Whistleblower Policies in Turkey: The Employment, Criminal Law, and Data Protection Perspectives

1 Jul 2015

Whistleblowing poses considerable risks for employers: as well as dealing with any corruption-related issues that they may pose, they need to be careful in the way in which they interact with the whistleblower or any employees whose conduct has been reported by the whistleblower.

Turkey has not yet enacted any specific whistleblowing regulation. Employers must, therefore, consider the general provisions and obligations imposed by the relevant legislation when dealing with whistleblowing. This legislation includes employment, criminal and data protection law.

This article outlines the main considerations for employers when establishing and implementing whistleblower policies. It considers the following:

- The existing Turkish whistleblower legal framework.
- Overview of whistleblowing procedure.
- Criminal law aspects of whistleblowing.
- Employment law aspects.
- Data protection aspects.

Turkish whistleblowing law and practice should also be considered against the perspective of international whistleblower regimes, and the models of certain other national whistleblowing regimes (*see below*, *International whistleblower regimes* and *National whistleblower regimes*).

Turkish whistleblower legal framework

No specific whistleblower legislation yet exists in Turkey. The OECD recently criticised Turkey's lack of specific whisleblower legislation (*Phase 3 Report on Implementing the OECD Anti-Bribery Convention in Turkey*), as whistleblowing is, in the experience of countries which applies successful whistleblower protection models, among the main sources for revealing corruption.

Turkey is a party to international instruments and entered into obligations concerning the fight against wrongdoing. These include:

- OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions 1997.
- UN Convention against Transnational Organized Crime 2000.
- UN Convention against Corruption 2003.
- Council of Europe Civil and Criminal Law Conventions on Corruption.

See below, *International whistleblower regimes*.

After ratification of these international legal instruments, Turkey starting adopting national legislation that would satisfy its obligations under these instruments. Therefore, the obligations under international instruments have to a large extent become part of local law through national legislation.

In the absence of a specific framework, general legislative provisions and principles apply to employers investigating corruption allegations, reporting them, and related employment and data protection issues. Unfortunately, however, without a coherent and centralised approach, Turkish whistleblower requirements for employers may seem insufficient and confusing.

Overview: dealing with whistleblowing reports

Employers must be diligent in avoiding any unintended legal consequences and ensuring that the decisions on the whistleblowing are informed decisions with reasonable foresight of the legal consequences. This requires a full picture before taking any action, and means that employers must show due care in investigating the issue that is being reported, and due care in gathering evidence, because of concerns over confidentiality. Only after the process is concluded can an employer take action.

There are two dimensions to whistleblowing: internal and external reporting.

Internal reporting

This concerns reporting made to the relevant bodies within the company. On receiving an internal report, it is prudent for employers to conduct a solid and thorough internal investigation to reach conclusions which could have criminal law, employment law and data protection law ramifications. Employers should gather and keep evidence during the internal investigation process, since this is crucial in investigating the conduct in question. It is also vital to determine whether only the reported employee or employees are involved in the wrongdoing.

From the employer's perspective, the purpose of the investigation should be to examine the reported conduct and to identify all employees involved in that conduct. Employers should also give weight to recording information which shows a solid and fair investigation process was followed, as well as substantive information about the alleged inappropriate activities. Only after this has been done will it be possible to decide:

- What course of action should be followed towards the reporting, reported employees and any other employees involved (that is, what employment law consequences should follow) (*see below, Employment law considerations*).
- Whether it is necessary to make an external report (where the conduct is of a criminal nature) (*see below, External reporting*).

Employers should avoid any retaliation or maltreatment (or the perception of maltreatment) against the reported or reporting employee while the investigation is ongoing. For this reason, among others, it is vital to keep the investigation strictly confidential and only inform persons on a need-to-know basis, depending on their duties and tasks in the company. Employers should wait until an internal decision has been reached about the legitimacy or good faith of the reporting before taking any positive or negative actions towards the reported and/or reporting employee. If an employer acts inappropriately, it may be subject to adverse employment law or civil law consequences.

The investigation will need to consider whether there are criminal law, employment or data protection considerations (*see below*).

External reporting

This concerns reporting made to the relevant governmental authorities. It is a legal obligation under the Penal Code to report information and evidence of ongoing criminal activity, or a commissioned crime, to the Public Prosecutor's Office. Failure to report may lead to personal criminal liability (*see below, Criminal law considerations*).

Many international companies, and also a growing number of local companies, require their employees or a larger circle of third parties to comply with internal reporting requirements and to acknowledge wrongdoing in the course of their activities with the company (*see above, Internal reporting*). In most cases, this will not involve criminal activity, but it is vital for the compliance officers and company management to investigate the wrongdoing and assess whether it must be reported to a governmental authority.

Criminal law considerations

Failure to report

Statutory provisions for failure to report. Penal Code 5327 requires all people who have knowledge of criminal offences which are in progress or have been completed (if it is possible to limit the offence's consequences) to report these offences to the Public Prosecutor's Office, with personal criminal liability for failures to report (*Article 278, Penal Code*) (*see above,Overview: dealing with whistleblower reports: external reporting*). Failure to report an offence is punishable by imprisonment of up to one year. Offences must be reported to the Public Prosecutor's Office (*Article 158, Code of Criminal Procedures No. 5271*). If a crime is committed abroad, it should be reported to the Turkish ambassador or consulate in the country where the crime was committed. Reports made to public institutions concerning crimes committed during performance of a public service must be transmitted to the Public Prosecutor's Office without delay. Procedural proceedings in the investigation phase must be kept confidential, except as required by the Criminal Procedure Code, and provided the right of defence is protected (*Article 157, Criminal Procedure Code*).

The Penal Code does not discuss liability for legal entities failing to report a corruption offence. However, an individual employed by an entity that acknowledges that a criminal offence has been committed or commissioned (including members of the board of directors, managers, and all other employees with such knowledge) must report corruption or face criminal liability under the Penal Code for failure to report.

Although there are no legislative requirements with regard to the level of suspicion which must exist before reporting a criminal offence to the Public Prosecutor's Office, it would be prudent to report externally any conduct which goes beyond a reasonable suspicion. The Penal Code provides that any person who slanders another person by raising a criminal complaint or notifying authorised bodies to enable commencement of an investigation and prosecution against this person, despite knowing his or her innocence, is punished with imprisonment (*Article 267, Penal Code*). Therefore, the evidence gathered should be carefully evaluated before reporting a crime, to prevent the risk of facing slander charges while trying to comply with the reporting obligation under Article 278 of the Turkish Penal Code. Under this provision of the law, it can be argued that the reporting obligation could be deemed to have ceased if the wrongdoing is reported, and subsequent reports would have a higher possibility of leading to slander charges.

Best practice for employers. Employers must ensure that the channel for external reporting for employees is left open at all times. The internal compliance policies and/or internal investigation processes must clearly respect the duty of external reporting for those who have been exposed to the information on wrongdoing, if that wrongdoing involves any criminal elements.

In practice, there have been examples of internal compliance policies or internal investigations in which employees are prohibited from discussing any details regarding the matter, without the employer's prior authorisation. Internationally, there is increasing attention given to introducing bars to external reporting: on 1 April 2015, for example, the SEC fined a public company US$30,000 for requiring employees involved in internal investigations to sign a confidentiality agreement that the Commission deemed violated the whistleblower protections contained in the Dodd-Frank Act. Therefore, it would be prudent for the employers in Turkey to respect the duty of external reporting, as acting otherwise has both criminal law and employment law consequences.

Destroying or concealing evidence

The Penal Code makes it a criminal offence to destroy, delete, hide, or obliterate criminal evidence with the intention of concealing the truth (Article 281, Penal Code). Committing such a crime is subject to imprisonment of between six months and five years. If a person provides an opportunity to another person to save that person from investigation, arrest, or sentence, they can also face imprisonment of between six months and five years (Article 283, Penal Code).

Employment law considerations

Whistleblowing by employees raises significant employment considerations and risks for employers. Employers should be careful when dealing with an employee alleging wrongdoing by the employer or another employee, and aware of the legislative rights and expectations which employees have. Being fully aware of the mechanisms and rights which protect employees will allow employers to avoid breaching these within a whistleblowing context, and reduce the risk of later being accused of inappropriately handling a whistleblowing situation.

Considerations while the internal investigation is ongoing

General. The Labour Law imposes a duty of loyalty on employees. Employers should first investigate a reporting on a wrongdoing before deciding on whether:

- The reporting itself is a breach of duty of loyalty (that is, a bad faith reporting about a fellow employee).
- The reported employee has breached his duty of loyalty (that is, the conduct that was reported is actually a wrongdoing).

Therefore, employers must be diligent before acting towards the reporting and/or reported employee in any way, either positively or negatively. Having a well-designed internal investigation and evaluation procedure will support employers from later having to defend themselves against claims of maltreatment after an employee has reported a wrongdoing. A code of ethics or conduct enforced on a world-wide scale by international companies, in many cases, will not comply with local law requirements for such an investigation.

While the internal investigation is ongoing, employers should avoid committing, in any circumstances, retaliation or maltreatment (or the perception of retaliation or maltreatment) towards the employee. The Labour Law No. 4857 (*Labour Law*) contains no specific provisions or guidance for circumstances where an employee reports suspected corruption by a co-worker, or how employers should act in those circumstances to prevent actual or perceived retaliation. However, general provisions apply to employers regarding their duty to protect employees from facing wrongdoing and unequal treatment.

Protection against termination. The Labour Law specifically prohibits employers from terminating an employment agreement on the basis that the employee has filed a complaint, or participated in proceedings against the employer (that is, external reporting) seeking fulfilment of obligations or rights arising from law or the employment agreement (*Article 18(c), Labour Law*). If the employer does so, it runs the risk of being forced to defend a re-employment lawsuit, initiated by the terminated employee. The employee can initiate the lawsuit within one month of being notified that the employee's employment agreement is being terminated.

The lawsuit can be based either on a claim that the employer terminated the employment agreement without valid reason, or did not identify a reason for the termination. The burden of proof is on the employer to prove that the termination was based on a valid ground. However, this evidentiary onus shifts to the employee if he or she claims the termination was based on a reason that is different from the one presented by the employer. Re-employment lawsuits are only possible where the terminated employee has worked for more than six months with the employer and the employer has more than 30 employees (*Article 18, Labour Law*). However, under the Supreme Court's settled practice, for Turkish-resident subsidiaries of multinational companies this number is calculated by considering not only the number of employees hired by the Turkish-resident subsidiary, but the total number of employees of the multinational group globally (*Supreme Court 9th Chamber Decision No: E. 2008/32408 K. 2010/1126 dated 25.01.2010*). Therefore, even where a Turkish branch or subsidiary of a multinational company employs fewer than

30 employees, the terminated employee can claim his or her re-employment based on the fact that the total number of employees globally is above 30.

Protection against abuse and discrimination in the workplace. Employers must consider the Turkish Code of Obligations No. 6098 (Code of Obligations), which provides general protection for employees against physiological and physical abuse in the workplace which includes also retaliation (*Article 417, Code of Obligations*). If any employee has his or her personal rights violated due to the employer's non-compliance with the Code of Obligations, the employer is liable to pay compensation to the employee.

Employees are legislatively protected from discrimination by the Turkish Constitution under the equality principle (*Article 10*) and under the Labour Law (*Article 5*). Employers should be aware of those protections and make best efforts to avoid any discriminatory or degrading treatment towards an employee on or after filing a complaint.

The Labour Law outlines penalties for violations of its prohibition on employee discrimination. If an employer violates this principle, the employee is entitled to demand compensation of up to four months' salary, as well as claim for any other amounts which the employee has been deprived of.

Considerations after the internal investigation is completed

Approach to the reported employee. Under the Labour Law, employers can:

- Terminate an employment agreement immediately with a valid reason.
- Terminate an employment agreement with notice where certain justified grounds exist.

The possible actions against the employee may differ depending on the results of an internal investigation:

- The results demonstrate strong evidence of a crime. The employer has the option to terminate employment agreements with just cause, where the employee (*Labour Law*):
    - commits a dishonest act against the employer, such as a breach of trust (*Article 25/II (e)*);
    - commits an offence on the premises of the employer which is punishable by seven days' or more imprisonment without probation (*Article 25/II (f)*).

When terminating with just cause, the employer can terminate the employment agreement with immediate effect and is not obliged to pay a severance payment or serve the employee a notice of termination.

The right to terminate the employment agreement with just cause must be used within six working days as of the date of finding out about that behaviour. The beginning date of this period might be among the disputed matters in a possible re-employment lawsuit.

If the evidence gathered against the employee is strong, the employer must also file a criminal complaint. Furthermore, employers can bring a civil action for compensation against the employee on the basis of damage caused to the employer's reputation.

- **The results do not demonstrate strong evidence of a crime**. Where the employer cannot obtain strong evidence against the suspected employees at the end of the internal investigation, but there is reasonable suspicion that irregularities occurred which would lead to an impairment of trust, termination with valid reason may be an option.Even if there is not sufficient evidence that a crime is committed by the employees, it may still be possible for the employer to terminate the employment agreement with valid reason under Articles 17 and 18 of the Labour Code, an option which should be assessed on the merits of each specific case. If a termination option is applicable, employers must take written defences from the employees before the termination with valid reason. When this pre-condition is satisfied, an employer can initiate disciplinary action against the employee for not complying with the employment terms and disciplinary rules and proceedings adopted by the employer before termination.When terminating with valid reason, the employers must make the severance payment and serve the employee with a notice of termination. A terminated

employee can challenge the existence of a valid reason by initiating a re-employment lawsuit. In this case, the burden of proof is on the employer and the employer must demonstrate the existence of the valid reason.If the employer cannot obtain strong evidence against the suspected employees at the end of the internal investigation, making a criminal complaint would not be advisable, as presenting a complaint without evidence may lead to slandering charges against the employer (see above, Criminal law considerations in Turkey: Failure to report: Statutory provisions for failure to report).

Wrongly accusing an employee of corruption. If an employer wrongly accuses an employee of corruption, the employee has the right to terminate the employment agreement.

If the employer does any of the following, the employee can terminate the employment contract, without waiting for the end of the contract period (if the contract is for a fixed term) (Article 24, Labour Law):

- Speaks in a way that dishonours the virtue and integrity of the employee or one of his or her family members.
- Provokes or threatens the employee or one of his or her family members or encourages or provokes that person to commit illegal acts.
- Commits a crime against the employee or his or her family members which is punishable by imprisonment.
- Makes inaccurate accusations about the employee causing indignity to the employee.

If an employee has his or her personal rights infringed by a wrongful accusation, the employee can initiate legal proceedings against the employer, seeking moral and material compensation. If a wrongfully accused employee has the employment agreement terminated on the basis of immoral, dishonourable, or malicious conduct (*Article 25, Labour Law*), the terminated employee could initiate a lawsuit against the employer seeking both compensation and re-employment.

Whistleblowing complaints made in bad faith. An employer may legitimately terminate an employment agreement if it is determined that the reporting employee made a whistleblowing complaint in bad faith. Bad faith in this context exists where a reporting was groundless and made in order to harm the employer's reputation, cause difficulties for the reported co-worker, or for some other personal interest.

The Labour Law outlines the just causes and valid reasons for rightful termination in detail. These circumstances include where an employee is found guilty of any speech or action constituting an offence against the employer's honour or dignity, or makes groundless accusations against the employer in matters affecting the employer's honour or dignity (*Article 25(II) , Labour Law*). Accordingly, employers can argue that an unfounded reporting by an employee constitutes immoral, dishonourable, or malicious conduct within the scope of the Labour Law.

Further, the Labour Law imposes a duty of loyalty on employees. An employee's illegitimate reporting of corruption could conceivably violate these principles of good-faith and integrity if the employee externally discloses the employer's professional or trade secrets. This would arguably constitute valid grounds for the employer to terminate the employment agreement (*Article 25, Labour Law*). Therefore, when investigating alleged corruption and considering options against an employee, employers should give careful consideration to the level and nature of information the reporting employee has disclosed externally.

Data protection considerations

The information which a whistleblower uses to support his or her corruption allegation may raise issues with regard to data protection requirements and the right to use that information. Employers are required by legislation to store and deal with personal data in specific ways.

An employee reporting alleged corruption by a co-worker may attempt to use the co-worker's personal data to support the allegations, which itself may have been obtained by violating data privacy rights (for example, e-mail exchanges or personal conversations). Using that personal data without the knowledge of the person which the data relates to could conflict with the employer's obligation to protect personal information. Accordingly, an employer that

uses, keeps, or acts on such data should consider its rights and obligations carefully.

Legislative framework for data protection in Turkey

There is no specific data protection legislation in Turkey. Data protection rights and obligations for both employers and employees are found in the following legislation.

Turkish Constitution. The Turkish Constitution establishes grounds for protection of personal data by giving everyone the right to require the protection of that data. The constitutional rights include requesting information on personal data held, accessing the data, correcting and erasing data, as well as knowing whether personal data is being used in accordance with the purpose it was gathered for. The Turkish Constitution prohibits personal data being processed unless this is explicitly permitted by law, or consent is obtained from the related person (*Article 20, Turkish Constitution*).

Turkish Civil Code No. 4721 (*Civil Code*). Under the Civil Code, any violation of personal rights is considered unlawful unless justified by private or public interest, or undertaken by a lawfully empowered authority, or with consent from the related person (*Article 24, Civil Code*). An individual who has his or her personal rights unlawfully violated is entitled to request protection from a judge (for example, an injunction), file a civil action, or seek compensation for the violation. Under Turkish law, no person can (*Article 23, Civil Code*):

- Wholly or partially waive that person's rights or capacity to act freely.
- Give up personal freedom.
- Have any restrictions imposed on that person's freedoms which are contrary to law and morality.

Penal Code. The Penal Code criminalises:

- Violating the secrecy of communication (Article 132).
- Tapping and recording private conversations between individuals (Article 133).
- Violating the secrecy of private life (Article 134).
- Storing personal data (Article 135).
- Unlawful delivery and acquisition of personal data (Article 136).

These criminal actions are punishable by imprisonment (natural persons) and monetary fines (legal entities).

Code of Obligations. The Code of Obligations outlines how an employer must deal with an employee's personal data. An employer can only use its employee's personal information to the extent required to determine the employee's competency and qualification for the work (Article 75, Labour Law). Employers must also arrange a personnel file for each employee (Article 75, Labour Law). Employers must keep information about the employee's identity, along with all the documents and records arranged in accordance with the Labour Law and other legislation. Employers must show this information to authorised persons and authorities on request. Employers are legislatively obliged to use the information held about an employee in line with the principles of honesty and law. Employers must not disclose information concerning which the employee has a justifiable interest in keeping confidential.

Data protection considerations for employers in a whistleblowing context

Employers are prohibited from using an employee's personal data for any reason, without prior consent from the employee. Before using, disclosing, or acting on data in a whistleblowing context, employers should consider the data's nature and their obligations. In practice, it will be far easier for employers to obtain consent before the matter arises, since an employee may have an interest in withholding such consent after the fact. Accordingly, employers should obtain explicit written consent from employees to the effect that business-related e-mail addresses and mail boxes must not be used for personal reasons and the employer is entitled to monitor these. Employers are not entitled to access or monitor an employee's personal correspondence made from a personal e-mail account. The precedents (*Court of Appeals 9 HD E.2009/447 K. 2010/37516 T. 13.12.2010*) of the Court of Appeals also supports

this position. Accordingly, the business-related e-mail addresses and mail boxes are in the employer's domain and thus can be monitored by the employer. That said, considering that there is no regulation and/or precedent on monitoring personal devices which are used for business-related purposes, employers are advised to obtain explicit written consent from the employees.

Complications arise where an employee reports alleged corruption by another employee to the employer and seeks to use personal data to support the allegation. An employer facing that situation should immediately apply to the Public Prosecutor's Office and report its suspicion of criminal activity, without presenting or using the personal data. The Public Prosecutor may then order inspection of the suspected employee's personal data.

Final thoughts

Since Turkey has not yet enacted specific whistleblowing regulation, general provisions under multiple legislative instruments apply when dealing with whistleblowing. These include civil as well as criminal elements, complemented by internal employment policies. The legislative framework is not consolidated, however, and may cause confusion and uncertainty for employers when applied in practice.

A comprehensive and coherent regulation outlining the rights and responsibilities of parties involved in whistleblowing is necessary to establish a clear and sustainable framework to combat corruption in Turkey.

In the absence of such a regulation, the legal ramifications of whistleblowing spans over a wide range of different practice areas and requires complex legal analysis under the specific rules of each respective practice area. A reporting would have legal consequences for each of the parties involved and the position of each party must be separately analysed on a case-by-case basis. Therefore, before taking any positive or negative legal actions towards the parties involved, it is necessary to await the outcome of that case-by-case analysis, to grasp the approach that should be taken.

International whistleblower regimes

International regulations and agreements outline a framework of obligations for employers with regard to employee whistleblowers, including:

- UN Convention against Corruption 2003.
- OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions 1997.
- OECD Recommendation by the Council for Further Combating Bribery of Foreign Public Officials in International Transactions 2009.
- Council of Europe Civil and Criminal Law Conventions on Corruption.
- Inter-American Convention against Corruption.
- UN Convention against Transnational Organized Crime 2000.

Countries can adopt the content of these international instruments into their own jurisdiction's legislative frameworks, either by introducing specific legislation, or amending existing legislation to include related measures.

National whistleblower regimes

The US and UK whistleblower regimes are generally viewed as representing good practice models. Both jurisdictions have long experience with whistleblower-related matters (*Source: OECD report: "Study on Whistleblowers Protection Frameworks, as well as a Related Compendium of Best Practices and Guiding Principles for Legislation*"). The following sections summarise the whistleblowing regimes of the US and the UK.

US whistleblower regime

The Whistleblower Protection Act 1989 protects government employees in the US who report misconduct of federal agencies.

Further provisions were introduced in relation to reporting violations of the Foreign Corrupt Practices Act in the United States by:

- **The Sarbanes-Oxley Act 2002**. Sarbanes-Oxley amended the United States Federal Criminal Code to introduce fines and/or imprisonment for employers that retaliate against employees who report to law enforcement authorities that a federal offence has been committed.
- **The Dodd-Frank Wall Street Reform and Consumer Protection Act 2010**. Dodd-Frank amended the Securities Exchange Act 1934 to empower the United States Security Exchange Commission (SEC) to pay monetary awards to individuals who provide original information to the SEC about federal securities law violations. These awards can range from 10% to 30% of the assets recovered out of the respective investigation. Securities law violations can be past, ongoing, or pending. Under this system, individuals are eligible for a monetary award if they voluntarily provide the SEC with original information which leads to a successful enforcement action. The SEC has initiated a whistleblower programme, which includes the ability to reporting alleged violations anonymously via an electronic complaint line and adopted rules for whistleblower protection, including confidentiality of the identity of the whistleblower and also prohibition on retaliation.

United States laws regarding labour, administration, and civil services contain additional provisions which protect employees from employer retaliation.

UK whistleblower regime

The UK Bribery Act 2010 does not specifically outline whistleblower protections or obligations, nor does it provide details about related procedures for employees or employers. The Financial Conduct Authority has a unit for whistleblowing, which receives complaints and scrutinises how whistleblowing is dealt with by the companies. The authority and purpose of this unit differs significantly from its US counterpart, and the unit does not provide financial incentives for whistleblowers. The FCA and the Prudential Regulation Authority are planning to introduce new measures to assist firms in applying whistleblower policies, but these explicitly do not include introducing financial incentives for whistleblowers (*www.fca.org.uk/static/documents/financial-incentives-for-whistleblowers.pdf*).

Whistleblower procedures and protections exist under the Public Interest Disclosure Act (PIDA), enacted in 1999 within the UK's employment legislation framework. The PIDA is the primary piece of legislation in the United Kingdom for whistleblowing matters. It outlines a framework for public interest whistleblowing, protecting workers from employer retaliation for raising concerns about employer malpractice.

The PIDA applies to every employee in the UK, irrespective of whether the employee works in the private, public, or voluntary sector. The legislation also covers workers, contractors, trainees, agency staff, homeworkers, police officers, and every professional in the National Health Service (NHS). Disclosures which are protected under the PIDA are specifically listed, along with details of protection mechanisms and remedies.

The Civil Service Code of the United Kingdom also outlines the circumstances in which a civil servant can make a disclosure regarding an alleged wrongdoing.

Related Practices

- Anti-Bribery and Anti-Corruption
- Anti-Money Laundering

Related Attorneys

- BURCU TUZCU ERS?N, LL.M.