Practical Law™
MULTI-JURISDICTIONAL GUIDE 2013/14
CORPORATE CRIME, FRAUD AND INVESTIGATIONS

Internal investigations in Switzerland: key issues and pitfalls in dealing with employees' criminal conduct, data protection and the use of evidence

Thomas A Frick and Adrian W Kammerer
Niederer Kraft & Frey Ltd

global.practicallaw.com/2-549-4104

TRIGGERS FOR AN INTERNAL INVESTIGATION

Duties to prevent criminal conduct of employees

Although there is no general obligation under Swiss law to report criminal activities to the authorities, the management and the board of directors of a company may have special duties to prevent the criminal conduct of their employees. These special duties can derive from specific legislation (for example, export restrictions) or from the general duty to take care of the company's assets. Members of the management and the board of directors can face civil liability and, in certain cases, even criminal liability if they do not intervene where there is a suspicion of criminal conduct by employees against the interests of the company.

In addition, under Swiss corporate criminal liability rules, if the criminal conduct was furthered by lack of adequate organisation and appropriate compliance within the company, the company itself can also be liable for the following criminal conduct (*Article 102, Swiss Penal Code*):

- Corrupt practices.
- Money laundering.
- Terrorist financing.
- Furthering of, or participation in, a criminal organisation.

Specific circumstances triggering investigations

In general, Swiss enterprises initiate internal investigations where there is a clear suspicion of fraud or other criminal conduct by employees within the enterprise. There are also several particular circumstances which can trigger an internal investigation:

- Companies which are subject to prudential supervision (which is typically the case in the financial sector) must report extraordinary events (including criminal activity) to the supervisory authority. Enterprises failing to report will, as a rule, be reported by their (external) auditor to the competent supervisory authority as required by Swiss law. It is therefore, advisable to act in a fully transparent, co-operative manner and initiate an approach to the regulator if inadequacies are spotted.
- The suspicion of competition (cartel) law infringements. Managers in certain departments can often breach competition rules without the knowledge of management at board level. However, if the company becomes aware of an investigation by the competition authorities, the management can opt for a leniency application to avoid severe fines. Such leniency applications can even be filed during a dawn raid, however, it will only be fully successful if the company is the first cartel participant to file an application. Where there is a suspicion of illegal conduct by company personnel, the management must conduct an internal investigation to determine whether the company should prepare a leniency application.
- Where Swiss regulators have instructed supervised entities to conduct an internal investigation according to certain rules imposed by the regulator. Typically, the regulator asks for a third party, mandated by the supervised company, to conduct the investigation and prepare a report to disclose to the regulator. This has been happening with increasing frequency, in particular in the finance sector.
- Where foreign regulators, parent companies abroad or independent third parties, conduct investigations of their foreign business and disclose the report or at least a summary of the investigation's results to the foreign regulator and the parent instigating the investigations. For example, the programme for non-prosecution agreements or non-target letters for Swiss domiciled banks issued by the US Department of Justice on 29 August 2013 (which requires independent examiners to verify the findings of the banks participating in the programme) was a trigger for a majority of Swiss-domiciled banks to launch internal investigations.
- Merger and acquisition transactions, where, increasingly, the purchaser limits the pre-acquisition due diligence to a red flag due diligence (mainly for cost reasons) and conducts a post-acquisition due diligence of the target company once it has taken over the target company and has full access to its files, electronic data and employees. Such post-acquisition due diligence is usually broader in scope compared to a typical internal investigation but will take the form of an internal investigation in the areas of its key focus.

HOW SHOULD AN INTERNAL INVESTIGATION BE CONDUCTED?

External investigations or employees?

Where voluntary internal investigations are considered, in Switzerland, as in other jurisdictions, the entity decides whether an internal investigation should be conducted by external (and, therefore, independent) investigators or by its employees. The following are the general considerations:

- Employees usually have better knowledge about the typical business processes and incentives within the enterprise.
- External investigators have less of a conflict of interest and can add specialist know-how to the investigation.

Employees' knowledge can, to a certain extent, be gathered through interviews by an external adviser. Employees may not be sufficiently familiar with Swiss regulations which can be triggered by internal investigations such as, in particular:

- Cross-border investigations.
- Blocking statutes in the Swiss Penal Code.
- Data protection issues.

In general therefore, internal investigations in Switzerland are conducted by an external investigator with substantial support from internal personnel.

Structure of the investigation

The project organisation usually includes a project board, staffed by both internal and external personnel, often under the chairmanship of an external person from an audit company or an attorney-at-law (to claim legal privilege if necessary).

Investigations can often involve internal company politics, so it is highly advisable that the project board report to a special steering committee composed of:

- Shareholders.
- Members of the management board.
- Members of the board of directors of the investigated company.

Both for practical and legal reasons, a project mandate should state in writing, the:

- Trigger for the investigation.
- Mandate of the project board.
- Competence and reporting frequency of the project board.

A clear mandate helps the investigation team to demonstrate its authority to investigate, and will be relevant in balancing the interests of the various persons involved during the investigation (for example, in connection with data protection law issues). The ultimate product of the investigation must be defined (usually a report to the steering committee). Depending on the nature of the investigation, there are cases where the report is simply read to the board of directors of the company.

AUTHORISATIONS TO CONDUCT AN INVESTIGATION

Unlike certain other jurisdictions, it is not necessary in Switzerland to have an internal investigation pre-approved by employee representatives or worker's councils, even if the investigation is in respect of employees of the company. It may not be necessary even to provide information to the employee being investigated. In principle, an employer can only process personal data relating to the employee in so far as it is necessary to:

- Implement the contract of employment.
- Determine the employee's fitness for employment.

Any other handling of personal data must be both adequate and necessary to achieve a company goal which prevails over the employee's interests. Whether this test is satisfied will depend on the:

- Severity of the breach (of internal regulations or laws) by the employee.
- Strength of the suspicion against the employee.

If the company's interests in a covert investigation outweigh the employee's interests, a covert investigation is deemed proportionate and the employee does not have to be informed. However, in practice, it is usually beneficial to inform employees about pending investigations since employees are likely to find out or suspect their existence. Employees usually consent to investigations and grant, for example, free access to their e-mails without employers having to balance interests each time. This considerably simplifies investigations.

LIMITATIONS ON DATA COLLECTION

Overview

The main limitation on data collection by a company is the Swiss Data Protection Act which protects individuals and legal entities.

Under the general rules of the act, data can only be obtained lawfully and must be processed in accordance with the principles of good faith and proportionality. The collection of data and the purpose for which the data is used must generally be notified to the person concerned.

However, the processing of data can be justified by:

- The consent of the person concerned.
- Provisions of the law.
- Overriding public or private interests.

Therefore, it is not necessary that an employee is always aware of the collection of data if an employer can claim an overriding private interest in collecting the data.

In a number of cases, Swiss courts have considered specific data collection issues. The following issues (among others) have been decided:

- An employer must not install cameras unless in high security areas or if an employee is not subject to monitoring by the camera all the time (for example, the camera is only pointed at the cash register). The data collected must not be used for general monitoring but only to prevent fraud.
- General monitoring of telephone calls is illegal but specific data, such as the numbers called and the duration of the call, can be collected for general monitoring purposes.
- GPS in company cars is permitted, unless the car is also used for private purposes.

In the case of an internal investigation, the employee is under a duty to participate in the investigation and to support the employer (which does not mean that he has to incriminate himself). In general, employees are willing to participate in, for example, interviews by the employer and it is not necessary (though sometimes suggested by the employee or employer) for employees to have their own legal counsel present during the interviews.

The employment law section of the Swiss code of obligations grants an even more far-reaching protection to employees: an employer can only process data about the employee to the extent that this data concerns his suitability for the employment or if the information is necessary for the performance of the contract of employment. A prior and non-specific consent granted by the employee (for example, in the contract of employment) is not deemed valid under Swiss law.

Limitations on electronic discovery

As in other jurisdictions, a key element of any internal investigation in Switzerland is the review of electronic data, in particular e-mails sent by and received by employees. The Swiss Federal Data Protection and Information Commissioner has issued guidelines on internet and e-mail supervision by employers and regularly updates the guidelines (the latest version, updated September 2013, is not available in the English language).

The general supervision of e-mails or the surfing habits of employees is deemed illegal and disproportionate. However, if there is a suspicion of fraud or abuse of the IT system, investigations can be carried out on specified employees, including a review of the log files, although it is recommended that results

are presented anonymously. If the suspicion of an abuse becomes more specific, the contents of e-mails can also be reviewed. If the employer saves e-mails, business-related e-mails can be reviewed or scanned for search terms. E-mails of a private nature must not, however, be reviewed.

Whether an employer can assume that all e-mails are of a commercial nature depends on the employer's internal regulations on the use and supervision of e-mails during employment. It can be assumed that e-mails are of a commercial nature if the regulations state that:

- E-mails will be saved and may be reviewed by the employer.
- Employees must not use their computers for private correspondence.

However, if an e-mail is clearly of a private nature in spite of such regulations, employers are not entitled to review it. If there is a serious suspicion of criminal action (such as a leakage of company secrets), the employer may have to involve state criminal investigation authorities to access the employee's data. A balancing between the interests of the employer and the employee must be carried out. In summary, it is crucial under Swiss law that Swiss employers have stringent e-mail supervision polices and can demonstrate that employees are aware of and have consented to such polices.

Secrecy provisions

Swiss law traditionally places great emphasis on the protection of personal rights and imposes a variety of secrecy provisions which apply not only to persons but also to legal entities (*see above, Overview*). The most famous and controversial is Swiss banking secrecy under Article 47 of the Swiss Federal Law on Banks and Saving Banks.

There are similar provisions relating, for example, to collective investment schemes and securities traders.

Finally, the Swiss Penal Code prohibits:

- Investigation of manufacturing or business secrets for the purpose of their disclosure to a (*Article 273, Swiss Penal Code*):
  - foreign official agency;
  - foreign organisation; or
  - foreign private enterprise or its agents.
- Disclosure of business secrets by employees (*Article 162, Swiss Penal Code*).
- Economic espionage.

These factors can be relevant when information relating to third parties is disclosed during an internal investigation, for example, information relating to the business partners of an enterprise. In summary, any internal investigation of a Swiss legal entity and in particular, any reporting of the results of such an investigation must, therefore, take into account a variety of Swiss secrecy provisions.

Transfer of data outside of Switzerland

The transfer of data to another country is subject to special provisions of the Swiss Data Protection Act and its implementing ordinance. In general, data can only be transmitted to countries having an adequate data protection level compared to Switzerland. The Federal Data Protection and Information Commissioner provides a list on his website (*www.edoeb.admin.ch/datenschutz/00626/00753/index.html?lang=en*) summarising, on a country-by-country basis, whether or not the respective jurisdiction's data protection regulation is deemed sufficient compared to Swiss standards.

In respect of the transfer of data to a country deemed to have insufficient data protection regulation in place, the foreign entity must either:

- Receive certification (for example, in the US, the US-Swiss safe-harbour certificate from the Department of Commerce).
- Enter into an agreement guaranteeing compliance with Swiss data protection principles (the Federal Data Protection Officer provides a sample agreement on his website).

In addition, provisions against economic espionage under the Penal Code must be observed, in particular, if information relating to third parties is transmitted.

USE OF EVIDENCE IN SWISS PROCEEDINGS

The results and findings of an internal investigation must be of a nature that they can be used in court proceedings if the enterprise decides, for example, to file a:

- Claim for damages against an employee.
- Criminal complaint.
- Claim for damages from a seller following an M&A transaction.

In general, Swiss law has a surprisingly relaxed attitude towards evidence collected illegally. There is no general "fruit of the poisonous tree" doctrine under Swiss law, that is, evidence collected legally can usually be used regardless of whether it was obtained with the help of evidence collected illegally.

In criminal proceedings, courts are willing to consider evidence even if the evidence was collected in breach of labour or data protection laws provided:

- The evidence could have been collected in a legal way.
- In balancing interests (severity of the criminal act and circumstances of how the evidence was collected), the court finds that the evidence should be considered.

In civil cases, evidence collected illegally is only taken into consideration if the "interest in finding the truth prevails". Under this principle, for example, an insurance company can photograph persons claiming disability engaged in activity and such evidence can be used in court to block claims against the insurance company.

GATHERING OF EVIDENCE IN CONNECTION WITH FOREIGN PROCEEDINGS

Data collected in connection with foreign court or administrative proceedings and the transfer of such data abroad may be a breach of the Penal Code, unless authorised by the Federal Government.

Gathering evidence which will be introduced in foreign proceedings on Swiss territory (irrespective of whether such proceedings are at the time of the collection of the data pending or will be initiated subsequently) is prohibited (*Article 271, Penal Code*). Only evidence that is under the direct control of the party interested in the foreign proceedings can be collected and disclosed. If evidence is collected from third parties, the collection will be illegal and the foreign authority must follow the traditional channels of judicial or administrative assistance proceedings. For this reason, it is often the case that for example, interviews of employees to be subsequently used in foreign proceedings such as in US pre-trial discovery, are conducted outside Switzerland, for example on German territory.

Under certain circumstances, as mentioned above, other regulations apply, such as Swiss Banking, Data Protection and Labour laws.

OBLIGATIONS TO NOTIFY AND PUBLISH INFORMATION

The findings and results of an internal investigation can trigger information obligations:

- If the employer is listed on a Swiss stock exchange, ad hoc publicity obligations must be observed.
- In cases of fraud or other criminal activities involving the transfer of funds, notification obligations under the Swiss Anti-Money Laundering Act and the corresponding clauses of the Penal Code may be triggered.
- Although, as mentioned above, there is no general obligation to report criminal conduct, a company prudentially supervised must notify its supervisory authority of any breaches of its internal regulations or law generally. This notification will usually only be made once the company determines the exact scope of the breach to avoid further complications in its relationship with the regulator. If the company is party to co-operation agreements or a lender under credit facility agreements with financial institutions, the findings of the investigation may trigger contractual notification obligations.
- Although there is no general obligation to notify employees about the investigation or its results, under the Swiss Data Protection Act employees have the right to demand disclosure of the data collected by their employer during the investigation (*see above, Limitations on data collection*).

CONCLUSIONS: KEY LEGAL CONSTRAINTS IN SWITZERLAND

Internal investigations are increasingly acknowledged as a tool for establishing facts both for the management of Swiss enterprises and Swiss and foreign regulators. However, in respect of information transmitted outside Switzerland, the enterprise conducting an internal investigation as well as third parties mandated by it, must act within the strict limits of Swiss legal constraints:

- **Data protection.** Swiss data protection law applies to both individuals and to legal entities. Therefore, an investigation must consider both the legality of the data processing in relation to individuals (such as employees) and to the legal entity. Transfer of data abroad (including data accessible from abroad), and in particular to non-EU member states, may be subject to severe restrictions.
- **E-mail policy is crucial.** It may depend on the wording of the e-mail policy of the enterprise whether the investigation can access the emails of employees which are not clearly of a business-related nature.
- **Strict secrecy provisions.** There are various secrecy provisions under Swiss law in addition to the well-known banking secrecy. Many provisions are of a penal nature, such as provisions against economic espionage or criminal law provisions in the Swiss Federal Act on Collective Investment Funds.
- **No legal privilege for in-house counsel.** When setting up the structure of the internal investigation, the fact that communication with in-house counsel is not subject to legal privilege must be taken into consideration. If there is a possibility that the investigation produces results of a delicate nature, it may be advisable to mandate an external law firm to conduct the investigation.
- **Data gathering in foreign proceedings.** The gathering of data (including conducting pre-trial interviews) on Swiss territory in connection with, or for the purpose of, foreign court or administrative proceedings can be a criminal act under Swiss law.

INVOLVEMENT OF THIRD PARTIES

Typically, an enterprise will involve independent third parties in an internal investigation, for example, employees of its auditing firm or an external attorney to benefit from Swiss attorney-client privilege and obtain an "independence stamp" from regulators. In Switzerland, corporate (in-house) counsel does not enjoy professional privilege. Therefore, whenever it seems advantageous for an investigation or its results to be privileged under Swiss law, it must be conducted by, or under the instruction of, external counsel. The same is true in connection with the "independence stamp" which may require the investigated entity to evidence the absence of a conflict of interests by the investigating personnel and increased transparency.

The mandating of a third party for an internal investigation is generally permitted under the Swiss Data Protection Act (*see above, Limitations on data collection*). The third party mandated (for example, an IT company engaged to screen e-mails or a forensic service company) must process the data in the same way as the mandating entity is entitled to. However, the employer mandating a third party must continue to exercise control over the data and instruct and supervise the third party. Additional provisions apply if the data is transmitted abroad, for example if the forensic company is located outside Switzerland or the information is transmitted to a server abroad (*see below*).

Practical Law Contributor profiles

Thomas A Frick, Partner

Niederer Kraft & Frey Ltd
T +41 58 800 8000
F +41 58 800 8080
E thomas.frick@nkf.ch
W www.nkf.ch

Professional qualifications. London School of Economics, London, LL.M. EU law (merits), 1994; University of Zurich, PhD (Dr. iur.), 1992; Georgetown University, Washington DC, 1992; Admitted to the Bar (Rechtsanwalt), 1992; Law Studies at Zurich University and at Heidelberg University, Germany, Master of Law (lic. iur.), 1991. Partner at Niederer Kraft & Frey Ltd. since 2001

Areas of practice. Specialises in counselling Swiss and foreign banks and other financial institutions in all kinds of legal and regulatory issues, with a particular focus on customer contracts, inter-bank contracts, syndicated finance, regulatory issues and investigations. Advises on competition law issues.

Languages. German, English, French

Professional associations/memberships

- Swiss Bar Association.
- Zurich Bar Association.
- Institute for Industrial Property Law.
- Europe Institute of Zurich.
- Swiss Association of Competition Law.
- Business Angels Switzerland.

Recent Publications

- *Financial Markets Criminal Law/Finanzmarktstrafrecht, by Peter C Honegger, Thomas A Frick, Presentation for the LL.M. in International Banking and Finance Law 2013/2014 University of Zürich.*
- *Anti-Money Laundering in Switzerland, by Adrian W Kammerer, Thomas A Frickin: Anti-Money Laundering in 20 jurisdictions worldwide 2013, published by Getting the Deal Through.*
- *Corporate Fraud & the Forensic Accountant, by Adrian W Kammerer, Thomas A Frick, in: Acquisition International, February 2013.*
- *Swiss parliament supports the Swiss asset management and fund industry in face of major regulatory changes, by Thomas A Frick, Sandro Abegglen, Marco Häusermann, in: Global Asset Management & Servicing Review 2013/14.*
- *Swiss asset management & fund industry facing major regulatory changes, by Thomas A Frick, Sandro Abegglen, Marco Häusermann, in: Global Asset Management & Servicing Review 2012/13.*

Adrian W Kammerer, Partner

Niederer Kraft & Frey Ltd
T +41 58 800 8000
F +41 58 800 8080
E adrian.kammerer@nkf.ch
W www.nkf.ch

Professional qualifications. Executive Master in Mediation, University of Liechtenstein, 2006; International Diploma in Anti-Money Laundering, International Compliance Association, UK 2005; Admitted to the Bar (Rechtsanwalt), 1999; University of Zurich, PhD (Dr. iur.), 1997; University of Zurich, Master of Law (lic. iur.), 1991. Partner at Niederer Kraft & Frey Ltd. since 2006.

Areas of practice. Advises companies in the areas of contract, company and commercial law; M&A transactions; litigation. Expert in compliance matters; supervisory-law proceedings; prevention of money laundering; white collar crime and investigations. Advising in aviation and employment law.

Languages. German, English, French

Professional associations/memberships

- Swiss Bar Association.
- Zurich Bar Association.
- International Compliance Association.
- FICA Certified Professional (*www.int-comp.org/fellowship-fica*).

Publications

- *Anti-Money Laundering in Switzerland, by Adrian W Kammerer, Thomas A Frick in: Anti-Money Laundering in 20 jurisdictions worldwide 2013, published by Getting the Deal Through (7 Pages).*
- *Corporate Fraud & the Forensic Accountant, by Adrian W Kammerer, Thomas A Frick, in: Acquisition International, February 2013 (1 page).*
- *Anti-Money Laundering in Switzerland, by Adrian W Kammerer, Thomas A Frick in: Anti-Money Laundering in 20 jurisdictions worldwide 2012, published by Getting the Deal Through (9 Pages).*
- *Summary Overview on Certain Swiss Employment Law Aspects, by Adrian W Kammerer, Michaela Zehnder, Allegra Sosso in: Expert Guide - Labour & Employment Law, April 2012.*
- *Employment Law Overview, by Adrian W. Kammerer, Michaela Zehnder, Allegra Sosso, in: Corporate INTL - Employment Law Online Guide Inclusion, 2012 (1 Page).*