TERRALEX

GLOBAL CRISIS MANAGEMENT REGULATORY GUIDE

Contents

TerraLex

Welcome to the TerraLex Global Crisis Management Regulatory Guide 2019.

When a crisis hits your organisation, you need to take action quickly. What practical steps can you and your team take to minimise the impact on your business? What are your reporting requirements in the relevant jurisdiction(s)? What legislation applies there?

Our guide provides you with the answers to these questions in relation to key jurisdictions and it supports your understanding of the relevant local legal framework. It also provides high level practical guidance for those crucial first 72 hours, together with contact details of the local TerraLex firm for when you need specialist advice.

We at RPC are very grateful to all who have taken part in and contributed to this project. We hope you will find our guide a useful resource for understanding your regulatory obligations following a crisis.

Find out more: visit terralex.org to get in touch with your local member firm.

TerraLex is the world's second largest law firm network:

- 19,000 lawyers practising in
- 50 leading independent law firms spanning
- more than 100 jurisdictions.

TerraLex network members are part of a global community. The strength of the network is built around not only the quality of its member firms and lawyers but also the depth of relationships – network members all know each other well, sharing best practice at regular meetings held all over the world throughout the year.

TerraLex was selected as the Global Network of the Year at The Lawyer's 2018 European Awards.

Introduction

A crisis, by its nature, is both serious and unexpected and your response and actions within the first 72 hours will most likely define its impact on your organisation.

It is therefore important to have in place robust procedures that, if followed, will help minimise the adverse consequences.

These next steps are common across all jurisdictions. Please refer to the chapter for the relevant jurisdiction for more detailed guidance on your obligations in that country.

Crisis Checklist	
Immediate actions	
Response team	Assemble a core team of individuals to manage the response (eg from HR, IT, data privacy, facilities, legal & compliance) and identify the main point of contact and reporting procedures
Appoint consultants	Depending on the nature of the crisis, appoint external advisers to assist, including: • **Forensic accountants** • **Cyber/IT specialists** • **Lawyers** • **PR agency (see below)**
Scoping and action plan	Have a clear plan of action with reference to internal policies and procedures. Identify key priorities for first 72 hours
Containment?	Consider whether any immediate measures are required
Criminal activity?	Consider involving the local law enforcement body (see country chapter guide)
Internal communications	
Board notification	Notify the Board
Staff communications	Consider who should be told, what information will be provided and how the message is best conveyed
Confidentiality	Remind staff of confidentiality obligations, including any relevant clauses in their contracts. Staff should not refer to the ongoing events on social media
Document preservation	Inform staff that they should not destroy any relevant paper or electronic documents
External communications	
Reputation management/PR	Inform your PR agency and/or in-house PR team. They should take charge of internal and external communications
Early communication?	Consider whether it would be advisable to issue a holding statement or early communication in order to control the narrative
Communication with shareholders	Consider what communication there should be with shareholders, including any obligations to report to the market for listed companies
Insurance	
	Consider your notification requirements under any relevant insurance policies covering, for example: • **Employers' liability** • **Cyber cover** • **Directors & officers**
Notifications and reporting to Regulators	
	Please refer to the individual country chapters.

Australia

When a crisis arises, which regulatory bodies do I need to notify and what is the relevant legislation?

Data breach

1. On discovering a data breach, which regulators or other government agencies should be notified?

- Agencies or organisations regulated by the Privacy Act 1988 (Cth) (Privacy Act) must notify the Office of the Australian Information Commissioner (OAIC) where an eligible data breach has occurred. This includes Australian Government agencies, businesses and not-for-profits with annual turnovers of $3 million or more, private sector health service providers, credit reporting bodies, entities that trade in personal information and tax file number recipients.
- An eligible breach occurs when serious harm is likely to result to individuals whose personal information is involved in the breach.

2. What legislation, relating to both criminal offences and civil wrongs, covers such a breach?

- The Privacy Act gives the OAIC power to apply for an order that an entity pay the Commonwealth a penalty if it contravenes a civil penalty provision of the Privacy Act. Civil penalty provisions in the Privacy Act relating to data breaches include serious or repeated interference with privacy, as well as credit reporting requirements in Part IIIA.
- The My Health Records Act also empowers the OAIC to apply for an order to pay a civil penalty where a person knows or is reckless to the fact the collection, use or disclosure of data is not authorised. This conduct also give rise to criminal liability.

"Dawn" raids

3. What agencies have the power to conduct dawn raids on private sector companies? What legislation gives those agencies the power to undertake those inspections?

- **Australian Securities and Investments Commission (ASIC)**:
  - Australian Securities and Investments Commission Act 2001 (Cth)
  - Corporations Act 2001 (Cth)
- **Australian Crime Commission**: Australian Crime Commission Act 2002 (Cth)
- **Australian Competition and Consumer Commission**: Competition and Consumer Act 2010 (Cth)
- **Australian Tax Office**: Taxation Administration Act 1953 (Cth)
- **The Australian Federal Police (AFP)**:
  - Australian Federal Police Act 1979 (Cth)
  - Crimes Act 1914 (Cth)
- **State Police (including but not limited to)**:
  - Crimes Act 1958 (Vic)
  - Law Enforcement (Powers and Responsibilities) Act 2002 (NSW)
- **Workplace health and safety regulators (including but not limited to)**:
  - Work Health and Safety Act 2011 (Cth)
  - Occupational Health and Safety Act 2004 (Vic)
- **Australian Securities Intelligence Organisation**: Australian Security Intelligence Organisation 1979 (Cth)
- **Environmental authorities (including but not limited to)**:
  - Environment Protection and Biodiversity Conservation Act (Cth)
  - Environment Protection Act 1993 (SA)

4. On what bases, including privilege and/or confidentiality, may such company refuse to permit the seizure of documents?

- A company may refuse to produce documents that are subject to legal professional privilege. Statutory protection is afforded to materials that attract legal professional privilege pursuant to section 118 and 119 or the Evidence Act 1995 (Cth) and prohibit them from being adduced as evidence. In Australia, there are two types of legal privilege (discussed in part 10 below).
- The Competition and Consumer Act 2010 (Cth) also provides that pursuant to section 155, documents do not need to be produced if the production would result in the disclosure of information that is subject to legal professional privilege.
- Generally, attempting to refuse access to documents on the basis of confidentiality or privilege against self-incrimination is not permissible and will not prevent the seizure of documents.

Whistleblowing

5. What are the circumstances under which an employee is entitled to protection when reporting an alleged wrongdoing?

- Employees working within the private sector, who provide information about potential misconduct or illegal activity are afforded whistleblower protection through the Corporations Act 2001 (Cth).
- An employee will be protected under the Corporations Act 2001 (Cth) as a whistleblower if they meet all the following criteria:
  - they must currently hold a position at the company that they are making a disclosure about, or be a current contractor
  - the disclosure must be made to designated employees within the firm, such as those authorised by the company to receive whistleblower disclosures, or to ASIC
  - they must provide their name when making the disclosure
  - they must have reasonable grounds to suspect that the information being disclosed indicates that the company or officer may have breached the Corporations Act 2001 (Cth) or Australian Securities and Investments Commission Act 2001 (Cth), and
  - the disclosure must have been made in good faith.

6. What legislative protection does that employee enjoy?

- The information provided by a whistleblower is known as a "protected disclosure". If that information is provided to ASIC, it will be kept confidential and the identity of the whistleblower will not be disclosed.
- The Corporations Act 2001 (Cth) also affords the employee protection from litigation, where they may use the whistleblower protection as a defence, should they find themselves subject to an action for disclosing protected information. Further, there is protection from victimisation.
- A whistleblower is also protected from being terminated for making a protected disclosure. Where this occurs, they can seek to be reinstated or placed in a comparable position.
- From mid-2019, new laws will be introduced in Australia as the Government has passed the Treasury Laws Amendment (Enhancing Whistle-blower Protections) Bill 2018. The new laws will expand the scope of classes of whistleblower eg to include relatives, former employees and associates, and generally strengthen protection for whistleblowers. In addition to this, the amendments will introduce tax whistleblower protections into the Taxation Administration Act 1953 (Cth).
- Workplace safety laws (such as the Work Health and Safety Act 2011 (Cth)) and the Fair Work Act 2009 (Cth) provide protection to employees against discriminatory conduct for exercising a workplace right or raising a safety concern.

Anti-bribery and corruption

7. What are the main anti-corruption laws and regulations in your jurisdiction?

- Each State and Territory has its own legislation criminalising bribery with a predominant focus on the public sector.
- On the federal level, section 70.2 of the Schedule to the Criminal Code Act 1995 ("Code") prohibits the bribery of both federal and foreign public officials.

8. Does the legislation have extra-territorial effect?

- Federal offences arising out of breaches of the Code have extraterritorial application. State laws do not have extraterritorial reach.
- The offence of bribing a foreign official will only be committed under section 70.2 of the Code if the alleged offence occurs:
  - wholly or partly in Australia, or
  - wholly or partly on board an Australian aircraft or ship, or
  - wholly outside Australia and the person is an Australian citizen, resident of Australia or a body corporate incorporated under a law of Australia.

9. What are the main enforcement bodies?

- Australian Federal Police
- Office of the Commonwealth Director of Public Prosecutions
- State-based offences prosecuted by State DPPs.

Internal investigations

10. Is there any duty to report the issue, for example to a regulator?

Documents generated as part of an investigation will generally not be disclosable if they are privileged. There are two types of legal privilege in Australia:

- **Legal advice privilege** protects all communications between a lawyer and client created in the context of seeking legal advice. Where the client is a company, the protection only applies to communications with individuals authorised to seek legal advice on behalf of the company in relation to the investigation.
- **Litigation privilege** protects documents and communications if they are created for the dominant purpose of litigation and that litigation is reasonably in contemplation at the time the document is created. Litigation privilege applies to communications between any employees of the company, third parties and/or legal advisers.

11. What is the protection from disclosure for documents generated as part of the investigation (for example, privilege)?

Generally, advice given by an in-house lawyer regarding an investigation is confidential and privileged if structured correctly. At the outset of an investigation, it is most likely that legal advice will apply. However, if litigation becomes likely as the investigation develops, then litigation privilege will also become likely to apply.

Contact details

Lander & Rogers
Lawyers

Johnathan Quilty
Lander & Rogers
Direct line: +61 392 699 171
jquilty@landers.com.au

Back to contents>

Bolivia

When a crisis arises, which regulatory bodies do I need to notify and what is the relevant legislation?

Data breach

1. On discovering a data breach, which regulators or other government agencies should be notified?

When a data breach occurs, the police or a similar enforcement agency must be notified. In Bolivia there is no specific cyber-crime division. Some regulated industries (such as banking, insurance) must report to their corresponding regulators.

2. What legislation, relating to both criminal offences and civil wrongs, covers such a breach?

In addition to the above, there is no specific law relating to data breach, although there are laws such as the Criminal Code and the Bolivian Constitution that superficially cover data protection.

- **Criminal Code** – Article 363 ter. – (Alteration, Access and Wrongful use of Computer Data) Whoever, without authorization, accesses, uses, modifies, deletes or disables data stored in a computer or any computer support, causing damage to the owner of the information, will be sanctioned with work up to one year or a fine of up to two hundred days.
- **Bolivian Constitution** – Privacy Protection Action ARTICLE 130. – I. Any individual or collective that believes that it is being unduly or illegally prevented from knowing, objecting or obtaining the elimination or rectification of data held by any physical, electronic means, magnetic or computer, in public or private archives or data banks, or believes that its fundamental right to personal or family privacy, or image, honor and reputation has been affected, can file a Privacy Protection Action.

"Dawn" raids

3. What agencies have the power to conduct dawn raids on private sector companies? What legislation gives those agencies the power to undertake those inspections?

Supreme Decree N° 0071 from April 9th 2009

- **Supervision and Social Control Authority of Telecommunications and Transport**: ATT
- **Authority for the Control and Social Control of Drinking Water and Basic Sanitation**: AAPS
- **Forest and Land Social Monitoring and Control Authority**: ABT
- **Pension Control and Social Control Authority**: AP
- **Electricity Control and Social Control Authority**: AE
- **Supervision and Social Control of Companies Authority**: AEMP

According to several Ministerial Resolutions, the Labor Ministry can conduct raids to assess companies' compliance with work legal provisions.

4. On what bases, including privilege and/or confidentiality, may organisations refuse to permit the seizure of documents?

Raids usually take place to control, supervise and verify compliance with legal provisions, such as having all permits updated or maintained, etc.

In circumstances where an organization requires the disclosure of any confidential document, that would have to be authorized by a court order or by a competent authority.

Whistleblowing

5. What are the circumstances under which an employee is entitled to protection when reporting an alleged wrongdoing?

There is no specific law relating to whistleblowing.

6. What legislative protection does that employee enjoy?

Not applicable.

Anti-bribery and corruption

7. What are the main anti-corruption laws and regulations in your jurisdiction?

- Criminal Code (for bribery, arts. 145 and 173 relating to public servers; and art. 158 for other acts)
- Law N° 004 "Marcelo Quiroga Santa Cruz" from March 31, 2010 – Fight against corruption, illicit enrichment and fortunes research.

The purpose of this law is to establish mechanisms and procedures, within the framework of the State's Political Constitution, laws, treaties and international conventions, aimed at preventing, investigating, prosecuting and punishing acts of corruption committed by public and

former servants. In relation to former public servants, the law covers the exercise of their functions, and natural or legal persons and legal representatives of legal entities, public or private, national or foreign that compromise or affect State resources. It also covers the recovery of State resources through competent jurisdictional bodies.

8. Does the legislation have extra-territorial effect?

Yes, articles 30 and 31 of Law N° 004, provides sanctions for bribery acts performed by foreign institutions or servants.

9. What are the main enforcement bodies?

- Ministry of Institutional Transparency and Fight Against Corruption
- Government Ministry
- Public Prosecutor's Office
- General Comptroller of the State
- Financial Investigation Unit
- State Attorney General's Office
- Representatives of the Organized Civil Society.

Internal investigations

10. Is there any duty to report the issue, for example to a regulator?

- Companies whose shares are traded on a regulated market are required to disclose inside information.
- All companies are required to inform and register any event relating to company to the Commercial Registry: eg issuance or revocation of mandates, capital increase, instalments transfer, contracts, etc. Moreover, each year companies must renew their registration by filing balance sheets and other financial statements. This registry is public.
- For other important matters such as competition, there is no legal obligation to report.

11. What is the protection from disclosure for documents generated as part of the investigation (for example, privilege)?

- Although documents or contracts may have a confidentiality clause, they must be disclosed if the court orders it, privileged or not.
- The only documents or investigations that must remain confidential under Bolivian law, are judicial proceedings involving minors.

12. Is the advice given by an in-house lawyer in relation to the investigation privileged and/or confidential?

Under Bolivian Law, there is no such distinction between the advice given by an in-house or external lawyer; they both are privileged.

The Law of the Practice of the Legal Profession states that any lawyer must: "*Keep professional secrecy, except in the cases of your own defense, defense of the truth or if the sponsored person authorizes its disclosure in an express manner or court order*."

Contact details

Miguel Apt. B
APT Law Firm
Direct line: +591 2 244 1809
mapt@legalapt.com

Back to contents>

Brazil

When a crisis arises, which regulatory bodies do I need to notify and what is the relevant legislation?

Data breach

1. On discovering a data breach, which regulators or other government agencies should be notified?

- Federal Law No. 13.709 of 2018 (the General Law for the Protection of Personal Data) will come into force in February 2020, and will serve as the legal framework for data protection in Brazil (which is so far non-existent).
- Although this new law constitutes a step forward, there is some criticism regarding the presidential vetoes included in the legislation. Amongst others, vetoes have been included for provisions relating to the creation of a National Council for the Protection of Personal Data and Privacy and of a regulatory body – the National Protection Authority of Personal Data – both of which would help to enforce the new law.
- At this point in time, the Prosecutor Office for the Federal District and the Territories has created Commissions for Personal Data Protection on an informal basis. Amongst other functions, such commissions will be in charge of:
  - promoting and encouraging the protection of personal data, in accordance with the new legislation
  - suggesting guidelines for a national policy for the protection of personal data and privacy
  - promoting studies on national and international practices for the protection of personal data and privacy
  - receiving communications on any security incidents that could lead to risk or material injury to data holders
  - suggesting the adoption of binding corporate rules (BCRs) for the purpose of international data transfer, and
  - suggesting the adoption of standard contractual clauses for international data transfers.
- In addition, other authorities will be directly involved in the regulation, supervision and investigation of cases of data breaches. Pursuant to Law No 9.472 of 1997 and Law Decree No. 8.711 of 2016, Agência Nacional de Telecomunicações – ANATEL (the National Telecommunications Agency), should communicate any occurrence involving data protection to the Public Prosecutor Office.
- Similarly, Law No. 8.078 of 1990 provides that where there is a consumer relationship between the parties involved in a data breach, the Consumer Protection Officer – PROCON should be notified.
- With regard to cybercrimes, the local police or the federal police should be notified whenever a violation of data protection occurs. Moreover, there is also a Brazilian civil association engaged in the prevention of cybercrimes, named Safety Brazil (www.safernet.org.br), which has signed cooperation agreements with local governmental institutions aimed at encouraging notification.

2. What legislation, relating to both criminal offences and civil wrongs, covers such a breach?

The main legislation in Brazil concerning criminal offenses and civil wrongs is as follows:

- **The Federal Constitution (article 5, X and XII)** – protects rights relating to privacy, prohibiting the invasion of domicile and the violation of correspondence.
- **The Federal Constitution (article 5, item LXXII)** – sets out habeas data, a constitutional remedy that guarantees citizens access to personal data and information held under the control of the Brazilian State and of private entities.
- **Law No. 8.078 of 1990 (the Consumer Protection Code)** – provides that the consumer will have access to the information contained in records and personal data, including any consumer data filed, as well as in their respective sources.
- **Law No. 12.414 of 2011** – establishes the limits that must be observed in the creation of information databases aimed at forming an individual credit history.
- **Law No. 12.527 of 2011 (the Law on Access to Information)** – regulates access to personal information.
- **Law No. 12.965 of 2014 (the Internet Regulatory Act)** – partially regulates issues relating to privacy and data protection in relation to the internet.
- **Law 12.737 of 2012 (the Cyber Crimes Law)** – regulates cybercrime.
- **Law No. 13.709 of 2018 (effective in 2020)** – will provide the new regulatory framework for the protection of personal data.

"Dawn" raids

3. What agencies have the power to conduct dawn raids on private sector companies? What legislation gives those agencies the power to undertake those inspections?

Pursuant to Decree No. 3.689 of 1941, as modified (the Brazilian Code of Criminal Procedure), "dawn" raids ("*busca e apreensão*") on private sector companies are conducted by the Federal or the State Police and/or by members of the judicial authority, upon the issuance of an order by the competent judicial authority. Furthermore, according to the Brazilian Code of Criminal Procedure, the seizure of documents can only be undertaken by the judicial authority or by the police in compliance with a judicial order.

4. On what bases, including privilege and/or confidentiality, may such company refuse to permit the seizure of documents?

Once a judicial order has been issued, the company involved cannot refuse to permit the seizure of documents. However, that company may request that the competent judicial authority determines the confidentiality of any seized documents.

Whistleblowing

5. What are the circumstances under which an employee is entitled to protection when reporting an alleged wrongdoing?

The employee will be entitled to protection when reporting an alleged wrongdoing by the company or by another employee in all circumstances.

6. What legislative protection does that employee enjoy?

There is no specific protection for the reporting employee under current legislation. Law No. 12.846 of 2013, however, provides that where a company has in place a mechanism for reporting wrongdoings, that company may benefit from a reduced penalty in the event that corruption is discovered. Most companies have anonymous hotlines for this purpose.

Anti-bribery and corruption

7. What are the main anti-corruption laws and regulations in your jurisdiction?

- Law number 12.846 of 2013.
- Law number 13.303 of 2016.

8. Does the legislation have extra-territorial effect?

Yes, the purpose of Law number 12.846 of 2013 is to establish liability of any legal person – even foreign companies, which have their headquarters, branch or representation in the Brazilian territory, whether they are constituted in fact or under the law, even on a temporary basis – in relation to acts against the public, or the national or foreign administration.

9. What are the main enforcement bodies?

The main enforcement bodies are:

- **the Federal Comptroller Office** ("*Controladoria Geral da União*"), which is responsible for the defence of public assets and for the prevention of white collar crime and corruption (administrative proceeding); and
- **the Public Attorney Offices**.

Internal investigations

10. Is there any duty to report the issue, for example to a regulator?

Irregularities must be disclosed to a government authority in accordance with applicable legislation or the company's code of conduct.

11. What is the protection from disclosure for documents generated as part of the investigation (for example, privilege)?

The documents generated as part of the private investigation will be deemed confidential and intended only to be used by the directors and officers of the company.

12. Is the advice given by an in-house lawyer in relation to the investigation privileged and/or confidential?

Yes. As a general policy, under the rules of the Brazilian Bar Association, lawyers are required to maintain professional secrecy about matters relating to their clients at all times. The advice given by an in-house lawyer in relation to an investigation will be confidential and intended only to be used by the directors and officers of the company.

Contact details

PINHEIRO MOURÃO RASO E ARAÚJO FILHO
ADVOGADOS

Patrícia Vilhena
Pinheiro, Mourão, Raso E Araújo Filho Advogados
Direct line: +55 313 116 1500
patriciavilhena@pmraf.com.br

Back to contents>

Canada

When a crisis arises, which regulatory bodies do I need to notify and what is the relevant legislation?

Data breach

1. On discovering a data breach, which regulators or other government agencies should be notified?

- Federally-regulated organizations and organizations that process data in Canada in the course of commercial activity (except in Alberta, British Columbia or Quebec) must notify the federal Privacy Commissioner of data breaches involving personal information that create a real risk of significant harm. The organization must also notify affected individuals and organizations or government institutions that can reduce or mitigate the risk of harm.
- Organizations in Alberta must notify the Alberta Privacy Commissioner of any data breach involving personal information that may create a real risk of significant harm. The commissioner may require the organization to notify affected individuals.
- The respective private sector privacy legislation in British Columbia and Quebec does not contain similar notification obligations.
- We note that some jurisdictions also have public sector and industry-specific legislation that require breach notification in certain circumstances.

2. What legislation, relating to both criminal offences and civil wrongs, covers such a breach?

The notification requirements referenced in the first two paragraphs of the preceding response are pursuant to:

- The federal **Personal Information Protection and Electronic Documents Act**; and
- **Alberta's Personal Information Protection Act**.

As noted above, additional applicable public sector and industry-specific legislation may require notification in certain circumstances. Additionally, Canada's Criminal Code contains various provisions relevant to data protection and cyber security.

"Dawn" raids

3. What agencies have the power to conduct dawn raids on private sector companies?

Numerous agencies have the power to conduct dawn raids on private sector companies, depending on the enforcement regime. These agencies include: provincial and federal police; the Competition Bureau; the Canada Border Services Agency; environmental protection, labour, securities commissions, and tax authorities. In almost all situations, except by reason of exigent circumstances, the agency must obtain a search warrant from a court.

4. What legislation gives those agencies the power to undertake those inspections?

- The search and seizure powers of the federal Criminal Code can be used regarding all offences violating federal laws (eg bribery, fraud, forgery, money laundering, customs violations, export/import controls, trade sanctions, etc). The federal **Competition Act** also has concurrent search powers (eg hard-core cartel conduct, abuse of dominant position and misleading advertising).
- As well, a number of federal and provincial statutes have regulatory inspection powers. These include legislation relating to securities, environmental protection, occupational health and safety and tax. There is also sector-specific legislation that provide search and/or inspection powers (including legislation regarding financial services, food and beverage, pharmaceuticals, energy and transportation).

5. On what bases, including privilege and/or confidentiality, may such company refuse to permit the seizure of documents?

- Provided the authority conducting the search complies with the scope of the warrant, there is rarely any basis pursuant to which confidentiality could prevent the seizure and review of documents.
- Claims of solicitor-client or other types of legal privilege over documents may be asserted during the search and seizure process. Documents will be collected without being examined and sealed until a

judge can assess the privilege claim. Review of these documents by the authorities conducting the search will only be undertaken once issues of privilege have been resolved.

Whistleblowing

6. What are the circumstances under which an employee is entitled to protection when reporting an alleged wrongdoing?

- Most notably, the Criminal Code protects employees who have provided information to the enforcement authorities in relation to federal or provincial criminal offences that they believe have or are being committed. As a result, the Criminal Code's protections of whistleblowers extend beyond offences listed in the Criminal Code. As well, certain other legislation, such as the Competition Act, some provincial securities legislation and some public sector legislation, provide whistleblowers with additional protections.
- However, in many circumstances, employees who are considering whistleblowing have a duty to their employer that requires the employee to raise the potential issue to the appropriate manager or supervisor within the organisation.
- Outside of the concept of reprisal under provincial employment standards, human rights and occupational health and safety legislation, the principles of whistleblower protection generally do not apply to non-criminal offences as well as issues with respect to following human resources or other internal policies.

7. What legislative protection does that employee enjoy?

- Under the **Criminal Code**, no employer or person acting on behalf of an employer or in a position of authority over an employee shall take a disciplinary measure against, terminate or otherwise adversely affect the employment of a whistleblower or of a potential whistleblower (as a threat against whistleblowing), when such whistleblowing involves reporting a criminal offence to the enforcement authorities.
- As noted above, other legislation may include additional protections. For example, a whistleblower's identity will be kept strictly confidential under the **Competition Act**. As well, the Competition Act protects an employee who believes a Competition Act offence **will** be committed. Another example is the Ontario Securities Act, which protects whistleblowers and persons that cooperate with the Ontario Securities Commission. There is also a remedial process in place whereby an employee can receive compensation if their employer retaliated against them for whistleblowing. A number of additional whistleblowing protections also apply to public sector employees.

Anti-bribery and corruption

8. What are the main anti-corruption laws and regulations in your jurisdiction?

Canada's Criminal Code includes domestic offences for bribery, fraud, corruption, influence-peddling, and breach of trust, among other offences. These offences apply to both private parties and public officials. Bribery of foreign public officials has been criminalized in the Corruption of Foreign Public Officials Act. Quebec's Anti-Corruption Act is the only sub-federal anti-corruption legislation in Canada.

9. Does the legislation have extra-territorial effect?

- The Corruption of Foreign Public Officials Act provides for jurisdiction based on nationality. Offences under the Act are deemed to have been committed in Canada, regardless of where the offence actually occurred, when a Canadian citizen, permanent resident, or corporation commits the offence (or conspires or attempts to commit, or being an accessory after the fact, or counselling in relation to that offence).
- Canada's criminal law is based on territorial jurisdiction, which precludes convictions for offences committed outside Canada unless explicitly stated by Parliament. However, the activities constituting an offence need only have a "real and substantial connection" to Canada to be subject to the jurisdiction of Canadian courts.

10. What are the main enforcement bodies?

Federal, provincial and major municipal police services enforce the Criminal Code. Only the RCMP, Canada's national police force, has authority to enforce the Corruption of Foreign Public Officials Act. Unlike other jurisdictions, there is no civil or administrative enforcement of anti-bribery and anti-corruption laws in Canada.

Internal investigations

11. Is there any duty to report the issue, for example to a regulator?

Any duty to report will originate from specific legislation and will depend on the particular issue discovered. In most cases, there is no duty to report. However, some cases where an internal investigation yields an issue will require reporting. This includes provincial securities legislation that require public companies to disclose material changes and provincial environmental legislation that requires the reporting of certain environmental contamination events.

12. What is the protection from disclosure for documents generated as part of the investigation (for example, privilege)?

Documents generated for the purpose of obtaining or providing legal advice are privileged as pertaining to legal advice and are protected from disclosure. As well, documents created for the purpose of anticipated litigation are privileged and protected from disclosure until such litigation is concluded.

13. Is the advice given by an in-house lawyer in relation to the investigation privileged and/or confidential?

Advice provided by in-house counsel in relation to an investigation is privileged (and confidential) if it meets the general requirements for solicitor-client privilege or litigation privilege as described above. Other communications which contain non-legal advice or are not prepared for the purposes of litigation will not be privileged.

Contact details

mcmillan

Benjamin M. Bathgate
McMillan LLP
Direct line: +1 416 307 4207
ben.bathgate@mcmillan.ca

Back to contents›

Cayman Islands

When a crisis arises, which regulatory bodies do I need to notify and what is the relevant legislation?

Data breach

1. On discovering a data breach, which regulators or other government agencies should be notified?

- There is currently no designated authority until the **Data Protection Law, 2017 (DPA)**, which was passed on 27 March 2017, and comes into effect on 30 September 2019. However, it is proposed under the DPA that the relevant authority will be the Information Commission (the "Commissioner") appointed under section 35 of the **Freedom of Information Law (2015 Revision)**.
- In the case of a personal data breach, the DPA provides that the data controller is required to notify the data subject and the Commissioner of the breach, without undue delay, but no longer than five days after the data controller should, with reasonable diligence, have been aware of the breach. Failure to do so is an offence for which the fine is US$1,000 on conviction.
- Notification of the breach should include the nature of the breach, the consequences of the breach, the measures proposed or taken by the data controller to address the breach and the measures recommended by the data controller to mitigate the possible adverse effects of the breach.

2. What legislation, relating to both criminal offences and civil wrongs, covers such a breach?

The legislation is the **Data Protection Law, 2017** (not yet in force). The DPA, once it comes to effect, will cover civil and criminal offences, as well provide a cause of action for compensation to a person who suffers damage by reason of a contravention of the DPA by a data controller. The offences are punishable by a fine of up to US$120,000 and imprisonment for a term up to five years.

"Dawn" raids

3. What agencies have the power to conduct dawn raids on private sector companies? What legislation gives those agencies the power to undertake those inspections?

- **Cayman Islands Monetary Authority**: Banks and Trust Companies Law, Companies Management Law, Monetary Authority Law, Securities Investment Business Law
- **The Police**: Police Law, Proceeds of Crime Law
- **HM Customs**: Customs Law, Proceeds of Crime Law

4. On what bases, including privilege and/or confidentiality, may such company refuse to permit the seizure of documents?

- A company may ordinarily refuse to hand over documents which are legally privileged. Confidentiality alone will not normally be sufficient grounds to avoid disclosure.
- The terms of any warrant or similar authority for the search should be carefully checked to ensure that any document sought to be seized falls within its terms (as to date, subject matter etc).

Whistleblowing

5. What are the circumstances under which an employee is entitled to protection when reporting an alleged wrongdoing?

- The **Whistleblower Protection Law (2015 Revision)** provides protection for whistleblowers who make known information which is in the public interest.
- Under this legislation, persons may disclose to the designated authority any information that they have a reasonable belief shows or tends to show that improper conduct has occurred, is occurring or is likely to occur.

6. What legislative protection does that employee enjoy?

- These protections include safeguards against "detrimental action", such as intimidation, discrimination, adverse treatment or retaliation by employers or other employees. Detrimental action is defined in the law as including:
  - action causing injury, loss or damage
  - intimidation or harassment
  - unlawful discrimination, disadvantage or adverse treatment in relation to a person's employment, family life, career, profession, trade or business, including the taking of disciplinary action
  - preventing, restraining or restricting an employee from making a protected disclosure, and
  - inducing any person by threats, promises or otherwise to contravene this Law.
- If any such detrimental action is taken by an employer against a whistleblower it will be deemed

a criminal offence carrying a sentence of two to five years imprisonment.

- There will be no protection offered under the law for frivolous or vexatious complaints intending only to humiliate employers, nor will it be offered if the reporting of the information is in itself an offense or the information being reported is legally privileged, and will only gain the protection offered if they are made in the public's interest.
- Other protections offered by the Whistleblower legislation include departmental transfer of a government employee who has reported suspected wrongdoing if the employee requests such a transfer and there is a real risk of retaliation if they were to remain in their current position.
- An employer can be held liable for the actions taken by their other employees against any employee who reports suspected wrongdoing and suffers "detrimental action" as a result. The employer may be required in some instances to pay damages.

Anti-bribery and corruption

7. What are the main anti-corruption laws and regulations in your jurisdiction?

The **Anti-Corruption Law (2018 Revision)** sets out a number of corruption offences including bribery (of public officers, members of the Legislative Assembly and foreign public officer), frauds on the government, breach of trust (by public officer or member of the Legislative Assembly); influencing or negotiating appointments or dealing in offices; false claims by public officers; abuse of office; contractor subscribing to election fund, secret commissions, facilitation payments, false statements to the Anti-Corruption Commission, conflict of interests.

8. Does the legislation have extra-territorial effect?

Yes. Section 39 (1)(b) of the **Anti-Corruption Law (2018 Revision)** provides that an offence may be committed where the conduct constituting the alleged offence occurs wholly outside the Cayman Islands and at the time of the alleged offence, the person committing the offence has Caymanian status, is a resident of the Cayman Islands, or is a body corporate incorporated by or under a law of the Cayman Islands.

9. What are the main enforcement bodies?

- **The Anti-Corruption Commission (the "Commission")** – is the designated anti-corruption authority which is comprised of persons appointed by the Governor to receive and investigate any reports of corruption. Where the Commission has reason to suspect the commission of an offence under the Anti-Corruption Law (2018 Revision), following a report being made, the Commission is empowered to carry out an investigation with all the power of investigation provided under Anti-Corruption Law (2018 Revision) and the Criminal Procedure Code (2017 Revision) (including the power of arrest without a warrant).

  If following its investigation, the Commission determines that a corruption offence has been committed it will refer the matter to the Director of Public Prosecution.

- **Royal Cayman Islands Police** – supports the Commission in its investigations.
- **The Director of Public Prosecutions (DPP)** – will assist the Commission in determining whether to decline to carry out investigations into a report or to proceed with further investigations. In addition to prosecuting, the DPP will assist the Commission in obtaining Grand Court orders and warrants necessary for the purposes of an investigation.

Internal investigations

10. Is there any duty to report the issue, for example to a regulator?

- The requirement to report will depend on the nature of the company's business, whether it is subject to regulation and the seriousness of the issue identified by the investigation. In the case of a regulated entity, the duty to report is a matter which must be kept under constant review as and when further information becomes known.
- If there is a suspicion of money laundering a Suspicious Activity Report should be made immediately to the Cayman Islands Monetary Authority ("CIMA"). Other circumstances such as fraud which could have a detrimental effect on investors also give rise to an obligation to report to CIMA.

11. What is the protection from disclosure for documents generated as part of the investigation (for example, privilege)?

Documents generated as part of the investigation will generally not be disclosable if they are privileged. There are two relevant types of privilege under Common law:

- **Legal advice privilege** protects all communications between a lawyer and client created in the context of seeking legal advice. Where the client is a company, the protection only applies to communications with the individuals authorised to seek legal advice on behalf of the company in relation to the investigation.
- **Litigation privilege** may protect documents/communications if they are created for the **dominant purpose of litigation** and that litigation is reasonably in contemplation at the time the document is created. Litigation privilege applies to communications between any employees of the company, third parties and/or legal advisors.

12. Is the advice given by an in-house lawyer in relation to the investigation privileged and/or confidential?

Generally, advice given by an in-house lawyer regarding an investigation is confidential and privileged, if structured correctly. At the outset of an investigation, it is most likely that legal advice privilege will apply (see above). However, if litigation becomes likely as the investigation develops, then litigation privilege will also be likely to apply.

Contact details

HIGGS & JOHNSON
Counsel & Attorneys-at-Law

John Harris
Higgs & Johnson
Direct line: +1 345 914-4620
Mobile: +1 345 938-4616
jharris@higgsjohnson.com

Back to contents>

Czech Republic

When a crisis arises, which regulatory bodies do I need to notify and what is the relevant legislation?

Data breach

1. On discovering a data breach, which regulators or other government agencies should be notified?

All data breaches must be notified to The Office for Personal Data Protection (Office), located in Prague. The Office is competent to lead any investigations related to actual and suspected data breaches.

2. What legislation, relating to both criminal offences and civil wrongs, covers such a breach?

- Data breaches are regulated by Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (repealing Directive 95/46/EC (General Data Protection Regulation or GDPR) – by articles 33, 34, 77) and following; and Act No. 127/2005 Coll., on Electronic Communications and Amendment to Certain Related Acts (Electronic Communications Act), as amended by articles 88 and 118
- In addition, a data subject may raise claims under Act No. 89/2012 Coll., Civil Code, as amended – especially under article 81 and following (Personality rights of an individual) and article 2894 and following (Obligations arising from torts, Compensation for pecuniary and non-pecuniary harm)
- Data breaches may also be considered crimes under Act No. 40/2009 Coll., Criminal Code, as amended – specifically under articles 180(2) (Unauthorised Use of Personal Data), 220 (Violation of Obligations of Trust), 230(2) (Unauthorised Access to Computer Systems and Information Media), 255 (Misuse of Information in Business Relations), 270 (Violation of Copyright, Rights Related to Copyright and Rights to Databases) and 248 (Violation of Regulations on Rules of Competition).
- A company may be liable for committing the crimes described above under Act No. 418/2011 Coll., on the Criminal Liability of Legal Entities and on Proceedings against them, as amended.

"Dawn" raids

3. What agencies have the power to conduct dawn raids on private sector companies?

The Office for the Protection of Competition (the Office) in Brno is competent to lead any investigations into actual and suspected breaches of competition law (especially in relation to prohibited agreements between organisations).

4. What legislation gives those agencies the power to undertake those inspections?

Dawn raids are led by the Office **in general** in accordance with Act No. 500/2004 Coll., on Administrative procedures, as amended (as a general procedural Act), being granted specific competence and prerogatives by Act No. 143/2001, on the Protection of Competition, as amended (Competition Act) – especially by its articles 1(4), 20a, 21 to 21h.

The Office may also directly apply under Articles 101 and 102 of the Treaty on the Functioning of the European Union in individual cases should the investigated behaviour have an impact on the European market (cf. especially article 20a of the Competition Act).

Whistleblowing

5. On what bases, including privilege and/or confidentiality, may such company refuse to permit the seizure of documents?

- As a general rule, during the investigation, organisations must provide the Office with the assistance necessary to perform its powers and must submit to the exercise of those powers. The Office's officials are entitled to obtain access to business premises, open locked cabinets or cases, or otherwise gain access to business records. Every person in the business's premises must submit to the investigation; if this obligation is not fulfilled, the Office's officials shall be entitled to obtain access to the business premises (with the assistance of locksmiths or the Police if necessary). If such access is not granted, severe sanctions may be imposed on the company, ie, up to 1% of the net early turnover (cf. article 22a).

- The Office's officials, or other persons authorised by the Office, may, amongst other things, verify whether documents and records are business records, inspect business records found on or accessible from business premises regardless of the format in which they are stored (ie, in safes, hidden drawers, etc.) and copy or acquire copies or extracts from business records in any form. These rights can only be exercised within the defined scope of the investigated case.
- The Office **is however not entitled** to seize originals of documents or to take those documents off the business premises. The Office is however allowed to make copies of any documents.
- A company **may refuse to submit** any documentation that is covered by Attorney-Client privilege, and is thus labelled and recognizable. The Office's officials must stop investigating any document that is covered by this privilege immediately after being notified by the company that is covered by privilege or when realizing its nature.
- A company **may also label any information** that is being provided to the Office as **confidential information** (according to article 504 of the Civil Code). Every person from the Office is obliged to keep confidential such information, even after terminating his/her working relationship with the Office. **However**, such company, if requested by the Office, is obliged to submit a version of any document with the confidential information deleted. **Confidentiality is not a legitimate reason for not providing access of the Office to specific documents.**

6. What are the circumstances under which an employee is entitled to protection when reporting an alleged wrongdoing?

Czech law does not include any specific regulations regarding whistleblowing, so only relevant legislation applicable to all employees will apply. The employee may be protected by an internal regulation in compliance with general binding legislation.

Anti-bribery and corruption

7. What legislative protection does that employee enjoy?

Current Czech legislation does not include any specific protection for whistleblowers.

8. What are the main anti-corruption laws and regulations in your jurisdiction?

- Act No. 40/2009 Sb., the Criminal Code
- Act No. 418/2011 Sb., on the Criminal Liability of Legal Entities and Proceedings against Them
- Act No. 134/2016 Sb., on Public Procurement
- Act No. 253/2008 Sb., on Certain Measures against the Legalisation of Proceeds of Crime and the Financing of Terrorism
- Act No. 254/2004 Sb., on Restrictions on Cash Payments

9. Does the legislation have extra-territorial effect?

Acts undertaken in the Czech Republic are judged under Czech criminal law. A crime is considered committed in the Czech Republic;

- if the perpetrator committed the act in the Czech Republic even though an interest protected by criminal law was or allegedly was interfered with or jeopardised, in part or in its entirety, abroad or
- if the perpetrator committed an act abroad where an interest protected by Czech criminal law was infringed or jeopardised or the consequences of which, at least partly, occurred in the Czech Republic.

The criminality of acts undertaken by Czech citizens or stateless persons who have obtained a permanent residence permit in the Czech Republic is also considered under Czech law.

Internal investigations

10. What are the main enforcement bodies?

There are no specific enforcement bodies. The Police of the Czech Republic investigate all corruption cases and subsequently refer them to general courts. The Office for the Protection of Competition deals with certain aspects of public procurement tenders. Nevertheless, if the Office concludes that an act of corruption occurred and consequently, that a crime was committed, it refers the matter to the Police.

11. Is there any duty to report the issue, for example to a regulator?

Czech law does not include any specific regulation for internal investigations. In any internal investigation, the employer must always proceed in compliance with valid legislation; an internal investigation need not be notified to any specific body and no consent is required.

12. What is the protection from disclosure for documents generated as part of the investigation (for example, privilege)?

As there is no specific regulation regarding an internal investigation and the documents generated as part of such an investigation, only general binding legislation must be respected, specifically concerning personal data.

The rules for handling personal data obtained in an internal investigation are identical to those applicable to the handling of any other personal data. The rules for handling certain types of personal data (sensitive data) must be observed, but these rules apply to all cases of personal data processing (irrespective of the purpose for which they were obtained).

13. Is the advice given by an in-house lawyer in relation to the investigation privileged and/or confidential?

Czech law has specific legislation regarding the advice given by lawyers only in connection with legal advice given by attorneys-at-law registered with the Czech Bar Association.

There is no regulation regarding the advice given by an in-house lawyer (not an attorney-at-law) in relation to an investigation, so this advice should not be considered privileged or confidential.

Contact details

PETERKA PARTNERS

THE CEE LAW FIRM

Mr Stanislav Beran
Peterka & Partners
Direct line: +420 225 396 380
beran@peterkapartners.cz

Back to contents>

Ecuador

When a crisis arises, which regulatory bodies do I need to notify and what is the relevant legislation?

Data breach

1. On discovering a data breach, which regulators or other government agencies should be notified?

In the event a of data breach, the Prosecutor would be the competent authority to investigate. Other competent authorities may be required to be alerted, depending on the type of data.

2. What legislation, relating to both criminal offences and civil wrongs, covers such a breach?

- Ecuadorian Criminal Code (**COIP**)
- Ecuadorian Constitution.

"Dawn" raids

3. What agencies have the power to conduct dawn raids on private sector companies? What legislation gives those agencies the power to undertake those inspections?

- Internal Revenue Service (IRS)
- Superintendence of Companies, Superintendence of Power and Control of the Market and other Superintendences depending on their internal regulations.
- Ecuadorian Social Security Institute.

Constitution of Ecuador and Executive Decrees enacted by the President.

4. On what bases, including privilege and/or confidentiality, may such company refuse to permit the seizure of documents?

In anti-trust matters it is not possible to claim confidentiality or privilege as a basis to refuse the seizure of documents. An individual or corporation might refuse the seizure of documents when they have not been requested by a competent authority within the context of an administrative process or a criminal investigation.

Whistleblowing

5. What are the circumstances under which an employee is entitled to protection when reporting an alleged wrongdoing?

If the employee has knowledge of a criminal offense conducted by their employers or other parties, then they must report it. Also, some companies do have internal regulations and codes of conduct which protect employees so they can report alleged wrongdoings.

6. What legislative protection does that employee enjoy?

- Ecuadorian Criminal Code
- Ecuadorian Constitution
- Labour Code of Ecuador

Anti-bribery and corruption

7. What are the main anti-corruption laws and regulations in your jurisdiction?

- Ley de Prevención de Lavado de Activos y Financiamiento de Delitos.
- Ecuadorian Criminal Code
- We also have international agreements signed and ratified to fight against corruption.

8. Does the legislation have extra-territorial effect?

No. However, Ecuador has signed and ratified international agreements of mutual cooperation to fight against corruption and money laundering in tax havens.

9. What are the main enforcement bodies?

- Ecuadorian Prosecution Office
- Financial Analysis Unit

Internal investigations

10. Is there any duty to report the issue, for example to a regulator?

Yes, there is a duty to report the issue in accordance with the Ecuadorian Criminal Code and Codes of Conduct held by each company. Also the financial regulatory system has codes of conduct that impose a duty to report these matters.

11. What is the protection from disclosure for documents generated as part of the investigation (for example, privilege)?

Yes, local laws do offer protection against disclosure of documents as part of an investigation, as individuals have the obligation to collaborate with competent authorities.

12. Is the advice given by an in-house lawyer in relation to the investigation privileged and/or confidential?

Yes, there is client-attorney privilege.

Contact details

TOBAR ZVS ®
SPINGARN

Álvaro Sevilla
Tobar ZVS Spingarn
Direct line: +593 2 2986456 ext 107
asevilla@tzvs.ec

Back to contents>

England and Wales

When a crisis arises, which regulatory bodies do I need to notify and what is the relevant legislation?

Data breach

1. On discovering a data breach, which regulators or other government agencies should be notified?

- When a personal data breach occurs, a "data controller"[1] organisation in the UK must notify the Information Commissioner's Office (ICO) immediately (within 72 hours of knowledge of the breach if there is a risk to data subjects' rights and freedoms). Notification does not require full details. Organisations can report using the ICO's breach reporting telephone service or in a written report.
- If there is a high risk to people's rights and freedoms (eg if a hospital accidentally discloses patient records), the breach must be reported to the data subjects themselves.
- It may also be necessary or appropriate to notify relevant enforcement agencies, local police or other regulatory authorities. For example, if IT systems have been hacked, this must be reported to the cyber-crime division of the police. Regulated organisations may also have to report to their own regulators and the National Cyber Security Centre may also be notified (but there is no legal obligation to do so), which provides advice/ assistance to victim organisations.
- Providers of essential services, such as energy, transport, health and water must notify significant network and information systems incidents, such as cyber-attacks to competent authorities under the Network and Information Systems Regulations 2018.

2. What legislation, relating to both criminal offences and civil wrongs, covers such a breach?

- The **Data Protection Act 2018 (DPA)**. This covers civil wrongs and criminal offences. The main criminal offence that relates to data breaches is unlawfully obtaining or disclosing personal data without the consent of the data controller[2].
- The Privacy and Electronic Communications Regulations 2003. This relates to electronic marketing communications to consumers.
- The Electronic and Identification and Trust Services for Electronic Transactions Regulations, which relate to providers of trust services such as website authentication certificates.
- In addition, legislation relating to areas such as financial crime and breach of regulatory governance requirements may be relevant. For example, a firm regulated by the Financial Conduct Authority is required to report material cyber incidents[3]. The Network and Information Systems (NIS) regulations also impose specific reporting requirements on large digital service providers and operators of essential services.

"Dawn" raids

3. What agencies have the power to conduct dawn raids on private sector companies; what legislation gives those agencies the power to undertake those inspections?

- **HM Revenue & Customs**: Police and Criminal Evidence Act 1984/Serious Organised Crime and Police Act 2005
- **The Financial Conduct Authority**: Financial Services Act 2000
- **The Prudential Regulation Authority**: Financial Services Act 2000
- **Information Commissioner's Office**: Data Protection Act 2018
- **The Serious Fraud Office**: Criminal Justice Act 1987
- **The Competition and Markets Authority**: Competition Act 1998
- **The European Commission:** EC Regulation 1/2003
- **The Police:** Police and Criminal Evidence Act 1984
- **Health and Safety Executive:** Health and Safety at Work Act 1974
- **Environment Agency:** Environment Act 1995

4. On what bases, including privilege and/or confidentiality, may organisations refuse to permit the seizure of documents?

- A company may refuse the seizure of documents that are "privileged". (NB communications to and from in-house counsel do not attract privilege in the context of a dawn raid regarding EU competition investigations[4])
- There is usually little scope to refuse the seizure of documents on the grounds of confidentiality alone
- A company may refuse to allow the seizure of documents which are outside the scope of the investigation. Check the wording of the search warrant (or equivalent document), specifically any limitations, such as:
  - date ranges

- custodians, and
- subject matter.

- Common practice is for any disputed documents to be placed in a sealed envelope so that arguments regarding privilege and/or scope may be addressed after the dawn raid.

Whistleblowing

5. What are the circumstances under which an employee is entitled to protection when reporting an alleged wrongdoing?

- Workers have special legal protection when they report an alleged wrongdoing at work if it is a "qualifying disclosure"[5]. Whether or not a disclosure is protected also depends how and to whom the disclosure is made.
- A "qualifying disclosure"[6] is a disclosure of information which relates to one of six types of "relevant failure" (including criminal offences and civil wrongs) where the worker has a reasonable and genuine (albeit possibly wrong) belief that: (i) the information demonstrates a relevant failure; and (ii) disclosure is in the public interest.

6. What legislative protection does that employee enjoy?

- Protection under the Employment Rights Act 1996
- Workers have the right not to be subjected to any detriment on the ground of having made a protected disclosure. Claims can be made against the employer and/or against other workers individually.
- Employees have an automatic unfair dismissal claim if the principal reason for their dismissal is that they made a protected disclosure.

Anti-bribery and corruption

7. What are the main anti-corruption laws and regulations in your jurisdiction?

The **Bribery Act 2010** – this covers bribery of public officials and commercial bribery. The most significant offence for corporates is failing to prevent bribery. The only available defence for a corporate is if it can prove that it had "adequate procedures" in place to prevent the bribery that took place.

8. Does the legislation have extra-territorial effect?

Yes. It applies to persons with a close connection to the UK and companies that carry on or have a part of their business in the UK. Within that context, any acts of bribery that take place anywhere in the world with the intention of obtaining a business advantage for the company will constitute a breach of the Bribery Act and may be prosecuted in the UK.

9. What are the main enforcement bodies?

- **The Serious Fraud Office** investigates and prosecutes serious and/or complex fraud, bribery and corruption matters in England, Wales and Northern Ireland
- The **police** and **Crown Prosecution Service** will investigate and prosecute all other types of fraud, bribery and corruption in these jurisdictions.

Internal investigations

10. Is there any duty to report the issue, for example, to a regulator?

- When an issue arises, a company should consider its self-reporting obligations. These will vary, depending upon:
  - the identity of the agency/agencies that regulate the company
  - the nature of the issue
  - the seriousness of the issue, and
  - what is known about the issue at that time.
- We set out below considerations relating to the key UK agencies:

The National Crime Agency

Regulated sectors under the Proceeds of Crime Act and Terrorism Act 2000; if there is a suspicion of money laundering, a Suspicious Activity Report should be made to the National Crime Agency. The report should be made immediately via the National Crime Agency's website.

The Serious Fraud Office

There is no obligation to self-report fraud, bribery and/or corruption to the Serious Fraud Office. However, self-reporting may assist in persuading the Serious Fraud Office that a prosecution would not be in the public interest and a deferred prosecution agreement would be more appropriate.

The Competition and Markets Authority

If the issue relates to a competition law infringement, self-reporting to the Competition and Markets Authority (CMA) should be considered. While there is no legal obligation to report, the CMA operates a leniency policy that can provide the first self-reporting company involved in a cartel with a reduction in a fine or even total immunity from a fine. The timing of any leniency application therefore can be critical. The CMA will not, however, grant immunity from criminal prosecution.

The Financial Conduct Authority

Firms authorised by the Financial Conduct Authority have self reporting obligations under the FCA Supervision Manual (SUP 15). These require a firm to notify the FCA if certain issues arise, including any involvement in fraudulent activity (including if the company is a victim of fraud), or an issue that could have a significant adverse impact on the company's reputation and/or could result in serious detriment to its client.

Publicly Listed Companies

Firms whose shares are traded on a regulated market in the UK may have to make an announcement to the market. Such companies are required to disclose "inside information" (non-public information that would be likely to have a significant effect on the company's share price if it were made public) to the market as soon as possible.

The Information Commissioner's Office

See the section above on data breaches.

11. What is the protection from disclosure for documents generated as part of the investigation (for example, privilege)?

- Documents generated as part of the investigation will generally not be disclosable if they are privileged. There are two relevant types of privilege under English law:
  - **Legal advice privilege** protects all communications between a lawyer and client created in the context of seeking legal advice. Where the client is a company, the protection only applies to communications with the individuals authorised to seek legal advice on behalf of the company in relation to the investigation.
  - **Litigation privilege** may protect documents/communications if they are: (i) created for the **dominant purpose of litigation**; (ii) that litigation is reasonably in contemplation at the time the document is created; and (iii) the litigation is adversarial in nature. Litigation privilege applies to communications between any employees of the company, third parties and/or legal advisors.
- It is possible for privilege to be lost or waived unless arrangements are put in place to maintain privilege once it has been established.

12. Is the advice given by an in-house lawyer in relation to the investigation privileged and/or confidential?

Generally, advice given by an in-house lawyer regarding an investigation is confidential and privileged, if structured correctly. At the outset of an investigation, it is most likely that legal advice privilege will apply (see above). However, if litigation becomes likely as the investigation develops, then litigation privilege will also become likely to apply. However, as noted above, advice from in-house lawyers will not be treated as privileged in relation to European Commission investigations regarding competition matters.

Contact details

Jonathan Cary
RPC
Direct line: +44 203 060 6418
Mobile: +44 7545 100 478
jonathan.cary@rpc.co.uk

Notes:

1. S. 1(1) Data Protection Act 2018 (DPA).
2. S.170 DPA.
3. Principle 11 FCA Handbook.
4. *Akzo Nobel Chemicals Ltd and Akcros Chemicals Ltd v European Commission* Case C-550/07 P.
5. S. 43A Employment Rights Act 1996.
6. S. 43B Employment Rights Act 1996.

European Union

When a crisis arises, which regulatory bodies do I need to notify and what is the relevant legislation?

Introduction

The European Union is a unique economic and political union between 28[1] EU Member States. Generally, it is the European Commission that proposes new laws which are then adopted by the European Parliament and Council. The Member States and EU institution(s) concerned then implement them.

In most crisis situations, even in areas covered by EU-wide legislation, the primary focus will be on the relevant regulatory body(/ies) and national legislation in the EU Member State(s) in question rather than at EU level.

Data breach

1. On discovering a data breach, which regulators or other government agencies should be notified?

Enforcement is carried out at a national level and each Member State has established an independent, supervisory authority for GDPR purposes. Please see the relevant Member State Chapter for details of the relevant regulator.

2. What legislation, relating to both criminal offences and civil wrongs, covers such a breach?

- The EU General Data Protection Regulation (GDPR) (EU Regulation 2016/679) became directly effective in Member States from 25 May 2018. Its purpose is to harmonise data privacy laws throughout the EU, as well as give greater protection and rights to individuals.
- Nonetheless, Member States have implemented their own national legislation to reconfirm, supplement and/or adopt permitted derogations from the scope of the GDPR's requirements. It is, therefore, important to be aware of applicable national variations in addition to the EU requirements.

"Dawn" raids

3. What agencies have the power to conduct dawn raids on private sector companies; what legislation gives the agencies the power to undertake those inspections?

- Most dawn raids are carried out by regulatory authorities in individual EU Member States which exercise their inspection powers granted under national legislation.
- The main exception is the European Commission, which has the power under EU Regulation 1/2003 to conduct dawn raids within Member States for suspected breaches of EU competition law. It will often seek the assistance of the relevant national competition authority.

4. On what basis, including privilege and/or confidentiality, may organisations refuse to permit the seizure of documents?

- A company may refuse the seizure of documents which are "privileged". Under EU law, privilege does not extend to communications to and from in house counsel, but must relate to communications involving an external, EEA-qualified lawyer for the primary purpose of their client's right of defence[2].
- Confidentiality/ business secrets do not preclude the European Commission's ability to examine documents and seize them.
- A company may refuse to allow the review and copying/seizure of documents which are outside the scope of the European Commission's investigation, but care needs to be taken in handling this situation if relevance cannot be agreed.
- Check the wording of the European Commission's decision or authorisation (and any accompanying documentation) to establish any limitations on the scope of its investigation, such as:
  - date ranges
  - subject matter in terms of product(s) and or service(s), and
  - geographic scope.

Whistleblowing

5. What are the circumstances under which an employee is entitled to protection when reporting an alleged wrongdoing?

Currently, the position regarding the protection available to an employee when reporting an alleged wrongdoing is fragmented across the EU and, thus, the nature and extent of any protection depends upon the EU Member State concerned.

6. What legislative protection does that employee enjoy?

- This will depend upon the national legislation in the relevant EU Member State.
- In its Work Programme for 2019, one of the European Commission's key initiatives is the proposal for a Directive on the protection of persons reporting on breaches of European Union law[3]. Once this Directive has been adopted, it will still require implementation by each Member State through national legislation. Under the proposal, the implementation deadline for Member States is May 2021.

Anti-bribery and corruption

7. What are the main anti-corruption laws and regulations?

These will depend upon the relevant EU Member State. Most EU Member States are party to the OECD's Anti Bribery Convention and have corresponding national legislation in place. The EU's most recent Anti-Money Laundering Directive entered into force in July 2018 and Member States have until 20 January 2020 to transpose these regulatory requirements into national law.

8. Does the legislation have extra-territorial effect?

The national legislation of the relevant Member State is likely to have such an effect.

9. What are the main enforcement bodies?

These will depend on the relevant Member State as enforcement in this area is generally carried out at Member State rather than EU level.

Internal investigations

10. Is there any duty to report the issue, for example, to a regulator?

- In most situations, where a company is considering any self-reporting obligations, it should do so in the context of the relevant Member State(s) covered by the conduct in question.
- However, if the issue relates to an EU competition law infringement, it is appropriate to consider whether to self report to the European Commission (and potentially to any relevant national competition authority(/ies) individually as well). Whilst there is no legal obligation to do so, the European Commission does operate a leniency policy which can result in a reduction in any fine for leniency applicants or even total immunity from a fine for the first applicant to come forward, depending upon the specific circumstances. The timing of any leniency application can be crucial.

11. What is the protection from disclosure for documents generated as part of the investigations (for example, privilege)?

Documents generated as part of the investigation will generally not be disclosable, if they are privileged. As mentioned above, under EU law, written communications between an independent, external EAA-qualified lawyer for the purpose of the company's right of defence will be privileged.

12. Is the advice given by an in-house lawyer in relation to the investigation privileged and/or confidential?

Advice from and communications with an in house lawyer and the company do not generally attract privilege under EU law. Care needs to be taken in relation to in house counsel reporting external lawyers' advice in order to maintain privilege. In house counsel should simply forward the advice without comment or opinion. Preparatory documents created exclusively for the purpose of seeking external legal advice in the exercise of the company's rights of defence in connection with a European Commission investigation may benefit from privilege.

Contact details

Jonathan Cary
RPC
Direct line: +44 203 060 6418
Mobile: +44 7545 100 478
jonathan.cary@rpc.co.uk

Notes

1. The UK will withdraw from the EU in due course.
2. *Akzo Nobel Chemicals Ltd and Akros Chemicals Ltd v European Commission* Case C.550/07P
3. COM(2018) 218.

Back to contents>

Finland

When a crisis arises, which regulatory bodies do I need to notify and what is the relevant legislation?

Data breach

1. On discovering a data breach, which regulators or other government agencies should be notified?

- Office of The Data Protection Ombudsman (data breaches concerning personal data)
- Finnish Communications Regulatory Authority (data breaches concerning networks).

2. What legislation, relating to both criminal offences and civil wrongs, covers such a breach?

- General Data Protection Regulation (2016/679 EU)
- Data Protection Act (as of 1 January 2019)
- Information Society Code (Act 914/2014 as amended)
- Criminal Code (Act 39/1889 as amended)

"Dawn" raids

3. What agencies have the power to conduct dawn raids on private sector companies? What legislation gives those agencies the power to undertake those inspections?

The following agencies have the power to conduct unannounced inspections on private sector companies:

- **The Finnish Competition and Consumer Authority (competition matters)**: Competition Act (Act 948/2011 as amended)
- **The Finnish Tax Administration (tax matters)**: Tax Procedure Act (Act 1558/1995 as amended)
- **The Finnish Customs (customs and tax matters)**: Customs Act (Act 304/2016 as amended)
- **The Finnish Safety and Chemicals Agency (product safety and chemical matters)**: Safety and Chemicals Agency Act (Act 1261/2010 as amended)
- **The Finnish Food Safety Authority, Regional State Administrative Agencies and Municipal Food Control (food matters)**: Regional State Administrative Agencies Act (Act 896/2009 as amended), Food Act (Act 23/2006 as amended)
- **The Police of Finland – National Bureau of Investigation and Local Police Departments (criminal matters)**: Criminal Investigation Act (Act 805/2011 as amended), Police Act (Act 872/2011 as amended)
- **Centres for Economic Development, Transport and the Environment as well as Municipal Environment Protection Authorities (environmental matters)**: Act on Centres for Economic Development, Transport and the Environment (Act 897/2009 as amended), Environmental Protection Act (Act 527/2014 as amended), Waste Act (Act 646/2011 as amended) and Water Act (Act 587/2011 as amended).

4. On what bases, including privilege and/or confidentiality, may such company refuse to permit the seizure of documents?

- Legal privilege, ie correspondence with an external lawyer, in competition matters.
- Administrative inspections are in principle carried out on the spot, and the seizure of documents for further inspection requires specific stipulations in the law authorising the seizure. The seizure is authorised by law in eg tax audits.

Whistleblowing

5. What are the circumstances under which an employee is entitled to protection when reporting an alleged wrongdoing?

- There is no specific legislation that protects the employee as whistleblower.
- Legitimate whistleblowing does not constitute a ground for termination of the employment or other disciplinary action.
- Most of the whistleblowing takes place anonymously. Many larger Finnish companies have digital channels that make anonymous whistleblowing possible.

6. What legislative protection does that employee enjoy?

- Fundamental and human rights, eg freedom of expression.
- Protection of the source of information when providing information to the media.
- Legitimate whistleblowing does not constitute a ground for termination of the employment or other disciplinary action.
- A directive on whistleblower protection is currently being prepared in the European Union. Provided that

the directive enters into force, its implementation may lead to adoption of specific whistleblowing legislation in Finland.

Anti-bribery and corruption

7. What are the main anti-corruption laws and regulations in your jurisdiction?

Criminal Code (Act 39/1889 as amended).

8. Does the legislation give extra-territorial effect?

Yes.

9. What are the main enforcement bodies?

The Prosecution Service and the General Courts.

Internal investigations

10. Is there any duty to report the issue, for example to a regulator?

- Suspicion of serious offences must be reported pursuant to the Criminal Code (Act 39/1889 as amended).
- A reporting obligation may also follow from other sector specific legislation.

11. What is the protection from disclosure for documents generated as part of the investigation (for example, privilege)?

There is no specific protection. Documents must be disclosed if there is a duty to disclose under law, eg if the issue must be reported.

12. Is the advice given by an in-house lawyer in relation to the investigation privileged and/or confidential?

- Advice given by in-house lawyers does not enjoy legal privilege in competition matters.
- Otherwise, the application of legal privilege to advice given by in-house lawyers is somewhat unclear.

Contact details

WASELIUS & WIST

Lotta Pohjanpalo
Waselius & West
Direct line: +358 40 522 6760
lotta.pohjanpalo@ww.fi

Jan Waselius
Waselius & West
Direct line: +358 40 522 0589
jan.waselius@ww.fi

Jouni Kautto
Waselius & West
Direct line: +358 45 127 2603
jouni.kautto@ww.fi

Back to contents>

Germany

When a crisis arises, which regulatory bodies do I need to notify and what is the relevant legislation?

Data breach

1. On discovering a data breach, which regulators or other government agencies should be notified?

- When a personal data breach occurs, a "data controller" organisation in Germany must notify the competent supervisory authority – Landesdatenschutzbehörde (there is one for each state (Bundesland)[1]) – immediately (within 72 hours of knowledge of the breach if there is a risk to data subjects' rights and freedom). Notification doesn't require full details. Organisations can report using the digital form on the supervisory authority's website, by writing an e-mail or calling.
- If there is a high risk to people's rights and freedoms (eg if sensitive data is disclosed), the breach must be reported to the data subjects themselves.
- It may also be necessary to notify relevant enforcement agencies, local police or other regulatory authorities. For example, if IT systems have been hacked, this must be reported to the cyber-crime division of the police. Regulated organisations may also have to report to their own regulators.

2. What legislation, relating to both criminal offences and civil wrongs, covers such a breach?

- The Bundesdatenschutzgesetz (BDSG) covers criminal offences. The main criminal offence[2] relating to data breaches is unlawfully disclosing or processing personal data without being authorised to do so. Compensation for civil wrongs can be claimed in accordance with Art. 82(1) of the General Data Protection Regulation (GDPR).
- Outside of data protection laws, legislation relating to areas such as financial crime and breach of regulatory governance requirements may be relevant.

"Dawn" raids

3. What agencies have the power to conduct dawn raids on private sector companies; what legislation gives those agencies the power to undertake those inspections?

- The Department of Public Prosecution (Staatsanwaltschaft) as the general investigation authority – when it comes to criminal investigations – is always entitled to apply for and execute search and seizure measures pursuant to the Strafprozessordnung – StPO (Code of Criminal Procedure). In this respect the Staatsanwaltschaft can make use of further authorities, supporting resp. taking care of the actual search and seizure operation, such as
  - **Polizeibehörden (Police)**: § 103 StPO
  - **Finanz- und Zollverwaltung (Tax and customs authorities)**: §§ 208 (1) subseq.1, 404 subseq.1 Abgabenordnung (German Fiscal Code) in conjunction with § 103 StPO
  - **Zollbehörden** (customs authorities) re illegal employment due to the Schwarzarbeitsbekämpfungsgesetz (Law against illegal labor)
- Additionally certain authorities have a limited search and seizure competence regarding their area of competence:
  - **Landesdatenschutzbehörde** § 16 (4) in conjunction with § 40 (5) BDSG
  - **Kartellbehörden (antitrust authorities)**: § 57 Gesetz gegen Wettbewerbsbeschränkungen (Antitrut Law)
  - **Bundesamt für Finanzaufsicht/Deutsche Bundesbank**: Kreditwirtschaftsgesetz (re financial services)
  - **Bundesnetzagentur/Landesregulierungsbehörden**: Energiewirtschaftsgesetz/Telekommunikationsgesetz (re energy supply and telecommunication)

4. On what bases, including privilege and/or confidentiality, may such company refuse to permit the seizure of documents?

- A company may refuse the seizure of documents that are "privileged", ie specifically, client-attorney communication (communications to and from in-house counsel do not fall under the privilege-rules).
- There is usually little scope to refuse the seizure of documents on the grounds of confidentiality alone.
- A company may refuse to allow the seizure of documents which are outside the scope of the investigation. Check the wording of the search warrant (or equivalent document), specifically any limitations, such as:
  - date ranges
  - custodians, and
  - subject matter.

Whistleblowing

5. What are the circumstances under which an employee is entitled to protection when reporting an alleged wrongdoing?

- In contrast to other countries, whistleblowers in Germany are not protected by a specific law. Rather, protection against disciplinary measures by the employer is governed by general laws, specifically § 612 a German Civil Code (BGB) and §§ 1 et seq. of the Dismissal Protection Act (KSchG).
- On the basis of the general laws, case law has developed standards for when a whistleblower can report grievances within companies or externally to authorities.
- According to the case law of the German Federal Labour Court, the employee is initially obliged to submit the facts of the case for internal determination, pursuant to the employment contract. This obligation does not exist if internal determination cannot be expected of the employee. So, it is unreasonable if it is a serious offence or if the offence has been committed by the employer his or herself or his or her legal representatives, if the employee would make himself or herself liable to prosecution by not reporting the offence, or if the employer does not remedy the situation after having already received internal information.
- If a prior internal determination can be reasonably expected, a premature criminal complaint by the employee may constitute a reason for ordinary or extraordinary dismissal.
- An exception exists for certain financial service providers if malpractices are reported according to the provision in § 4 d of the Act on the Federal Financial Supervisory Authority (FinDAG) to a specific body within that authority, unless a false report was made deliberately or gross negligently.
- A conviction of the employer company or its legal representatives in subsequent criminal proceedings indicates that submitting the report was correct. However, even if the accusation made turns out to be incorrect subsequently, it may not always be considered that the employee breached his/her contractual obligations. This is only the case if the employee knew or could easily have known that the facts were incorrect at the time the complaint was made.
- The employee must not suffer any disadvantage under civil law if, in criminal proceedings initiated by authorities ex officio, (s)he makes incorrect statements that are not knowingly untrue or carelessly misrepresented. Insofar he is only obliged to pay damages if he has filed the criminal complaint against better knowledge or recklessly without recognisable reason.

6. What legislative protection does that employee enjoy?

- Where the employee does not report to the external authorities criminal-law-relevant transactions until after an internal determination has been made, or reports prior to that in circumstances where waiting for internal determination appears unreasonable to him, he is entitled to protection against dismissal pursuant to §§ 1 ff KSchG and disciplinary measures pursuant to § 612 a BGB.
- The primary legal consequence of protection against disciplinary action pursuant to § 612 a BGB is that any measures taken against the employee are null and void. Such measures are unlawful and do not have to be adhered to by the employee. In addition, the employee may demand that the employer revokes the measure and prevents recurrence. If the employee has suffered financial loss as a result of the measure, he may claim compensation from the employer.

Anti-bribery and corruption

7. What are the main anti-corruption laws and regulations in your jurisdiction?

Strafgesetzbuch (Criminal Code), specifically, §§ 298, 299, 333 und 334 Strafgesetzbuch.

8. Does the legislation have extra-territorial effect?

To some extent, where the offence has a connection with a German territory or German nationals.

9. What are the main enforcement bodies?

Staatsanwaltschaft.

Internal investigations

10. Is there any duty to report the issue, for example to a regulator?

- That depends on the issue. As a rule of thumb, there is no obligation to disclose any breach.
- Exceptions are expressively stated in the law. e.g. regarding taxes and customs duties, companies are obliged to provide the authorities with the results of an internal investigation where the result indicated an incorrect notification of duties (§ 153 Abgabenordnung).

11. What is the protection from disclosure for documents generated as part of the investigation (for example, privilege)?

Specific protection for documents generated as part of the investigation does not exist, except in relation to client-attorney correspondence. Such documents should be marked "Confidential and privileged".

12. Is the advice given by an in-house lawyer in relation to the investigation privileged and/or confidential?

The advice of an in-house-lawyer is neither confidential nor privileged. Thus, it can be seized by the authorities. Whether or not authorities have to treat information as confidential, ie are not entitled to publish it, depends on the author of such information.

Contact details

SKW Schwarz Rechtsanwälte

Oliver Korte, Rechtsanwalt
SKW Schwarz Rechtsanwälte
Direct line: +49 403 3401-41
o.korte@skwschwarz.de

Notes

1. § 40 BDSG
2. § 43 BDSG

Back to contents>

Hong Kong

When a crisis arises, which regulatory bodies do I need to notify and what is the relevant legislation?

Data breach

1. On discovering a data breach, which regulators or other government agencies should be notified?

The Privacy Commissioner for Personal Data is the responsible party for any matter related to data breach.

2. What legislation, relating to both criminal offences and civil wrongs, covers such a breach?

Personal Data (Privacy) Ordinance (Cap. 486) is the main ordinance governing the rights of a person in relation to personal data. Any non-compliance with the data protection principles enshrined in the ordinance does not automatically constitute a criminal offence. The Commissioner for Personal Data may serve an enforcement notice against the data user to remedy the contravention/non-compliance.

Contravention of an enforcement notice is an offence which could result in a maximum fine of HK$50,000 and imprisonment for 2 years.

Any affected individual party can initiate a civil action to seek compensation from the data user concerned.

"Dawn" raids

3. What agencies have the power to conduct dawn raids on private sector companies?

- The Hong Kong Police Force
- The Independent Commission Against Corruption (**ICAC**)
- The Securities and Futures Commission (**SFC**) and
- The Competition Commission (**CC**)

all have the power to gain entry and search private premises for investigations.

4. What legislation gives those agencies the power to undertake those inspections?

- The Independent Commission Against Corruption Ordinance (Cap 204)
- Securities and Futures Ordinance (Cap 571) and
- The Competition Ordinance (Cap 619)

give the above authorities the power to undertake a 'dawn-raid'.

5. On what bases, including privilege and/or confidentiality, may such company refuse to permit the seizure of documents?

Legal professional privilege has two limbs:

- **Legal advice privilege** protects the concerned documents in the course of the investigation, which includes documents and communications made in confidence between the lawyer and the company
- **Litigation privilege** protects the documents made for the sole purpose of an actual contemplated litigation.

Whistleblowing

6. What are the circumstances under which an employee is entitled to protection when reporting an alleged wrongdoing?

In Hong Kong there is no comprehensive whistleblowing legislation but in general an employer cannot terminate an employment by reason of the employee giving evidence in proceedings or enquiry for the enforcement of the Employment Ordinance, or in any proceedings or enquiry in relation to safety at work.

7. What legislative protection does that employee enjoy?

The existing legislative measures in Hong Kong are fragmented and different legislation provides separate protection to employees. As illustrated above, the Employment Ordinance offers direct protection.

Also depending on the alleged wrongdoings, different legislation may offer different protection to the whistle-blower. A whistle-blower will be protected from civil liability for reporting any financial irregularities or non-compliance with any financial resources rules which occurred in the company under the Securities and Futures Ordinance. And for any wrongdoings persecuted under the Prevention of Bribery Ordinance, the identity of the whistle-blower will be kept confidential and the whistle-blower may be entitled to witness protection under the Witness Protection Ordinance.

Anti-bribery and Corruption

8. What are the main anti-corruption laws and regulations in your jurisdiction?

The Prevention of Bribery Ordinance is the main legislation in this area of law.

9. Does the legislation have extra-territorial effect?

The Prevention of Bribery Ordinance lacks an explicit offence which gives extra-territorial effect. The limitation of the extraterritorial effect of the legislation is confirmed in the case *HKSAR v. Krieger & Anor.* (06/08/2014, FAMC1/2014), which holds that a bribe offered outside Hong Kong, although being mainly conspired in Hong Kong, is insufficient.

10. What are the main enforcement bodies?

The Independent Commission Against Corruption (ICAC) is the main enforcement body.

Internal investigations

11. Is there any duty to report the issue, for example to a regulator?

Employees owe a duty of good faith to the employer and such duty can also oblige an employee to disclose misconduct of fellow employees including assisting the employer to identify employees who have perpetrated acts of misconduct. However this duty does not, generally, impose a duty to disclose information incriminating the employee himself.

12. What is the protection from disclosure for documents generated as part of the investigation (for example, privilege)?

See above section on 'dawn raids' for the description of legal privilege available in Hong Kong.

13. Is the advice given by an in-house lawyer in relation to the investigation privileged and/or confidential?

Advice given by In-house lawyers is privileged in the same way as the advice given by external lawyers. Under recent case law, whether the advice by an in-house lawyer is privileged will be determined on the basis of whether or not the recipient of the advice is defined as 'client' and whether the in-house lawyers are acting in a legal rather than an executive capacity.

Contact details

Dorothy Siron
Zhong Lun Law Firm
Direct line: +852 2298 7620
dorothysiron@zhonglun.com

Back to contents>

India

When a crisis arises, which regulatory bodies do I need to notify and what is the relevant legislation?

Data breach

1. On discovering a data breach, which regulators or other government agencies should be notified?

- When a data breach occurs in India, any person, including a company affected by it, should report it to the Indian Computer Emergency Response Team (CERT-In) established under the Information Technology Act, 2000 within a reasonable time. Certain cyber security incidents, for example, compromise of critical systems or information, malicious code attacks, identity theft, DoS and DDos attacks, etc. are required to be mandatorily reported to CERT-In. The report can be communicated to the authority by telephone, fax, email, post and/or through CERT-In's website – www.cert-in.org.in.
- In the case of a data breach in a banking company or a non-banking financing company (NBFC), a report must be filed to the Reserve Bank of India (RBI) in a Security Incident Reporting (SIR) form by the company within two to six hours from the time of occurrence or on noticing such data breach. The SIR form requires particulars of the incident, specifically name of bank, details of incident, chronological order of events, etc. Further, a subsequent update must be sent to the RBI in Cyber Security Incident Reporting (CSIR) outlining further details of the breach.

2. What legislation, relating to both criminal offences and civil wrongs, covers such a breach?

- No legislation in India expressly defines data breach. However, The Information Technology Act, 2000 provides for protection to sensitive personal data or information as defined therein. It covers both civil wrongs and criminal offences. A company can be liable for a civil wrong when a breach of data is caused by its negligence in the implementation and maintenance of security protecting sensitive personal data or information which it owns, controls or operates. That failure must result in wrongful loss to the person whose data has been compromised or wrongful gain to the company causing the breach.
- A criminal breach of data is when any person, including a company, gains access to any material containing information about another person and discloses the same, without consent or in breach of a lawful service contract, to another person with an intent or with knowledge that the disclosure will cause wrongful loss to the person whose data has been compromised or wrongful gain to the person committing breach.

"Dawn" raids

3. What agencies have the power to conduct dawn raids on private sector companies? What legislation gives those agencies the power to undertake those inspections?

- **Competition Commission of India**: The Competition Act, 2002
- **Registrar of Companies**: Companies Act, 2013[1]
- **Central Board of Direct Taxes**: Income Tax Act, 1961
- **Food Safety and Standards Authority**: The Food Safety and Standards Act, 2006
- **Directorate of Enforcement**: The Foreign Exchange Management Act, 1999[2]; Prevention of Money-laundering Act, 2002[3]
- **The Police**: The Information Technology Act, 2000; The Code of Criminal Procedure, 1973; The Trademarks Act, 1999[4]

4. On what bases, including privilege and/or confidentiality, may such company refuse to permit the seizure of documents?

A company in India cannot be compelled to disclose confidential communication with its legal advisors unless such company offers itself as a witness before any court.[5] Privilege in India extends to the documents which have come into existence in anticipation of litigation for the purpose of seeking legal advice with the client's legal advisors.[6] However, privilege does not extend to in-house counsel employed by the company. Further, a company may refuse to permit the seizure of documents which are outside the scope of the warrant for search and seizure.

Whistleblowing

5. What are the circumstances under which an employee is entitled to protection when reporting an alleged wrongdoing?

India has enacted the Whistle Blowers Protection Act, 2011 (the Act); however, it is not yet in force. The Act provides protection for a whistle blower in circumstances where relevant disclosures are made by the employee under the Act in good faith. The disclosures must be accompanied by a personal declaration stating that the complainant reasonably believes that the information disclosed or the allegations made by him/her are substantially true. Such disclosures can be made in writing or by electronic mail message and must contain full particulars and supporting documents, together with other relevant materials, if any.

6. What legislative protection does that employee enjoy?

The employee blowing the whistle against their employer or rendering assistance in the inquiry into a whistleblowing investigation enjoys the following protection under the Whistle Blowers Protection Act, 2011:

- **Protection against victimisation** – An employee can file for redress before the competent authority under the Act in circumstances where that employee is being victimised
- **Protection of identity of the employee** – The competent authority under the Act is obligated to conceal the identity, documents and information furnished by the employee for the purpose of inquiry under the Act unless so decided by the competent authority or the court directs otherwise;
- **Protection of action taken in good faith** – No prosecution or suit or other proceeding can lie against an employee whose actions were undertaken in good faith or the intent was in good faith;
- The competent authority under the Act can issue appropriate directions to concerned authorities including police for protection of the employee if it is of the opinion that such employee needs protection.

Anti-bribery and corruption

7. What are the main anti-corruption laws and regulations in your jurisdiction? What are the main enforcement bodies?

- **The Prevention of Corruption Act, 1988**: Central Vigilance Commission
- **The Prevention of Money Laundering Act, 2002**: Directorate of Enforcement

8. What are the main enforcement bodies?

- **Central Bureau of Investigation** – investigates and prosecutes cases under the Prevention of Corruption Act, 1988 of undue advantage of or by public servant and the employees of Central Government, Public Sector Undertakings, Corporations or Bodies owned or controlled by the Government of India.
- **Enforcement Directorate** – investigates and prosecutes the offence of money laundering under the provisions of Prevention of Money Laundering Act, 2002 and takes actions for attachment or confiscation of property if the same is determined to be proceeds of the crime.

9. Does the legislation have extra-territorial effect?

- The Prevention of Corruption Act, 1988 applies to all the citizens of India, whether located in or outside India.
- The Prevention of Money Laundering Act, 2002 (the 2002 Act) is applicable to the Indian territory, and extends beyond India in the following circumstances:
  - where any act by a person outside India constitutes an offence in that place and such act would also be an offence under Part A, Part B or Part C of the 2002 Act had it been committed on the Indian territory and such person transfers the proceeds of such offence to India, or
  - where an offence has been committed under Part A, Part B or Part C of the 2002 Act and proceeds of such crime have been transferred, or an attempt has been made to transfer such proceeds or part thereof, to a place outside India.

Internal investigations

10. Is there any duty to report the issue, for example to a regulator?

Where an internal investigation has been undertaken into the affairs of a company, the company must report it a regulator in the following circumstances:

- **Regional Director** – Under the Companies Act, 2013 (the 2013 Act), an internal investigation may be initiated on receipt of information by the company itself; however, such reporting is not obligatory. A company may, by passing a special resolution, intimate to the Regional Director that its affairs ought to be investigated.[7] A company may also, subject to the provisions of the 2013 Act, make an application to the Regional Director for compounding of offences if the company is of the view that it has contravened any of provisions of the Act or rules or regulations made thereunder.[8]
- **Reserve Bank of India or Directorate of Enforcement** – The Foreign Exchange Management Act, 1999 (the 1999 Act) provides that a company may submit an application to the Reserve Bank of India or Directorate of Enforcement, as the case may be, for compounding of offence if the company is of the view that it has contravened any of the provisions of the Act, regulations, rules, notifications, directions or orders thereunder.[9]

11. What is the protection from disclosure for documents generated as part of the investigation (for example, privilege)?

- A company in India cannot be compelled to disclose confidential communications with its legal advisors, unless such company offers itself as a witness before any court.[10] Privilege in India extends to the documents which have come into existence in anticipation of litigation for the purpose of seeking legal advice with the client's legal advisors. However, privilege does not extend to any in-house counsel employed the company.
- A barrister, attorney, pleader or lawyer practicing in India is also barred from disclosing any communication made to him in the course and for the purpose of engagement by the company, except with the express consent of the company.[11]

12. Is the advice given by an in-house lawyer in relation to the investigation privileged and/or confidential?

In order to take advantage of client-attorney privilege in India, an attorney, pleader, barrister or lawyer must be a full-time practicing attorney. However, an in-house lawyer is a full-time employee of the company and therefore outside the protection of client-attorney privilege.[12]

Contact details

Dipak Rao
Singhania & Partners LLP
Direct line: +91 (11) 4747 1430
dipak@singhania.in

Notes

1. Section 208 of the Companies Act, 2013.
2. Section 37 of The Foreign Exchange Management Act, 1999.
3. Section 17 of the Prevention of Money-laundering Act, 2002.
4. Section 115 of The Trademarks Act, 1999.
5. Section 129 of the Indian Evidence Act, 1872.
6. *Larson & Tourbo Limited v Prime Displays (P) Ltd and Ors* 2002(5) BomCR158.
7. Section 210 of the Companies Act, 2013.
8. Section 441 of the Companies Act, 2013.
9. Section 15 of the Foreign Exchange Management Act, 1999.
10. Section 129 of the Indian Evidence Act, 1872.
11. Section 126 of the Indian Evidence Act, 1872.
12. Rule 49 of Chapter II – The Standards Of Professional Conduct And Etiquette, Part VI of the Bar Council of India Rules.

Back to contents>

New Zealand

When a crisis arises, which regulatory bodies do I need to notify and what is the relevant legislation?

Data breach

1. On discovering a data breach, which regulators or other government agencies should be notified?

- In New Zealand there is currently no mandatory requirement to report a data breach. However, there is legislation before Parliament which would introduce such a requirement. This legislation is likely to be passed, and to come into force in the second half of 2019.
- Voluntary disclosure of a data breach can be made to the Office of the Privacy Commissioner, which can provide information and guidance about dealing with the breach. If the data breach involves computer systems, it should also be reported to CERT NZ (Computer Emergency Response Team) which provides information and advice on how to respond and prevent further attacks, while also collating a profile of the threat landscape in New Zealand.

2. What legislation, relating to both criminal offences and civil wrongs, covers such a breach?

The Privacy Act 1993 deals with the collection and disclosure of personal information, and includes inadvertent disclosure.

"Dawn" raids

3. What agencies have the power to conduct dawn raids on private sector companies? What legislation gives those agencies the power to undertake those inspections?

- In addition to the New Zealand Police, there are a number of agencies in New Zealand that investigate corporate activities, and which may search premises under the authority of a search warrant issued by the court or an issuing officer. These include:
  - **Serious Fraud Office (which investigates and prosecutes serious or complex financial crime):** Serious Fraud Office Act 1990
  - **Financial Markets Authority** (which is responsible for enforcing securities, financial reporting and company law as they apply to financial services and securities markets, and the regulation of securities exchanges, financial advisers and brokers, auditors, trustees and issuers): Financial Markets Authority Act 2011
  - **Commerce Commission** (which enforces competition, fair trading and consumer credit contracts laws): Commerce Act 1986
  - **Inland Revenue Department**:(which collects taxes and investigates tax-related offending): Income Tax Act 2007
  - **New Zealand Security Intelligence Service** (which provides security and intelligence services to keep New Zealand and New Zealanders secure): Intelligence and Security Act 2017
  - **WorkSafe** (New Zealand's primary workplace health and safety regulator): Health and Safety at Work Act 2015
- Each agency is authorised to undertake searches under their own pieces of legislation.
- In addition, any person with a civil claim may, if that person has the grounds to do so (a strong prima facie case, serious loss or damage if the order is not granted, and sufficient evidence that the material will be destroyed or caused to be unavailable at a trial), request a court order for a civil search order. These orders (also known as Anton Piller orders) allow a person to seize specified items, and will be made on a without notice basis.
- The Search and Surveillance Act 2012 also governs both the New Zealand Police and other agencies, to standardise their powers.
- The New Zealand Bill of Rights Act 1990 places some limits on an agency's actions, by providing that "everyone has the right to be secure against unreasonable search or seizure, whether of the person, property, or correspondence or otherwise."

4. On what bases, including privilege and/or confidentiality, may such company refuse to permit the seizure of documents?

Documents may be withheld if they are privileged. This includes legal advice privilege, which covers communications between a person and their legal adviser if the communication was in respect of legal services and was intended to be confidential; and litigation privilege, which covers any communication or other information which is for the dominant purpose of dealing with litigation and the proceeding is either already on foot

or is anticipated. In New Zealand, the privilege against self-incrimination is only available to natural people, so a company cannot use this to avoid providing documents.

Whistleblowing

5. What are the circumstances under which an employee is entitled to protection when reporting an alleged wrongdoing?

- An employee of an organisation who reports serious wrongdoing is protected by the Protected Disclosures Act 2000, as long as:
  - the information is about serious wrongdoing in or by that organisation
  - the employee believes on reasonable grounds that the information is true or likely to be true
  - the employee wishes to disclose the information so that the serious wrongdoing can be investigated
  - the employee wishes the disclosure to be protected, and
  - the disclosure is made in the correct manner.
- The default position is that the employee must disclose information in accordance with the internal procedures for receiving and dealing with information about serious wrongdoing established by and published in the organisation. If the organisation has no published internal procedures for making the disclosure, or the employee believes that the person that they are required to report the serious wrongdoing to is him or herself involved or is otherwise an inappropriate person to report to, the employee may report the serious wrongdoing to the head or deputy head of the organisation.
- If the employee believes that the head of the organisation is involved in the serious wrongdoing, there is an element of urgency, or the organisation has taken no action within 20 working days after the disclosure was made, the employee may disclose the serious wrongdoing to an appropriate authority (and in some cases to a Minister of the Crown or the Ombudsman).
- There are special rules that apply to a disclosure relating to an intelligence and security agency or any other organisation which holds classified information, and to the disclosure of information concerning the international relations of the Government of New Zealand.

6. What legislative protection does that employee enjoy?

The Protected Disclosures Act 2000 provides that an employee who makes a disclosure:

- may raise a personal grievance if he or she suffers retaliatory action, including dismissal, from his or her employer
- has immunity from any civil or criminal proceeding which could otherwise have been brought by reason of having made the disclosure (such as a breach of confidence claim), and
- should have his or her identity kept confidential, unless disclosure is either required or consented to.

Anti-bribery and corruption

7. What are the main anti-corruption laws and regulations in your jurisdiction?

New Zealand's anti-corruption laws are primarily found in:

- **The Crimes Act 1961** – which criminalises bribery and corruption of New Zealand judges, government ministers, members of Parliament, police officers and other public officials, and makes it an offence corruptly to use official information or to trade in influence (for example, accept a bribe in return for using one's influence over an official)
- **The Secret Commissions Act 1910** – which contains bribery and corruption style offences relevant to the private sector (though also relevant to public sector employees and contractors), including the key corruption offence which criminalises the bribing of an agent, and

- **The Anti-Money Laundering and Countering Financing of Terrorism Act 2009** (AML/CFT Act) – which aims to assist in the detection and deterrence of money laundering and the financing of terrorism, by facilitating co-operation amongst reporting entities, AML/CFT supervisors, and various government agencies.

8. Does the legislation gave extra-territorial effect?

The Crimes Act 1961 criminalises the bribery of foreign public officials in the course of an international business transaction (which includes the provision of international aid). This offence captures bribes paid by New Zealand persons operating anywhere in the world, including the actions of intermediaries acting on behalf of a New Zealand business.

9. What are the main enforcement bodies?

The main enforcement bodies for breaches of the Crimes Act or the Secret Commissions Act are the New Zealand Police and the Serious Fraud Office. There can be a variety of regulators for the AML/CFT Act, but the principal one is the Department of Internal Affairs, which supervises lawyers, conveyancers, casinos, non-deposit taking lenders, money changers, money remitters, payroll remitters, debt collectors, factors, safe deposit box vaults, non-bank credit card providers, stored value card providers and cash transporters.

Internal investigations

10. Is there any duty to report the issue, for example to a regulator?

- A privately owned company is not required to report any issue or the existence of any internal investigation.
- However, a publically listed company must disclose any material information, being information that:
  - a reasonable person would expect to have a material effect on the price of the issuer's quoted securities, if that information were generally available to the market, and
  - relates to particular securities or issuers, rather than to securities or issuers generally.

11. What is the protection from disclosure for documents generated as part of the investigation (for example, privilege)?

Correspondence between the company and their legal advisor related to the investigation would generally be privileged, as long as the correspondence was for the purpose of obtaining or providing legal advice, and was intended to be kept confidential (not disseminated to the public). This privilege will generally not extend to documents generated by any other third party as part of the investigation.

12. Is the advice given by an in-house lawyer in relation to the investigation privileged and/or confidential?

Advice given by an in-house lawyer will usually have the same level of privilege as that of external counsel, as long as the in-house counsel continues to hold a current practicing certificate. However, the advice must be legal advice, and where in-house counsel are involved there is often greater consideration given to whether the advice was legal advice or general commercial advice.

Contact details

Duncan Cotterill

Jonathan Scragg
Duncan Cotterill
Wellington
Direct line: +64 4 471 9422
Mobile: +64 21 878 972
jonathan.scragg@duncancotterill.com

Rob Coltman
Duncan Cotterill
Auckland
Direct line: +64 9 374 7187
Mobile: +64 29 915 2417
rob.coltman@duncancotterill.com

Back to contents>

Scotland

When a crisis arises, which regulatory bodies do I need to notify and what is the relevant legislation?

Data breach

1. On discovering a data breach, which regulators or other government agencies should be notified?

- **UK Information Commissioner's Office (ICO)** – any organisation which is a controller of personal data has a responsibility to report personal data breaches to the ICO within 72 hours unless it concludes that the breach will be unlikely to pose a risk to the individuals concerned.
- **Essential services** – providers of services in the energy, transport, health, water and digital infrastructure sectors, must notify significant network and information systems incidents, for example cyber-attacks, to **competent authorities** designated under the Network and Information Systems Regulations 2018.
- **Other sectors** – other regulated industries are required to report breaches involving personal data to their sector regulator eg duty on financial services institutions to report data security breaches to the **UK Financial Conduct Authority**.
- **National Cyber Security Centre** – part of the UK Government's GCHQ, the NCSC. While there is no legal obligation to notify the NCSC about an incident, the NCSC encourages early engagement so that it can provide advice and assistance to victim organisations. The NCSC does not share information with the ICO or other regulators unless the victim organisation requests that it does so.

2. What legislation, relating to both criminal offences and civil wrongs, covers such a breach?

Relevant legislation in this area includes:

- The Data Protection Act 2018: this covers civil wrongs and criminal offences. The main criminal offence that relates to data breaches is unlawfully obtaining or disclosing personal data without the consent of the controller.
- The Privacy and Electronic Communications Regulations 2003
- The Network and Information Systems Regulations 2018
- The Electronic Identification and Trust Services for Electronic Transactions Regulations 2016
- Financial Services and Markets Act 2000

"Dawn" raids

3. What agencies have the power to conduct dawn raids on private sector companies? What legislation gives those agencies the power to undertake those inspections?

- **The European Commission**: EC Regulation 1/2003
- **Competition and Markets Authority**: Enterprise Act 2002 ; Competition Act 1998
- **Serious Fraud Office**: Criminal Justice Act 1987
- **The Police**: Serious Organised Crime and Police Act 2005
- **HM Revenue & Customs**: Serious Organised Crime and Police Act 2005
- **Revenue Scotland**: Revenue Scotland and Tax Powers Act 2014
- **Prudential Regulation Authority**: Financial Services and Markets Act 2000
- **Financial Conduct Authority**: Financial Services and Markets Act 2000
- **Information Commissioners Officer**: Data Protection Act 2018
- **Health and Safety Executive**: Health and Safety at Work etc. Act 1974
- **Scottish Environment Protection Agency**: Environment Act 1995

4. On what bases, including privilege and/or confidentiality, may such company refuse to permit the seizure of documents?

Investigators are not entitled to review documents which are privileged, or outside the scope of the warrant or authorisation held by the investigators, for example due to their date or subject matter (see questions 11 and 12 for more information on privilege). Common practice is for disputed documents to be placed in sealed envelopes so that the question of privilege or scope may be considered after the raid. Documents cannot be withheld from investigators on the grounds of commercial confidentiality or sensitivity.

Whistleblowing

5. What are the circumstances under which an employee is entitled to protection when reporting an alleged wrongdoing?

A worker is entitled to legal protection if they have made a "qualifying protected disclosure" but certain conditions must be met. Firstly, the worker must make a disclosure of information. Gathering evidence or threatening to make a disclosure is not enough for protection to apply.

Secondly, the information must fall under one of the six types of "relevant failure". These are:

- Criminal offences
- Legal obligation breach
- Miscarriages of justice
- Dangers to health and safety
- Damage to the environment and
- Deliberate concealing of information about the above.

Thirdly, the worker must have a reasonable belief that the information shows one of the relevant failures and that the disclosure is in the public interest.

Whether a qualifying disclosure is protected also depends on who the disclosure is made to.

6. What legislative protection does that employee enjoy?

Workers are protected under the Employment Rights Act 1996 as follows: the right not to be subjected to any detriment, such as facing disciplinary action, or being bullied or harassed, on the ground that they have made a protected disclosure. Claims can be made against the employer and/or against other workers individually.

The dismissal of an employee will be automatically unfair if the principal reason for the dismissal is that they have made a protected disclosure.

Anti-bribery and corruption

7. What are the main anti-corruption laws and regulations in your jurisdiction?

The UK-wide Bribery Act 2010 ("the Act") sets out four principal corruption offences, the most significant for corporates being failure of a commercial organisation to prevent bribery. The Act applies to both public and private sector bribery. A commercial organisation has a statutory defence if it can prove that it had "adequate procedures" in place to prevent bribery.

8. Does the legislation have extra-territorial effect?

The offences apply to those with a close connection to the UK wherever they are located. If a commercial organisation operates a business, or part of a business, in Scotland, the Act applies to its global operations and the entity can be prosecuted in Scotland for bribery conducted by it or on its behalf in another jurisdiction. Associated persons acting on behalf of the corporate anywhere in the world can expose the corporate to criminal prosecution in Scotland if the bribe is to obtain or retain a business advantage for the corporate.

9. What are the main enforcement bodies?

In Scotland, bribery offences are enforced by **the Crown Office and Procurator Fiscal Service** which is the sole prosecutorial authority in Scotland. **Police Scotland** conducts investigations into allegations of bribery in Scotland.

Internal investigations

10. Is there any duty to report the issue, for example to a regulator?

Self-reporting obligations will vary according to the sector in which the business operates and what obligations it has under any relevant regulatory regime, as well as the nature and seriousness of the issue itself.

The main bodies to consider are:

- **Crown Office and Procurator Fiscal Service** – there is no obligation to self-report fraud, bribery or corruption. The Crown Office operates a self-reporting regime for Bribery Act and older corruption offences.

Self-reporting may result in civil recovery rather than criminal prosecution.

- **National Crime Agency** – the Proceeds of Crime Act 2002 and the Terrorism Act 2000 place obligations on regulated sectors to make a Suspicious Activity Report to the NCA if there is a suspicion of money laundering, and this should be made as soon as possible to the NCA (online reporting systems/templates available).
- **Competition and Markets Authority** – self-reporting is not mandatory but issues of possible competition law infringements can be self-reported to the CMA under its leniency programme -the first company to report may obtain a reduction or immunity from a fine (though not from possible civil claims). Timing is critical. The CMA will not grant immunity from criminal prosecution.
- **Financial Conduct Authority** – the FCA's Supervision Manual imposes self-reporting obligations on FCA-authorised financial services companies for issues including fraud (victims must report too) or other circumstances which could have a significant adverse impact on the firm's reputation or customers, or on the UK financial system.
- **Information Commissioner's Office** – see section 1.
- **Publicly Listed Companies** – must make public announcements in respect of certain non-public information which, if released, would have the potential to significantly impact the value of the company's shares.

11. What is the protection from disclosure for documents generated as part of the investigation (for example, privilege)?

Documentation generated in the course of an investigation can be protected from disclosure if the criteria for asserting legal privilege are met. There are two sub-heads of privilege:

- **Legal advice privilege** applies to all communications between a lawyer and client for the purpose of obtaining/receiving legal advice. In a corporate context, it is important to clearly define who is "the client" by ensuring that those seeking/receiving legal advice have explicit authority to do so on behalf of the entity.
- **Litigation privilege** can protect both communications and other documentation if: (i) litigation is reasonably in contemplation; (ii) the document's dominant purpose is that litigation; and (iii) the litigation is adversarial in nature. Privilege can only apply if all criteria are met when the document is created. Litigation privilege can apply to documentation created by third parties if it has been instructed by the client or the lawyer and meets the criteria.

Privilege can be lost or waived unless arrangements are made to maintain privilege once it has been established. Importantly, until there is a real likelihood of adversarial litigation, only legal advice privilege may apply which does not protect as broad a spectrum of documentation as litigation privilege.

12. Is the advice given by an in-house lawyer in relation to the investigation privileged and/or confidential?

If the criteria in section 11 are met, privilege may apply but care should be taken in communications between in-house lawyers and employees without explicit authority to seek legal advice. In European Commission investigations, in-house lawyers' advice, and that of lawyers located outside the EU, is not privileged.

Contact details

Paul Marshall
Brodies
Direct line: +44 131 656 0062
Mobile: +44 7581 064 801
paul.marshall@brodies.com

Back to contents>

Slovakia

When a crisis arises, which regulatory bodies do I need to notify and what is the relevant legislation?

Data breach

1. On discovering a data breach, which regulators or other government agencies should be notified?

The Office for Personal Data Protection (the OPDP) in Bratislava leads investigations into actual and potential data breaches. All data breaches must be notified to the OPDP.

2. What legislation, relating to both criminal offences and civil wrongs, covers such a breach?

- Data breaches are regulated by Regulation (EU) 2016/679 of the European Parliament and of the Council, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR) – specifically Articles 33, 34, 77 and Act No. 18/2018 Coll. on Personal Data Protection, and Act No. 351/2011 Coll., on Electronic Communications, Article 55 et seq.
- In addition, a data subject may raise claims under Act No. 40/1964 Coll., Civil Code, as amended – under Article 11 et seq. (Personality rights of an individual).
- Data breaches may also be considered crimes under Act No. 300/2005 Coll., Criminal Code, as amended – Articles 264 (Endangering of Trade, Banking, Postal, Telecommunications and Tax Secrets), 374 (Unauthorised Use of Personal Data), 376 (Harm Done to Rights of Another – in relation to a breach of secrecy of private records or documents), 377 (Violation of the Confidentiality of Spoken Conversation and other Personal Expression), 247 (Unauthorised Access to Computer Systems) and 265 (Misuse of Information in Business Relations).
- A company may be liable for committing crimes under articles 247 and 265, of the Criminal Code, as described above, and under Act No. 91/2016 Coll., on the Criminal Liability of Legal Entities, as amended.

"Dawn" raids

3. What agencies have the power to conduct dawn raids on private sector companies? What legislation gives those agencies the power to undertake those inspections?

- The Antimonopoly Office of the Slovak Republic (the Office) in Bratislava can lead any investigations into potential breaches of competition (specifically in relation to prohibited agreements between companies).
- Dawn raids are led by the Office **in general** in accordance with Act No. 136/2001, on the Protection of Competition, as amended (the Competition Act); the Competition Act contains comprehensive procedural rules, specifically in articles 22 and 22a, with additional application of some complementary provisions from Act No. 71/1967 Coll., on Administrative Procedures, as amended (as a general procedural Act).
- The Office may also directly apply articles 101 and 102 of the Treaty on the Functioning of the European Union in individual cases, should the investigated behaviour have an impact on the European market.

4. On what bases, including privilege and / or confidentiality, may such company refuse to permit the seizure of documents?

- As a general rule, during the investigation, organisations must provide the Office with the assistance necessary to perform its powers. The Office's officials are entitled to obtain access to business premises, open locked cabinets or cases, or otherwise gain access to business records. Every person in the business's premises must submit to the investigation; if this obligation is not fulfilled, the Office's officials shall be entitled to obtain access, including with the assistance of locksmiths or the Police. If access is not granted, severe sanctions may be imposed on the company, ie up to 5% of the net early turnover depending on the type of breach (cf. article 38a(2) of the Competition Act).

- The Office's officials, or anyone authorised by that office, may verify whether documents and records are business records, inspect business records found on, or accessible from, business premises, regardless of the format in which they are stored (ie in safes, hidden drawers, etc), copy or acquire copies or extracts from, business records in any form. All of these prerogatives need to pertain exclusively to the defined scope of the investigated case.
- If the Office cannot make copies, or otherwise gain the relevant information during the inspection due to technical reasons, it **is entitled, only for the time necessary for making such copies/gaining such information**, to seize originals of documents or to take those documents off the business premises. The Office has the right to make copies of any documents.
- A company **may refuse to submit** any documentation that is covered by Attorney-Client privilege, and is thus labelled and recognizable. The Office's officials must stop investigating any document that is covered by this privilege immediately after being alerted to it by the company, or when realizing it by the nature of the examined document.
- A company **may also label any information** that is being provided to the Office **as confidential information** or a **trade secret**. Officials from that office must keep confidential such information, even after terminating his/her working relationship with the Office. However, such company, if requested by the Office, must submit a version of any document without the confidential information or trade secret. **Confidentiality and trade secrets are not legitimate reasons for failing to provide the Office with access to specific documents**.

Whistleblowing

5. What are the circumstances under which an employee is entitled to protection when reporting an alleged wrongdoing?

- Protection for employees is provided by Act No. 307/2014 Coll. on Certain Measures Related to the Reporting of Anti-Social Activities (the "Anti-Social Activities Reporting Act"); it applies to both the private and public sectors.
- An employee is entitled to protection if a report is made in good faith, and he or she learned of the reported facts in the performance of his/her work or function, and that report may assist in resolving "serious anti-social activities" or finding or convicting the offender. The protection also applies to persons close to the employee if they are employed by the same employer.
- Serious anti-social activities are:
  - specific crimes listed in the act, relating to corruption, manipulation in public procurement, etc
  - all crimes for which a maximum custodial penalty of more than three years pursuant to the Criminal Code may be imposed
  - administrative offences for which a maximum penalty of more than 50,000 EUR may be imposed.
- Reports on other anti-social activities are considered non-serious.

6. What legislative protection does that employee enjoy?

- If reporting a non-serious anti-social activity, the employee may file a complaint with the Labour Inspectorate if he or she faces penalties or discrimination.
- An employee reporting a serious anti-social activity can apply for protection even before any retaliation occurs. Such request must be filed with the relevant competent authority, depending on the nature of the reported activity/activities. The protection takes the form of a prohibition on the employer from making decisions relating to the employment of the reporting employee without the prior consent of the Labour Inspectorate, unless the employee agrees with those decisions. If an act is made without this consent, it is considered void.
- Another form of protection is granted to all employees reporting anti-social activities under this act following an internal regulation of the employer.
- If a person who filed a report following an internal regulation of the employer deems that a legal act related to their employment, with which they do not agree, was taken due to the report, they may request that the Labour Inspectorate suspend the effects of such act within a 7-day period. If the request is approved, the suspension of the legal act remains

effective for 14 days from the delivery of the approval to the employee concerned. Within this period, the employee has the opportunity to file for a preliminary measure with the competent tribunal. In such case, the legal act remains suspended until the tribunal decides on the preliminary measure.

Anti-bribery and corruption

7. What are the main anti-corruption laws and regulations in your jurisdiction?

- Constitutional Act No. 357/2004 Coll. on the Protection of Public Interest in the Performance of Functions of Public Officials
- Act No. 300/2005 Coll., the Criminal Code
- Act No. 91/2016 Coll., on the Criminal Liability of Legal Entities
- Act No. 343/2015 Coll., on Public Procurement
- Act No. 297/2008 Coll., on the Prevention of Legalisation of Proceeds of Criminal Activity and Terrorist Financing
- Act No. 394/2012 Coll., on Restrictions on Cash Payments

8. Does the legislation have extra-territorial effect?

- In general no; however, the Slovak Criminal Code may, subject to certain conditions, apply to crimes committed outside Slovakia. A criminal offence shall be deemed committed in the territory of the Slovak Republic, and thus assessed pursuant to the Slovak Criminal Code, also in the following cases:
  - the offender committed the act in the Slovak Republic, either in part or entirely, although the violation or endangering of an interest protected by Slovak criminal law occurred, or was supposed to occur, either in whole or in part, outside of the Slovak Republic territory, or
  - the offender committed an act outside the territory of the Slovak Republic, however the violation or endangering of an interest protected by this Act was intended to take place, or such a consequence was supposed to occur, either entirely or partially, in its territory, or
  - the act was committed outside the territory of the Slovak Republic, aboard a vessel sailing under the State flag of the Slovak Republic or aboard an aircraft registered in the Aircraft Registry of the Slovak Republic.
- The criminality of acts of Slovak citizens or aliens with permanent residence in the Slovak Republic committed abroad shall also be assessed pursuant to the Slovak Criminal Code.

9. What are the main enforcement bodies?

Currently, the investigation of corruption/bribery cases is entrusted to the National Criminal Agency's National Anti-Bribery Unit. From an organisational perspective, the National Anti-Bribery Unit is a specific unit of the Police; otherwise, criminal investigation proceedings follow standard rules.

Internal investigations

10. Is there any duty to report the issue, for example to a regulator?

- The duty to report identified cases of corruption/bribery applies to all persons. In fact, if someone learns in legitimate circumstances that another person committed any criminal offences relating to corruption/bribery and fails to report such crime or criminal offence immediately to the law enforcement authorities or the Police, they shall be punished by a prison sentence of up to three years. Please note that exemptions apply, such as a legally-recognised confidentiality duty or if the person is not able to report the crime without putting themselves or a close person in danger of death, bodily harm or other grievous harm, or criminal prosecution.
- Moreover, the Anti-Social Activities Reporting Act requires employers who (i) are a public authority body or (ii) employ at least 50 employees, to implement a specific internal system for the investigation of anti-social activities (these may include corruption/bribery).
- Such employer must, in particular, (i) designate a person (even an external person) or organisational unit to be entrusted with the performance of duties

under the Anti-Social Activities Reporting Act, eg, the receiving, investigating and keeping of records of notifications about (serious) anti-social activities and (ii) adopt an internal regulation governing the details of the procedure.

- Nevertheless, no duties are set out in the Act itself on how to deal with an identified case of corruption/bribery. The general reporting duty should apply also in this case to all persons aware of the corruption/bribery in a "credible manner".

11. What is the protection from disclosure for documents generated as part of the investigation (for example, privilege)?

- There is no specific regulation covering documents generated as part of an internal investigation. Nevertheless, generally binding legislation, especially concerning personal data, must be respected.
- The rules for handling personal data within the course of an internal investigation may be specified in an internal regulation. However, it is expressly stated that the employer keeps confidential the identity of the person notifying the anti-social activities.

12. Is the advice given by an in-house lawyer in relation to the investigation privileged and/or confidential?

- There is no regulation regarding the advice given by an in-house lawyer (not an attorney-at-law) in relation to an investigation so this advice should not, in the absence of specific circumstances of the case such as a bank secret, be considered privileged or confidential.
- Communication in relation to an investigation between a client company and an external lawyer – an attorney-at-law/attorney clerk registered with the Slovak Bar Association, is protected by attorney privilege and must be kept confidential by the external lawyer.

Contact details

PETERKA PARTNERS
THE CEE LAW FIRM

Ms Kristina Nankova
Peterka & Partners (Slovakia)
Direct line: +420 225 396 854
nankova@peterkapartners.sk

Back to contents>

Switzerland

When a crisis arises, which regulatory bodies do I need to notify and what is the relevant legislation?

Data breach

1. On discovering a data breach, which regulators or other government agencies should be notified?

- Swiss law does not require organisations to report data breaches to either the Swiss authorities or data subjects. However, in the case of data subjects, different obligations may exist pursuant to any contract between the parties (eg employment or agency) or under the principles of good faith, transparency and duty of loyalty to the client.
- Under the proposed amendments currently being considered in Parliament to the Swiss Federal Data Protection Act (DPA), data controllers would be responsible for reporting any data breaches to the Federal Data Protection and Information Commissioner (FDPIC) as well as to the affected data subjects. Specifically, the data controller would need to inform the FDPIC of breaches likely to pose a high risk to an individual's rights.

2. What legislation, relating to both criminal offences and civil wrongs, covers such a breach?

- Data protection issues are generally regulated under the Swiss Federal Data Protection Act (DPA) and Federal Data Protection Ordinance (DPO); however, the DPA does not set forth criminal or civil penalties specifically for data breaches.
- Violations of related obligations under the Swiss Code of Obligations (SCO), including the duty of care and loyalty (Art. 321a SCO), duty of care and faithful performance (Art. 398 SCO) or business secrecy, may result in civil proceedings. Furthermore, criminal sanctions may be imposed for violations of professional confidentiality obligations (Art. 35 DPA), protection of business secrets (Art. 162 SCC), breach of banking secrecy (Art. 47 of the Swiss Banking Act) and breach of professional secrecy (Art. 321 SCC).

"Dawn" raids

3. What agencies have the power to conduct dawn raids on private sector companies? What legislation gives those agencies the power to undertake those inspections?

- **All cantonal and federal criminal prosecution authorities (ie the cantonal and federal police, the cantonal prosecution offices, the Office of the Attorney General (OAG) and the cantonal and federal courts)**: Swiss Criminal Procedure Code (SCPC) and Federal Act on the Organization of Criminal Authorities
- **The Federal Tax Administration**
- **The Swiss Competition Commission (COMCO)**: Federal Cartel Act
- **The Federal Customs Administration** (within border areas).

4. On what bases, including privilege and / or confidentiality, may such company refuse to permit the seizure of documents?

- Right of refusal to testify for one's own protection (right against self-incrimination) or that of a relative (Art. 248(1) cum 113(1), 158(1)(b), 168, 169 and 180(1) SCPC)
- Attorney privilege (Art. 248(1) cum 171 SCPC)
- Official secrecy (for officials and members of public authorities) (Art. 248(1) cum 170 SCPC)
- Any business, trade or commercial secrets or right of privacy (eg private correspondence, medical documents), which override the interest in establishing the truth (Art. 248(1) cum 173(2) SCPC).

Whistleblowing

5. What are the circumstances under which an employee is entitled to protection when reporting an alleged wrongdoing?

- For the time being, there is no whistleblowing regulation in Switzerland and employees who report corporate wrongdoing are generally not protected under Swiss law. In fact, disclosure of alleged wrongdoing directly to the authorities or to the public may result in both criminal liability, for instance in violation of business secrecy (Art. 162 SCC) or banking secrecy (Art. 47 of the Swiss Banking Act), as well as civil liability for violating the duty of loyalty to the employer (Art. 321 SCO).

- In September 2018, the Swiss government re-submitted to the Parliament a supplementary, partial revision to the SCO proposing clear procedures and rules for reporting wrongdoing to organisations and the responsible authorities.

6. What legislative protection does that employee enjoy?

- As stated above, Swiss law does not grant specific protection to employees who report wrongdoing directly to the authorities. The partial revision to the Swiss CO details the situations in which reporting to the employer, the authorities or public are permitted. At present, those unlawfully dismissed in retaliation for whistleblowing, or who refuse to commit a criminal act, would only be entitled to remedies under Swiss employment law.
- For bank employees and representatives, a breach of professional confidentiality ("Swiss banking secrecy"), even under the auspices of whistleblowing, can result in a sentence of up to 3 years in prison or fines up to a maximum 360 daily penalty units at a cap of 3,000 Swiss Francs per unit.
- The proposed revision of Art. 321a SCO sets forth a three-step reporting system, first to the reporting employer, then to the responsible authorities and finally to the public. Provided that certain conditions are met, the employee would be protected from civil penalties as well as retaliatory measures by the employer.

Anti-bribery and corruption

7. What are the main anti-corruption laws and regulations in your jurisdiction?

- The Swiss Criminal Code (SCC) covers bribery of public officials (Art. 322ter, quarter and septies SCC) and bribery in the private sector (Art. 322^{octies} and 322^{novies} SCC)
- Private commercial bribery within the context of the distortion of competition is covered by Art. 4a of the Federal Act on Unfair Competition
- The Federal Act on Foreign Illicit Assets (FIAA) also covers the freezing, confiscation and restitution of assets obtained unlawfully and deposited in Switzerland by foreign potentates who have been or are about to be ousted.

8. Does the legislation have extra-territorial effect?

Yes. The SCC may apply to foreign companies if the matter is sufficiently related to Switzerland to establish Swiss jurisdiction. A foreign parent company may thus for example be sanctioned under the corporate offence up to a fine of CHF 5m (Art. 102(2) SCC) if an employee of its Swiss subsidiary committed an act of bribery, provided that the foreign parent company has not taken all adequate and necessary measures to prevent the misconduct.[1]

Bribery of foreign officials and employees is also considered a criminal offence (Art. 322^{septies} SCC).

9. What are the main enforcement bodies?

The OAG is competent to investigate the misconduct if it involves federal authorities or if the suspected crime has been committed abroad. Otherwise, the case falls within the competence of the cantonal public prosecutors.

Internal investigations

10. Is there any duty to report the issue, for example to a regulator?

- There is no obligation on organisations to self-report suspected misconduct and no statutory framework for self-reporting.
- Statutory duties to self-report legal risks apply in specific cases (which have not yet been tested in court). For instance:
  - Members of the board of directors and the executive committee of an undertaking should conduct an internal investigation in cases of suspected or actual (material) misconduct (eg bribery of foreign officials), as part of the duty of care and loyalty imposed upon them (eg Art. 717 SCO)

- Based on the Financial Market Supervision Act (FINMASA), supervised persons and entities (eg financial intermediaries and traders) as well as their auditors must disclose to the Swiss Financial Market Supervisory Authority (FINMA) any incident that is of material importance for supervisory purposes, such as the suspicion of money laundering involving significant assets or any incident that may have an impact on the institution's or the financial market's reputation[2]
- The Cartel Act specifically outlines self-reporting and the leniency an applicant may receive, including full immunity from fines. Applications are typically filed with the COMCO's Secretariat within the first hours of an investigation.

11. What is the protection from disclosure for documents generated as part of the investigation (for example, privilege)?

If an organisation decides to self-report misconduct and disclose information in the absence of a legal obligation, it must comply with:

- The DPA, which requires personal data (ie all data relating to a natural or legal person) to remain confidential. Personal data resulting from internal investigations may only be disclosed if a statutory exception applies or if the data subject provides a waiver
- Its duties under employment law, in particular its duty of care towards its employees, according which it shall ensure the latter's privacy (Art. 328 SCO)
- With respect to privilege, all work product (memoranda, reports, correspondence or interview notes) related to the "typical" activity of a registered lawyer (by contrast to non-registered lawyers or in-house counsel), ie fact-finding and related legal advice, carried out within the context of an internal investigation are in principle protected by privilege and may thus be withheld from the authorities. Privilege shall however not apply if (i) invoking it constitutes an abuse of right (eg the use of a registered lawyer was solely intended to hide proceeds of the offences or means of evidence)[3] and if (ii) the tasks assigned to the registered lawyer are equivalent to a delegation, by the undertaking, of its compliance-related obligations under specific laws (eg a bank has in effect delegated to its external counsel its duties of compliance, controlling and auditing as set forth by the Anti-Money Laundering Act (AMLA) and its relevant ordonnance).[4]

12. Is the advice given by an in-house lawyer in relation to the investigation privileged and/or confidential?

The answer depends on the applicable procedure. The issue is debated within the legal doctrine as it has not been decided by the Swiss Supreme Court yet. Some scholars consider that privilege may apply to in-house lawyers (i) admitted to the bar, in relation to (ii) their legal advice and/or (iii) information and documents entrusted and available to him/her only, while others see that privilege shall only apply to lawyers currently registered with the bar. There is currently a legislative proposal to clarify privilege for in-house counsel and the issue is being considered in Parliament.

Contact details

LALIVE

Daniel Lucien Bühr
Lalive
Direct line: +41 58 105 2100
dbuhr@lalive.law

Notes

1. See OAG criminal order of 22 September 2011 against Alstom Network Schweiz AG, acting on behalf on Alstom Group.
2. Art. 9(2) FINMASA, and, for instance, Section 4.5. of FINMA position paper of 22 October 2010 on legal and reputational risks in cross-border financial services.
3. Swiss Supreme Court Decision dated 11 September 1991 (case reference: 117 Ia 341) and
4. Swiss Supreme Court Decisions dated 20 Septembre 2016 (case reference: 1B_85/2016) and 21 March 2018 (case reference: 1B_433/2017) and the decision of the Supreme Criminal Court dated 13 September 2018 (case reference: BB.2018.3).

Back to contents>

Turks and Caicos Islands

When a crisis arises, which regulatory bodies do I need to notify and what is the relevant legislation?

Data breach

1. On discovering a data breach, which regulators or government agencies should be notified?

None. See below.

2. What legislation, relating to both criminal offences and civil wrongs, covers such a breach?

There is no legislation which criminalizes data breach and no statutory provisions in respect of civil wrongs arising from such breach. There is no free standing legislation regulating the disclosure of personal data and no regulatory body. Under the Electronic Transactions Ordinance, power is given to the Minister of Communications for prescribing standards for the processing of personal data by data controllers but no standards have been prescribed.

"Dawn" raids

3. What agencies have the power to conduct dawn raids on private sector companies? What legislation gives those agencies the power to undertake those inspections?

The Royal Turks and Caicos Islands Police Force, Integrity Commission, and Department of Customs: The Police Force Ordinance, Integrity Commission Ordinance, Customs Ordinance and Proceeds of Crime Ordinance.

4. On what bases, including privilege and/or confidentiality, may such company refuse to permit the seizure of documents?

An organisation may refuse to permit seizure if the search/seizure is not covered by a warrant properly issued and/or the documents are covered by legal professional privilege. Confidentiality is not sufficient grounds for refusing search and seizure.

Whistleblowing

5. What are the circumstances under which an employee is entitled to protection when reporting an alleged wrongdoing?

Public sector officials are entitled to protection if they make a protected disclosure in good faith. A protected disclosure is a disclosure:

(a) that a criminal offence has been committed, is being committed or is likely to be committed

(b) that a person has failed, is failing or is likely to fail with a legal obligation to which he is subject

(c) that a miscarriage of justice has occurred, is occurring or is likely to occur

(d) that the health or safety of an individual has been, is been or is likely to be endangered

(e) that the environment has been, is being or is likely to be damaged, or

(f) that information tending to show a matter within any of paragraphs (a) to (e) has been, is being or is likely to be deliberately concealed.

A person, whether a public officer or not, also benefits from protection if (s)he discloses to the Integrity Commission that another person has committed is committing or is about to commit an offence of bribery. Private sector employees are protected against victimization for making complaints or exercising their rights under the Employment Ordinance.

6. What legislative protection does that employee enjoy?

It is an offence for an employer or any person with authority over a public officer to subject that officer to detriment by reason of making a protected disclosure. A public official who makes a protected disclosure does not breach any duty of confidentiality owed to any person by making the protected disclosure. It is an offence to victimize an employee for making disclosure or exercising their right. A provision in an employment agreement which prevents an employee from making a protected disclosure is void and unenforceable.

Anti-bribery and corruption

7. What are the main anti-corruption laws and regulations in your jurisdiction?

- The Integrity Commission Ordinance
- The Bribery Ordinance
- The House of Assembly (Powers and Privileges) Ordinance.

8. Does the legislation have extra-territorial effect?

Yes, under the Bribery Ordinance in certain cases where the person committing the offence has a close connection with the Turks and Caicos Islands and where the person bribed is a foreign public official or a public international organisation.

9. What are the main enforcement bodies?

The Integrity Commission and the Police and the Director of Public Prosecutions.

Internal investigations

10. Is there any duty to report the issue, for example to a regulator?

Yes, depending on the nature of the activity and the identity of the public body. Persons who carry on financial services business, including lawyers and real estate agents, are required to report suspicions of money laundering and terrorist financing to the Financial Intelligent Agency. Public officers are required to report knowledge or suspicion of acts of corruption and bribery to the Integrity Commission.

11. What is the protection from disclosure for documents generated as part of the investigation (for example, privilege)?

Documents generated as part of the investigation will generally not be disclosable if they are privileged. There are two relevant types of privilege under English common law which applies in the Turks and Caicos Islands:

- **Legal advice privilege** – protects all communications between a lawyer and client created in the context of seeking legal advice. Where the client is a company, the protection only applies to communications with the individuals authorised to seek legal advice on behalf of the company in relation to the investigation.
- **Litigation privilege** – may protect documents/communications if they are created for the dominant purpose of litigation and that litigation is reasonably in contemplation at the time the document is created. Litigation privilege applies to communications between any employees of the company, third parties and/or legal advisors.

12. Is the advice given by an in-house lawyer in relation to the investigation privileged and/or confidential?

Generally, yes.

Contact details

MISICK & STANBROOK
BARRISTERS AND ATTORNEYS

Ariel Misick
Misick & Stanbrook
Direct line: +1 649 946 4732
ariel@misickstanbrook.tc

Back to contents>

USA – North Carolina

When a crisis arises, which regulatory bodies do I need to notify and what is the relevant legislation?

Data breach

1. On discovering a data breach, which regulators or other government agencies should be notified?

- Once the extent of the incident is understood and the affected parties are identified, counsel will need to evaluate whether a data breach has occurred according to the legal framework of the states in which the affected customers reside. Unauthorized access to certain types of data by a third party may automatically trigger a notice obligation in some states, while other states require a risk of material harm to the affected party as a result of the unauthorized access. What is considered "personal information" or sensitive data in one state, such as name and physical address, may not be considered personal information in another state and give rise to a notice requirement.
- Under North Carolina law, a security breach is defined as either: (1) unauthorized acquisition of unencrypted data containing personal information where illegal use of the personal information has occurred or there is a material risk of harm; or (2) unauthorized access and acquisition of encrypted data containing personal information and the encryption key. Once it is determined that a breach has occurred under the affected parties' state law, each state law will also need to be examined to determine if notification to the affected party must be made as well as notice to that state attorney general or other government office. If a breach occurs in North Carolina, notifications must be sent to the North Carolina customers and to the North Carolina Attorney General.
- All businesses should consider whether it is appropriate to notify local law enforcement or federal agencies such as the Federal Bureau of Investigation or U.S. Secret Service. Certain businesses may also have notification obligations to federal regulators, including the Securities and Exchange Commission and/or law enforcement. In the case of certain types of information, such as protected health information, a business may need to notify the Federal Trade Commission and/or the U.S. Department of Health and Human Services. Businesses may also have obligations under international laws including the European Union's General Data Protection Regulation.

2. What legislation, relating to both criminal offences and civil wrongs, covers such a breach?

Data Breach notification is regulated in North Carolina pursuant to the Identity Theft Protection Act of 2005, codified at N.C. Gen. Stat. §§ 75-60.

"Dawn" raids

3. What agencies have the power to conduct dawn raids on private sector companies?

In the very general definition of the term, the number of agencies that have the power and authority to conduct dawn raids is as plentiful as the number of agencies that exist. All law enforcement agencies including the FBI, Secret Service, and Interpol can petition a magistrate with evidence and allegations that establish probable cause and can be granted a search warrant to examine the contents of offices and seize relevant documents.

4. What legislation gives those agencies the power to undertake those inspections?

- The legislation that empowers investigating agencies to conduct dawn raids include, among many others, the International Antitrust Enforcement Assistance Act, the Sherman Antitrust Act, the Clayton Antitrust Act, and the Federal Trade Commission Act (United States).
- It is worth noting that in the United Sates enforcement agencies may elect not to conduct a dawn raid and can compel production of documents or information via a civil investigative demand or a subpoena.

5. On what bases, including privilege and/or confidentiality, may such company refuse to permit the seizure of documents?

The issue of the search and seizure of privileged documents is as complex as the laws of competition themselves and vary widely from jurisdiction to jurisdiction. The United States allows great deference to materials protected by the attorney-client privilege and the attorney work product doctrine.

Whistleblowing

6. What are the circumstances under which an employee is entitled to protection when reporting an alleged wrongdoing?

If a publicly traded company or federal agency takes or threatens to take an adverse personnel action against an employee in retaliation for the disclosure of information by that employee, the entity can be sanctioned and financial remuneration can be awarded to the whistleblower. Further, the U.S. Supreme Court has held that whistleblower protection applies to employees of privately held contractors and subcontractors of public companies.[1] Pursuant to Dodd-Frank, the whistleblower must voluntarily provide the SEC with original information that leads to the successful enforcement by the SEC in which the SEC obtains monetary sanctions totalling more than $1 million.

7. What legislative protection does that employee enjoy?

The Whistleblower Protection Act protects federal employees who report violations of various federal statutes. OSHA's Whistleblower Protection Program enforces the whistleblower provisions of more than twenty whistleblower statutes protecting employees who report violations of various workplace safety and health laws, among others.[2] The SEC pursuant to § 922 of Dodd-Frank, supports a whistleblower program that rewards individuals who provide the agency with "high-quality" tips that lead to successful enforcement actions. Whistleblowers are financially incentivized to report financial misconduct. The amount awarded to a successful enforcement by a whistleblower is required to be between 10% and 30% of the total monetary sanctions collected in the SEC's action or any related action, such as in a criminal case.

Anti-bribery and corruption

8. What are the main anti-corruption laws and regulations in your jurisdiction?

- The main anti-corruption law that U.S. companies and individuals must be concerned about is the Foreign Corrupt Practices Act (FCPA). This statute has been in place since 1977 and has been rigorously enforced over the past decade. Enforcement penalties and fines levied under the FCPA for 2018 will likely top $2 billion, so it is an important statute to be aware of for companies conducting international business.
- Although the FCPA is the primary anti-corruption statute in the United States, many other countries have passed anti-corruption legislation in the last decade, and U.S. companies should be aware of any applicable statutes in the countries they do business in. Notably, the United Kingdom passed the U.K Bribery Act in 2011 and is beginning to enforce the statute more aggressively.

9. Does the legislation have extra-territorial effect?

- The FCPA has a very broad extraterritorial reach. The FCPA governs the conduct of "domestic concerns" and "issuers."Domestic concerns are defined as "any individual who is a citizen, national, or resident of the United States, or any corporation, partnership, association, joint-stock company, business trust, unincorporated organization, or sole proprietorship that is organized under the laws of the United States or its states, territories, possessions, or commonwealths or that has its principal place of business in the United States."[3] A company is an "issuer" under the FCPA if it "has a class of securities listed on a national securities exchange in the United States, or any company with a class of securities quoted in the over-the-counter market in the United States and required to file periodic reports with SEC."[4] Thus, foreign companies can be, and often are, "issuers" for purposes of the FCPA.
- In addition to applying to conduct occurring within the United States, all conduct by domestic concerns and issuers that uses any means of interstate commerce (including mail, phone lines, bank transfers, travel, etc.) that furthers a corrupt payment to a foreign official is also subject to FCPA jurisdiction. In practical terms, it is hard to imagine acts related to the bribery of a foreign official that are committed by a domestic concern or issuer that would not be subject to FCPA jurisdiction, even if the conduct did not occur on U.S. soil.

10. What are the main enforcement bodies?

The FCPA is jointly administered by the U.S. Department of Justice (DOJ) and the Securities and Exchange Commission (SEC). Both agencies have actively enforced the statute over the last decade.

Internal investigations

11. Is there any duty to report the issue, for example to a regulator?

- Generally, employers do not have a duty to report criminal conduct by their employees. However, every day federal and state prosecutors indict criminal conduct committed by or on behalf of corporations. Every Deputy Attorney General ("DAG") since the late 1990's has promulgated guidelines regarding the prosecution of corporations. In 2015, in a memorandum titled "Individual Accountability for Corporate Wrongdoing" released by then DAG, Sally Yates, the United States Department of Justice committed to prosecuting both culpable individuals and, when appropriate, the corporation on whose behalf they acted. In order for the corporation to receive credit for cooperation in reporting criminal conduct, the corporation must "provide to the [DOJ] all relevant facts about the individuals involved in corporate misconduct." During a speech on November 29, 2018, DAG Rod Rosenstein announced changes to the DOJ policy concerning individual accountability in corporate cases. His focus now includes senior management and members of Boards of Directors.
- Also, in many cases, for example in environmental-related matters, there is an obligation on companies to report illegal or unethical behavior to its regulators or face severe sanctions. This often requires an internal investigation by outside counsel.

12. What is the protection from disclosure for documents generated as part of the investigation (for example, privilege)?

There are a number of protections from disclosure available to various industries. For example, 12 CFR 261.20 strictly protects supervised financial institutions and financial institution supervisory agencies' confidential supervisory information (CSI) from disclosure to third parties. In an internal inquiry related to a criminal investigation, the DOJ, pursuant to updates to various DAG memos, is prohibited from requiring the waiver of privileged material to achieve cooperation credit. However, this is a heavily nuanced and sometimes litigated issue. The DOJ's position is that facts are not privileged; however there is an underlying question as to whether the attorney's ability and work product in uncovering certain facts privileged?

13. Is the advice given by an in-house lawyer in relation to the investigation privileged and / or confidential?

This depends. Often, in-house counsel wears a number of hats during their work day. A corporate Board secretary may be a lawyer who provided legal advice but may also give non-legal advice related to furthering the cause of a business. Typically, a privilege holder who communicates with in-house counsel for the purpose of receiving legal advice can assert the privilege of an in-house counsel's legal advice provided, of course, that the in-house counsel is a lawyer and is acting in his/her capacity as an attorney.

Contact details

Parker Poe
Attorneys & Counselors at Law

Brian Cromwell
Parker Poe
Direct line: (704) 778 7123
briancromwell@parkerpoe.com

Bruce Thompson
Parker Poe
Direct line: (919) 345 1161
brucethompson@parkerpoe.com

Notes

1. *Lawson v FMR LLC*, 571 U.S. 429
2. https://www.whistleblowers.gov/
3. A Resource Guide to the Foreign Corrupt Practices Act, p.11. Available at https://www.justice.gov/sites/default/files/criminal-fraud/legacy/2015/01/16/guide.pdf.
4. *Id*.

Back to contents>

terralex.com

18674