Austria

Wolf Theiss Bettina Knoetzl

1. INTRODUCTION

This chapter focuses on a concise overview of the legal situation in Austria when planning or conducting internal investigations targeting presumed fraudulent behaviour on the part of a company's employees.

When investigating suspicions of internal fraud, employers are faced with an ever-changing multiplicity of legal provisions ranging from questions of civil (substantive and procedural) and contractual law to questions of basic and human rights, European Union legislation as well as criminal law.

A legal evaluation of investigative measures is highly dependent on the individual facts of the case. With technical advancements in information technology (that also allow for controlling its users) being incorporated into business processes at an ever-faster pace and with Supreme Court decisions regarding *ad hoc* control measures being scarce, future court decisions on this matter cannot – if at all – be predicted easily.

Actually, under Austrian law, the available options are largely dependent on existing company-wide policies, eg regarding private use of office infrastructure and permanent control measures, agreement with works councils, the employees' previous and individual consent to certain control measures, and provisions of the individual employment contracts.

Therefore, assessing the legal situation is, in most cases, a highly complex task requiring specialised knowledge in this specific legal field. It is advisable to obtain local expert advice for each individual case and even more – as a precautionary measure – to design a control regime that will not only allow for the potentially necessary *ad hoc* control measures to be taken but one that may even prevent internal fraud in the first place. In this context, the *Verbandsverantwortlichkeitsgesetz* (the Act on Companies' Criminal Liability, in force since 2006) should be considered as well. If a company fails to implement necessary precautionary measures, this may lead to criminal liability for the company itself, even if its management was not aware of the employee's misconduct.

In order to provide a practical view, this chapter's emphasis lies, aside from a general overview of the legal provisions concerning fraud and asset tracing, on the steps that may simplify and expedite internal investigations, as well as on potential measures to be taken at an early stage, ie when employees enter into their employment contracts.

Many internal investigations will stem from suspicions of fraudulent and/or corrupt behaviour. Section 6 takes a closer look at anti-bribery and/or anti-corruption considerations that might arise from the fraudulent activity being investigated. Since the second edition of this book (2011),

Austria's anti-bribery and/or anti-corruption legislation has been amended significantly. First of all, the anti-bribery provisions have been severely strengthened, expanding the scope of illicit activities and also increasing the criminal penalties. The Centralized Prosecution for White-Collar Crime and Corruption (*Zentrale Staatsanwaltschaft zur Verfolgung von Wirtschaftsstrafsachen und Korruption*) is now in charge of enforcing the anti-bribery laws as well as any white-collar crime suspicions – in most cases – if the damage exceeds EUR 5 million. Furthermore, a national whistleblowing online platform and a leniency programme for whistleblowers and/or key witnesses have been implemented. Austria is striving hard to fight corruption in an effective way. In particular, if business is conducted with the involvement of government officials/the public sector, suspicions of white-collar crime and/or corruption may quickly come under the spotlight of public and/or official interest. The media, which is playing an increasingly important role in revealing white-collar criminal cases, recognises itself as a public watchdog. Avoiding or mitigating the impact of negative publicity is an important positive side-effect of efficiently carried out internal investigations.

In a nutshell, the swift successful completion of its own internal investigations is of the utmost importance to companies which are subject to or suspected of fraudulent behaviour.

The author gratefully acknowledges the highly appreciated assistance of Philip Marsch, senior associate at Wolf Theiss.

2. MANAGING THE INTERNAL INVESTIGATION

The internal monitoring of employees is a sensitive subject. Not only must one take into account Austria's fragmented employment laws, EU legislation, statutes regarding data protection, and criminal provisions – applicable provisions also may be found in collective bargaining agreements, agreements between an employer and the works council, individual employment contracts, special provisions and general civil law provisions.

Therefore, professional consultation is highly advisable not only when a concrete suspicion of internal fraud exists with regard to certain employees, but also in advance as a precautionary measure. Designing and implementing appropriate and permissible systematic control measures, disciplinary codes and/or policies regarding the private use of office infrastructure helps to detect internal fraud at an earlier stage. Also, it legally facilitates *ad hoc* control measures (eg checking the contents of emails).

The following provides a brief overview of the general legal questions that arise in managing an internal investigation and obtaining the traditional forms of evidence (ie hard copy and electronic documents, oral statements from suspects or potential witnesses).

(a) *Ad hoc* control – systematic control measures

Austrian employment law differentiates between:

- (permanent) systematic or general control measures; and
- individual *ad hoc* controls or investigations conducted upon a concrete suspicion.

The introduction of systematic or general control measures, as well as technical systems designed to exercise control over employees, requires an agreement between the employer and the works council if such control measures or systems affect the employees' human dignity. In organisations without a works council, the employer needs to obtain the individual consent of those employees exposed to the respective control measure or system. Ideally, the employment contract itself should already contain the relevant provisions.

Individual *ad hoc* control measures upon a concrete suspicion of, for example, internal fraud do not require an agreement between the employer and the works council or the consent of those employees exposed, as they are not considered systematic or general control measures. Special (internal) procedural rules may apply if a disciplinary code is in effect within the company involved. A company may issue a disciplinary code upon reaching an agreement with the works council.

(b) Timeframe

Upon a concrete suspicion of internal fraud, the employer is required to clarify the situation within an adequate timeframe and, if need be, give the employee an opportunity to clarify the situation. Also, if an internal investigation reveals any proof of fraudulent behaviour on the part of certain employees, there is only a narrow window of (legal) opportunity to announce an immediate termination of the employment contract without notice (see the following section (c) for the different consequences resulting from specific types of termination of an employment contract).

If the employer does not act upon a concrete suspicion within an adequate timeframe or fails to announce the immediate termination without notice within an adequate timeframe, such employer may only terminate the employment contract with notice.

An immediate termination without notice has to be announced without delay after the employer has been made aware of the fact (not a mere suspicion) that the employee has created an important reason for immediate termination without notice. 'Without delay' allows adequate time, for example, to take into account economic considerations or obtain legal advice, depending on the complexity of the issue. The acceptable timeframe defined by Austrian case law ranges from less than one day to longer periods of time (in some cases, awaiting the outcome of criminal or administrative proceedings has been considered adequate). To avoid any such risk, employers are urged to consult with their legal counsel in order to define the maximum time period available for a termination without notice

A delayed immediate termination without notice without an important reason given on the part of the employee will still terminate the employment contract, but the employer will be liable for the employee's loss of income and loss of termination payments (in such a case, the calculation basis is a fictitious termination with notice on the same date).

The question of compensation for damages has to be considered independent of the termination of the employment contract. Most civil claims (eg compensation for damages) are subject to a statute of limitations of three years after notice of the damage and knowledge of the tortfeasor (calculated from the point in time at which the causal link between the damage and the wrongful behaviour of the tortfeasor became obvious to the damaged party).

(c) Termination of employment contract

After obtaining proof of fraud in the course of an internal investigation, the question of terminating an employment contract(s) frequently arises.

Austrian employment law requires the employer to act upon a suspicion of internal fraud because the options available to terminate employment contract(s) depend on how fast the employer took action. Under Austrian employment law, an employment contract may be terminated, in particular, by either:

- immediate termination without notice;
- termination with notice observing the applicable notice period; or
- mutual dissolution at any time.

Regarding the timeframe for an immediate termination without notice, see section (b) above. If the rather short timeframe cannot be met, only a mutual agreement between the parties to dissolve the employment contract or a unilateral termination is possible, where each party to it may terminate the employment contract by adhering to the applicable notice period. In both cases, neither the employee nor the employer is required to cite a reason for termination. Upon termination with notice, employees may be eligible for compensation for any unused annual leave, *pro rata* annual bonus payments, payments owed under a retirement plan, compensation for adhering to a restrictive covenant, etc (in addition, employees hired before 1 January 2003 may be eligible for severance payments). A mutual dissolution will only take place if the parties agree upon an amicable settlement of the outstanding claims.

In contrast, immediate termination without notice needs to be justified by an important reason (*gewichtiger Grund*). However, the employer is not obliged to inform the employee involved of the concrete reason for such immediate termination without notice when announcing a termination of the employment contract; it suffices to refer to an 'important reason' and save the information for a later surprise effect in potential subsequent proceedings (in civil proceedings before the labour court regarding the justifiability of immediate termination without notice, the burden of proof falls on the employer).

The Austrian Salaried Employees Act (*Angestelltengesetz*) specifically defines an important reason with regard to the topic at hand as disloyal conduct within the realm of the employer-employee relationship, one's acceptance of the receipt of unjustified benefits (commissions) from third parties without the employer's knowledge or consent, or any kind of conduct that shows the employee to be unworthy of the employer's trust.

Whether a specific kind of behaviour can be qualified as an important reason is always a question of fact in each individual case; generally, executive employees are subject to a higher standard than non-executive personnel. Furthermore, certain groups of employees enjoy special protection against termination (eg members of the works council, employees on maternity/paternity leave, apprentices, handicapped employees).

(d) Costs of the internal investigation

The employer may claim compensation for the costs of individual *ad hoc* controls from the employee if the investigation proves that the employee has indeed acted against the interests of the employer and the employee's prior actions had caused a concrete suspicion.

Employees acting against the employer's interests without raising any concrete suspicion are not liable for the costs of individual *ad hoc* controls if they are only revealed accidentally in the course of an internal investigation focused on other employees.

(e) Exclusionary rules

The Austrian Civil Procedure Code (*Zivilprozessordnung*) does not stipulate any exclusionary rules regarding evidence. The Austrian Supreme Court has not yet decided whether evidence obtained illegally may be used in any case or whether a civil court must decide whether to exclude the evidence after considering and weighing the legally protected interests of the opposing parties. Thus, even evidence that has been obtained in a way that exposes the company or the investigators to civil, administrative or criminal liability may still be used in subsequent civil proceedings against the subjects of an investigation.

The Austrian Code of Criminal Procedure's (*Strafprozessordnung*) exclusionary rules regarding evidence (eg the exclusion of evidence obtained by use of torture) are not applicable to private investigations. If evidence is obtained illegally, it will still be admissible in criminal proceedings – though it might also incriminate those conducting the private investigation.

2.1 Hard copy documents

The employer may monitor or investigate all work-related hard copy documents in the course of an individual *ad hoc* control measure upon a concrete suspicion of internal fraud, preferably in the presence of the employee and another witness. *Ad hoc* control measures upon a concrete suspicion do not require any form of agreement between the employer and works council or the consent of those exposed, as they are not considered systematic or general control measures. Special (internal) procedural rules may apply if a disciplinary code is in effect within the company. A company may issue a disciplinary code upon reaching an agreement with the works council.

Private letters or any such documents (eg personal notes, diaries) that are kept enclosed or that are locked (eg in an employee's desk) are protected by criminal law (privacy of communication). Any person not being the sender or the dedicated receiver who gains or tries to gain access to such letters or

documents is committing a criminal offence. Also, it is considered a criminal offence to suppress private letters or any such documents.

To be on the safe side, all hard copy documents that are kept enclosed or locked within any kind of container and that are obviously of a private nature or are declared private by the employee (eg judging from the file name) should not be opened.

Breaches of privacy of communication will not be prosecuted by the public prosecutor; the person injured by such criminal offence will have to pursue private criminal action (see section 3.4 for more information on private criminal action).

2.2 Electronic documents

The employer may control and/or monitor employees' electronic documents, internet usage and email traffic within the boundaries of collective and individual labour law, criminal law and data protection legislation. Individual *ad hoc* control measures upon a concrete suspicion allow for measures stronger than (permanent) systematic control measures (for information on the distinction between systematic control measures and *ad hoc* controls see section 2(a) above).

(a) *Ad hoc* control measures

Other than the introduction of (permanent) systematic control measures, individual *ad hoc* control measures upon a concrete suspicion of internal fraud do not require any form of agreement between the employer and the works council or the consent of those exposed. Special (internal) procedural rules may apply if a disciplinary code is in effect within the company. A company may issue a disciplinary code upon reaching an agreement with the works council.

The employer may access work-related electronic documents and emails in the course of an *ad hoc* control upon a concrete suspicion, but it is unclear to what extent employees' private electronic documents and private emails stored on an employer's computer system are protected by criminal law (there is no Supreme Court precedent on this issue).

The Austrian Penal Code (*Strafgesetzbuch*) protects the privacy of correspondence; some scholars argue that encrypted or password-protected private emails are protected by criminal law. Thus, any person (other than the sender or the dedicated receiver) who accesses or tries to access such communication may be committing a criminal offence.

To be on the safe side, emails and electronic documents that obviously are of a private nature (eg judging from the file name) should not be accessed.

(b) Company policies and procedures

A company's policies and procedures on monitoring software, electronic documents, email traffic, internet log-files, etc are considered systematic or general control measures. Any (technical) system that allows for the monitoring of employees' actions is considered a systematic or general control measure irrespective of the employer's intent or its actual use. Other

than individual ad hoc controls upon a concrete suspicion, the introduction of (permanent) systematic or general control measures, as well as technical systems designed to exercise control over employees, requires an agreement between the employer and the works council if these control measures or systems affect the employees' human dignity. In organisations without a works council, the employer needs to obtain the individual consent of those employees exposed to such control measure or system. Ideally, such consent should be contained already in the employment contract.

Employees enjoy certain personal and basic rights within the realm of their employment contracts, which are the standards upon which human dignity is defined. A control measure that does not (in itself) obviously affect human dignity has to be judged by comparing and weighing the employer's legally protected interests and the employees' personal and basic rights. Thus, it depends on the individual facts of the case as to whether a control measure affects human dignity or not. Examples of control measures that require an agreement between the employer and the works council before the introduction of such measures are: telephone systems that allow monitoring and/or the storage of individualised log-files of telephone conversations, video surveillance systems and entry controls.

A (permanent) systematic or general control measure that monitors software, internet usage and email traffic and that thereby generates and stores individual-related data is also subject to the Data Protection Act (*Datenschutzgesetz*), which describes a basic right to secrecy regarding individual-related data, particularly with respect to data regarding private and family life. Special protection is guaranteed for sensitive data, ie individual-related data concerning racial and ethnic backgrounds, political views, union membership status, religious or philosophical views, health and sex life. Log-files documenting private use of the internet and emails are considered sensitive data.

Organisations that allow private use of the internet and email accounts (as well as organisations without a specific policy on this issue) may only collect and store internet and email log-files after obtaining the express consent of the employees being monitored. In addition to the agreement between the employer and the works council regarding the systematic or general control measure, the individual consent of each employee has to be obtained on the basis of the Data Protection Act. The agreement between the employer and the works council cannot serve as a substitute for obtaining the consent of such individual employee.

In organisations in which private use of the internet and email is expressly prohibited, the employer may trust that only work-related data (and not private data) may be subject to control measures. In such case, the employer does not need to obtain the employee's consent regarding the processing of individual-related (sensitive) personal data.

Note also that employees may withdraw their consent regarding the use of sensitive data at any time. Consequently, it is highly recommended that employers link their policies, and in particular the permission to use internet

and email accounts privately, to the employees' consent regarding the use of sensitive data.

A prohibition against private use of the internet and email is therefore a proper means available to employers to carry out the necessary investigations.

2.3 Obtaining oral evidence from employees

Employees' duty of good faith and their fiduciary duty towards the employer include the duty to report facts which might be detrimental to the company including fraudulent actions by other employees. Failure to inform the employer of such may entitle the employer to immediately terminate the employment contract without notice (see above section 2(c)).

Thus, obtaining oral evidence of work-related facts from employees in the course of an internal investigation is covered by the employment contract. Special (internal) procedural rules may apply if a disciplinary code is in effect within the company. A company may issue a disciplinary code upon reaching an agreement with the works council.

The employer may interview or question employees regarding the fraudulent behaviour of other employees without providing advanced notice of the topic of the meeting or, for example, advanced notice of the documents that will be discussed. Generally, the employee has no right to legal representation at such meeting and no right to be accompanied by a colleague or a member of the works council. Nevertheless, the employee may discuss the case and his position with (his or her) outside legal counsel; such consultation does not breach the obligation of confidentiality. The investigating employer also may 'inform' employees that a failure to report the fraudulent behaviour of co-workers may lead to an immediate termination of their employment contract without notice (see above section 2(c)).

Although active information on fraudulent behaviour is part of the employees' fiduciary duty, spying on fellow employees is not covered by the employees' fiduciary duty. The employer may interview employees about the behaviour of other employees, but may not request or instruct employees to spy on particular individuals or on one another.

The implementation of a whistleblowing hotline is considered an introduction of a systematic control measure that affects human dignity. It therefore requires an agreement between the employer and the works council or the individual consent of each employee if there is no works council. Also, a disciplinary code requiring employees to report misconduct within companies needs to be agreed upon between the employer and the works council.

Furthermore, the implementation of a whistleblowing hotline is, like many other measures touching human dignity, subject to the Data Protection Act (*Datenschutzgesetz*) and, as such, subject to registration in the Data Processing Register (*Datenverarbeitungsregister*). A whistleblowing hotline may not be introduced before the successful completion of an inspection by the Data Protection Commission (*Datenschutzkommission*).

2.4 Legal privilege

On the one hand, parties to legal proceedings enjoy only a limited privilege in Austrian proceedings. On the other hand, the duty to disclose documents is, generally, extremely narrowly defined (see section 3.2). Whereas the legal representative's duty of confidentiality is protected in both civil and criminal proceedings, the parties themselves must take into account the fact that documents and/or facts discovered in the course of an internal investigation might have to be disclosed in subsequent proceedings if the (narrowly set) rules applicable to disclosure apply (see sections 3.1 *et seq*). However, a party might choose to release its counsel from the duty of confidentiality. In such case, counsel may no longer refer to or rely on such a duty when requested to make disclosures.

The Austrian Civil Procedure Code does not provide for (pre-trial) discovery proceedings, but there are tools to request the disclosure of documents by the opposing party or by non-parties. If the rules for the disclosure of documents apply, the court will order the opposing party or non-party to produce the requested evidence. If documents are in the custody of a person's legal counsel, the court will still order the person to disclose the documents rather than its legal counsel. Parties' legal counsel are simply not considered an opposing party or non-party, but rather persons within the sphere of influence of either the party or non-party.

In criminal proceedings, the counsel for the defence does enjoy legal professional privilege – but this is limited to any new evidence in its custody. The bottom line is that the legal professional privilege in criminal proceedings is limited to evidence documenting the attorney-client relationship.

Also, the function of documents to serve as evidence in legal proceedings is protected by criminal law. A person loses the power of disposal over any means of evidence that may potentially be subject to disclosure in foreseeable civil, criminal or administrative proceedings. It is a criminal offence to (intentionally) withhold any such evidence.

3. DISCLOSURE FROM THIRD PARTIES

General overview

In Austria, taking evidence is considered a sovereign act performed by the court, which means that the court will hear evidence (generally) upon the parties' requests in the course of a trial, which is determined by the principle of oral presentation. As a result, the Austrian Civil Procedure Code (*Zivilprozessordnung*) does not provide for pre-trial discovery proceedings. Pre-trial discovery proceedings may only be performed by an Austrian court via judicial assistance. In these proceedings of judicial assistance, the Austrian Civil Procedure Code is to be applied unless the requesting court asks for the application of its local procedural law and these provisions are not in violation of the *ordre public*.

In Austrian civil proceedings, it is each party's responsibility to produce the evidence necessary to support its case. There are only a few circumstances in which the opposing party or third parties may be obliged

to disclose evidence upon one party's request. Since a request for third party disclosure of documents or a request for the disclosure of documents by the opposing party is to be stated during the main proceedings, it will always come to the immediate attention of the opposing party.

In many cases involving internal fraud, the wrongdoer also may have committed criminal offences and be subject to criminal prosecution. Criminal proceedings can be utilised to obtain documents in the opponent's or third parties' possession. These documents can be used as evidence in subsequent civil proceedings. The Austrian Criminal Procedure Act (*Strafprozessordnung*) was recently amended to empower victims of criminal offences in criminal actions (see section 3.4).

Disclosure of documents from the opposing party

The Austrian Civil Procedure Code (*Zivilprozessordnung*) specifies the conditions under which the opposing party may be obliged to disclose documents. Documents are subject to disclosure if:

- the opposing party itself referred to the document in the course of the proceedings;
- the opponent is obliged to hand the document over by substantive law; or
- the document is qualified as a 'joint deed' (*gemeinschaftliche Urkunde*) between the parties.

'Joint deeds' are documents created in the interest of the party requesting disclosure, documents that contain information regarding reciprocal rights and obligations between the parties, or any documents that are in fact written negotiations between the parties.

Other than in pre-trial discovery proceedings, the party requesting disclosure has to clearly specify the evidence, ie the document (requests to produce 'all relevant' documents are not permissible). If the above criteria are met, the court will then order the opposing party to produce the requested documents. The disclosing party is not eligible for any reimbursement of costs.

However, a court order for the opposing party to produce documents is non-enforceable. Failure to comply with the order is sanctioned inasmuch as the court will have to take this behaviour into account in its evaluation of the entire case.

The opposing party may justifiably refuse the disclosure of documents if the evidence concerns matters of family life, the disclosure violates an obligation of honour, the evidence renders the party subject to criminal prosecution, the evidence is privileged or other reasons of the same importance exist.

Disclosure of documents from third parties

Because it is each party's responsibility to produce the evidence necessary to support its case, there are only very few circumstances under which a non-party may be obliged to produce evidence in civil proceedings. A request for third party disclosure of documents is to be stated during the main proceedings; thus, it will always come to the immediate attention of the opposing party.

In civil proceedings, third or non-parties may only be obliged to disclose documents that are in their custody if the non-party is obligated to hand the document over to the party requesting disclosure by substantive law or the document is qualified as a joint deed (see section 3.2) between the non-party and the party requesting disclosure.

The evidence must be clearly specified by the party requesting disclosure and the court may even hear from the non-party on the question of the disclosure obligation. The court may then order the non-party to produce the specified documents with an executable court order. If the non-party fails to produce the specified documents, the court may exercise coercive means. The non-party is eligible for the reimbursement of costs by the party requesting disclosure (eventually, legal costs follow the event, ie the losing party pays the other party's costs).

Disclosure of documents through criminal action

In many cases of internal fraud, the wrongdoer may also have committed criminal offences and be subject to criminal prosecution. The Austrian Penal Code (*Strafgesetzbuch*) describes certain criminal offences often committed in cases of internal fraud that make the suspect subject to public prosecution (eg fraud, disloyalty, misappropriation, theft, active and passive bribery, misuse of subsidies, illegal arrangements in submissions, money laundering, etc).

It is the legislature's goal to empower those injured by criminal offences and to give them the necessary procedural tools to effectively participate in criminal proceedings. Also, criminal proceedings are now taking an ever broader view of the interests of those injured by a criminal offence by considering, securing and – as far as possible – settling their civil claims against the offender (see section 4.2).

The public prosecutor may (upon authorisation by the criminal court) order house searches and the securing or seizure of objects (including letters and other documents) that might serve as evidence or secure civil claims, the monitoring of a suspect's communication, etc. Any person injured by a criminal offence is entitled to access to files and to make use of such evidence in subsequent civil proceedings. However, for purposes of a criminal investigation in its early (pre-trial) stage, access to files may often be subject to certain restrictions.

In any criminal proceeding, those injured by the criminal offence have the following procedural rights, namely the right to:

- legal representation;
- access files (may be subject to restriction);
- be kept informed actively about the course of the proceedings;
- access translation services free of charge (may be subject to restriction);
- participate in certain steps of the pre-trial proceedings; and

- participate in the main trial proceedings, to direct questions to the accused, witnesses and expert witnesses, and to be heard regarding civil claims.

Any legal entity or natural person injured by a criminal offence may also join criminal actions as a party on the prosecutor's side. In addition to the above rights, this entitles the injured person, among other things, to formally request that certain evidence be collected.

Certain criminal offences do not result in public prosecution. In these cases, the injured legal entity or natural person may pursue a private criminal action in which the private prosecutor effectively takes the place of the public prosecutor (eg breach of industry or business secrets, breach of intellectual property rights, certain acts of unfair competition).

In any case, criminal actions allow the injured person to make use of the state's *imperium* and gain access to documents and information that would not be accessible through civil proceedings. The downside is that criminal actions might pose a risk in terms of public relations.

Any person that is subject to criminal proceedings (be they on the basis of private criminal actions or public prosecution) must be informed of the ongoing criminal proceedings, as well as of the suspicion against him or her as soon as possible; only if it is vital for the purposes of the criminal investigation that the suspect does not have any knowledge of the ongoing criminal proceedings (eg in order to successfully obtain evidence) may the suspect be left uninformed for the necessary time.

4. STEPS TO PRESERVE ASSETS/DOCUMENTS

Preserving documents

(a) Preserving documents for litigation

Although there is no general rule that requires employers to retain and preserve all (internal) documents, nevertheless the function of documents to serve as evidence in legal proceedings is generally protected by criminal law. (Please note that special rules may apply in terms of administrative law or special statutory requirements, eg accounting documents, annual statements, documents regarding clinical drug studies, etc). In fact, a person loses the power of disposal over any means of evidence that may potentially be subject to disclosure in foreseeable civil, criminal or administrative proceedings. It is a criminal offence to (intentionally) withhold any such evidence. Consequently, serious thought should be given to introducing a data deletion and document shredding policy.

(b) No pre-trial discovery proceedings in Austria

There are no pre-trial discovery proceedings available in Austrian civil proceedings. It is considered each party's responsibility to produce the evidence necessary to support their case. A party may – in the course of the proceedings – request that the court order the opposing party or non-party to disclose documents if certain criteria are met (see sections 3.1 *et seq*).

An Austrian civil court may only perform pre-trial discovery proceedings via judicial assistance. Generally, the court will apply the Austrian Civil Procedure Code in cases involving judicial assistance. If certain procedural

tools unknown to Austrian procedural law are available in the legal system of the requesting court, the Austrian court may apply these if the foreign court specifically requests that its local procedural law is to be applied to the proceedings. In cases involving judicial assistance, foreign procedural rules may be applied as long as there is no violation of the *ordre public*.

If the wrongdoer has committed a criminal offence in his or her fraudulent actions, the initiation of criminal proceedings is a powerful option to gain access and to preserve documents from the suspect as well as third parties. The victims of a criminal offence can influence criminal proceedings by joining the proceedings as a party on the prosecutor's side. The evidence gathered by the authorities in the course of criminal proceedings can be utilised in subsequent civil proceedings by the persons injured by the criminal offence (see section 3.4).

Preserving assets

Just like in other legal systems, it takes time to reach an enforceable decision from a civil court in Austria. Average civil proceedings with a value in dispute surpassing EUR 15,000 will take approximately 15 months until the court of first instance renders its decision. Due to relatively low court fees proceedings often reach the next (two) instances.

Civil law as well as criminal procedural law recognises that most claimants' primary interest – namely to receive financial compensation for damages – is put at risk by lengthy proceedings. If the defendant has enough time to cloud his or her financial situation and to make objects or any other kind of asset effectively inaccessible, an enforceable court decision serves very little purpose.

The Austrian Code of Enforcement (*Exekutionsordnung*) provides a tool for preliminarily securing assets (preliminary injunction, *Einstweilige Verfügung*) in order to prevent the enforcement of a future court decision from being considerably more difficult or even impossible. Parties may request injunctive relief while the proceedings are in progress or before filing a claim.

Upon the party's request, the court may issue injunctive relief for securing monetary claims, most importantly in cases of the 'subjective endangerment' of the requesting party. Subjective endangerment exists when the opposing and potentially liable party has made it obvious that it will make it difficult for the other party to realise any enforceable court order, eg by threatening to move abroad or relocate assets abroad. Merely denying a claim's validity does not constitute subjective endangerment. The court may take the following measures when issuing injunctive relief in order to secure monetary claims:

- movable objects (and money): judicial custody or administration/management; order to refrain from giving away, selling or pawning movable objects;
- immovable objects: judicial administration/management; order to refrain from giving away, selling, hypothecating or registering any encumbrances in the land registry; or
- receivables: issue of garnishment order.

If the wrongdoer has also committed a criminal offence through his or her fraudulent behaviour, the initiation of criminal actions is also a powerful tool to secure potential civil claims resulting from the criminal offence. The new Code of Criminal Procedure (*Strafprozessordnung*) effective starting 1 January 2008 was also aimed at empowering those injured by criminal offences in their efforts to obtain compensation for damages.

The public prosecutor may order the temporary securing (*Sicherstellung*) of objects and/or any kind of assets for the sole purpose of securing the civil claims of the persons injured by a criminal offence. Such securing of assets is accomplished by establishing direct custody or by ordering the suspect to refrain from giving away, selling or pawning objects and/or any other kind of asset. Upon the request of the public prosecutor, the court may order the seizure of (secured) objects and/or assets. The victims of a criminal offence may influence criminal proceedings by joining the proceedings as a party on the prosecutor's side (see section 3.4).

5. CIVIL PROCEEDINGS

Remedies against the fraudulent employee

Regarding (intentional) fraudulent actions, the employer may sue the (former) employee for compensation for damages on the basis of breach of contract, criminal offence and breach of protective law. The recoverable damages comprise compensation for damages, lost profits, as well as a claim for unjust enrichment for the general advantages derived from the fraudulent behaviour; punitive damages will not be awarded by Austrian courts.

Most civil claims are subject to a statute of limitations of three years after notice of the damage and knowledge of the tortfeasor (calculated from the point in time at which the causal link between the damage and the wrongful behaviour of the tortfeasor became obvious to the damaged party).

The Employees' Liability Act (*Dienstnehmerhaftpflichtgesetz*) contains differing provisions regarding non-intentional or negligent actions causing damages, allowing the court to reduce an employee's liability according to one's degree of negligence and seniority.

Remedies against third parties

Third parties (non-employees) who knowingly collaborate with internal wrongdoers are basically subject to the same legal remedies as employees. Both the employee who commits the fraudulent act and the third party are subject to joint liability, ie the employer need not claim proportional compensation for damages from its (former) employee and the third party, but rather may choose to claim compensation for 100 per cent of the damages from either party.

6. ANTI-BRIBERY/ANTI-CORRUPTION LEGISLATION

Many internal investigations will stem from suspicions of fraudulent and/or corrupt behaviour. Since the second edition of this book (2011), Austria's anti-bribery and anti-corruption legislation has been amended significantly. In an attempt to address criticism raised on international levels, Austria's government introduced a so-called *Transparenzpaket* (transparency package), which included a strengthening of the anti-bribery laws and their enforcement provisions. The following overview is focused on the risk factors of criminal prosecution against a legal entity that is not an individual, eg a company.

EU legislation and international treaties had and continue to have a profound effect on Austria's anti-bribery and anti-corruption legislation. As in most western countries, the following acts are crimes in Austria:

- general offences: fraud, embezzlement, debtor/bankruptcy offences, organising Ponzi schemes, money laundering, accounting fraud, etc;
- corruption offences: bribery in the public and private sectors (demanding, accepting a promise of, accepting, promising, offering and giving bribes); any 'benefit(s)' granted to officials or employees of public or private enterprises may be problematic, as it is not a requirement that there be a direct link between the benefit and a specific (unlawful) act; and
- special offences: agreements to restrict competition in tender proceedings, anti-trust offences, organised illicit labour, withholding social security contributions, misuse of subsidies, etc.

In any internal investigation, the Act on Companies' Criminal Liability (*Verbandsverantwortlichkeitsgesetz*) has to be considered: a legal person, eg a company, is held criminally liable if its management or employees have committed a criminal offence (i) to the company's benefit or (ii) in breach of the company's public and/or private obligations/duties (eg employee safety regulations). The company is directly responsible for members of its management. With regard to lower ranking employees, the company will be held criminally liable if no sufficient and reasonable organisational/personnel measures were in place to prevent such criminal behaviour.

The Act on Companies' Criminal Liability specifies penalties for legal entities ranging up to EUR 1.8 m. A conviction will also leave the legal entity with a criminal record.

If the prosecution authority has already started a criminal investigation, the company may avoid a criminal record, in particular by: (i) full cooperation with the authorities; (ii) restoration of/compensation for the damages caused by the criminal conduct; and (iii) amending or introducing organisational and personnel measures to prevent similar criminal conduct in the future. The prosecution may then cease the criminal proceedings or merely impose a fine that will leave the company's criminal record "clean".

If the company should learn about likely criminal conduct before criminal prosecution proceedings have been initiated by the prosecution authority, the company will have to carefully weigh its options, including civil and criminal consequences (with legal counsel). One important aspect is timing: with respect to certain kinds of offence, the Austrian Act on Criminal Procedure allows for a leniency programme with regard to offenders volunteering new and vital information to the prosecution; this provision may be applied to natural as well as other legal persons. The focus lies on

new information: whoever volunteers the information first has a chance to enjoy immunity. Thus a potential conflict of interest can arise between the company and managers/employees who are subject of the internal investigation.

It should be noted that offenders may also report their offences in an anonymous way and still retain the benefits of the leniency programme. The Department of Justice has introduced an internet-based whistleblower communication tool that allows for offenders (and mere witnesses) to notify and communicate with the authorities.

Any victim of anti-bribery and/or anti-corruption offences may join the criminal proceedings at the stage of the criminal investigation (or during the main trial) as an injured party. Such status allows that party to gain access to the criminal files and also to push the criminal proceedings in a certain direction, to a certain extent, by requesting that certain evidence be taken, by examining witnesses and exercising certain rights which only victims have. The public prosecution authority assigns the status of a 'victim' to a party. In most cases, a company which is subject to a white-collar crime is well advised to aim at gaining victim status by playing – ideally rather early on – an active, supportive role in the criminal investigation. Choosing the right strategy is, of course, dependent on having all the relevant information available. This highlights once again the importance of successfully conducted, swift internal investigations.