# Aligning corporate ethics compliance programs with data protection

*Karin Retzer, Partner at Morrison Foerster, examines the data protection compliance challenges that arise with operating an anti-corruption policy*

In order to ensure transparent and ethical business operations, and to address anti-corruption laws around the globe and increasingly aggressive enforcement, more and more multinational companies are undertaking efforts to implement comprehensive anti-corruption strategies. By their very nature, these programs require organisations to collect data on management and staff, as well as suppliers, customers and their employees and representatives. European data protection and data security laws often limit the amount of data that may be collected in relation to corporate ethics programs.

While global companies face inherent tension between complying with anti-corruption laws and applicable privacy and data protection laws, careful consideration can help to overcome these challenges. Below we outline some of the challenges related to data collection and provide recommendations for companies looking to strike a balance that will align corporate ethics and data protection. Particular focus is given to companies with operations in both the US and Europe.

## An overview of anti-corruption laws

Compliance with anti-corruption laws is not an issue unique to the US. Many countries have adopted laws that prohibit and sanction bribery and corruption, including criminalising bribery of foreign government officials, even in jurisdictions that may not have their own anti-corruption laws. The obligation to comply with such legislation provides the legal justification required under data protection laws for the collection of personal data. However, this only holds true where there are local statutory requirements. Compliance with a foreign statute is usually not sufficient to justify processing of personal data. Companies must demonstrate a legitimate interest or obtain individual consents to disclose personal data pursuant to laws with extraterritorial reach, such as the US Foreign Corrupt Practices Act ('FCPA') and the UK Anti-Bribery Act 2010 ('Bribery Act').

The FCPA has prohibited bribery of foreign government officials for the purpose of obtaining or retaining business since 1977. However, it was not until about a decade ago that US regulators started to enforce the law. Since then, the Department of Justice ('DOJ') and the Securities and Exchange Commission ('SEC') have actively and aggressively enforced the FCPA. The FCPA applies broadly to numerous categories of US and non-US persons and businesses, including issuers, and in certain cases, can give rise to liability even where the improper conduct takes place entirely outside the US. According to the DOJ and SEC, in some instances, a US parent company may be liable for its foreign affiliates' conduct.

The Bribery Act also has a fairly broad extraterritorial reach and prohibits active and passive bribery not only in relation to public officials but also commercial bribery. It covers any act of bribery that takes place in the UK or is committed by a person or company with a 'close connection' to the UK.

## Being prepared — compliance programs

Global companies implement compliance programs to mitigate the risk of corruption violations by employees. In the event of an external investigation, having a compliance program is likely to either prevent enforcement proceedings or limit the consequences. The FCPA only requires internal controls for issuers. However, in practice, both the DOJ and the SEC will consider a comprehensive compliance program when deciding whether or not to bring charges. Because the Bribery Act contains sanctions for the failure to prevent bribery, having adequate internal procedures is an affirmative defence for companies.

Effective programs must be tailored to a company's business needs and to the associated risks. Although 'one-size-fits-all' compliance programs are ineffective, most include core elements such as a code of conduct, procedures for third party due diligence, detection and investi-

(Continued on page 6)

(Continued from page 5)

gation of violations, and employee monitoring and training.

Below we outline how anti-corruption compliance programs can be developed to include those essential elements and ensure compliance with data protection rules.

## Developing a framework for due diligence

Under both the FCPA and the Bribery Act, a company can be held liable for the actions of its third party intermediaries. For this reason, it is essential that companies understand who they are doing business with, and conduct reasonable due diligence prior to entering the relationship. There are various tools available to obtain information about third parties with whom companies are about to enter into business relationships. Such due diligence typically involves questionnaires designed to collect commercial information and information about executives and key personnel. As a result, companies collect and retain personal data, which may include individuals' financial information, inclusion on public watch lists or their relationships with public officials.

Sensitive data, such as political affiliation or criminal and judicial data, may also be collected. Most countries prohibit or severely limit the collection of sensitive data.

In designing third party due diligence programs, companies should be cognizant of data protection requirements and integrate privacy protections into the third party due diligence processing. The following are specific measures that a company can take in this regard:

- limiting data collection to individuals in relevant positions and relevant data sets, depending on the risk factors;
- providing notice about data collection and obtaining individual consents where appropriate;
- where providing notice as above is not feasible, obtain contractual guarantees from the party providing personal data that the required notices will be provided;
- formulating due diligence questions to minimise the collection of sensitive data, such as political beliefs, health information, criminal records and judicial data, such as information on bankruptcy proceedings;
- where possible, anonymising data by omitting names and other identifying information;
- limiting access to due diligence data to relevant personnel with a need to know and putting in place adequate cross-border transfer mechanisms such as Standard Contractual Clauses, Safe Harbor certification or Binding Corporate Rules ('adequate safeguards');
- retaining data for a specified period and no longer than permitted or required; and
- filing local registrations and obtaining the required authorisations from national data protection authorities ('DPAs').

***"Conducting an internal investigation is a reasonable, and often expected, response to suspected corrupt activity, and will invariably involve the collection of personal data. In order to limit the risk of privacy violations, companies should implement rules on handling internal investigations."***

## Detecting violations via whistleblowing hotlines

A comprehensive anti-corruption compliance program often includes methods for employees to report misconduct or violations of the company's policies. The US Sarbanes-Oxley Act of 2002 ('SOX') requires the operation of whistleblowing hotlines ('hotlines') for reporting questionable accounting or auditing matters. Compliance with SOX is mandatory for publicly listed companies and may incur liability and hefty fines. Foreign affiliates of a US publicly listed parent company must also comply with SOX. The Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 ('Dodd-Frank Act') created a rewards program for whistleblowers to report issues directly to the SEC; arguably, this goes outside the internal reporting structure. In practice, the Dodd-Frank Act strengthens internal controls and implements internal reporting channels to help minimise the risk of employees reporting potential violations to the SEC. The Dodd-Frank Act whistleblower provisions are separate from its hotline reporting requirements.

The operation of hotlines and the related privacy aspects are not specifically regulated in Europe, although some countries, such as the UK and Hungary, have enacted laws on whistleblowing. Companies establishing hotlines throughout the European Economic Area ('EEA') must follow local privacy laws implementing the EU Data Protection Directive 95/46/EC ('Directive'); guidance from the Article 29 Working Party, and guidance from the local data protection authority.

Under the Working Party guidance, the operation of hotlines is permitted if they are established as a result of local laws or where they are required by foreign laws to fulfil a 'legitimate purpose', such as SOX, which is specifically addressed in the guidance (the guidance pre-dates the Dodd-Frank Act). Importantly, as the guidance recognises the employer's legitimate interest in operating a hotline, employee consent is in general not required. Potential users and individuals about whom reports are filed must be informed about the details of the hotline and their access and correction rights:

(i) prior to the hotline's implementation; and (ii) when a report has been filed about them.

As a general rule, hotlines should be voluntary and used only as an alternative complaint mechanism, and limited in scope to accounting, auditing, financial corruption and banking matters (as required by SOX).

Some countries have additional rules: in France, hotlines may be used to report anti-competitive practices and, in Germany, serious environmental breaches. In Spain, reports must be limited to any wrongdoing that could affect the labour relationship and, in Sweden, to reports about executives and key employees. Apart from Spain and Portugal, anonymous reporting is generally permitted but should not be encouraged. Specific registrations and authorisations for hotline are required by the data protection authorities in some countries, for example in Denmark or Portugal.

Because processing reports often involves transfers of personal information to a US parent company, adequate safeguards must be in place to protect the transfer. In any case, a service agreement with the vendor operating the hotline will be required.

## Monitoring employee communications

While not necessarily part of a formal compliance program, employee monitoring can be a useful tool for preventing and detecting corrupt behaviour, and can alert company management to corrupt activities at an early stage. In the EEA, employees' right to a certain level of privacy in the workplace must be respected and permanent or blanket monitoring will not be permitted. All electronic communications in the workplace are subject to confidentiality protections, including those sent from workplace equipment for private purposes.

However, monitoring is not explicitly covered in the Directive and rules vary across the EEA. Some countries, such as Finland, have adopted specific laws and, in other countries, data protection authorities have adopted guidance. The Working Party guidance on monitoring of employee communications and the technology employed constantly expanding.

Case law regarding employee monitoring is particularly useful. The Working Party recognises the employer's legitimate interest in monitoring and does not require employee consent. Monitoring must be necessary and proportionate for the intended purposes, and the least intrusive methods must be used.

Companies that integrate monitoring into their anti-corruption compliance program should implement a comprehensive policy covering email, internet and telephone usage. Often, a standard policy can be used across the EEA, although local laws must be considered. Employees must receive prior notice about the monitoring and that IT equipment is provided primarily for work purposes. Adequate safeguards for data transfers should be ensured and, where required, local registrations filed and authorisations from data protection authorities obtained.

## Internal investigations

The existence of comprehensive anti-corruption compliance programs does not guarantee perfect compliance. Even the DOJ and SEC do not hold companies to a standard of perfection, and they recognise that no compliance program can ever prevent all unlawful activity. Companies should therefore develop strategies to address violations if and when they occur, including, for example, a protocol for initiating and conducting internal investigations.

Conducting an internal investigation is a reasonable, and often expected, response to suspected corrupt activity, and will invariably involve the collection of personal data. In order to limit the risk of privacy violations, companies should implement rules on handling internal investigations. Generally, individuals should be informed when their personal data are collected for internal investigations. Such notice may, however, jeopardise the investigation if provided when the investigation is launched. Therefore, companies are advised to provide a general up-front notice (before there is a need) to all employees about the possibility of internal investigations, for example, via a technology use policy.

The collection of personal data should be limited to the minimum necessary for the investigation and, where possible, rendered anonymous. To limit the disclosure of data, investigations should be handled by a dedicated team, and access to data should be limited to those with the need to know. For investigations resulting from whistleblowing reports, the Working Party requires that reports be handled by a dedicated department or service provider that guarantees data security and confidentiality.

Personal data should be retained only for as long as necessary to complete the investigation. Data included in whistleblowing reports should be deleted two months after the investigation ends or upon the closure of all disciplinary and judicial procedures. Unsubstantiated reports should be deleted without undue delay.

## Conclusion

In order to avoid 'compliance clashes' between anti-corruption and data protection laws, companies should address privacy and data security from the outset and develop anti-corruption compliance in tandem with data protection policies and procedures. US authorities are engaging in increasingly aggressive enforcement of anti-corruption laws and data protection awareness and enforcement are expanding in the EEA. Under the European Commission's draft General Data Protection Regulation, sanctions for violations of EEA data protection laws are only expected to increase. To ensure comprehensive compliance, companies must therefore seek to comprehend and navigate the sometimes conflicting obligations under anti-corruption and data protection laws.

**Karin Retzer**
Morrison Foerster
kretzer@mofo.com