A. Initiation of internal investigations

I. When and to what extent should internal investigations be initiated?

1 Internal investigations serve to reveal a company's weaknesses, with the purpose of then rectifying such weaknesses and attempting to avoid any further damage to the company. In detail:

- If employee or management misconduct becomes public, confidence in the company will ultimately decline and its reputation as a whole, as well as that of any of its individual brands will suffer. Internal investigations are aimed at restoring the public, customers and business partners' faith and confidence in the company.
- The company must make it clear not only to third parties, but also to its employees, that it will not tolerate any type of misconduct. By conducting internal investigations, companies are able to implement a "zero tolerance" stance and ensure that misconduct and violations will be exposed and appropriate sanctions imposed.
- The purpose of internal investigations is to reveal a company's weaknesses and to remove them once and for all. In order to prevent employees from violating any laws, an efficient control system should be set in place.

Under French law, misconduct by management and/or an employee can have several serious consequences for both the company and its management. 2

Under French Criminal Law, legal entities are considered criminally liable for the offences committed on their behalf by their representatives.[1] The maximum fine applicable to legal entities is five times the amount of the standard fine set forth in the French Criminal Code. The amount of the standard fine depends on the exact nature of the offence. For instance, in the event a company is found liable of corruption, a maximum fine of 750.000 EUR could be imposed. The company may also be subject to a number of other measures, such as liquidation/winding up, disqualification from taking part in public procurement bids, prohibition to use bank checks, court supervision and publication of the court judgment.

A company may also be found liable in tort (i. e. "*civilement responsable*") for offences committed by its employees. In this case, the employer is generally ordered to pay damages to the victim, however it may even be ordered to pay the applicable fine instead of the convicted employee under the theory that the employee acted during his employment and using the means placed at his/her disposal by the company, the employer is thus liable in tort. The employer is deemed to have breached the obligation of proper supervision of the employee.

If the company has already conducted internal investigations to correct weaknesses, the findings of such investigations may be decisive for the discretionary decision of the Public Authorities as to whether and to what extent it will take measures or initiate an official investigation.

If management is involved in misconduct, its members may be directly subject to criminal sanctions. Company management is personally liable for its own misconduct. Executives may also be found liable for offences committed by company employees – in particular when occupational health and safety rules have been disobeyed within the company. From a more general perspective, based on their supervision obligations, members of management may be liable for the offences committed by employees. Company management must therefore address all indications of possible offences and take all the necessary measures to restore compliance.

Management is responsible for initiating and defining how and to what extent internal investigations are to take place. It is important however, that when management is contemplating an internal investigation, it carefully considers all possible negative factors and or consequences which could result from such an investigation and whether it would ultimately be worthwhile. If an internal investigation is not thorough, it may give the impression that nothing is out of order. As a result, misconduct left uncovered may be reinforced or even continued. Furthermore, if an investigation reveals negative results at a later stage, it may be assumed that management was trying to cover up a transgression and as a result, backfire. Internal investigations may be carried out with respect to individuals as well as individual departments. Additionally, if there is a suspicion of widespread misconduct throughout the company – or even that criminal structures are in place – a more comprehensive internal investigation beyond the scope of individual departments or divisions is recommended. 3

[1] Art. L. 121–2 of the French Criminal Code.

http://www.pbookshop.com

II. Should an internal investigation be of an open or covert nature?

4 If suspicions arise that employees are misappropriating funds and/or giving or taking bribes, a covert internal investigation should be initiated. A covert internal investigation is necessary in order to effectively identify the offenders and possible accomplices, without risking the destruction of evidence. Data protection laws can be a special challenge when it comes to conducting covert investigations, as certain measures within the scope of an investigation are only admissible if the employee concerned is given prior notice.

5 In some cases, however, it can be important for a company to openly communicate that an internal investigation is to take place; in particular by informing employees. An open investigation would for example be necessary when rumors circulate that an internal investigation is being conducted or that the Authorities have begun initial enquiries. A company must always assess whether the advantages of conducting an open investigation outweigh the risk of certain individuals concealing or even destroying evidence.

6 Depending on the information available, investigations may firstly be carried out covertly, then partially and finally completely open.

III. Is it advisable to involve external investigators?

7 The involvement of external investigators basically depends on the company involved, the specific circumstances and the suspected breaches of the law.

8 One advantage in favor of using internal investigators, such as a legal department or an auditing department, as opposed to external investigators, is the cost. Internal personnel are more familiar with the internal operations and activity of the company than external investigators. There are, however, strong arguments in favor of external investigators, such as attorneys and auditors. External personnel often specialize in conducting such investigations and therefore have the necessary expertise and know how to construct a comprehensive solution to ongoing breaches. Very few companies have internal investigators who are equally qualified.

9 Additionally and more importantly, external investigators enjoy special privileges. For example, they have the right to refuse to give evidence (professional secrecy of attorney for example). With limited exceptions, client-related records may not be seized. Furthermore, external investigators are – as a general rule – viewed as more credible than internal investigators. The use of external investigators makes it easier to convince the Authorities that management is genuinely determined to resolve the current situation. With this in mind, company management should preferably select external investigators from firms who have not dealt extensively with the company in the past.

IV. Are foreign attorneys allowed to conduct internal investigations in France?

10 Foreign attorneys may conduct internal investigations in France, provided they do not disclose to third parties any collected information and/or documents "*of an economic, commercial, industrial, financial or technical nature*" which may then constitute evidence in the framework of foreign judicial or administrative proceedings. According to Art. 1bis of the French "Blocking Statute" (i. e. Act dated 26 July 1968, as amended by the Act dated 16 July 1980), "*Subject to treaties or international agreements and the law and regulations in force, any person is prohibited from requesting, seeking or disclosing, in writing, verbally or by any other means, any documents or information of an economic, commercial, industrial, financial or technical nature tending to constitute evidence in view of foreign judicial or administrative proceedings or in the framework of such proceedings*". Therefore, except in investigations based on specific proceedings authorized by international treaties, the possibility for foreign attorneys to take part in internal investigations in France is limited. Their investigations must be conducted in accordance with the limitations of the Blocking Statute, breach of which is criminally punishable. As an illustration, a French attorney acting as correspondent attorney for a US colleague was recently ordered by the French Supreme Court to pay a fine for having requested information from a French company within the framework of judicial proceedings that were ongoing in the United States.[2]

However, apart from the exception established by the Blocking Statute, foreign 11
attorneys may conduct internal investigations within French companies.

V. When should National Authorities be called in?

The earlier the better. Early involvement of National Authorities shows that the 12
company is serious and sincere about remedying misconduct and finding a solution. Involving Public Authorities early can serve as a confidence building tool. This will particularly be the case where the accusations against the company or its employees are of a serious nature and the matter attracts significant public attention. A company should however only call in the Authorities when an internal investigation has already produced specific results. The premature involvement of Public Authorities e.g., when only vague suspicions exist, can be counterproductive and may lead the Authorities to initiate their own criminal investigations.

Official investigations additionally attract great public interest and the company 13
will inevitably have media exposure. There is also a strong possibility that evidence will be destroyed once it is known that Public Authorities are involved.

Additionally, if criminal investigations are opened, the company will no longer 14
have access to the investigation results until it becomes a party to the proceedings; either when charged of an offence or as the victim thereof. As soon as National Authorities are involved, it becomes more difficult to correct bad or even illegal practices within the company.

[2] French Supreme Court (Criminal section), December 12, 2007.

http://www.pbookshop.com

B. Admissibility and implementation of individual measures within the scope of internal investigations

I. What measures are admissible within the scope of internal investigations?

15 In order to investigate French employees, employers must comply with strict labor law, criminal law and data privacy regulations.

1. Employee interviews

16 Employee interviews constitute the key instrument and the starting point of internal investigations.

17 Employee interviews within the scope of internal investigations are permissible in the workplace during working hours and the employee cannot refuse to respond if the employer's request concerns his/her personal work space.

18 The employee can only be interviewed alone if the company knows that no disciplinary sanction will be taken (otherwise the employee may be assisted by an employee representative and the employer must comply with the disciplinary process pursuant to the applicable Internal Regulations).

2. Email and (electronic or physical) file screening

19 Email and file screening, e.g. electronic monitoring of employees' professional emails and files may be carried out to ensure that employees collectively comply with French law and with company policies. Access to an employee's professional emails and (electronic or hard copy) files during an investigation may be performed for evidentiary purposes. Such access is however strictly regulated under French law and monitoring an employee's individual activity or accessing professional emails (i. e., those not marked as private or personal) must be justified by legitimate business reasons.

20 All personal emails are protected in the same manner as private correspondence.

21 French labor and criminal law as well as data privacy regulations and applicable case law strictly protect a person's right to privacy.[3] Secrecy of correspondence is protected *erga omnes* and may be enforced in all situations.

22 In order to investigate an employee's emails and files, two key distinctions must be made:
- distinguish between **personal** and **professional** (or business related) documents and files;
- distinguish between **files** (whether electronic or physical) and **emails.**

23 Failure to observe the above rules may result in:
1. significant fines for breach of the secrecy of correspondence, which is sanctioned by up to one year imprisonment and by a fine of up to 45.000 EUR (a fine of up to 225.000 EUR for a company); and/or

[3] Art. 8 of the European Convention of Human Rights, Art. 9 of the French Civil Code and Art. L. 1121–1 of the French Labor Code.

2. significant fines for breach of data privacy regulations (e.g., unfair collection of personal data is sanctioned by a fine of up to 300.000 EUR and up to five years imprisonment, and a fine of up to 1.500.000 EUR for a company); and/or
3. damages for breach of privacy; and/or
4. any collected evidence being considered inadmissible from a procedural standpoint.

The evidence obtained by the employer through such employee monitoring may 24
be declared unlawful, and consequently may not be used against the employee. Furthermore, the employee concerned could claim for damages if his/her right to privacy has been unlawfully infringed.

a) Conditions governing the access and use of an employee's emails

aa) Prior formalities

(1) Labor Consultation with the works council and Work Health and Safety 25
Committee. Under French labor law, the employer must consult with the Work's Council prior to the implementation of a system of monitoring the employees' activity. If the Information Technology (IT) Policy provides for sanctions in cases of non compliance by the employees of its provisions, the IT Policy must be attached to the company's Internal Regulations in order to be enforceable against the employees. This would in particular require modifying the Internal Regulations and consulting with the Works Council and filing same with the Labor inspector.

(2) Notification with the French data protection authority (the CNIL). The 26
company must duly notify the CNIL of any human resources data processing, in accordance with applicable law. If the company monitors its employees, a specific notification to the CNIL for monitoring purposes must be made with the CNIL.

The French Supreme Court considers that no means of evidence may be used by 27
the employer against employees if the means of control were not previously known by the employees.

Under the above conditions, the employer may access and use evidence employees' 28
professional emails, i. e., not marked as personal.

(3) Prior informing of the employees through the implementation of an IT 29
Policy. The employer must implement an IT Policy in order to comply with the information and transparency principle set forth under both the French Labor Code and the Data Protection Act. This IT Policy must provide that emails and files sent/received or stored on the information system provided by the company are deemed to be for business purposes.

However, in accordance with French case law, it is not possible to prohibit total 30
personal use of computers (as long as such use in reasonable). Employees are required to clearly identify their personal emails and files.

The IT Policy must set out the conditions under which the employer may be 31
entitled to access professional and/or exceptionally personal files and/or emails.

bb) Conditions of access

Generally speaking, access by the employer (or its representatives) to emails 32
identified as "**personal**" (i. e. not for business use) is normally not allowed, unless:

http://www.pbookshop.com

61 (2) If the investigators were able to separate private emails from business-related emails by means of respective filtering, the requirements mentioned under a) apply to the screening of business-related emails. With respect to private emails, provided always that the above referenced privacy requirements are duly in place, only measures related to the outer appearance of the emails, such as the screening of the number, time and data volume, are admissible, and always provided that the above referenced privacy requirements are duly in place. A screening of the traffic data or the content of private emails is only admissible in exceptional cases if it is suspected that individual emails contain indications of material breaches of duties or criminal offences relating to the employment relationship.

c) Handover, review and processing of files, letters and documents of employees

62 *aa)* The employer has unrestricted access to files, letters and documents of its employees that are produced in the course of the work relationship and that are business related. Upon request, the employee must hand them over to the employer. Internal and external investigators commissioned by the employer may inspect, review and process business-related documents of the employees without restriction. The employee who has compiled or maintains the files may not refuse inspection or even destroy the files. The above referenced privacy requirements must in any case be duly complied with (see *supra* paras. 52 *et seqq.*).

63 *bb)* As a general rule, the investigators may not access private files, letters or documents within the scope of internal investigations. The employee must assist in the separation of private files, letters and documents from the documents produced in connection with the duties assigned. If the employee refuses to cooperate, the investigators may inspect the files, letters and documents in order to determine their private or business-related nature. If they are private files, letters and documents, the investigators must immediately discontinue the inspection. The above referenced privacy requirements must in any case be duly complied with (see *supra* paras. 52 *et seqq.*).

64 *cc)* If the business-related or private files, letters or documents contain personal data, the provisions of the Privacy Code (Legislative Decree 196/2003 consolidated) must be complied with. Personal data means information concerning personal or material circumstances of a person and of a legal entity. This includes, for instance, the address, marital status, date of birth, nationality or characteristics of the employee. The investigators require a separate consent for the collection or processing of personal data, unless they are appointed as data processor of the employer. The collection or processing of personal data is deemed justified if it serves to clarify material breaches of duties or criminal offences relating to the employment relationship. Before the investigators may collect personal data from the files, letters or documents, they must inform the employee of the upcoming investigative measure; consent of employees may be required. If external investigators are intended to be allowed to retrieve personal data automatically, the employer must additionally agree on the following with the external investigators in writing:
- reason for and purpose of the retrieval,
- data recipient,

- type of the collected or transferred data,
- technical and organizational protective measures taken.

Please note that the requirements referenced under *supra* paras. 52 *et seqq.* must be complied with.

d) Handover and mirroring of the computer and subsequent processing of the business-related data and electronically stored business-related documents of employees (other than emails)

65 *aa)* The employer or, upon its instruction, private investigators may request from the employee the handover of a company-owned computer used for business purposes and carry out a mirroring, i. e. copy the business data stored on the computer to another storage medium. The investigators may access the company-owned computer and inspect and process business-related data and electronic documents stored on this computer; the requirements referenced under *supra* paras. 52 *et seqq.* must be complied with.

66 *bb)* The inspection of the employee's private data, especially if protected by a password, is inadmissible and constitutes a criminal offence. A password protection means that the individual files or a separate private drive, as applicable, are protected by passwords. If the employees are expressly prohibited from using the company-owned computer for private purposes, the inspection of private files protected by a password can be performed if there is a specific suspicion of a material breach of duties or criminal offence relating to the employment relationship, and the requirements referenced under *supra* paras. 52 *et seqq.* are complied with.

67 *cc)* If the company-owned computer or the individual business-related files or electronically stored documents contain personal data of the employee, the provisions of the Privacy Code must be complied with. The investigators may only collect or process any personal data contained in business-related documents if they inform the employee of the upcoming measure in advance and if the measure serves to clarify breaches of duties or criminal offences relating to the employment relationship; the requirements referenced under *supra* paras. 52 *et seqq.* must be complied with.

e) Inspection of the personnel files of employees

68 *aa)* The personnel files of employees constitute a further source of information for the investigators. They can contain indications of previous breaches of duties on the part of employees. The employees, however, have a special interest that the information contained in the personnel file is not accessed or disclosed because the file may contain personal or intimate information. The employer is therefore obliged to keep the circle of employees who have access to personnel files as small as possible. The more sensitive the data, the larger the access obstacles. In addition to the relevant employees in the company's human resources department or management, employees in the internal auditing department may to a certain extent inspect the personnel files within the scope of internal investigations.

http://www.pbookshop.com

69 *bb)* If the external investigators are subject to a professional confidentiality obligation, they may be granted at least partial access to the personnel files provided that the information in the personnel files is relevant to the investigations in the individual case. The requirements referenced under *supra* paras. 52 *et seqq.* must be complied with. The external investigators may under no circumstances inspect sensitive information, such as existing illnesses or similar information that is of no relevance to the internal investigations.

f) Video surveillance of employees

70 The video surveillance of employees constitutes a considerable interference with the rights of the employees under surveillance and therefore, strict requirements must be met for video surveillance to be admissible. As already mentioned above, the Italian Workers' Charter expressly forbids the employer to install tools with the aim of controlling employees at the distance. Tools able to control the employees from a distance, as the video surveillance, may be installed and used by the employer only if: the employer i) has organizational or productive reasons for its installations or the tools are required for health and safety reasons; and ii) there is the consent of the Works Council. Where no agreement with the Works Council is reached or the company doesn't have a Works Council, an employer with a legitimate aim to use video surveillance may apply to the Labor Office for an authorization determining way and limits of the video surveillance use. Providing that the appropriate authorization on video surveillance has been obtained by the employer and that the employer itself has a prevailing legitimate interest in the video surveillance, internal or external investigators may avail themselves of such instruments and monitor employees by means of video recordings. The requirements vary depending on whether it is an open or a covert video surveillance.

71 *aa)* An open or visible video surveillance is admissible – if the above mentioned authorization has been obtained within the limits provided in the agreement with the Works Council or anyway in accordance with the relevant policy approved by the Works Council or by the Labor Office. Usually, if there is a specific suspicion of a criminal offence or another serious misconduct, video surveillance may be considered legitimate.

72 *bb)* A covert or secret video surveillance is only admissible if there is specific suspicion of a criminal activity or other serious misconduct and the covert surveillance constitutes the only remaining measure and is not disproportionate as a whole. Such surveillance may only be implemented so long as the appropriate procedure (Works' Council consent or approval from the Labour office) is followed. The measure must be temporary and restricted to the area to which the suspicion extends. In any event, the employer's intention to verify whether an employee complies with his/her duties does not constitute a sufficient justification for a covert video surveillance.

For implementation of a video surveillance system, the employer should also take into account the rules set forth by the Privacy Code and the regulation of the Italian Data protection Authority in video surveillance.[13] 73

g) Tapping of telephone conversations

The tapping of the employee's telephone conversations is a glaring interference with the rights of the employee and generally speaking it is not permissible. As for video surveillance, tapping is a mean of controlling employees and therefore is subject to the restrictions provided by the Workers' Charter. In principle, only the monitoring of "outer factors" is admissible, while a monitoring of the content of the conversation is only admissible in exceptional cases. 74

aa) The superficial monitoring of telephone conversations, such as collecting and checking date, time and costs, may be admissible, always provided however that employees have been duly informed and gave their consent when required by privacy requirements. Although this type of tapping sometimes includes the collection of the employee's personal data, this compilation may be justified on grounds of the employment relationship, specifically if the monitoring is implemented for organization, production or health and safety reasons or for detecting illicit conducts of the employees (provided that the employer obtained the Works Council consent or approval from the Labor Office). In case of purely private telephone conversations; telephone numbers may not be stored. Purely private telephone conversations are only such telephone conversations that the employee pays out of his/her own pocket, e.g. on the basis of a special dial-in into the company's telephone system. 75

bb) Whether or not the content of telephone conversations may be monitored depends on the reason for monitoring and on the circumstance that the persons taking part to the conversation are aware of the monitoring. 76

Neither internal nor external investigators may tap private or business-related telephone conversations of employees. Tapping means the monitoring of the content of a telephone conversation without the knowledge of all participants in the conversation. According to the Italian Criminal Code tapping constitutes a criminal offence. Also listening in on a telephone constitutes a criminal offence.[14] The tapping of an employee's telephone conversation can only be performed with a specific order of the competent judicial authority, *i.e* in the context of an investigation made by the police upon instructions of the public prosecutor. 77

h) Search of the workplace

The employer may grant internal and external investigators free access to the Company's premises. However, this does not include permission to inspect the employees' offices. With reference to the protection of the company's properties, the Workers' Charter provides the possibility for the employer to use security 78

[13] The regulation in video surveillance is available in English at the following web address: www.garanteprivacy.it/garante/doc.jsp?ID=1116810.

[14] Art. 617 of the Italian Criminal Code – Knowledge, interruption or illicit impediment of communications or telegraphic or telephone conversations.

http://www.pbookshop.com

Bibliography: *Berni/Livschitz*, Rechtsfolgen mangelhaften Compliance Managements, in: Internationales Handelsrecht III (2009); *Böckli*, Schweizer Aktienrecht, 4th ed. (2009); *Brühwiler*, Kommentar zum Einzelarbeitsvertrag, Art. 319 – 343 OR, 2nd ed. (1996); *Cassani*, Grenzüberschreitende Korruption – Internationale Zuständigkeit der schweizerischen Strafjustiz, in: Ackermann/Wohlers (ed.), Korruption in Staat und Wirtschaft, 2010, p. 17 *et seqq.*; *Daeniker*, Kann eine Publikumsgesellschaft ihre Organe von Verantwortlichkeitsansprüchen schadlos halten?, in: GesKR 3/2009, p. 278 *et seqq.*; *Donatsch* (ed.), Schweizerisches Strafgesetzbuch, 18th ed. (2010); *Egli*, Die Verdachtskündigung nach schweizerischem und deutschem Recht (2000); *Forster*, Die strafrechtliche Verantwortlichkeit des Unternehmens nach Art. 102 StGB (2006); *Geiser*, Die Treuepflicht des Arbeitnehmers und ihre Schranken (1983); *Godenzi*, Private Beweisbeschaffung im Strafprozess, Diss. (2008); *Hauser/Schweri/Hartmann*, Schweizerisches Strafprozessrecht, 6th ed. (2005); *Honsell/Vogt/Wiegand* (eds.), Basler Kommentar – Obligationenrecht I, Art. 1 – 529 OR, 5th ed. (2011); *Livschitz*, Strafrechtliche Risiken für international tätige Schweizer Unternehmen und deren Leitung – Unternehmensstrafbarkeit, Geschäftsherrenhaftung, Geldwäscherei, in: EIZ Vol. 84, (2006), 57 *et seqq.*; *Livschitz*, Liability of Legal Persons for Corruption – a Swiss Perspective, in: OSCE et al., Criminalisation of Corruption, Paris 2007, p. 9 *et seqq.*; *Maurer-Lambrou/Vogt* (eds.), Basler Kommentar – Datenschutzgesetz, 2nd ed. (2006); *Müller*, Whistleblowing – ein Kündigungsgrund?, NZA (2002), 424 *et seqq.*; *Niggli/Wiprächtiger* (eds.), Basler Kommentar – Strafrecht I, Art. 1-110 StGB; Strafrecht II, Art. 111 – 392 StGB, 2nd ed. (2007); *Niggli/Heer/Wiprächtiger* (eds.), Basler Kommentar – Schweizerische Strafprozessordnung. Jugenstrafprozessordnung (2010); *Portmann/Stöckli*, Schweizerisches Arbeitsrecht, 2nd ed. (2007); *Rehbinder*, Schweizerisches Arbeitsrecht, 15th ed. (2002); *Rosenthal/Jöhri*, Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen (2008); *Schmid*, Handbuch des schweizerischen Strafprozessrechts (2009); *Schwenzer*, Schweizerisches Obligationenrecht, Allgemeiner Teil, 5th ed. (2009); *Streiff/von Kaenel*, Arbeitsvertrag, Praxiskommentar zu Art. 319 – 362 OR, 6th ed. (2006); *Swiss Data Protection and Information Commissioner*, Guideline on the Monitoring of Internet and Computers at the Work Place (SDPIC Guideline, available at www.edoeb.admin.ch/dokumentation/00445/00472/00532/index.html, last visited on 11 February 2010); *Wiprächtiger*, Strafbarkeit des Unternehmens, AJP/PJA 2002, 754 *et seqq.*; *Zulauf*, Kooperationen mit dem Ausland: Verrat an der Schweiz?, Festschrift Peter Nobel (2004).

A. Initiation of internal investigations

I. When should internal investigations be initiated and to what extent?

The answer to this question can be split into two parts: the first deals with the duty of either the company or its management or Board of Directors to initiate an internal investigation; the other deals with the extent of such investigation, both in terms of its depth and scope. 1

1. Duties to investigate

Under Swiss law, a number of duties to initiate internal investigations can be identified, either for senior management – or as the case may be – the Board of Directors, and for the company itself. While these duties can not be enforced *in forma specifica*, violation thereof might entail either criminal or civil liability:

a) Duty of senior management to initiate investigations

First, under the concept of Officers' and Directors' Liability in Swiss criminal law, each member of senior management is responsible for preventing criminal conduct within his or her ambit of responsibilities, provided the conduct in question is anticipated as a typical business risk for the company. This entails, besides putting in place and maintaining those compliance structures which are appropriate and necessary to prevent business-related criminal conduct, the relevant manager's duty to intervene against specific criminal conduct which he becomes aware of or at least deems possible based on circumstantial indications.[1] Under the case law of the Swiss Federal Supreme Court,[2] the duty to intervene against specific criminal conduct encompasses the duty to investigate. Once a suspicion or even a reasonable doubt of possible non-compliance with penal laws relating to the company's business arises, senior management must stop the activity in question and investigate relevant facts until sufficient clarity is obtained so as to judge conclusively whether or not there is a violation.[3] A duty to investigate also results from senior management's duty to put in place and maintain sufficient compliance structures;[4] those structures encompass amongst other things, reasonable and appropriate spot checks and audits. If as a result, a suspicion of criminal violations arises, the relevant pattern of facts must be investigated in depth in order to demonstrate within the company that wrongdoing is not tolerated and potential criminal perpetrators will not be left unpunished. In other words, the concept of officers' and directors' liability in criminal law entails the duty to investigate, both in order 2

[1] BSK-*Seelmann*, Art. 11 PC N 51 *et seqq.* with references; see particularly BGE 122 IV 103.
[2] BGE 122 IV 103, consideration VI.2.a.
[3] BGE 122 IV 103 *ibidem*.
[4] (Amongst others) BSK-*Seelmann*, Art. 11 PC N 52 with references; see also Swiss Federal Penal Court, ruling no. SK.2007.21 of 16 May 2008, considerations 5.1.2 and 5.3.3.

http://www.pbookshop.com

to prevent as well as to deter criminal wrongdoing connected with the company's business.[5]

3 Second, the above holds equally true not only for senior management but also for executive Directors (since under Swiss company law, membership in a Board of Directors does not conflict with executive tasks within the company). Non-executive Board members however, do not generally fall under the concept of officers' and directors' criminal liability pursuant to the case law of the Swiss Federal Supreme Court.[6] Nevertheless, in a relatively recent ruling, the Swiss Federal Penal Court held that also non-executive Board members must ensure the existence of all structures and policies appropriate and necessary for the company to be compliant with criminal law relevant to its business.[7] Therefore, non-executive Directors are well advised to ensure, amongst other things, the existence of corporate policies which define along the lines mentioned above, under what circumstances the company has to commence internal audits or spot checks or where necessary, full-fledged investigations.

4 Third, each Board member holds a fiduciary duty towards the company and its shareholders consisting of, amongst other things, a duty to protect the company's assets from damage.[8] Under this fiduciary duty, the Board of Directors is to put in place and maintain appropriate systems of internal controls and risk management. In supervising these systems for proper functioning, the Board has a duty of "enhanced alertness whenever suspicions of misconduct or damaging activities arise".[9] Logically, this means that the Board is well-advised in such cases to investigate the pattern of facts in question in order to gain sufficient clarity and to prevent damage to the company.[10]

Finally, the Swiss Code of Best Practices, a soft law code enacted by the Swiss business federation "Economiesuisse" and an important practical source of guidance when interpreting the Board of Directors' fiduciary duty towards the company – especially in cases of large corporations – not only provides for the Board's duty to put in place and maintain an appropriate system of internal controls and risk management, but also entails the explicit duty of the Board to have an effective compliance function within the company. The Board shall review "proper compliance" within the company at least once a year.[11] Logically, there cannot be any fundamental difference between ensuring "proper compliance" with relevant laws under the corporate fiduciary duty (as interpreted by the Swiss Code

[5] Similar: *Wiprächtiger*, 756; *Livschitz*, Strafrechtliche Risiken, 69. Under the case law of the Swiss Federal Supreme Court, it is conceivable to impose such duty not only on senior management but in addition also on lower-ranking management within the scope and possibilities of their corporate responsabilities and powers, see BGE 6S. 447/2003; 120 IV 300.

[6] BGE 105 IV 172.

[7] Swiss Federal Penal Court, ruling no. SK.2007.21 of 16 May 2008, consideration 5.3.3.

[8] See for instance Art. 717 of the Swiss Code of Obligations relating to share corporations, the most popular corporate form under Swiss law. Similar provisions exist relating to other corporate forms, see *e.g.* articles 538 para. 1, 812 and 902 para. 1 Swiss Code of Obligations.

[9] Swiss Federal Supreme Court decision no. 4C.358/2005 of 12 February 2007, consideration 5.2.1.

[10] Apparently dissenting in the sense that the Board of Directors should refrain from its own investigation and simply involve prosecutorial authorities: SDPIC Guideline, section 9; this opinion is, however, neither based on relevant authority nor does it otherwise reflect a reasonable approach in line with the Board's overall duties under company law.

[11] Swiss Code of Best Practices, ed. 2008, Sections 19 & 20.

of Best Practices) on the one hand, and that of officers' and directors' liability under criminal law on the other. It can thus be referred to what was elaborated upon under the duty to investigate under criminal law.

b) Duty of a company to initiate investigations

Under Swiss corporate criminal liability rules, a company can be held liable for 5
active corrupt practices, money laundering, terrorism financing and furtherance of, or participation in, a criminal organization, provided an organizational flaw within the company was conducive to the criminal conduct in question.[12] The organizational flaw referred to in this rule is nothing but the lack of necessary and appropriate compliance structures within the company in order to prevent the said criminal offences from occurring within the enterprise, provided that those offences form a part of the business risk which a particular company must reasonably anticipate.[13] Similar to the relevant rules under the concept of officers' and directors' liability in criminal law (see *supra* paras. 2 *et seqq.* "Duty of senior management to initiate investigations"), the company will have to investigate internally – as a part of its appropriate compliance system – whenever a suspicion of criminal wrongdoing arises, be it as a consequence of a spot check or internal audit, be it due to a whistleblowing report or any other indication the company may receive. In analogy to the concept of officers' and directors' criminal liability, the company's duty to investigate serves the purpose of both intervening against specific misconduct and deterring others from violating the law by getting the message across that no perpetrator gets away.

It must be pointed out that no relevant case law exists relating to the company's 6
duty to investigate under the rules of corporate criminal liability. However, given that those rules were developed based on the concept of officers and directors' criminal liability in essence by replicating the same principles for the company,[14] it must be assumed that the case law cited above (see *supra* paras. 2 *et seqq.* "Duty of senior management to initiate investigations") with regard to officers' and directors' liability will apply *mutatis mutandis* to the company.

Finally, a duty to investigate may arise from relevant regulation for companies in 7
the regulated financial sector, *i. e.* for banks, insurance companies, stock exchanges, casinos, companies administrating collective investment schemes as well as financial intermediaries outside the banking business which, instead of joining self-regulatory organizations, opted for direct supervision by FINMA (the Swiss financial market regulator). All those companies might be ordered by FINMA to have an internal investigation conducted by an external audit firm ("*Prüfgesellschaft*") appointed and paid by the company.[15] The external audit firm then reports both to the Board of Directors and, in parallel, to FINMA.[16] Furthermore, FINMA may request from any company in the regulated sector any information or data it requires in order to

[12] Art. 102 para. 2 Swiss Penal Code in connection with articles 322ter *et seqq.*, 305bis, 260ter, and 260^{quinquies} Swiss Penal Code, as well as with articles 4a and 23 Swiss Act on Unfair Competition.

[13] BSK-*Niggli/Gfeller*, Art. 102 PC N 246 *et seqq.*; *Livschitz*, Liability of Legal Persons, 18 *et seq.*

[14] For an in-depth analysis of the underlying concept of liability: *Forster*, 74 *et seqq.*

[15] Art. 24 Swiss Financial Market Supervision Act (FINMASA).

[16] Art. 27 para. 1 FINMASA.

http://www.pbookshop.com

meet its duties under the Swiss Federal Act on Financial Market Supervision.[17] Logically, this duty to respond to information requests will entail an internal investigation in the company if the requested information cannot be retrieved otherwise. The companies in the regulated sector must then also spontaneously report to FINMA all occurrences that are of relevance for FINMA's supervision such as significant legal violations, occurrences that would likely require adjustments in the company's risk mapping, etc.[18] A regulated company is well-advised to properly verify and document relevant indications before reporting them to FINMA, which logically results in relevant (albeit initially perhaps limited) internal investigations. Finally, for each regulated industry, more detailed rules relating to their duty to investigate internally may exist under FINMA's regulations, such as under *e.g.* a regulation dated December 8, 2010, on the countering of money laundering and terrorism financing in the banking, securities dealing and collective investment businesses[19] (providing for, amongst others, the duty to investigate and evaluate in detail transactions with increased risk under Articles 14 and 19).

2. Extent of investigations

8 The extent to which a company must conduct an investigation can be defined both by subject matter (depth) and geographically (scope):

a) Depth of investigations

9 In terms of subject matter, it is important to limit the same to what is necessary and appropriate under the circumstances because, as will be shown below at B. "Admissability and implementation of individual measures within the scope of internal investigations", limiting the investigation to the necessary and appropriate is a crucial element allowing the company to justify, as the case may be, intrusions into personality and data protection rights of its staff.

10 Limiting to what is necessary and appropriate varies in changing circumstances: If for instance, the investigation is triggered by a specific suspicion of non-compliant conduct, then the conduct in question should be investigated thoroughly, so as to be in a position to prove the wrongdoing in court; be it *e.g.* in proceedings where the company attempts to recover damages caused by the conduct or, in a labor dispute where the staff in question challenges disciplinary punishment. In these cases, the company will bear the burden of proof for its cause of action or, as the case may be, defense. To this end, the company should not only gather documentary evidence but also talk to potential witnesses about their observations so as to identify who might be offered to the court as a witness in case of litigation, and to be able to better contextualize retrieved documentary evidence, etc.[20] If indications of additional wrongdoing arise during these fact gatherings, such additional wrongdoing should

[17] Art. 29 para. 1 FINMASA.
[18] Art. 29 para. 2 FINMASA.
[19] SR no. 955.033.0.
[20] Such contact with potential witness is permissible for lawyers even in the context of criminal proceedings, provided the witness is not unduly influenced, see e.g. BSK-*Ruckstuhl*, art. 128 PPC N9. It is advisable to such extent to talk to the witness with another lawyer or paralegal present, and to invite the witness in writing or by email to attend the conversation which ideally should take place on the lawyer's premises, see BGE 136 II 551, 555 *et seq.*

be investigated as well based on the duties explained above at 1. "Duties to investigate". If, on the other hand, the company investigates not based on a specific suspicion but rather in order conduct a routine spot check, then the extent of the same is simply driven by the risk management methodology the company applies, etc. In the latter case it is, of course, important to be able to demonstrate that the risk management methodology is a consistent one and thus, spot checks etc. conducted under that methodology are not just arbitrary but rather a necessity in order to adequately manage the company's client-, country- and transaction-related risks.

However, what the company should not do generally and what is not required to 11
be done as a rule under Swiss law, is to fish for non-compliant conduct without any indication and beyond what is necessary under risk management rules within the framework of spot checks or internal audits. The reason being that besides disrupting effects such "fishing expeditions" might have for the business, they will often entail non-justifiable intrusions into legally protected (data) privacy spheres of the company's staff.

How does one avoid "fishing expeditions"? For instance, if non-compliant 12
conduct occurs in a specific place within the company, it does not necessarily mean that the company or even its division in question is under general suspicion of non-compliance. Such general suspicion is in principle contrary to the presumption of innocence that both the company and its staff enjoy under Swiss law. Large-scale screening of data, emails, documents etc. for indications of wrongdoing beyond the specific division in question is then unnecessary and legally not warranted. However, if certain parts of the company are exposed to high risk of a certain type of wrongdoing according to its *bona fide* risk assessment, then it might be defensible for the company to also screen the remainder of the company division or affiliate in question for analogous wrongdoing other than the specific suspected one, as the high risk exposure might per se indicate additional violations. Also, the company might need to engage in broad screening of data and documents throughout a plurality of divisions or countries without any suspicion or indication of non-compliance whatsoever (and hence, in a "fishing expedition") because it is pressured into doing so by a foreign authority. Even though such pressurizing is in conflict with Swiss legal principles, agreeing to the fishing exercise sought by the foreign authority might in some instances be simply the cheapest and least burdensome way out of serious legal risk exposure the company might face in the particular country and thus, the exorbitant investigation will not only ultimately be in the shareholders' interest but it will also likely be warranted by the Board's and managements fiduciary duty.

Further, the subject matter extent of investigations might of course be different if 13
in the regulated sector, the investigation is a result of a FINMA enquiry. In such instance, the subject matter extent is driven in the first place by FINMA's request for information, and might also be extended if indications of additional wrongdoing emerge in the course of the investigation.

Finally, subject matter-wise, the investigation might extend to third party sup- 14
pliers used by the company such as sales agents, distributors and other suppliers of services and goods if a suspicion arises that those third parties, or individuals employed by them, were involved in non-compliant conduct. This is particularly true where the conduct of such third parties may be imputed to the company such

http://www.pbookshop.com