourced to a third party IT partner. As the technology landscape in the data world is evolving extremely fast it could be helpful to work with a strong and innovative technology partner who can help create the right IT architecture to efficiently adapt to changes in the landscape.

In addition, any introduction of Compliance Tech should be accompanied with a change management approach that includes an extensive communication effort. Many companies fail to recognize that new analytics often requires new behaviors.[17] For this reason, communication plays an essential role to educate, inform and explain a Compliance Tech approach within a company or legal department. Personal experience has shown that it takes a considerable amount of time to introduce the concepts of Compliance Tech and their benefits to employees, business stakeholders, management and IT teams. The management must be willing to change in order for the data and models to yield better compliance decisions.[18]

In addition, it is important to find the right applications for Compliance Tech. Sometimes companies are lured into thinking that running analytics on a very large set of data is data analytics. But data analytics only shows it best results when it's used on a concrete and meaningful compliance case. Therefore, it is essential that the compliance team identifies the right data and has a good understanding of the data structure within a company. The sheer volume of information, particularly from new sources such as social media, is growing rapidly. Bigger and better data give companies a more panoramic and granular view of their business environment and potential compliance pitfalls. This all makes it more difficult to detect the right data or to see the potential value of data. Often the existing IT architecture may prevent the integration of stored information, and managing unstructured data often remains beyond traditional IT capabilities. It is therefore important to ensure an adequate IT infrastructure when using Compliance Tech.

Leveraging big data often means working across multiple disciplines such as IT, engineering, finance and procurement, and the ownership of data is fragmented across these disciplines. Addressing these organizational challenges means finding new ways of collaborating across functions and businesses. In this regard, it might be also sensible to

---

17 Michael Schrage, *Why your analytics are failing you*, Harvard Business Review (Apr. 8, 2014, 11:49 AM), https://hbr.org/2014/04/why-your-analytics-are-failing-you.

18 Dominic Barton & David Court, *Making advanced analytics work for you*, Harvard Business Review (Oct., 2012, 11:53 AM) https://hbr.org/2012/10/making-advanced-analytics-work-for-you.

drive an integrated approach to data sourcing, model building, and organizational transformation.

Data privacy and data security laws are one area of law that any business using big data will have to take very seriously.[19] In addition to local, state, national, and, even international laws, there are many other potentially applicable standards and guidance's. If a company uses Compliance Tech, it needs to ensure that its use is consistent with the above rules and regulations. In addition, as with many technological endeavors, big data analytics is prone to data breaches. Any data provided to a third party IT partner could get leaked, and needs to be protected accordingly.

It would be naive to see Compliance Tech as a panacea to cure all the woes of a compliance program. Although Compliance Tech is a remarkable tool that can help to enhance compliance efforts within a company, it is important to bear in mind that (a) the setup of a technology enhanced compliance program will take a considerable amount of time and effort and (b) that Compliance Tech has its inherent limitations. However, if these are understood properly Compliance Tech tools will be invaluable in compliance programs of the 21th century.

[19] For more information refer to JAMES R. KALYVAS & MICHAEL R. OVERLY, BIG DATA: A BUSINESS AND LEGAL GUIDE 33 ff. (2015).

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

WHEN COMPLIANCE FAILS

Jens Bergmann

AUTHOR

Dr. Jens Bergmann is an academic assistant at the Leibniz University of Hannover, Germany, where he researches and teaches at the Institute of Sociology since 2010. Before that he received his doctoral degree from the University of Bielefeld and a diploma in criminology at the University of Hamburg, Germany. His research interests lie in the fields of sociology of work and organizations, criminology and research methods. Current research activities are concerned with structures of corporate crime and with a comparison of organizational control strategies in different fields. He is the co-publisher of a book on the topic of failure in organizations and the author of sociological publications on corruption and compliance-structures.

TABLE OF CONTENTS

I. INTRODUCTION 87

II. COMPLIANCE AND THE ORDER OF CONTROL IN ORGANIZATIONS 88

III. CONSULTANCY EXPRIENCES IN THE FIELD OF COMPLIANCE 90

A. The functions of Compliance 91

B. Vagueness and Operationalization of Legal Norms 92

C. Role Conflicts and Organization-internal Disregard 93

IV. CONCLUSION 94

I. INTRODUCTION

Just about three months before the Volkswagen-manipulations of exhaust fumes were revealed and caused the biggest corporate scandal in the history of this carmaker, the group proudly published latest the results of their compliance-related measures. For VW, at that time the world still seemed to be in order. Due to an intensive preventive work, it was said, as a consequence of suspected independent controls, of "intensive investigations" and of checking "basic procedures", one would conduct "a very effective", successful and sustainable compliance management. Representatives of VW´s compliance department supported their statements by presenting the following figures: in the year 2014 every third employee (185.000 persons) had participated in compliance training events, the internal audit department had started investigations in 365 cases, 72 employees had lost their jobs because of irregularities, and one had terminated contracts with business partners in 16 cases because they had given cause for suspicion.[1] Furthermore, even the anti-corruption organization Transparency International in their sustainability report at the end of 2014 ranked VW in the leading group of world`s largest transparent companies.[2]

When shortly thereafter the scandal came to light, all these assurances and assessments turned out to be untenable assertions. The whole compliance management suddenly was left foolishly dangling in the winds. And especially after it was revealed that officials of VW already had been informed about possible illegal manipulation in 2011, the case raises the following questions: why did it to take so much time unless the fraud came to light? Where have the company`s inspectors been? What went wrong with the communication and cooperation between the internal investigators, the engineers and the management staff? Why could compliance not fulfill its purpose? Because the actual case of VW is not an isolated incident – similar phenomena of failing compliance procedures were already observed in cases like Siemens, Daimler or MAN –, this paper focuses on a general reason for the failure of compliance.

In the following the reason for this will be primarily identified with failing processes of establishing legal norms within an organizational context. Therefore the text highlights the topic of failing compliance from an organizational sociological perspective based on observations made during a training seminar for compliance officers. Organizations, this will be the underlying basic assumption of the following argumentation, normally act as

1 Statements *by* Peter Dörfler, Head of Auditing and Stephan Wolf, Member of the Compliance Council of VW.

2 Transparency International Deutschland e.V., *Nachhaltigkeitsberichte Deutscher Großunternehmen Wiederholungsstudie* 2014, *available at* https://www.transparency.de/fileadmin/pdfs/Themen/Wirtschaft/Nachhaltigkeitsberichte_ Grossunternehmen_2014.pdf (last visited Jan. 5, 2016).

co-producers in processes of enforcing legal norms.[3]

By using programs, guidelines, instructions and controls, they translate social law into internal, formal rules or "organizational law". Such organizational activities are legally binding and normally there is nothing new or problematic with them. Implementing legislation, for example in the fields of consumer law, tax law or labor law, has a long history and has long been carried out by routine work. Members of organizations by and large became familiar with these topics and normally employees understand what is expected of them. This looks different in the field of corporate crime law. Here, a routine implementation of legal norms is difficult because business criminal law is a very dynamic and complex law sector, marked by numerous changes on the one hand. On the other hand a translation of legal norms is complicated for organizations here because of internal, structural reasons. This article will examine some of these reasons. The thesis is that in the case of compliance, the coexistence of organizational norms and legal rules ("hard law" and "soft law") causes tensions and structural conflicts, because it disturbs the inner order, cooperative relationships and the role structure of the organization. Newly established compliance systems tend to undermine the legitimacy of legal norms, because they tend to prevent routine procedures of control, and they tend to fail to provide target groups with definite orientation.

In the following sections such assumptions will be explored empirically. In a first step, general characteristics and consequences of compliance as a new form of control of white-collar crime are sketched from an organizational sociological perspective (II.). Second, expectations and perceptions of compliance officers will be described when it comes to implementing legal norms. These perceptions are reconstructed on the basis of a participant observation made during a training seminar for compliance officers in Germany (III.). The article concludes with a statement that identifies the problems of translating legal norms into organizational structures with the fundamental and structural characteristics of organizations as social forms (IV.).

II. COMPLIANCE AND THE ORDER OF CONTROL IN ORGANIZATIONS

The ongoing boom of compliance as a subject and a market for corporations worldwide can be explained by a change of the legal situation in the field of economic crime. Reflecting on the development in this field, one can say that there has happened a kind of "outcry" for control as a consequence of the scandals, accounting frauds and

[3] Lauren Edelman & Marc C. Suchman, *When the Haves hold Court: Speculations on the Organizational Internalization of Law*, Berkeley Law Scholarship Repository (1999), *available at* http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1802&context=facpubs (last visited Oct. 12, 2015); SIM B. SITKIN & ROBERT J. BIES (eds.), THE LEGALISITIC ORGANIZATION (1994).

smashups around Enron and WorldCom in the early 2000nds. Since then the relevant laws have been continuously tightened. As a consequence of changes in corporate criminal law, corporations are faced with increasing demands to take action themselves. The state and the public expect more "translation work" from business corporations. These are forced to launch new forms of control, and therefore new compliance systems are established in order to strengthen the link between organizational processes and legal norms.[4]

What might this development mean for the internal structure of organizations and their orders of control? What kind of measures seems appropriate and reasonable to put the new legal norms into controlling practice? Controlling structures in organizations, this is an old and proven finding in organization sociology, work best when they are based on routines, clear cut tasks, comprehensible instructions and when they are embedded in satisfactory exchange relations.[5] But in contrast to this, a new feature of the law-compliance-control-constellation is a combination of various distinct requirements, heterogeneous purposes and demands on the firms. Besides an increase of regulative rules, judicial criminal controls and besides increasing liability risks, an increased sensibility of the public towards economic crime constitutes an additional factor corporations have to take into consideration. Accordingly, organizations are expected to adapt to possible rule-breaking behavior or to violations of norms simultaneously in a preventive, actively controlling and reactively-investigative manner. This bundle of necessities can lead to a mutual reinforcement of each sub-target of compliance, involving a rebuilding of the organizational structure as a whole. By this, the new legal requirements show new characteristics in three dimensions:

- With regard to the factual accuracy of organizational behavior and responsibilities, the new regulatory-legal expectations are causes of disorder. They are less clearly and less uniquely defined as before and they are sometimes topically diffuse. Different areas of organizational work can simultaneously be affected by the tightening of criminal law. Therefore, as a result of numerous new regulations, grey areas between "still allowed" and "forbidden" ways of behavior increase.
- Concerning the social sphere of organizations, new social roles, new contact areas and new potential conflicts between employees can develop. Due to creating new compliance-jobs or departments, new responsibilities emerge in organizations that tend to collide with already existing controlling institutions (for in-

4 Ralf Kölbel, *Wirtschaftskriminalität und unternehmensinterne Strafrechtsdurchsetzung*, 91 MschrKrim, 22, 22 (2008); Hans Krause Hansen, *Managing corruption risks*, REVIEW OF INTERNATIONAL POLITICAL ECONOMY 251, 253f. (18.2011).

5 Jeffrey Pfeffer, *The costs of legalization*, *in* The Legalisitc Organization (Sim B Sitkim & Robert Bies eds.1994); ARNOLD. S. TANNENBAUM, CONTROL IN ORGANIZATIONS 14ff. (1971).

stance the internal audit department). Relationships of trust, loyalties, workflows and routines can be jeopardized by compliance.

- From a temporal perspective, the new compliance control differs from conventional references to law insofar it is now put on a permanent footing. Now law as an external premise of organizational decision making is not a single, exceptionally activated medium anymore. Rather, it has developed to an ongoing background-theme of work, for example mentioned in regular trainings, in codes of conduct, in risk assessments or in monitoring processes. By compliance, legal considerations in general are more strongly connected to everyday-practices.

To sum it up: the described factors and characteristics of compliance are meant to strengthen the connection between organizational and legal norms. Law shall be more "embedded"[6] in organizational rules of procedures as well as in areas of responsibility. It is supposed to guide activities much stronger. For this purpose, controls become more formalized and differentiated, rules are modified. In general, one could say, for organizations the introduction of compliance takes on the character of a reform. But still today it seems to be generally difficult to implement these rights based compliance-reforms. Research on this topic, among other things, report on credibility problems or on a deficient deterrence of corporate misconduct.[7]

Regarding this, the crucial issue we are confronted with is how this problem presents itself from the point of view of compliance officers. How are problems of the translation/ implementation of legal norms practically articulated? We will discuss these questions on the basis of experiences made during a compliance-training seminar.

III. CONSULTANCY EXPRIENCES IN THE FIELD OF COMPLIANCE

The observations described in the following result from data recorded during participation in a one-week further education seminar for business professionals and executives. This seminar, conducted in winter 2014, aimed at qualifying the participants as certified so called "compliance officers". The total number of participants was 19, most of them being in charge of compliance, i. e. they were executives from organizational

6 ARTHUR L. STINCHCOMBE, WHEN FORMALITY WORKS 6 (2001).

7 Kimberly D. Krawiec, *Cosmetic Compliance and the Failure of Negotiated Governance*, 81 Washington University Law Quarterly 487, 490 f. (2003); Jonas Pape, *Zur Wirksamkeit von Corporate Compliance*, CORPORATE COMPLIANCE ZEITSCHRIFT 233, 236 (6.2009); CHRISTINE PARKER & VIBEKE LEHMANN NIELSEN, EXPLAINING COMPLIANCE (2011); Ralf Kölbel, *Wirksamkeit und Funktionsbedingungen von Compliance aus wirtschaftskriminologischer Sicht*, *in* Handbuch Criminal Compliance 1443 (Rotsch ed., 2014).

supervisory departments (e. g. internal audit or legal department), most of whom working for bigger, sometimes internationally operating industrial, services or financial enterprises. In the course of the seminar, a total number of six different experts gave lectures of four to eight hours every day, among them experts for commercial criminal law, a public prosecutor, a compliance officer from a DAX-30 enterprise as well as auditors. The lectures were, among others, on legal bases, liability risks, compliance organization, prevention, public prosecutor investigations, compliance in the commercial field, data protection and IT compliance as well as so called reactive compliance (internal investigations). The author made notes during his participation and fixed his observations in writing immediately after the end of the seminar. Furthermore, seminar-related documents were assessed, and there was the possibility to interview selected participants.

A. The functions of Compliance

Despite the participants showing a basically reserved attitude towards the topic of the seminar ("*This is just a fashionable issue*"; "*We're breaking a butterfly on a wheel*")[8], the predominant opinion among the participants was that the establishment of compliance control in their own companies was necessary. The function of compliance – this became clearly obvious by the questions and discussions – was first of all considered a means to be on the safe side when it comes to external prosecution and to avoiding liabilities and image damages for their own companies. The lecturers and the future compliance officers considered it their predominant task to protect colleagues from prosecution by the state: "*This is what we're all interested in: I must internally protect the staff member*". The prevention of business delinquency was only of secondary interest. Thus, from the point of view of those concerned – and this is a first astonishing insight – a crucial action-stimulating risk results rather from the activities of state supervision and sanctioning authorities than from the threat of potential business delinquents. The threat was symbolized by the figure of the prosecutor. The prosecutor, about whom jokes were made already on the first day, symbolized the hostile forces and bound the participants together. The threat scenario of a humiliating "*visit*" by the prosecutor together with his marauding customs officers appeared again and again ("*The customs officers are always armed; they even come early in the morning when the children are still sitting at the table*"), anecdotes of this kind were told eight times on the whole. Also the US American Securities and Exchange Commission (SEC) was mentioned: "*I'd rather like to have trouble with the Mafia than with the SEC*", one compliance officer was heard. "*Take care that you're on the safe side, because in case of doubt you are the scapegoat*", was a lecturer´s advice concerning the topic "cooperation with authorities". The repressive component of legal social control was much more emphasized than preventive or protecting aspects. Expenses resulting from legal prosecution seemed to be much

8 In the following, text in italics refers to quotations of seminar- participants.

weightier than possible damage by criminal business activities as such. Compliance functions such as informing staff members of marketing issues were discussed in much more detail than functions such as risk assessment or criminal law prevention.

B. Vagueness and Operationalization of Legal Norms

According to my observations, one crucial problem from the point of view of those being in charge of compliance was that the norms, regulations and instructions were said to lack "*concrete application examples and practical references*". "*The dirty work of operationalizing*", as one interview partner had it, or the "*question of implementation*" were considered a core problem of their tasks. As far as exemplary cases were presented, one took them up thankfully and discussed them. In such cases it was most of all about finding out about legal boundaries and about in which situations a legal norm could in which ways be practically implemented. This *operationalization problem* of legal norms can be exemplarily demonstrated by the example of the criminal law on corruption. The bête noire for those present was unclear limit between legal and illegal behavior in this field. Anti-corruption compliance, this is well known, is meanwhile considered an obligatory element of each organizational set of regulations, however due to the "mazy" legal situation it is difficult to implement. This was confirmed during the seminar. All participants estimated the risk of being liable under criminal or civil law to be high, however there was uncertainty when it came to the actual meaning of legal terms and thus also when it came to the actual design of effective compliance tools. For example, there was uncertainty concerning the "*appropriate extent*" of hospitality, the beginning of the "*illegal preference*" of clients, or concerning the question of which people may be invited on which business-relevant occasions. There were different opinions about appropriate ways of control, in particular when it comes to sales staff. There were extensive discussions about the fact that difference between legal cultivation of contacts and criminal corruption is difficult to define, in particular if a company operates within the scopes of different national laws und must take cultural differences concerning the habits of its clients into consideration. Against this background, it was said, the legal norms were damaging to business, in so far as they were said to ruin the trust in clients and business partners. In his branch, one participant stated, it had for decades been an essential element of corporate identity to invite business partners. After all, one had been successful only because one had highly estimated "*interpersonal relations*", and currently the topic was "*completely exaggerated*". Staff members moving "*in the minefields between criminality and social adequacy*", it was said, were increasingly feeling at a loss, and now one even had to "*spy on them*". The fact that furthermore the appropriate trainings or tests for staff members were often at "*kindergarten level*" (*approving laughter among those present*) confirms the overall impression that in this legal field it is difficult to practice any organization-internal operationalization of legal norms and that these norms meet little acceptance. As it is easy to see, the function of law, i. e. coding social situations in such a way as to make them distinctive, is not fulfilled in this field. The problems looked similar in the fields of antitrust law, money laundering legislation and data protection law. One lecturer got at the heart of the problem connected to the operationalization of

the appropriate legal norms when stating: "*One must work out clear rules and guidelines even if there is no explicit legal regulation.*"

C. Role Conflicts and Organization-internal Disregard

Beyond the so far sketched legal norms-related problems of operationalization, the participants in the seminar were also clearly under stress from inner-company role requirements as well as from thus connected conflicts and lack of recognition. Apart from tasks such as training, marketing and risk assessment, the compliance officers are most of all burdened by mediating and control tasks. The question of which tasks should be focus of a compliance officer in the ideal case was discussed by several participants. A consequence of the basically both many and unclear responsibilities of the compliance officer is disrespect at the company. For example, one participant told at his company initially he had been treated as an annoying "*miniature pinscher*" by the board (he had to "*beg*" for resources), as a competitor by colleagues from the legal and internal audit departments, and as a "*bloodhound*" by the staff members. He then had to spent much effort on receiving recognition, by "*canvassing from door to door*". To keep compliance processes out of power struggles and clashes of interests or to prevent competition and rivalry, one lecture recommended: "*Talk to everybody involved, talking is important*"; for: "*to survive in the long run you must not be a lone wolf*". At the same time, he said, the compliance officer had to be careful to stay independent and not to interfere with the operative business. Thus, one had to be involved without being allowed to participate in decision-making, as was the paradox looking advice. There were several lectures and discussions about this topic, the basic clarification of the compliance officer´s possibilities to influence and competences. According to these contributions, a compliance officer seldom meets acceptance. During a lunch break a staff member of an internationally active industrial company told what the management of his company thinks about compliance: "*They [the management] don't care about compliance, they say: `well, write a ten topics paper', they stay among themselves, you won't be allowed there*". Also other participants in the seminar told about lacking recognition at their companies as well as about the difficulties of wanting to advise and support colleagues on the one hand and, being internal controllers, the obligation to keep distance on the other. "*How do you avoid the impression that you secretly report on colleagues?*" was one question which was left unanswered.

These spotlights on the seminar or on the problems told by the compliance officers illustrate that the role of the compliance officer seems to be characterized by difficult tasks, by conflicts and contradicting demands. On the whole, attending this seminar left the impression that the inner-organization implementation of given norms of criminal law by way of compliance is problematic in several respects: It does not reduce complexity (rather it creates new uncertainties), it does not seem to provide those involved with fixed points of orientation, it does not initiate any standardized procedures, and it does hardly support motivation and identification with formal control structures. However, making law valid within an organization requires support by recognized, transparent,

legitimation-providing rules. It seems as if it is still a long way to go until a system of rules which is secured by established knowledge stocks and serves as a basis of the legitimacy of norms of criminal law becomes institutionalized.

IV. CONCLUSION

The starting point for the considerations here was the assumption that usually organizations contribute as co-producers to the making legal norms valid in society, by translating norms into formal organizational structures in the form of "secondary law" or "soft law". Some problems when it comes to implementing such translation, embedding and control processes of legal norms in the case of compliance in the context of commercial criminal law have been exemplarily sketched on the basis of experiences made at training seminar for compliance officers. This way it has become clear that obviously compliance generates inner-organizational structural conflicts, as it ties organizational norms more closely to legal norms, thus blocking the system´s own mechanisms legal norms are usually based on. Among these mechanisms there belong clearly defined roles and competences, implementable procedures and routines, but also the possibility to make, if necessary, trust-based adjustments of the inflexible framework of rules. Usually, efficient formal structures within an organization provide expectation-supporting certainty but also allow for flexibility; they are "informally embedded". In the case of compliance-control, both functions of organizational formality seem to fail: The structure does neither work as a stable point of reference one can rely on if necessary and which standardizes room for manoeuvre nor does it serve as a protective wall or ritual facade behind which one can make informal agreements. Non-transparency and flexibility – necessary preconditions for the functioning of organizational practice – are thus lost. The "costs of the statutory regulation of an organization",[9] the weakening of loyal relationships as well as the prevention of the capability to adjust are increased. If legitimacy is defined as the "generalized readiness to accept as yet undefined decisions within certain tolerance limits",[10] these costs or transparency expectations coming along with compliance in connection with criminal law make it ever more improbable. As a result of this legitimacy loss on the other hand commercial criminal law fails to act as a kind of social control, for it is hardly able any more to stabilize normative expectations. Thus, the intended privatization of commercial criminal law supports an erosion of norms, after all. This means that commercial criminal law as we know it is hardly able to keep its promise to prevent undesired or socially harmful conduct and to control business.

9 Pfeffer 1994, as cited above in footnote 5.

10 NIKLAS LUHMANN, LEGITIMATION DURCH VERFAHREN 28 (3rd Edition1983).