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

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).